ESTUDO TÉCNICO PRELIMINAR

Implantação de infraestrutura de rede Wi-Fi no TRT23

PROAD nº 7902/2021

Cuiabá, maio de 2023.

Modelo v3.0

HISTÓRICO – REVISÕES

Data	Versão	Descrição	Autor
07/05/2021	0.1	Preenchimento inicial	Rogério Pimenta
30/07/2021	0.2	Ajustes	Rogério Pimenta
29/08/2021	0.3	Adição de anexos de requisitos	Rogério Pimenta
10/09/2021	0.4	Adição de anexos de propostas comerciais	Rogério Pimenta
27/10/2021	1.0	Revisão	Hugo Pinho
22/11/2021	1.1	Correção de erro material no item 1.8	Rogério Pimenta
29/03/2022	1.2	Pesquisa de preços públicos	Rogério Pimenta
15/07/2022	1.3	Atualização de requisitos técnicos	Rogério Pimenta
19/07/2022	1.4	Revisão	Francisco Netto
01/08/2022	1.5	Indicação da fonte orçamentária	Hugo Pinho
02/05/2023	1.6	Revisão de requisitos técnicos	Rogério Pimenta
02/05/2023	1.7	Conversão do template anterior, baseado na Lei nº 8.666/93, para o atual, baseado na 14.133/21	Rogério Pimenta

INFORMAÇÃO DE ACESSO RESTRITO OU SIGILOSO?

Sim	Não
	X

Sumário

INTRODUÇÃO 4

CONTEXTUALIZAÇÃO 4

DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS 6

IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO 6

IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS 8

ALINHAMENTO AO PLANEJAMENTO DO ÓRGÃO 9

NORMATIVOS RELACIONADOS À DEMANDA 9

ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS 9

ANÁLISE DE SOLUÇÕES POSSÍVEIS 10

IDENTIFICAÇÃO DAS SOLUÇÕES 10

CONTRATAÇÕES PÚBLICAS SIMILARES 12

CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES **Erro! Indicador não definido.**

PESQUISA DE PREÇOS DE MERCADO 13

ANÁLISE COMPARATIVA DE SOLUÇÕES 21

REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS 22

ANÁLISE COMPARATIVA DE CUSTOS (TCO) 22

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE 22

MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE 23

DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA 23

ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO 23

ADEQUAÇÃO NO AMBIENTE **Erro! Indicador não definido.**

INTERCORRÊNCIAS EM CONTRATAÇÕES ANTERIORES 24

DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO 24

APROVAÇÃO E ASSINATURA 25

1. INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda (DOD), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

2. CONTEXTUALIZAÇÃO

Com o constante avanço tecnológico, a proliferação de dispositivos móveis como celulares inteligentes (smartphones) e tablets, e o aumento da capacidade de processamento desses dispositivos, houve também, concomitantemente, um significativo aumento da diversidade de aplicações disponibilizadas para esses dispositivos voltadas para uso no ambiente corporativo ou, pelo menos, úteis no ambiente de trabalho. A gama de serviços disponíveis em smartphones e sua popularidade entre os usuários são tão grandes, que hoje em dia ninguém mais abre mão de utilizá-los, inclusive no ambiente profissional.

No contexto deste E. Tribunal podemos citar como exemplo de aplicação útil desses dispositivos, dentre outros, o lançamento, em 2016, do aplicativo JTe – Justiça do Trabalho Eletrônica, desenvolvido especificamente para a plataforma de dispositivos móveis e que oferece serviços como: consulta processual e de pautas, prazos abertos, minutas de acordo de conciliação, recebimento de notificações, validação de autenticidade de documentos, chat, um módulo específico de apoio a oficiais de justiça, backup e recuperação de dados. Uma importante funcionalidade já disponível no JTe é um mecanismo de assinatura eletrônica de documentos baseado na utilização de QR Codes, que ao serem lidos pelo dispositivo previamente cadastrado e autorizado (smartphone), assinará digitalmente documentos e atos processuais, dispensando o uso dos tokens físicos com certificado digital A3, que têm custo de aquisição dos tokens e de emissão dos certificados digitais, que devem ser renovados a cada 3 anos, no máximo.

Outro exemplo bastante relevante de uso de smartphones no âmbito da Justiça do Trabalho é o mensageiro instantâneo WhatsApp, que em sua versão Business, foi adotado como ferramenta de comunicação entre magistrados, servidores, advogados e jurisdicionados, tornando-se mais um canal para atendimento às demandas da sociedade. Especialmente nesses tempos de pandemia, onde o atendimento presencial teve de ser suspenso por motivos de segurança sanitária, dispor de ferramentas de comunicação instantânea com alta penetração na sociedade tornou-se imprescindível para a manutenção dos serviços jurisdicionais dentro de padrões de qualidade e celeridade demandados. Para esse uso, já foram recebidos pela STIC alguns pedidos formais de disponibilização de rede sem fios por meio do PROAD.

Não obstante os exemplos acima, todos os magistrados deste Tribunal possuem à

sua disposição, um notebook, que também conta com conexão a redes Wi-Fi e tem objetivo de prover maior flexibilidade e mobilidade ao magistrado para trabalhar.

O que há em comum entre todos os dispositivos e suas consequentes aplicações citados acima é a necessidade de se conectar a uma rede sem fios para poder se beneficiar plenamente de seu potencial. Embora todos eles tenham conexões nativas com as redes de comunicação das operadoras de telefonia, essas conexões nem sempre oferecem velocidades satisfatórias para o desempenho das aplicações ou conexões disponíveis em todos os ambientes em que os usuários precisem delas. Um exemplo disso são os ambientes com baixa potência de sinal da rede celular, como ocorre nos andares inferiores de todo o complexo do TRT23, notadamente no prédio da Corte do TRT23, onde estão localizados os plenários de julgamento. Situação similar ocorre em diversas cidades do interior do estado, onde a velocidade e disponibilidade do sinal celular também oscilam bastante.

Adicionalmente, considerando o atual estágio evolutivo das redes locais sem fios, já é possível considerar o seu uso em substituição às redes locais cabeadas, haja vista aquelas primeiras conseguirem ofertar conexões em velocidades compatíveis com a destas últimas, sem a necessidade de realização de obras físicas para a passagem de cabeamento para cada ponto de acesso, revelando-se uma alternativa de maior flexibilidade e mais baixo custo para instalações novas ou de caráter provisório.

Um outro direcionador da ação de implantação uma infraestrutura de rede sem fios que possa abranger todo o TRT23 é a possibilidade de ofertar um serviço de conexão a internet aos advogados, jurisdicionados e público em geral que transita pelos ambientes deste Tribunal, viabilizando a essas pessoas um acesso ágil e gratuito aos serviços digitais que disponibilizamos, como o PJe-JT, o JTe, a consulta aos andamento e teor de processos, pautas de audiências e todas as demais informações do Portal TRT23. Isso resulta, portanto, em mais um importante mecanismo de inclusão digital, na medida em que democratiza o acesso a informação de maneira equânime entre todos aqueles que estejam nos ambientes do TRT23, independentemente da qualidade ou disponibilidade de sua operadora de telefonia, bastando dispor de um aparelho celular ou tablet.

Embora o TRT23 possua, tanto em seu Complexo Sede, como em diversas unidades judiciárias do interior, dispositivos que proveem acesso sem fios a seus usuários internos, tais dispositivos são de categoria de uso de pequena escala (SOHO – Small Office / Home Office) e, portanto, bastante limitados quanto a robustez e capacidade.

Soma-se a isso o fato de que a Estratégia Nacional de Tecnologia da Informação e Comunicações do Poder Judiciário (ENTIC-JUD) desde 2015 já estabelecia na Resolução CNJ 211/2015 (revogada) em seu Art. 24 inciso XIII, a necessidade de oferta de serviços por meio de rede sem fios como um dos requisitos mínimos de nivelamento tecnológico para os órgãos do Poder Judiciário. Este Tribunal não conseguiu, por falta de recursos financeiros, implementar à época da vigência da referida Resolução tal requisito de nivelamento, o que vem buscando até o presente momento.

3. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Implantação de uma infraestrutura de rede de comunicação sem fios com abrangência em todo o âmbito do TRT23, incluindo o fornecimento de equipamentos Access Points, controladoras de rede wireless (físicas ou virtualizadas), injetores de energia PoE, softwares de configuração e gerência, serviços de instalação e configuração e transferência de conhecimento para sua operação.

São apresentados no item seguinte os requisitos do demandante que, posteriormente, serão convertidos em requisitos técnicos para os equipamentos, softwares e serviços.

3.1 IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

3.1.1 Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir;

3.1.2 Todos os dispositivos de hardware e de software a serem fornecidos devem contar com as respectivas licenças de que necessitem para seu perfeito funcionamento, com garantia de funcionamento, atualização e suporte pelo período a ser estipulado na contratação;

3.1.3 A rede sem fios a ser implantada deve aproveitar, tanto quanto possível, a infraestrutura elétrica e de cabeamento de rede já existente no ambiente dos prédios do TRT23 e, quando necessárias adequações, ser indicado pela empresa responsável pela implantação de forma que as adequações possam ser realizadas pelas equipes internas do TRT23;

3.1.4 Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações;

3.1.5 Deve poder ser conectada à infraestrutura de rede corporativa atual do Tribunal e comunicar-se com todos os demais equipamentos mediante simples conexão por cabos e ajuste de parâmetros lógicos de roteamento e segurança;

3.1.6 Deve poder ser gerenciada por conexão de console local, acesso por terminal remoto em interface de texto (CLI – Command Line Interface) e acesso remoto por interface gráfica baseada em navegador de internet (Web Browser), independentemente do local de origem do acesso;

3.1.7 Os Access Points devem ser alimentados de eletricidade pelo mesmo cabo que conduz o sinal de rede, utilizando a tecnologia PoE (Power over Ethernet), de maneira nativa ou por meio adaptadores, que deverão neste caso ser fornecidos juntamente com os Access Points;

3.1.8 A rede sem fios deve oferecer cobertura de sinal de boa qualidade (>=70% de potência de sinal em pelo menos 80% da área de cada ambiente) em todas as dependências do TRT23 onde haja usuários de TIC;

3.1.9 A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede;

3.1.10 A rede sem fios, ainda que de geração mais recente, deve permitir a conexão de dispositivos móveis compatíveis com as tecnologias anteriores, como os padrões IEEE 802.11a/b/g/n/ac e operar simultaneamente nas frequências de 2.4 e 5 GHz;

3.1.11 A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points) do ambiente de instalação do contratante, podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede;

3.1.12 A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso;

3.1.13 A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, deverá ser ofertado, dentre outros, um portal de autenticação acessível por navegadores de internet (Captive Portal);

3.1.14 A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência;

3.1.15 A solução deve permitir a mudança transparente de célula (seamless roaming) quando o usuário se movimenta ao longo da área de cobertura da rede;

3.1.16 A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário;

3.1.17 A solução deve permitir o balanceamento de carga de tráfego pela realocação automática de usuários conectados a Access Points adjacentes;

3.1.18 A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança;

3.1.19 A solução deve ser entregue instalada, configurada e em pleno funcionamento;

3.1.20 Antes da implantação da infraestrutura de rede, deverá ser elaborado um relatório do tipo Pré Site Survey com imagens do tipo “mapa de calor” que demonstrem graficamente, por meio de códigos de cores, a expectativa de cobertura, obstáculos, atenuação e qualidade do sinal de cada ambiente de acordo com a posição prevista para instalação de cada Access Point, servindo como ferramenta de planejamento e apoio para a instalação;

3.1.21 Após a implantação da infraestrutura de rede, deverá ser elaborado um relatório do tipo Pós Site Survey com imagens do tipo “mapa de calor” que demonstrem graficamente, por meio de códigos de cores demonstrativos da cobertura e qualidade do sinal de cada ambiente onde haja Access Points. Este relatório deverá ser comparado com o Pré Site Survey para efeitos de validação do atendimento das expectativas do planejamento

3.1.22 Após o término da implantação e entrega da documentação requerida, deverá ser realizada uma transferência de conhecimento, no formato “hands on”, com duração mínima de 16 horas aula, de maneira presencial, nas instalações da sede do TRT23, para uma equipe de servidores a ser indicada pela Coordenadoria de Infraestrutura Tecnológica e Monitoramento. Tal transferência de conhecimento deverá ter como objetivo preparar os servidores envolvidos para assumir as tarefas cotidianas de operação, gerenciamento e “troubleshooting” (diagnóstico) básicos da solução.

3.2 IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

3.2.1 Para uma melhor organização deste documento, os Requisitos Técnicos da Solução foram dispostos na forma de anexo e encontram-se ao final, no Anexo II.

3.3 ALINHAMENTO AO PLANEJAMENTO DO ÓRGÃO

Plano	ID	Descrição
PETIC-TRT23	Objetivo 2.3	Aprimorar a segurança da informação e gestão de riscos de TIC
ENTIC-JUD	OE7	Aprimorar a segurança da informação e a gestão de dados
PETIC-JT		Aprimorar a gestão de riscos de TIC

Tabela 1 - Alinhamento ao planejamento

3.4 NORMATIVOS RELACIONADOS À DEMANDA

3.4.1 Resolução CNJ 370 de 2021 que estabeleceu o Guia da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário ENTIC-JUD 2021-2026 - Versão 1.1 de Agosto/2021, cujo Item 12 - Boas práticas advindas da Resolução CNJ 211/2015 recomenda: Rede sem fio para a promoção dos serviços ofertados aos usuários e respeitando a política de segurança da informação de cada órgão, sempre que possível (https://www.cnj.jus.br/wp-content/uploads/2021/11/guia-da-entic-jud-res370-2021-10-07-rev2.pdf).

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Considerando se tratar de uma tecnologia ainda não instalada no âmbito do TRT23, e também levando em conta a grande diversidade de formas de implementar a tecnologia de Wi-Fi por cada fabricante e, portanto, a diferença de características como alcance, cobertura e desempenho, para que fosse possível estimar de maneira minimamente razoável o quantitativo necessário de itens, foi solicitado a cada fornecedor consultado que se realizasse um "*Site Survey*" virtual. De posse dessa informações e, mais uma vez, considerando as variações entre os fornecedores, foi realizada uma estimativa pela média dos quantitativos estimados por cada fornecedor.

Item	Quantidade
Ponto de Acesso Tipo 1	100
Ponto de Acesso Tipo 2	100
Injetor de energia PoE	150
Controladora WLAN	2
Solução de Gerência de Rede	1

Tabela 2 - Estimativa da demanda

5. ANÁLISE DE SOLUÇÕES POSSÍVEIS

Para a implantação de uma infraestrutura de rede sem fios que atendam aos requisitos da demanda atualmente existe a possibilidade de utilizar dois padrões tecnológicos vigentes: o Wi-Fi 5 e o Wi-Fi 6, assim denominados pela Wi-Fi Alliance, e baseados nos protocolos do IEEE (Institute of Electric and Electronic Engineers) 802.11ac e 802.11ax, respectivamente.

5.1 IDENTIFICAÇÃO DAS SOLUÇÕES

ID	Descrição da solução (ou cenário)
1	Rede Wi-Fi 5 (IEEE 802.3ac)
2	Rede Wi-Fi 6 (IEEE 802.3ax)

Tabela 3 - Soluções identificadas

5.1.1 SOLUÇÃO 1: Rede Wi-Fi 5 (IEEE 802.3ac)

A tecnologia para infraestrutura de redes de computadores sem fios surgiu há pouco mais de 20 anos e desde então vem dando seus mais significativos saltos evolutivos em ciclos com intervalos de 4 e 6 anos, respectivamente, conforme ilustra a figura a seguir:

Figura 1 - Linha do tempo da tecnologia Wi-Fi (tradução livre de imagem da Alcatel Lucent Enterprise)

Dessa maneira podemos constatar que, embora a tecnologia mais recente seja a do Wi-Fi 6, pelo fato dela estar em processo de adoção pelo mercado, ainda está disponível a oferta de dispositivos da versão imediatamente anterior, a Wi-Fi 5, motivo pela qual deve ser considerada, já que atende aos requisitos da demanda.

Na primeira tentativa de implantação de um projeto desta natureza neste E. Tribunal, em 2019, a tecnologia de redes sem fios vigente era a Wi-Fi 5 (IEEE 802.11ac) e naquela ocasião foram realizados levantamentos do tipo Site Survey que serviram de base para a emissão de uma proposta comercial preliminar com a finalidade de estimar o custo de realização do projeto. Ambos os documentos serão juntados como anexos a este estudo e servirão como base de comparação da análise dos tópicos 1.6 e 1.7 mais adiante.

Ao procurar por propostas de implantação de infraestrutura de rede sem fios no presente momento estamos encontrando dificuldades em conseguir propostas atualizadas que contemplem uma instalação nova utilizando a tecnologia Wi-Fi 5, motivo pelo qual manteremos a proposta apresentada em 2019 para fins de comparação neste estudo.

5.1.2 SOLUÇÃO 2: Rede Wi-Fi 6 (IEEE 802.3ax)

Considerando a constante evolução de tecnologia das redes Wi-Fi, onde o padrão mais recente e em vigência é o IEEE 802.11ax ou Wi-Fi 6, e considerando que atende plenamente a todos os requisitos da demanda, esta versão será levada em consideração, tendo a avaliação de seus aspectos discutida nos tópicos 1.6 e 1.7 a seguir, sendo que, de momento, resta demonstrar brevemente as principais diferenças evolutivas do Wi-Fi 6 em relação ao Wi-Fi 5:

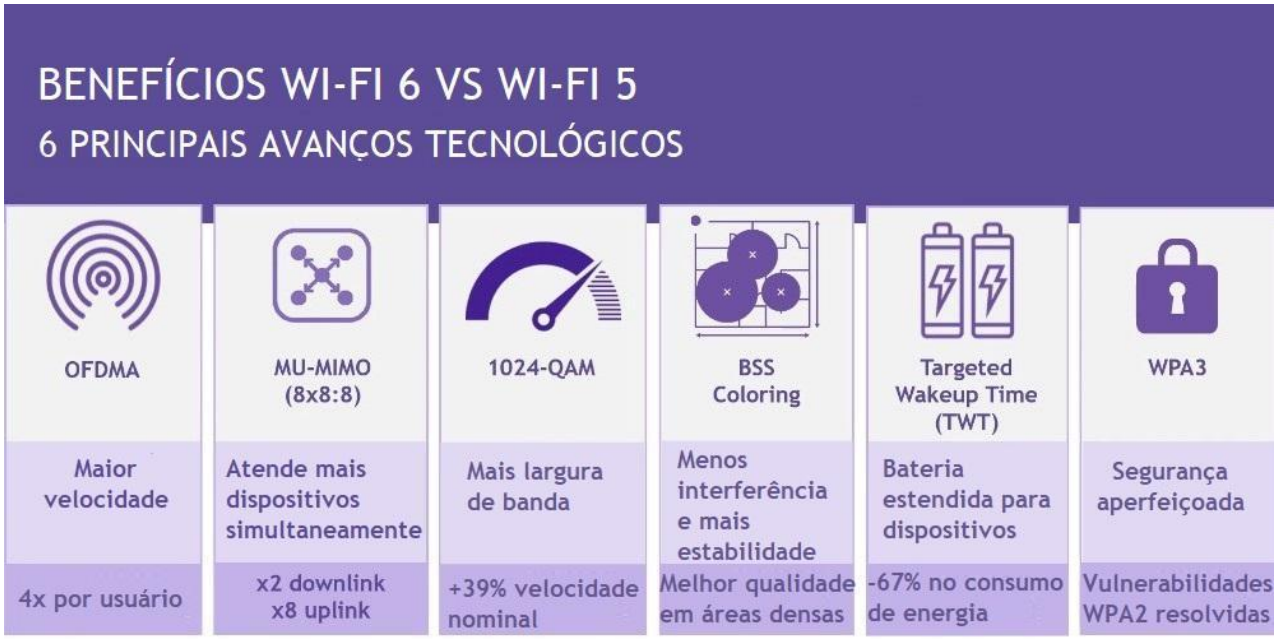

Figura 2 - Benefícios Wi-Fi 6 vs Wi-Fi 5 (tradução livre de imagem da Alcatel Lucent Enterprise)

Assim como no caso da solução baseada em Rede Wi-Fi 5, foram solicitados

também estudos do tipo Site Survey e, baseados neles, propostas comerciais com previsão preliminar de custos de implantação de uma Rede Wi-Fi 6 no âmbito deste Tribunal, cujos documentos estarão acostados ao processo administrativo, em anexos.

Uma informação que merece registro diz respeito à forma de aquisição da solução, que é composta por uma combinação de Pontos de Acesso, Controladoras Wireless e Soluções de Controle de Acessoa Redes (NAC).Enquanto no primeiro caso trata-se de dispositivos eminentemente físicos (de *hardware*) que não são passíveis de ser substituídos por uma versão "virtualizada" baseada em softwares, os demais componentes, embora possam ser encontrados em plataformas híbridas de hardware/software na forma de appliances, estes podem ser virtualizados ou, ainda, estar disponíveis em plataformas de software que desempenhem suas funções. Considerando o fato de que as Controladoras Wireless e os Softwares de Autenticação e Controle de Acesso à Rede (NAC) podem ter suas funções executadas puramente em software, este software pode, ainda, estar instalado no ambiente local do cliente (*on-premises*) ou estar instalado remotamente no ambiente de nuvem (*cloud*) de seu fabricante ou fornecedor. Para este último caso os fornecedores adotam uma abordagem comercial diferente onde, ao invés de vender a solução de hardware/software (físico ou virtual), comercializam o acesso às funcionalidades dos softwares no formato de assinatura de serviços (subscrição). Portanto, embora exista a possibilidade de adquirir os Pontos de Acesso físicos e contratar as soluções de Controladora Wireless e NAC como serviços por subscrição, esta opção não foi considerada no atual contexto por alguns motivos, a saber: o risco de a indisponibilidade técnica de acesso à nuvem do fornecedor inviabilizar, ainda que temporariamente, o gerenciamento da rede e seus dispositivos físicos; o risco de que, ao final do contrato de subscrição dos serviços, haja a perda de capacidade de gerenciamento da rede e seus dispositivos físicos; o fato de que, pela natureza da contratação se de serviços, há a necessidade de que seu custeio venha de recursos orçamentários de outra fonte, que deva ser assegurada a cada exercício, ao contrário do que ocorre com a aquisição de uma solução que, uma vez imobilizada não gera despesas recorrentes para os exercícios subsequentes, garantindo maior previsibilidade de sua manutenção pelo menos durante o prazo de vigência da garantia contratada. Por esses motivos, no momento deste estudo, optou-se pela especificação de que os componentes da solução não poderiam ser fornecidos como software em nuvem contratados como serviços por subscrição.

5.2 CONTRATAÇÕES PÚBLICAS SIMILARES

A Tabela 3 apresenta órgãos que realizaram recentemente contratações para atender essa demanda.

	Órgão	Instrumento	Item
Solução 2	Banco Central do Brasil	PE (SRP) 78/2021	-
	ICMBio	PE (SRP) 41/2021	-
	Tribunal Regional Federal da 1ª Região	ARP 009/2021	-

Tabela 3 - Contratações públicas similares

5.3 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não aplicável.

5.4 PESQUISA DE PREÇOS DE MERCADO

Preliminarmente é importante registrar que, em se tratando de uma aquisição de solução por entidade do Poder Público, regida pelos princípios do Direito Administrativo e subordinado à legislação própria, é sabido que se deve sempre buscar a contratação de bens e serviços que, atendendo aos requisitos objetivos da demanda, sejam resultado de uma disputa pública na qual se obtenha o melhor preço. Todavia, deve-se considerar que algumas tecnologias possuem diversas formas diferentes de serem implementadas para atender aos mesmos requisitos objetivos e, a depender da forma de implementação, tanto os custos como a qualidade do resultado (que é subjetiva), também podem variar bastante. Como forma de minimizar a exposição ao risco de eventual aquisição de soluções que, ainda que objetivamente atendam aos requisitos da demanda, em virtude de características intrínsecas a seu modelo de implementação, não assegurem padrões de qualidade necessários à preservação do investimento ao longo do tempo, pode-se lançar mão do resultado do trabalho de entidades independentes de mercado que visam analisar, relatar e/ou certificar fornecedores de tecnologias segundo critérios de mercado ou por meio de mecanismos de certificação de aderência a padrões (Certification Standards).

Dentre estas instituições, o grupo Gartner se destaca por sua notoriedade e independência na realização de análises do mercado de tecnologia, e que publica anualmente um relatório de pesquisa conjuntural do mercado no qual lista os principais fornecedores de determinado segmento tecnológico (neste caso, Redes LAN e WAN corporativas) e os classifica em quadrantes de acordo com seu principal posicionamento no mercado.

Dessa forma, e considerando que as equipes internas deste Regional não possuem meios técnicos de assegurar preliminarmente o atendimento a padrões mínimos de qualidade esperada, fica estabelecido neste instrumento que todos os itens a serem fornecidos deverão ser do mesmo fabricante, e este fabricante deve figurar em um dos quatro Quadrantes Mágicos da pesquisa “GartnerMagic Quadrant for Enterprise Wired and Wireless LAN Infrastructure” (“Quadrante Mágico para Infraestrutura de LAN com fio e sem fio corporativa” em tradução livre) da edição de 21/12/2022, conforme mostrado na Figura 1 abaixo.

Figure 1: Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure

Figura1 - Magic Quadrant for Entreprise Wired and Wireless LAN Infrastructure

Como este estudo vem sendo realizado desde 2019, é importante demonstrar a trajetória histórica das pesquisas de preço junto ao mercado, de forma a que se entenda, posteriormente, as razões que justificam a escolha por determinada solução. Assim, a Tabela 4 detalha os preços ofertados em propostas comerciais por empresas do mercado, entre 2019 e 2021, para cada solução identificada. Como para a solução 1 (Wi-Fi 5) não foram obtidas propostas recentes, e para equalizar as comparações de preços obtidos em momentos diferentes no tempo, os valores de todas as propostas foram convertidos para o Dólar Comercial pela cotação da data de cada proposta. Destaca-se também que, assim como na comparação de preços públicos, por força das particularidades de cada caso e como forma de promover comparações de preços equânimes, foi necessário promover o ajuste do quantitativo dos itens cotados pelas empresas consultadas ao quantitativo previsto neste estudo, mantendo os preços unitários e recalculando os valores totais por item e total geral.

	Item	Qtd.	Valor unit.	Valor total
Solução 1	Controladora Wireless Virtual Cisco licenciada para 5 Aps com suporte para	1	R$ 3.600,00	R$ 3.600,00

Fornecedor 1	até 200 Aps com garantia de 5 anos			
	Licença para expansão de controladora wireless virtual para 1 Ap com garantia de 5 anos	107	R$ 720,00	R$ 77.040,00
	Access Point Cisco 15821 802.11ac Wave2 Dual Band MIMO 4X4 com 3 spatialstreams – Mobility Express para até 50 Aps com garantia de 5 anos	112	R$ 5.200,00	R$ 582.400,00
	Injetor PoE Cisco	60	R$ 420,00	R$ 25.200,00
	Serviço de configuração da solução wireless	1	R$ 20.000,00	R$ 25.000,00
			Total da proposta	**R$ 708.240,00**
	Total em US$ em 26/07/2019 (cotação R$ 3,7735)*			**$ 187,687.82**
Solução 2 **Fornecedor 1**	Controladora Virtual Cisco Catalyst 9800-CL com suporte e garantia por 3 anos	2	R$ 5.750,00	R$11.500,00
	Acess Point Cisco Catalyst 9105 Wi-Fi 6 MIMO 2X2 com licença de software de gerenciamento e controladora e garantia de 3 anos	75	R$ 5.400,00	R$ 405.000,00
	Acess Point Cisco Catalyst 9115 Wi-Fi 6 MIMO 4X4 com licença de software de gerenciamento e controladora e garantia de 3 anos	45	R$ 9.940,00	R$ 447.300,00
	Acess Point Cisco Catalyst 9120 Wi-Fi 6 MIMO 4X4 com licença de software de gerenciamento e controladora e garantia de 3 anos	30	R$ 13.200,00	R$ 396.000,00
	Injetor PoE Cisco 802.3at	150	R$ 790,00	R$ 118.500,00
	Software de gerenciamento Cisco Prime Infrastructure com suporte e garantia de 3 anos	1	R$ 1.500,00	R$ 1.500,00
			Totais da proposta	**R$ 1.379.800,00**
	Total em US$ (cotação R$ 5,30 segundo o proponente)			**$ 260,339.62**
Solução 2 **Fornecedor 2**	Licença para Sistema de Gerenciamento NCE-iMaster Campus em Nuvem para Ponto de Acesso AirEngine 5760-51, por 5 anos	144	R$ 320,57	R$ 46.162,08
	Licença para Sistema de Gerenciamento NCE-iMaster Campus em Nuvem para	2	R$ 5.187,20	R$ 10.374,40

	Controladora AC6508, por 5 anos			
	Licença para Sistema de Autenticação NCE-iMaster Campus em Nuvem para para 1.000 usuariossimultaneos, por 5 anos	1000	R$ 4,46	R$ 4.456,33
	Licença para Sistema analítico NCE-iMaster Insight para configuração automatica de rede através de IA, com localicaçãogeografica de terminais e dispositivos RFID com identificação de aplicação de camada 3 a 7 sendo executadas na rede, por 5 anos	1	R$ 248.339,52	R$ 248.339,52
	Controladora AC6508 para até 256 pontos de acesso, com capacidade de atuar em alta disponibilidade, com 5 anos de garantia	2	R$ 9.490,97	R$ 18.981,94
	Ponto de Acesso Indoor WiFi 6 (802.11ax) mid-end, capacidade de comutação de 5.37 Gbps, MiMo 4x4, suporte de 1024 usuariossimultaneos e garantia de 5 anos	144	R$ 2.605,24	R$ 375.154,56
	Injeto PoE++ para ponto de acesso AirEgine, com 5 anos de garantia	144	R$ 942,07	R$ 135.658,08
			Totais da proposta	**R$ 839.126,91**
	Total em US$ (cotação R$ 5,30 segundo o proponente)			**$ 158,325.83**
Solução 2 **Fornecedor 3**	OV-AP-NM-100-N OV2500 NM R4 Lic. 100 AP NEW for 10 ALU-E Stellar	2	R$ 32.311,04	R$ 64.622,08
	OV-GA-1k-N OV2500 GA R4 Lic. 1000 GA-NEW for Guest Access	1	R$ 51.031,84	R$ 51.031,84
	OV2500 BYOD R4 Lic. 1000 BYOD-NEW for BYOD Access Policy Manager	1	R$ 52.733,75	R$ 52.733,75
	5YR 24X7 Partner Support for OV2500 NMS RELEASE 4 OV-AP-NM-100-N	2	R$ 24.574,97	R$ 49.149,94
	5YR 24X7 Partner Support Software for OV2500 NMS R4 OV-BYOD-1K-N	1	R$ 33.844,15	R$ 33.844,15
	5YR 24X7 Partner Support for OV2500 NMS RELEASE 4 OV-GA-500-N	1	R$ 27.107,38	R$ 27.107,38
	OmniAccess Stellar Indoor AP1321 Dual radio HW	160	R$ 6.846,92	R$ 1.063.507,20
	OmniAccess Stellar Indoor AP1321 Dual	160	R$ 3.105,01	R$ 496.801,60

	radio SFW			
	10 Pack mounting kit, Type A ceiling/wall mount	16	R$ 1.612,52	R$ 25.800,32
	5 Yr Renew Partner Support Software for OAWAP1301	160	R$ 326,76	R$ 52.281,60
	Totais da proposta			**R$ 1.916.879,86**
	Total em US$ (cotação em 09/05/22 R$ 5,157)			**$ 371,704.45**
Solução 2 **Fornecedor 4**	CONTROLADORA/FIREWALL PEQUENO PORTE PARA UNIDADES REMOTAS COM SUPORTE E GARANTIA DE 60 MESES	24	R$ 3.761,69	R$ 90.280,58
	CONTROLADORA/FIREWALL PEQUENO PORTE PARA UNIDADES REMOTAS COM SUPORTE E GARANTIA DE 60 MESES	1	R$ 30.139,94	R$ 30.139,94
	ACCESS POINT INDOOR FORTINET FAP-231F-N	150	R$ 6.932,86	R$ 1.039,928,65
	ACCESS POINT INDOOR FORTINET FAP-431F-N	20	R$ 10.075,52	R$ 201.510,39
	Injetor PoE Gigabit 802.3at	50	R$ 1.121,23	R$ 56.061,55
	Totais da proposta			**R$ 1.417.921,12**
	Total em US$ (cotação em 31/08/2021 R$ 5,14)			**$ 275,860.14**
Mediana das propostas apresentadas em Reais				**R$ 1.379.800,00**
Mediana das propostas convertidas para Dólar (comercial)				**$ 260,339.62**

Tabela 4 - Pesquisa de preços de mercado realizada entre 2019-2021

Por se tratar de dispositivos de alta tecnologia e que não têm fabricação no Brasil, seus preços normalmente estão vinculados ao dólar americano em razão de manterem-se alinhados com os preços globais e de seus mercados de origem. Outro aspecto que corrobora este raciocínio é o fato de que os proponentes destacaram uma observação em suas propostas, estabelecendo que os valores ali presentes poderiam ser renegociados ou perderiam sua validade caso o dólar (PTAX) sofresse alterações acima de um valor explicitado. Assim, para garantir uma maior fidedignidade na comparação dos preços apresentados pelos proponentes, conforme se pode observar na Tabela 4 acima, foi realizada a conversão dos valores nas datas das propostas para o dólar pelo câmbio do dia da emissão de cada proposta, ou conforme orientação do proponente.

	Item	**Qtd.**	**Valor unit.**	**Valor total**
Solução	Controladora Wi-Fi para até 200 pontos	2	R$ 104.641,00	R$ 209.282,00

2 Banco Central	de acesso			
	Ponto de acesso Wi-Fi 6	160	R$ 2.189,11	R$ 350.257,60
	Software de Gerenciamento	1	R$ 110.540,33	R$ 110.540,33
	Software de Controle de Acesso à Rede	1	R$ 131.980,93	R$ 131.980,93
			Total da proposta	**R$ 802.060,86**
Solução 2 ICMBIO	Controladora Física	2	R$ 100.459,00	R$200.918,00
	Serviços de instalação de Controladora Física	2	R$ 10.647,00	R$ 21.294,00
	Acess Point Indoor	160	R$ 4.030,00	R$ 644.800,00
	Serviço de instalação de Acess Point Indoor presencial	160	R$ 533,00	R$ 85.280,00
			Totais da proposta	**R$ 952.292,00**
Solução 2 TRF1	CONTROLADORA WIRELESS. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS + 1 OmniSwitch OS6860E-24-US + 2 FONTE REDUNDANTE OS6860-BP-US + PP5N-OS6860 (GARANTIA 5 ANOS) + SFP-10G-SR + LICENÇAS OV-AP + SUPORTE 5 ANOS	2	R$ 53.169,00	R$ 106.338,00
	SOLUÇÃO DE GERÊNCIA DE REDE SEM FIO (WLAN). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS + LICENÇAS OV-NM-EX + SUPORTE 5 ANOS	1	R$ 28.081,00	R$ 28.081,00
	SOLUÇÃO DE CONTROLE DE ACESSO. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS MODULO OV-GA-1K-N + PW5N-OVGA1KN (SUPORTE 5 ANOS)	1	R$ 32.497,00	R$ 32.497,00
	PACOTE DE LICENÇAS PARA USUÁRIOS VISITANTES (500 USUÁRIOS). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS MODULO OV-GA-500-N + PW5N- OVGA500N (SUPORTE 5 ANOS)	2	R$ 4.462,03	R$ 8.924,06
	SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS ITENS 1, 4, 5 E 6. DEMAIS CARACTERÍSTICAS DE	1	R$ 7.877,00	R$ 7.877,00

	ACORDO COM O ANEXO I DO EDITAL			
	PONTO DE ACESSO SEM FIO, COM GARANTIA DE 60 (SESSENTA MESES). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniAccess OAW-AP1221- RW + OAW-AP1221-SW + OAW-AP-MNT- W + PP5N- OAWAP1221 (GARANTIA 5 ANOS) + LICENÇAS E ACESSÓRIOS	160	R$ 2.405,00	R$ 384.800,00
	SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS ITENS 2 E 3. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL	160	R$ 297,00	R$ 47.520,00
			Totais da proposta	**R$ 616.037,06**
			Mediana dos preços totais	**R$ 802.060,86**

Tabela 5 - Pesquisa de preços públicos realizada em 2021

Dada a complexidade deste estudo, e por consequência disso, ele ter se estendido ao longo do tempo, torna-se necessário atualizar as pesquisas de preços junto ao mercado e órgãos públicos com o objetivo de evitar eventuais distorções na formação do preço estimado para a aquisição pretendida. Assim, se apresentam abaixo as pesquisas de preço atualizadas nos últimos 6 meses, destacando que, neste caso, já não foi mais possível obter preços para a Solução 1 em virtude de sua indisponibilidade no mercado:

	Item	**Qtd.**	**Valor unit.**	**Valor total**
Solução 2 **Fornecedor 1**	901-R350-WW02	97	R$ 4.298,00	R$ 416.906,00
	902-0120-0000	97	R$ 221,00	R$ 21.437,00
	901-R650-WW00	176	R$ 6.642,00	R$ 1.168.992,00
	902-0120-0000	176	R$ 221,00	R$ 38.896,00
	L09-VSCG-WW00	01	R$ 3.537,00	R$ 3.537,00
	L09-0001-SG00	273	R$ 356,00	R$ 97.188,00
	S01-VSCG-5L00	01	R$ 3.656,00	R$ 3.656,00
	902-0162-BR00	97	R$ 437,00	R$ 42.389,00
	S62-0001-5LSG	273	R$ 367,00	R$ 100.191,00
	Serviço - Treinamento	01	R$ 36.887,00	R$ 36.887,00
	Serviço de configuração e instalação lógica.	01	R$ 182.706,00	R$ 182.706,00
			Totais da proposta	**R$ 2.112.785,00**
Solução 2	Ponto de Acesso Wi-Fi 6 Indoor	200	R$ 13.280,00	R$ 2.656.000,00

Fornecedor 2	Marca: Alcatel-Lucent Modelo: OAW-AP1321-RW			
	Injetor de energia PoE Modelo: PD-9001GR/AT/AC	200	R$ 700,00	R$ 140.000,00
	Controladora Wireless Marca: Alcatel-Lucent Modelo: OmniVista 2500	2	R$ 120.000,00	R$ 240.000,00
	Solução de Gerenciamento e Controle de Acesso à Rede Marca: Alcatel-Lucent Modelo: OmniVista 2500	1	R$ 200.000,00	R$ 200.000,00
	Instalação	1	R$ 160.000,00	R$ 160.000,00
	Transferência de conhecimento “hands-on”	1	R$ 170.000,00	R$ 170.000,00
			Totais da proposta	**R$ 3.566.000,00**
Média das propostas apresentadas				**R$ 2.839.392,50**

Tabela 6 - Pesquisa de preços de mercado realizada em 2023

	Item	Qtd.	Valor unit.	Valor total
Solução 2 DETRAN DF	Controlador/Gerenciador WLAN Fabricante: CommscopeRuckus Modelo: Virtual Smartzone	1	R$ 34.450,00	R$ 34.450,00
	Ponto de Acesso (AP) 802.11ax Interno Fabricante: CommscopeRuckus Modelo: Ruckus R550	200	R$ 6.110,00	R$ 1.222.000,00
	Serviço de instalação Wi-Fi	200	R$ 590,00	R$ 118.000,00
	Solução de controle de acesso à rede (NAC) Fabricante: Commscope Ruckus Modelo: Cloudpath Base On-Site Server As a Virtual Appliance	1	R$ 15.500,00	R$ 15.500,00
	Licenciamento para solução de controle de acesso (NAC) Fabricante: Commscope Ruckus Modelo: Cloudpath Per User On-Site License for Enterprises	1	R$ 1.074.285,10	R$ 1.074.285,10
	Solução de gerência Fabricante: CommscopeRuckus Modelo: Virtual Smartzone + Ruckus Analytics	1	R$ 17.230,00	R$ 17.230,00

	Serviço de planejamento	1	R$ 200.000,00	R$ 200.000,00
	Serviço de treinamento para a solução NAC	1	R$ 11.900,00	R$ 11.900,00
	Garantia e suporte	60	R$ 9.190,00	R$ 551.400,00
			Total da proposta	**R$ 3.244.765,10**
			Mediana dos preços totais	**R$ 3.244.765,10**

Tabela 7 - Pesquisa de preços públicos realizada em 2023

5.5 ANÁLISE COMPARATIVA DE SOLUÇÕES

Ao realizar uma análise comparativa entre as soluções aqui elencadas, quais sejam, utilizar tecnologia Wi-Fi 5 ou Wi-Fi 6 para criar uma infraestrutura nova de rede sem fios, conclui-se que a tecnologia Wi-Fi 5 já não se encontra mais disponível para esta finalidade, tendo sido substituída por sua sucessora, a tecnologia Wi-Fi 6.

Importa registrar que a Solução 1, tecnologia de rede Wi-Fi 5, estava disponível no início deste estudo e por isso foi considerada, mas teve sua disponibilidade interrompida para a implantação de novas infraestruturas de redes sem fio nos últimos meses em virtude da consolidação e estabelecimento da tecnologia Wi-Fi 6 como o novo padrão de fato para este mercado.

	SOLUÇÃO 1	**SOLUÇÃO 2**
A solução encontra-se implantada em outro órgão ou entidade da administração pública?	S	S
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	NA	NA
A Solução é composta por software livre ou software público? (quando se tratar de software)	N	N
A Solução é aderente às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário;	NA	NA
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	NA	NA
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder	NA	NA

Judiciário? (Moreq-Jus)		

Legenda: *S-Sim, N-Não, NA-Não se aplica*

Tabela 8 – Análise das soluções em relação à aderência aos requisitos apontados no Guia de Contratações de STIC do Poder Judiciário

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução	Justificativa
Solução 1	O uso do padrão Wi-Fi 5 (IEEE 802.3ac) foi considerado inviável porque é uma tecnologia que, embora ainda esteja vigente, não se apresenta mais como o padrão do mercado e da indústria, tendo sido substituída pelo Wi-Fi 6 (IEEE 802.3ax). Isso significa dizer que qualquer contratação ou aquisição de rede sem fios com tecnologia Wi-Fi 5 terá um ciclo de vida útil reduzido pela indisponibilidade de peças de reposição ou da prestação de serviços de suporte e garantia. Uma demonstração desse fenômeno é o fato de não haver mais disponibilidade nos fornecedores para elaboração de projetos de implantação de infraestruturas de redes novas utilizando a tecnologia Wi-Fi 5.

Tabela 9 - Soluções inviáveis

7. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

7.1 CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Considerando o resultado da análise comparativa de soluções apresentada no item 5.5, onde se conclui que a Solução 1 não se apresenta mais como alternativa disponível para implantação de uma infraestrutura de rede sem fios nova, resta apenas considerar a Solução 2.

O custo total de propriedade da Solução 2, da forma como está previsto que ocorra sua aquisição, já leva em consideração os custos de aquisição, instalação, suporte e manutenção pelo prazo de 60 meses, e assim não há expectativa de outros custos incidentes ao longo desse período. Todavia, como estes custos nem sempre estão separados de forma clara nas propostas comerciais dos fornecedores consultados, fica prejudicada nesta fase a demonstração individual de cada custo que venha compor a matriz do TCO.

Dessa forma, e como dentro do período dos últimos 6 meses foram obtidas 2 cotações de preços junto ao mercado, e encontrado 1 preço público, será apresentado a seguir a mediana destes 3 preços encontrados como forma de compor o TCO da Solução 2:

	Item	Valor (R$)

Solução Viável 1 (Solução 2)	Custos de aquisição, instalação, suporte e manutenção pelo prazo de 60 meses	R$ 3.244.765,10
	Valor total	**R$ 3.244.765,10**

Tabela 10 - Cálculo dos custos totais de propriedade

7.2 MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE

Conforme já mencionado anteriormente, a Solução 2 é a única que se mostrou viável neste estudo, e seu TCO para o prazo dos primeiros 5 anos já está contemplado em sua totalidade no próprio processo de aquisição, o que quer dizer que essa estimativa será linear ao longo dos primeiros 4 anos e será demonstrado no quadro abaixo.

Solução	**Estimativa de TCO ao longo dos anos**				**Valor (R$)**
	Ano 2023	**Ano 2024**	**Ano 2025**	**Ano 2026**	
Solução Viável 1 (Solução 2)	R$ 811.191,28	R$ 811.191,28	R$ 811.191,28	R$ 811.191,28	**R$ 3.244.765,10**

Tabela 11 - Mapa comparativo dos custos totais de propriedade

8. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A Solução de TIC a ser contratada para que atenda a demanda apresentada no DOD (PROAD 7902/2021, documento 6), qual seja “Implantação de uma infraestrutura de rede de comunicação sem fios em todo o âmbito do TRT23”deverá ser a aquisição de uma rede sem fios, utilizando tecnologia Wi-Fi 6 e composta, pelo menos, dos seguintes elementos: Pontos de Acesso (Modelo 1 e Modelo 2), Injetores de energia PoE, Controladora Wireless, Solução de Controle de Acesso a Redes, Pacotes de licença para acesso de visitantes, serviços de instalação e transferência de conhecimento.

Para garantir a integração, interoperacionalidade e disponibilidade de todos os recursos dos Pontos de Acesso, é imprescindível que todos os itens sejam fornecidos pelo mesmo fabricante e, portanto, é inviável o parcelamento do objeto em mais de um lote.

Os itens devem ser fornecidos com serviços de suporte técnico e garantia por um período mínimo de 60 meses.

9. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

A Tabela 12 apresenta o orçamento estimado para a solução escolhida.

	Valor (R$)
Solução 2: Rede Wi-Fi 6	**R$ 3.244.765,10**

Tabela 12 – Estimativa de custo total da solução escolhida

10. PARCELAMENTO DO OBJETO

Para garantir a integração, interoperacionalidade e disponibilidade de todos os recursos dos Pontos de Acesso, é imprescindível que todos os itens sejam fornecidos pelo mesmo fabricante e, portanto, é inviável o parcelamento do objeto em mais de um lote.

11. ADEQUAÇÃO NO AMBIENTE

As equipes internas do TRT23, notadamente da STIC/CITM e da SISP/Manutenção Predial ou Engenharia, deverão, em consonância com a empresa contratada, no momento da elaboração do projeto executivo de instalação da Rede Sem Fios, elaborar um plano de instalação física dos Pontos de Acesso nos prédios do Regional, nos pontos a serem indicados pelo projeto de implantação a ser elaborado e entregue pela contratada, como etapa preliminar do processo de instalação da rede sem fios, e esta atividade engloba o fornecimento de ponto de alimentação elétrica, ponto de rede e a instalação física dos Pontos de Acesso propriamente ditos, conectando-os à rede lógica do TRT23 de forma que possam ser acessados remotamente pela contratada para sua configuração e ativação.

12. INTERCORRÊNCIAS EM CONTRATAÇÕES ANTERIORES

Não aplicável.

13. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

A **Solução 2: Rede Wi-Fi 6 (IEEE 802.3ax)** foi escolhida conforme a análise e dados apresentados neste estudo. Ela está perfeitamente alinhada às necessidades de negócio e requisitos tecnológicos apresentados.

A aquisição da Solução 2 trará os seguintes benefícios:

- Possibilidade amagistrados, servidores e outros colaboradores, de utilização de dispositivos móveis, como Notebooks, Smartphones e Tablets, em qualquer ambiente dos prédios do TRT23, para acesso à internet e à rede interna do próprio Regional;

- Facilidade para acesso de magistrados e servidores a recursos como chamadas de áudio e videoconferências por meio de dispositivos móveis;
- Possibilidade de utilização de aplicativos de mensageria eletrônica (WhatsApp, por exemplo) mesmo quando fora de seu ambiente habitual de trabalho, como quando em reuniões ou treinamentos, utilizando dispositivos móveis;
- Possibilidade de ativação de eventuais pontos de acesso a rede interna do TRT23, em caráter temporário ou até mesmo definitivo, sem a necessidade de instalação de cabeamento de rede onde não seja viável ou temporâneo;
- Oferta de acesso à internet a advogados, jurisdicionados e demais pessoas que transitem pelas dependências do TRT23.

O quantitativo a ser contratado está em sintonia com a demanda prevista pelo Tribunal.

Como a aquisição da Solução 2 pretende-se atingir os seguintes resultados:

- Utilização do dispositivo móvel ao invés do token físico para assinatura de documentos e atos processuais (quando a versão do JTe implemente essa funcionalidade).;
- Facilidade para conexão do notebook do magistrado à rede sem fios do Tribunal, sem a necessidade de configuração e conexão a ponto de rede cabeada;
- Possibilidade de utilização de todos os serviços disponíveis para dispositivos móveis em ambientes do TRT23 onde a cobertura de sinal celular é ineficiente, como por exemplo, nos plenários da Corte.

A Solução 2 poderá ser adquirida através da forma de bens com serviços de suporte técnico e garantia, e também poderá ser ampliada ou substituída no futuro, caso seja de interesse da administração.

Por fim, entende-se que a aquisição da Solução 2 é a mais viável no momento para o Tribunal.

14. APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria TRT/DG nº 946/2021 de 27 de outubro de 2021.

Conforme o Guia de Contratações de STIC do Poder Judiciário instituído pela Resolução CNJ Nº 468/2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Demandantes e pela autoridade máxima da área de TIC.

Cuiabá, 17 de maio de 2021.

Rogério Mendes Pimenta
Integrante Demandante

Rogério HaruoSakata
Integrante Técnico

Hugo Luis Barros Pinho
Secretário de TIC

Anexo I

Mapeamento de requisitos da demanda, requisitos técnicos e equipamentos de referência

Rede Wi-Fi

Requisitos técnicos				Catalyst 9115	AirEngine 5760-51	AP 1321	AP 505
Item	Tipo	Descrição do Requisito Técnico	Requisito da demanda a que atende	Cisco	Huawei	Alcatel	Aruba
1	Access Point	O modelo ofertado deve possuir Certificado de Conformidade Técnica de produto do tipo Tansceptor de Radiação Restrita homologado pela ANATEL, com vigência válida pelo menos até a data do certame.	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Não	Não	N/I
2	Access Point	O modelo ofertado deve ser certificado pela Wi-Fi Alliance na categoria Routers, sub-categoria "Enterprise/Service ProviderAcess Point, Switch/ControllerorRouter" e, no sumário de certificações, apresentar as certificações: 2.4 GHz Spectrum Capabilities 5 GHz Spectrum Capabilities Wi-Fi Certified a, b, g, n, ac, ax WMM	A rede sem fios, ainda que de geração mais recente, deve permitir a conexão de dispositivos móveis compatíveis com as tecnologias anteriores, como os padrões IEEE 802.11a/b/g/n/ac e operar simultaneamente nas frequências de 2.4 e 5 GHz	Sim	Sim	Sim	Sim

		WPA 3 Enterprise, Personal WPA 2 Enterprise, Personal Protected Management Frames					
3	Access Point	Possuir interface de rede padrão Gigabit Ethernet (IEEE 802.3 1000BASE-T/1000BASE-TX) com conector RJ-45 e suporte a Power over Ethernet (PoE) em conformidade com o padrão 802.3at	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim	Sim	Sim	Sim
4	Access Point	Atender as normas do IEEE 802.11a, b, g, n, ac e ax	A rede sem fios, ainda que de geração mais recente, deve permitir a conexão de dispositivos móveis compatíveis com as tecnologias anteriores, como os padrões IEEE 802.11a/b/g/n/ac e operar simultaneamente nas frequências de 2.4 e 5 GHz	Sim	Sim	Sim	Sim
5	Access Point	Deve permitir modo de gerenciamento e provisionamento de recursos através de controladora, física ou virtualizada, do mesmo fabricante	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	Sim

6	Access Point	Possuir porta de console para gerenciamento "in-band" e configuração via linha de comando CLI com conector RJ-45, RS-232 ou USB/Micro USB	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	N/I	N/I	Sim
7	Access Point	Operar simultaneamente nas frequências de 2,4 e 5 GHz	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	Sim
8	Access Point	Deve ser capaz de estar conectado à controladora que o gerencia, diretamente ou remotamente via roteamento de camada 3 com tráfego de gerenciamentoi protegido por túnel criptografado (IEEE 802.11w, Protected Management Frames)	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	N/I	Sim	N/I	N/I

9	Access Point	Possuir seleção automática de canal e ajuste automático de potência do sinal, visando o melhor desempenho (DFS/DFA)	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Sim	Sim	Sim
10	Access Point	Ser capaz de prover até 16 SSID's simultâneos por rádio	A rede sem fios deve oferecer cobertura de sinal de boa qualidade (>=70% de potência de sinal em pelo menos 80% da área de cada ambiente) em todas as dependências do TRT23 onde haja usuários de TIC	N/I	Sim	Sim	Sim
11	Access Point	Deve implementar cliente DHCP e possibilitar configuração inicial de modo que toda configuração seja baixada do controlador automaticamente	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	N/I	Sim	Sim	N/I
12	Access Point	Deve possuir sinalizadores luminosos de indicação de ligado, conectado à LAN e tráfego WLAN	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	Sim	Sim	Sim

13	Access Point	Suporte integrado à tecnologia Power over Ethernet (PoE) conforme o padrão IEEE 802.3af ou 802.3at (PoE+)	Os Access Points devem ser alimentados de eletricidade pelo mesmo cabo que conduz o sinal de rede, utilizando a tecnologia PoE (Power over Ethernet), de maneira nativa ou por meio adaptadores, que deverão neste caso ser fornecidos juntamente com os Access Points	Sim	Sim	Sim	Sim
14	Access Point	Deve implementar a utilização de canais de 20/40/80/160 MHz em 802.11ac e 802.11ax	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	N/I
15	Access Point	Suportar autenticação segundo o padrão IEEE 802.1X com suporte a servidor RADIUS padrão de mercado (tais como NPS e FreeRADIUS)	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim	Sim	N/I
16	Access Point	Equipamento para uso em ambientes internos (indoor), com estrutura e/ou suportes para fixação em paredes e tetos, acompanhado de todos os acessórios necessários	A rede sem fios a ser implantada deve aproveitar, tanto quanto possível, a infraestrutura elétrica e de cabeamento de rede já existente no ambiente dos prédios do TRT23 e, quando necessárias adequações, ser	Sim	Sim	Sim	Sim

			indicado pela empresa responsável pela implantação de forma que as adequações possam ser realizadas pelas equipes internas do TRT23				
17	Access Point	Suportar operação em temperaturas de 0 a 50°C e umidade de até 90% (não condensada)	A rede sem fios a ser implantada deve aproveitar, tanto quanto possível, a infraestrutura elétrica e de cabeamento de rede já existente no ambiente dos prédios do TRT23 e, quando necessárias adequações, ser indicado pela empresa responsável pela implantação de forma que as adequações possam ser realizadas pelas equipes internas do TRT23	Sim	Sim	Sim	Sim
18	Access Point	Deve suportar arquitetura centralizada, operando de modo dependente de controlador wireless (WLAN AC) que faça o gerenciamento das políticas de segurança, qualidade de serviço (QoS) e monitoramento de RF	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	Sim
19	Access Point	Deve suportar operação MU-MIMO (multiuser MIMO) em 2x2 e com 2 fluxos espaciais (2x2:2)	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria	Sim	Sim	Sim	Sim

			certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir				
20	Access Point	Deve possuir antenas internas ao equipamento, de radiação omnidirecional, com ganho mínimo de 3 dBi em 2.4 GHz e 4 dBi em 5 GHz.	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Não	Sim
21	Access Point	Deve possuir potência mínima de 100 mW em ambas as frequências. Não serão aceitos equipamentos com potência inferior	Requisito de demanda não identificado	Sim	N/I	N/I	N/I
22	Access Point	Deve suportar autenticação WPA3. Também deve suportar autenticação 802.1x incluindo EAP-TLS, EAP-TTLS, EAP-GTC, EAP-SIM e PEAP, e o algoritmo AES para criptografia	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim	Sim	Sim
23	Access Point	Deve implementar técnica de transmitbeamforming	Requisito de demanda não identificado	Sim	Sim	Sim	Sim

		(TxBF)					
24	Access Point	Deve suportar OFDMA	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Sim	Sim	Sim
25	Access Point	Deve suportar recurso de Target Wake Time (TWT)	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	Sim
26	Access Point	Deve suportar BSS Coloring	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim	Sim	Sim	N/I
27	Access Point	Garantia de 60 (sessenta) meses com envio de peças/equipamentos de reposição em até 3 dias úteis	Requisito de demanda não identificado	Sim			

28	Access Point	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 dos equipamentos deste grupo (lote)	Requisito de demanda não identificado	Sim			
29	Access Point	Suportar operação em MU-MIMO 2x2:2 em 2,4Ghz e MIMO 4X4:4 em 5 Ghz	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	N/I
30	Access Point	Deve possuir capacidade de comutação agregada de 5.3 Gbps ou superior	Requisito de demanda não identificado	Sim	Sim	Não	Não

31	Access Point	Possuir operação com padrões BPSK, QPSK, 1024-QAM, 256-QAM, 64-QAM, 16-QAM	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	N/I	Sim	Sim	Sim
32	Access Point	Operar com canais de 40MHz, 80MHz e 160MHz, para a frequência de 5GHz	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	N/I	Sim	N/I	N/I
33	Access Point	Na eventualidade da falha do controlador WLAN a que esteja conectado, deve conseguir se associar a um controlador WLAN alternativo de forma automática, não permitindo que a rede wireless se torne inoperante	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	N/I	Sim	N/I	N/I
34	Access Point	Deve implementar funcionamento em modo auto-gerenciado, provendo serviços mesmo sem estar conectado a uma controladora	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de	Sim	Sim	Sim	Sim

			forma a garantir altos índices de disponibilidade de serviços ao usuário				
35	Access Point	Deve implementar mecanismo para prevenção ou minimização do impacto da interferência de redes celulares - ACC (AdvancedCelullarCoexistence)	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	N/I	Sim	Sim	Sim
36	Access Point	Deve permitir a formação de conjuntos de pontos de acesso que se comuniquem e compartilhem as mesmas configurações (Mesh)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	Sim	Sim	N/I
37	Access Point	Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede	Sim	Sim	Sim	N/I
38	Access Point	Deve possuir rádio integrado BLE 5.0 e	Requisito de demanda não identificado	N/I	Sim	Sim	Sim

		capacidade de instalação de módulos Zigbee ou RFID					
39	Access Point	Antenas com difusão radial em ambiente interno com potência de transmissão de 23dBm e sensibilidade de recepção de -93dBm, por canal	A rede sem fios deve oferecer cobertura de sinal de boa qualidade (>=70% de potência de sinal em pelo menos 80% da área de cada ambiente) em todas as dependências do TRT23 onde haja usuários de TIC	Sim	Sim	Não	Sim
40	Access Point	Possuir recurso de análise de espectro para detecção e mitigação de interferências de rádio frequência	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Sim	Sim	N/I
41	Access Point	Permitir configuração de VLans, criptografia e QoS independentes por SSID	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	N/I	Sim	N/I	N/I
42	Access Point	Implementar WIDS e WIPS, com recursos de detecção de dispositivos intrusos e aplicação de contramedidas	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	N/I	Sim	Sim	N/I

43	Access Point	Deve ser compatível com os padrões 802.11k (Radio Resource Management), 802.11v (BSS Transition Management) e 802.11r (Fast roaming)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	N/I	Sim	Sim	N/I
44	Access Point	Deve implementar DHCP Snooping	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	N/I	Sim	N/I	N/I
45	Access Point	Implementar autenticação de clientes por via de servidor Radius, procolo 802.1x e endereço MAC	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim	Sim	Sim
46	Access Point	Ser capaz de suportar até 1.000 conexões de usuários ativas	A rede sem fios deve oferecer cobertura de sinal de boa qualidade (>=70% de potência de sinal em pelo menos 80% da área de cada ambiente) em todas as dependências do TRT23 onde haja usuários de TIC	N/I	Sim	N/I	N/I

47	Access Point	Implementar controle de detecção e alarmes contra acessos indesejáveis	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	N/I	Sim	N/I	N/I
48	Access Point	Antenas devem ser internas com tecnologia com irradiação do tipo omni-direcional	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	N/I	Sim	N/I	N/I
49	Access Point	Gerenciável via protocolo SNMP v1/2/3	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	N/I	Sim	Sim	N/I
50	Access Point	Configurável por navegador Web (HTTP e HTTPS)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como	N/I	Sim	Sim	N/I

			também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso				
51	Access Point	Possuir certificação IP41	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	N/I	Sim	N/I	N/I
52	Access Point tipo 2	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	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim	Sim	Sim	Não
53	Access Point tipo 2	Deve possuir potência mínima de 200 mW em ambas as frequências. Não serão aceitos equipamentos com potência inferior	Requisito de demanda não identificado	Sim	N/I	N/I	N/I
54	Access Point tipo 2	Deve suportar operação MU-MIMO (multiuser MIMO) em 4x4 e com 4 fluxos espaciais	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	N/I

55	Access Point tipo 2	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	A rede sem fios deve oferecer cobertura de sinal de boa qualidade (>=70% de potência de sinal em pelo menos 80% da área de cada ambiente) em todas as dependências do TRT23 onde haja usuários de TIC	Sim	Sim	Não	Sim
56	Access Point tipo 2	Deve implementar a utilização de canais de 160MHz em 802.11ac/ax	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim	Sim	Sim	Não
57	Access Point tipo 3	Deve implementar análise de espectro para detecção de interferências provenientes de outros equipamentos nas frequências de 2.4 e 5GHz, 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 e	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Não	Não	Não

		controlador wireless de forma que sejam utilizados nos pontos de acesso os canais menos afetados pelas interferências. Esta análise deve ocorrer simultaneamente nasfrequências de 2.4 e 5 GHz no mesmo AP sem perda de conectividade ou redução do data rate para os clientes conectados. No caso de não implementação deste recurso, devem ser fornecidos dois pontos de acesso (desde que atendam aos requisitos deste item): um para operação de rede e outro para operação como análise de espectro				
58	Controladora Wireless	A controladora wireless, seja física (appliance) ou virtualizada (virtual appliance), deverá ser do mesmo fabricante e controlar de maneira centralizada os Pontos de Acesso (Access Points) que compõem a solução, e poder ser instalada em Centro de Dados que suporte redundância e alta disponibilidade, possibilitando redundância geográfica e replicação entre equipamentos em centros de dados distintos. Não serão aceitas soluções baseadas em nuvem.	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede	Sim	Sim	Sim

59	Controladora Wireless	Deve suportar e ser capaz de gerenciar de forma centralizada todas as características e parâmetros dos Access Points ofertados conjuntamente nesta solução	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede	Sim	Sim	Sim
60	Controladora Wireless	Deve suportar e ser capaz de gerenciar todas as características e protocolos para os quais os Access Points adquiridos conjuntamente foram certificados, em especial: Wi-Fi Certified a, b, g, n, ac, ax WMM WPA 3 Enterprise, Personal WPA 2 Enterprise, Personal Protected Management Frames	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede	Sim	Sim	Sim
61	Controladora Wireless	Independentemente da controladora wireless ser oferecida em appliance físico ou virtual, deverá ser composta de todos os softwares e licenças necessários e suficientes ao perfeito funcionamento da solução	A solução deve ser entregue instalada, configurada e em pleno funcionamento	Sim	Sim	Sim

62	Controladora Wireless	Deve implementar o mecanismo de mudança de autorização dinâmica para 802.1x, conhecido como RADIUS CoA (ChangeofAuthorization) conforme RFC 3576 ou RC 5176	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim
63	Controladora Wireless	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	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim	Sim
64	Controladora Wireless	O equipamento deve suportar trabalhar em modo de alta disponibilidade (high availability), ou seja, prover serviços em conjunto com outro equipamento (nós ativo/ativo, ativo/passivo ou N+1) de mesmo modelo, mantendo-se constantemente com parâmetros de configuração e funcionamento automaticamente atualizados, de forma que se um dos nós sofra indisponibilidade, o outro assuma	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim	Sim

		integralmente a provisão de serviços, assegurando que não haja interrupção de funcionamento dos dispositivos controlados			
65	Controladora Wireless	Permitir a gravação de eventos em servidor externo por meio do protocolo syslog ou equivalente	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	Sim
66	Controladora Wireless	Oferecer a capacidade de ser gerenciado através de navegador padrão (HTTP/HTTPS), SSH, Telnet e interface console	Deve poder ser gerenciada por conexão de console local, acesso por terminal remoto em interface de texto (CLI – CommandLine Interface) e acesso remoto por interface gráfica baseada em navegador de internet (Web Browser), independentemente do local de origem do acesso;	Sim	Sim
67	Controladora Wireless	Implementar função de DFS e controle de TPC, conforme indicado no draft IEEE802.11h	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim	Sim
68	Controladora Wireless	Implementar varredura de RF, periódica e automática, classificando fontes de interferencia e APs não autorizados (rogues)	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por	Sim	Sim

			interferência		
69	Controladora Wireless	Ajustar dinamicamente canais e potência de radiofrequência 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	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Sim
70	Controladora Wireless	Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Sim
71	Controladora Wireless	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	A solução deve permitir o balanceamento de carga de tráfego pela realocação automática de usuários conectados a Access Points adjacentes	Sim	Sim
72	Controladora Wireless	Possibilitar fast roaming, melhorando a performance de aplicações em tempo real (802.11r)	A solução deve permitir a mudança transparente de célula (seamless roaming) quando o usuário se movimenta ao longo da área de cobertura da rede	Sim	Sim

73	Controladora Wireless	Implementar protocolo de autenticação para controle do acesso administrativo à controladora baseado em mecanismos de AAA (Authentication, Authorization and Accounting).	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim
74	Controladora Wireless	Possuir suporte a autenticação IEEE 802.1x, com pelo menos três dos seguintes métodos EAP: EAP-MD5, PEAP/EAP-GTC, EAP-PEAP, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim
75	Controladora Wireless	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	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim

		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			
76	Controladora Wireless	Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	Sim
77	Controladora Wireless	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)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	Sim

78	Controladora Wireless	Implementar segurança baseada nos padrões WPA/WPA2/WPA3 e 802.11i	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim	
79	Controladora Wireless	Deve implementar funcionalidades de wIDS com intuito de controlar e identificar tentativas de ataques a rede WLAN. Deve implementar mecanismos contra ataques tipo AuthFlood, DeauthFlood, EAPOL Flood e Broadcast Deauth	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim	Sim	
80	Controladora Wireless	Deve permitir tráfego IPv4, IPv6 e Multicast através do controlador (camada 2)	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim	Sim	Sim
81	Controladora Wireless	Deve ser possível, de forma integrada ao software da controladora, localizar usuários 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	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de	Sim	Sim	

		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)	uso	
82	Controladora Wireless	No caso da controladora wireless ser oferecida em appliance virtualizado, este deve ser compatível e homologado para operação com VMwareESXi 6 ou superior, KVM ou Hyper-V e ser compatível com as funcionalidades VMwarevMotion, VMware Snapshot e VMwareDistributedResourceScheduler (DRS), sem impacto ao funcionamento	Deve poder ser conectada à infraestrutura de rede corporativa atual do Tribunal e comunicar-se com todos os demais equipamentos mediante simples conexão por cabos e ajuste de parâmetros lógicos de roteamento e segurança	Sim
83	Controladora Wireless	Deve possuir funcionalidade baseada em reconhecimento de aplicações através da técnica de DPI (DeepPacketInspection) 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	Todos os dispositivos de hardware e de software a serem fornecidos devem contar com as respectivas licenças de que necessitem para seu perfeito funcionamento, com garantia de funcionamento, atualização e suporte pelo período a ser estipulado na contratação	Sim

		funcionamento deste recurso para a capacidade máxima de pontos de acesso que podem ser gerenciados pela controladora		
84	Controladora Wireless	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	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
85	Controladora Wireless	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	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
86	Controladora Wireless	Deve implementar recurso que evite automaticamente a conexão de usuários wireless em pontos de acesso classificados automaticamente como maliciosos/não autorizados	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

87	Controladora Wireless	Implementar opção de escritório remoto (local switching). Neste modo não é necessário que todo o tráfego seja direcionado para 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)	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
88	Controladora Wireless	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	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim

89	Controladora Wireless	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	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim
90	Controladora Wireless	A solução deve detectar, classificar e mitigar interferências não WiFi que impactem diretamente no funcionamento da rede em menos de 10 minutos	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim
91	Controladora Wireless	Deve implementar 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	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim

92	Controladora Wireless	Para fins de controle, deve permitir a restrição da quantidade de usuários conectados em um determinado domínio de mobilidade (SSID)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
93	Controladora Wireless	Implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente pontos de acesso próximos disponíveis para roaming	A solução deve permitir a mudança transparente de célula (seamless roaming) quando o usuário se movimenta ao longo da área de cobertura da rede	Sim
94	Controladora Wireless	Deve suportar a adição e gerenciamento de pontos de acesso que operem nos padrões WiFi 802.11ac e 802.11ax	Ser composta, no mínimo, de Controladoras Wireless para configuração e gerenciamento centralizados, baseadas em hardware ou virtualizadas por software, e de Pontos de Acesso (Access Points) dotados da tecnologia mais recente (Wi-Fi 5 ou Wi-Fi 6, IEEE 802.11ac ou 802.11ax) e fabricados por indústria certificada pela Wi-Fi Alliance, desde que compatíveis com os demais requisitos a seguir	Sim
95	Controladora Wireless	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. Devem acompanhar	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim

		todas as licenças necessárias para o funcionamento conforme os itens descritos neste documento		
96	Controladora Wireless	Deve implementar SNTP ou NTP para sincronização de tempo com outros dispositivos de rede	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
97	Controladora Wireless	Deve permitir o cadastramento de usuários visitantes na base interna da controladora	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
99	Controladora Wireless	Deve permitir a atualização remota do software (firmware) da controladora e do software (firmware) dos pontos de acesso (APs), mesmo quando conectado remotamente	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização,	Sim

			auditoria, geração e interpretação de métricas de uso		
100	Controladora Wireless	Implementar SNMP v2c e v3 incluindo a geração de traps e suportar MIB vII (conforme RFC 1213)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	
102	Controladora Wireless	Deve permitir o gerenciamento da controladora e dos pontos de acesso através de IPv6	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim	
103	Controladora Wireless	No caso da controladora wireless ser oferecida em appliance físico, o hardware deverá ser acompanhado, ainda, de fonte de alimentação com seleção automática de tensão (100-240 VAC), LEDs para a indicação do status das portas e atividade, e todos os acessórios e componentes necessários a sua instalação em rack de 19"	A solução deve ser entregue instalada, configurada e em pleno funcionamento	Sim	Sim

105	Controladora Wireless	Recursos técnicos de segurança relacionados à autenticação criptografada de usuários, ao suporte à criptografia assimétrica para todos os dados transmitidos e aos controles de acesso e de auditoria de usuários e administradores deverão estar inclusos na arquitetura da solução	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)		Sim	
106	Controladora Wireless	Deve implementar atribuição dinâmica de ACL (Access ControlLists), QoS e VLAN, com base nos parâmetros da etapa de autenticação	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso		Sim	
107	Controladora Wireless	Deve ser capaz de gerenciar, no mínimo, a quantidade de 256 pontos de acesso simultaneamente, com centralização das funcionalidades de autenticação	Requisito de demanda não identificado	Sim	Sim	Sim
108	Controladora Wireless	Permitir a conexão simultânea de, no mínimo, 4.000 clientes wireless	Requisito de demanda não identificado	Sim	Sim	

109	Controladora Wireless	Permitir gravação de múltiplas configurações no próprio equipamento	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
110	Controladora Wireless	A disposição de portas/interfaces deve ser de no minimo 2 (duas) portas GE/10G (SFP+) auto-sense, 8 (oito) portas 10/100/1000BASE-T	Requisito de demanda não identificado	Sim
111	Controladora Wireless	Oferecer performance mínima de tráfego cabeado de 6 Gbps	Requisito de demanda não identificado	Sim
112	Controladora Wireless	Suportar, no mínimo, 4000 VLANs	Requisito de demanda não identificado	Sim
114	Controladora Wireless	Possuir uma interface porta console para gerenciamento "in-band", por meio de porta serial ou USB, com o cabo	Deve poder ser gerenciada por conexão de console local, acesso por terminal remoto em interface de texto (CLI – CommandLine Interface) e acesso remoto por interface gráfica baseada em navegador de internet (Web Browser), independentemente do local de origem do acesso;	Sim
115	Controladora Wireless	Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários,	Sim

		configuração individual de cada equipamento	autenticação, autorização, auditoria, geração e interpretação de métricas de uso	
116	Controladora Wireless	Permitir operação em modo mesh (WMN), com suporte ao protocolo de roteamento Hybrid Wireless MeshProtocol (HWMP)	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim
117	Controladora Wireless	Permitir a configuração e o uso de múltiplos SSIDs simultaneamente em cada Access Point, associando parâmetros de segurança distintos para cada SSID	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim
118	Controladora Wireless	Ser capaz de ocultar o SSID automaticamente quando o número de dispositivos conectados, definido pelo administrador, for alcançado	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim
119	Controladora Wireless	Ser capaz de negar serviços, se assim configurado, para dispositivos não compatíveis com padrões de alta taxa de transferência (802.11n, 802.11ac e 802.11ax)	A rede sem fios, ainda que de geração mais recente, deve permitir a conexão de dispositivos móveis compatíveis com as tecnologias anteriores, como os padrões IEEE 802.11a/b/g/n/ac e operar simultaneamente nas frequências de 2.4 e 5 GHz	Sim
120	Controladora Wireless	Possuir mecanismo para realizar o roaming de "StickyClients" de maneira eficiente,	A solução deve permitir a mudança transparente de célula (seamless roaming) quando o usuário se	Sim

		evitando o uso prolongado do canal do AP por este tipo de dispositivo	movimenta ao longo da área de cobertura da rede	
121	Controladora Wireless	Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a fazer o melhor esforço para prover a cobertura da área não assistida	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim
122	Controladora Wireless	Permitir a priorização de serviços de voz sobre dados atraves de SpectralinkVoicePriority (SVP)	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
123	Controladora Wireless	Prover tempo de fast-roaming inferior a 60 milissegundos	Requisito de demanda não identificado	Sim
124	Controladora Wireless	Devesuportar Wireless Multimedia Extensions (WMM), Unscheduled Automatic Power Save Delivery (U-APSD) e Call Admission Control (CAC)	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
125	Controladora Wireless	Gerenciar centralizadamente a autenticação de usuários	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da	Sim

			rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	
126	Controladora Wireless	Possuir base de dados de usuários interna para autenticação de usuários, além de poder utilizar mecanismos e bases externos para autenticação	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
127	Controladora Wireless	Permitir autenticação em no mínimo três dos seguintes protocolos/sistemas de base de dados de usuários: LightweightDirectory Access Protocol (LDAP), Microsoft Active Diretor (AD), Remote Authentication Dial-In User Service (RADIUS), FreeRadius, A10 Networks, Cisco ACS server, IDSentrie e RSA-ACE	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

128	Controladora Wireless	Suportar protocolo Internet Key Exchange (IKE) nas versões IKEv1 e IKEv2, para securityassociation (SA)	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
129	Controladora Wireless	Deverá possuir capacidade de implementação de perfis de configuração de equipamentos, para a implementação de novos pontos de acesso sem a necessidade de configuração individual de cada equipamento	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
130	Controladora Wireless	Deverá suportar autenticação por Captive Portal externo.	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

131	Controladora Wireless	Realizar o controle de autorização baseado em perfis de acesso	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
132	Controladora Wireless	Permitir criação de Access ControlLists (ACLs) baseadas em horário	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
133	Controladora Wireless	Oferecer detecção e proteção integrada de ataques de negação de serviços TCP, ICMP	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim
134	Controladora Wireless	Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de	Sim

			dispositivos móveis conectados a esta rede	
135	Controladora Wireless	Permitir o controle de banda disponível (bandwithcontracts) por usuário ou através de perfis de usuários	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
136	Controladora Wireless	Possuir capacidade de gerar alarmes e executar contramedidas no caso de detecção de um ataque	A infraestrutura deve apresentar mecanismos de tolerância a falhas e capacidade automática de recuperação de eventos que gerem indisponibilidade de alguns de seus elementos, de forma a garantir altos índices de disponibilidade de serviços ao usuário	Sim
137	Controladora Wireless	Possuir mecanismo automático de QoS para protocolos de voz utilizando inspeção e realizando o taggingautomatico dos pacotes (SVP)	A solução deve oferecer desempenho suficiente para permitir o acesso satisfatório a serviços de dados, voz e vídeo, viabilizando inclusive o consumo de streaming de vídeo e participações em videoconferências a partir de dispositivos móveis conectados a esta rede	Sim
138	Controladora Wireless	Implementar o protocolo 802.1w (RapidSpanningTree)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários,	Sim

			autenticação, autorização, auditoria, geração e interpretação de métricas de uso	
139	Controladora Wireless	Oferecer suporte a roteamento e switching de camadas L2 e L3 na rede sem fio wireless e nas portas cabeadas do controlador	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
140	Controladora Wireless	Suportar protocolos OSPFv2 (RFC2328) e OSPFv3 (RFC2740)	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
141	Controladora Wireless	Virtual RouterRedundancyProtocol (VRRP - pode ser comprovado com RFC 2338)	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
142	Controladora Wireless	Suportar os protocolos IGMPv1, IGMPv2, IGMPv3 (podem ser comprovados com RFC 1112, 2236 e 3376)	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
143	Controladora Wireless	Poder atuar como Proxy Arp	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
144	Controladora Wireless	Possuir o recurso de criação de Pools de VLAN para permitir a escalabilidade de redes	Requisito de demanda não identificado	Sim
145	Controladora Wireless	Implementar servidor DHCP e oferecer suporte a DHCP Relay	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
146	Controladora Wireless	Oferecer os recursos de mobilidade entre VLANspara roaming de	Os componentes da rede sem fios devem poder ser conectados à rede cabeada	Sim

		camada L2	(UTP Cat 6) do TRT23 sem a necessidade de adaptações			
147	Controladora Wireless	Implementar tagging de VLANs através do protocolo 802.1Q	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações		Sim	
148	Controladora Wireless	Ser capaz de realizar a descoberta automática dos APs na infra-estrutura wireless	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede		Sim	
149	Controladora Wireless	Ser capaz de estabelecer conexão tunelada entre Access Points e controladora de maneira segura através de CAPWAP	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede		Sim	
150	Injetor PoE	Deve prover por meio do cabo de rede o fornecimento de energia capaz de alimentar os Access Points aqui descritos	Os Access Points devem ser alimentados de eletricidade pelo mesmo cabo que conduz o sinal de rede, utilizando a tecnologia PoE (Power over Ethernet), de maneira nativa ou por meio adaptadores, que deverão neste caso ser fornecidos juntamente com os Access Points	Sim	Sim	Sim

151	Injetor PoE	Deve possuir 2 portas RJ-45 fêmea, uma para ser conectada à porta de dados do switch não PoE, outra para fornecer energia e dados para o Access Point. Ambas as portas devem operar sob o padrão Gigabit Ethernet	Os Access Points devem ser alimentados de eletricidade pelo mesmo cabo que conduz o sinal de rede, utilizando a tecnologia PoE (Power over Ethernet), de maneira nativa ou por meio adaptadores, que deverão neste caso ser fornecidos juntamente com os Access Points	Sim	Sim	Sim
152	Injetor PoE	Deve acompanhar cabos e acessórios para o seu perfeito funcionamento	A solução deve ser entregue instalada, configurada e em pleno funcionamento	Sim	Sim	Sim
153	Injetor PoE	Deve ser fornecido com fonte de alimentação com capacidade para operar em tensões de 110V ou 220V com comutação automática e frequência de 60Hz. Deve ser incluído cabo para conexão à rede elétrica no padrão brasileiro	A solução deve ser entregue instalada, configurada e em pleno funcionamento	Sim	Sim	Sim
154	Injetor PoE	Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso I do artigo 15 da lei 8.666, de 21 de junho de 1993, todos os itens deste grupo devem ser do mesmo fabricante	A solução deve ser entregue instalada, configurada e em pleno funcionamento	Sim	Sim	Sim
155	Injetor PoE	Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at	Requisito de demanda não identificado	Sim		

156	Solução de Gerenciamento	Deve realizar o gerenciamento unificado de todos os elementos da solução de WLAN, devendo poder ser utilizado como única interface gráfica de administração da solução descrita neste documento	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede	Sim	Sim
157	Solução de Gerenciamento	Deve possuir ferramenta para de ajuste automático de configurações de espectro, onde configure, no mínimo, os seguintes parâmetros, baseados em dados colhidos dos próprios pontos de acesso: -Potência do rádio -Canal de difusão	A solução deve permitir o gerenciamento dinâmico e ajuste automático dos canais de transmissão quando detectado conflito de canais ou degradação de sinal por interferência	Sim	Sim
158	Solução de Gerenciamento	Permitir a visualização do mapa lógico da rede, com a representação gráfica dos equipamentos e sinalização por cor de seu estado operacional	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	Sim

159	Solução de Gerenciamento	Os componentes responsáveis pelos serviços de gerência da solução devem implementar acesso remoto administrativo através de navegador de internet (browser) padrão, com interface gráfica, utilizando os protocolos HTTP e HTTPS	Deve poder ser gerenciada por conexão de console local, acesso por terminal remoto em interface de texto (CLI – CommandLine Interface) e acesso remoto por interface gráfica baseada em navegador de internet (Web Browser), independentemente do local de origem do acesso;	Sim	Sim
160	Solução de Gerenciamento	Deve realizar varredura à procura de equipamentos existentes na rede e adicioná-los ao gerenciamento	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	
161	Solução de Gerenciamento	Deve permitir a utilização de mapas da Internet para melhor localização dos ativos espalhados em múltiplas unidades/prédios (geolocalização)	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim	

162	Solução de Gerenciamento	Deve possuir relatório de inventário da rede capaz de identificar a versão de software instalada e o número serial de todos os equipamentos monitorados na plataforma	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
163	Solução de Gerenciamento	Deve possuir suporte para gerenciamento de falhas via SNMP (Simple Network Management Protocol) versão 3 para gerenciamento seguro	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
164	Solução de Gerenciamento	A solução de gerenciamento, seja física (appliance) ou virtualizada (virtual appliance), deverá gerenciar de maneira unificada a Controladora Wireless e os Pontos de Acesso (Access Points) que compõem a solução, e poder ser instalada em Centro de Dados que suporte redundância e alta disponibilidade, possibilitando redundância geográfica e replicação entre equipamentos em	A solução deve ser dotada de sistema único e centralizado de gerenciamento de todos os equipamentos (Access Points), por sítio (ambiente de instalação), podendo ser baseado em conjunto de hardware e software, ou apenas software, que permita o monitoramento e manutenção de parâmetros de funcionamento da rede em tempo real e a partir de qualquer ponto da rede	Sim

		centros de dados distintos. Não será aceita solução de gerenciamento em nuvem.		
166	Solução de Gerenciamento	No caso da solução de gerenciamento ser oferecida em appliance físico ou virtual, deverá ser composta de todos os softwares e licenças necessários e suficientes ao perfeito funcionamento da solução	Todos os dispositivos de hardware e de software a serem fornecidos devem contar com as respectivas licenças de que necessitem para seu perfeito funcionamento, com garantia de funcionamento, atualização e suporte pelo período a ser estipulado na contratação	Sim
167	Solução de Gerenciamento	No caso da solução de gerenciamento ser oferecida em appliance virtualizado, deve ser compatível e homologada para operação com VMwareESXi 6 ou superior, KVM ou Hyper-V e ser compatível com as funcionalidades VMwarevMotion, VMware Snapshot e VMwareDistributedResourceScheduler (DRS), sem impacto ao funcionamento	Os componentes da rede sem fios devem poder ser conectados à rede cabeada (UTP Cat 6) do TRT23 sem a necessidade de adaptações	Sim
168	Solução de Gerenciamento	No caso da solução de gerenciamento ser oferecida em appliance físico, o hardware deverá ser acompanhado, ainda, de fonte de alimentação com seleção automática de tensão (100-240 VAC),	A solução deve ser entregue instalada, configurada e em pleno funcionamento	Sim

		LEDs para a indicação do status das portas e atividade, e todos os acessórios e componentes necessários a sua instalação em rack de 19"		
169	Solução de Gerenciamento	Deve possuir capacidade de gerenciamento hierárquico dos dispositivos com possibilidade de definição de grupos de equipamentos e alteração das configurações do grupo sem a necessidade de configuração individual de cada equipamento	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
170	Solução de Gerenciamento	A plataforma deve ser capaz de analisar, a nível de protocolo, falhas no momento de autenticação, mostrando em qual etapa da autenticação houve a falha	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
171	Solução de Gerenciamento	A plataforma deve ser capaz de registrar, na planta baixa, o caminho por onde um terminal autenticado circulou	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim

172	Solução de Gerenciamento	A plataforma deve ser capaz apresentar a quantidade de usuários conectados em um determinado andar	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
173	Solução de Gerenciamento	A plataforma deve ser capaz de identificar e apresentar dados analíticos de usuários que tiveram baixa qualidade de serviços dentro da rede	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
174	Solução de Gerenciamento	A plataforma deve ser capaz de apresentar em interface gráfica, o status anterior e atual da rede após uma calibração automática	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
175	Solução de Gerenciamento	Deve ser capaz de apresentar painel com as aplicações que estão sendo executadas na rede e mostrar o consumo de banda por aplicação	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim

176	Solução de Gerenciamento	Deve possuir em interface gráfica, ambiente em que mostre toda a jornada de um usuário, desde o início até o fim da conexão, informando, no mínimo, as seguintes informações: -RSSI médio da conexão -Tempo de conexão -Média de pacotes perdidos -AP no qual estabeleceu a conexão	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
177	Solução de Gerenciamento	A plataforma deve ser capaz de identificar interferências WiFi e não-WiFi, aplicar contramedidas, e mostrar na planta do pavimento a posição da ameaça/interferência, identificando o tipo de dispositivo (ad-hoc, rogue, controles sem-fio, etc)	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
178	Solução de Gerenciamento	Permitir a visualização de alertas da rede em tempo real, com indicação de níveis de severidade, permitindo o acesso simultâneo de, no mínimo, 5 usuários de monitoração, e o envio automático de alertas por e-mail	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
179	Solução de Gerenciamento	Deve ser possível acessar o terminal de comando dos pontos de acesso gerenciados através da plataforma de gerência	Deve poder ser gerenciada por conexão de console local, acesso por terminal remoto em interface de texto (CLI – CommandLine Interface) e acesso remoto por interface gráfica baseada em navegador de internet (Web Browser),	Sim

			independentemente do local de origem do acesso;	
180	Solução de Gerenciamento	Deve prover a capacidade de que um usuário mude de célula (roaming) sem perder a conexão com a rede sem fio	A solução deve permitir a mudança transparente de célula (seamless roaming) quando o usuário se movimenta ao longo da área de cobertura da rede	Sim
181	Solução de Gerenciamento	Permitir a monitoração do desempenho, em tempo real, das redes WLAN, reportando os seguintes parâmetros: falhas de autenticação, relação sinal-ruído, interferência, potência de sinal, utilização da rede por cliente, consumo de CPU e memória nas controladoras e APs	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
182	Solução de Gerenciamento	Deve implementar a listagem em tempo real das informações dos usuários conectados nas redes WLAN contendo os seguintes parâmetros: endereço IP, endereço MAC, banda utilizada pelo cliente, nível de potência de recepção, relação sinal-ruído, parâmetros de associação, autenticação e nome do usuário	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
183	Solução de Gerenciamento	Deve implementar visualização em tempo real o mapa de calor de usuários ou dispositivos na planta de um dado pavimento	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento	Sim

			de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	
184	Solução de Gerenciamento	Deve implementar busca dinâmica por usuários e dispositivos, retornando os pavimentos por onde o cliente/dispositivo passou	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
185	Solução de Gerenciamento	Deve implementar protocolo de autenticação para controle do acesso administrativo a qualquer componente da gerência da solução utilizando servidor Radius e auditoria de comandos com mecanismos de AAA	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
186	Solução de Gerenciamento	Deve permitir a criação de perfis de administradores, criando visões administrativas independentes como, por exemplo, superusers, operators e monitors	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim

187	Solução de Gerenciamento	Deve permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados nos Pontos de Acesso, Controladoras Wireless e Comutadores/Switches, a partir da plataforma de gerência	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
188	Solução de Gerenciamento	Deve implementar o controle de mudanças nas configurações dos pontos de acesso e comutadores/switches com agendamento da implantação das mudanças, backup de configurações e registro histórico destas implantações	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
189	Solução de Gerenciamento	Deve implementar o controle da distribuição das atualizações de software, mantendo um repositório de versões de softwares e permitindo o agendamento das atualizações	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim

190	Solução de Gerenciamento	Deve realizar a atualização de software do conjunto de controladores, pontos de acesso, comutadores/switches e demais componentes da solução de forma agendada e gradual (em grupos), sem causar indisponibilidade do respectivo serviço	A solução deve dispor de ferramentas que facilitem e automatizem os processos de configuração de toda a infraestrutura, considerando desde os aspectos mais básicos configuração dos acessos iniciais, assim como também os aspectos de criação de usuários, autenticação, autorização, auditoria, geração e interpretação de métricas de uso	Sim
191	Solução de Gerenciamento	Deve implementar autenticação 802.1x para os usuários da rede sem fios, podendo utilizar os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC e EAP-MD5	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
192	Solução de Gerenciamento	Deve permitir a integração com RADIUS Server com suporte aos métodos EAP citados no item anterior	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

193	Solução de Gerenciamento	Deve implementar autenticação RADIUS baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
194	Solução de Gerenciamento	Deve implementar autenticação via portal web (captive portal) para os usuários da rede que não puderem se autenticar via 802.1x. O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo.	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
195	Solução de Gerenciamento	Para redes abertas (guest VLAN) utilizadas em eventos e para visitantes, o cliente deverá poder se conectar sem senha à infraestrutura de rede e ter seu acesso redirecionado para o portal de autenticação	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

196	Solução de Gerenciamento	O Captive Portal deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
197	Solução de Gerenciamento	O Captive Portal deve possuir suporte aos idiomas Português do Brasil ou Inglês, quando não houver em idioma Português, a plataforma deve permitir que seja realizado a tradução	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
198	Solução de Gerenciamento	Deve suportar diferentes tipos de servidores de AAA (Authentication, Authorization and Accounting) de retaguarda ("BackendAuthentication Servers"), como RADIUS, LDAP e Microsoft Active Directory (sem alteração no Schema do AD)	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

199	Solução de Gerenciamento	Deve implementar funcionalidades de Classificação Automática de Dispositivos ("Deviceprofiling"), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso	A solução deve permitir a coleta e interpretação dinâmica de dados de tráfego e outras informações que permitam o planejamento de crescimento, provisionamento de recursos, detecção antecipada e em tempo real de falhas operacionais ou violações de regras de segurança	Sim
200	Solução de Gerenciamento	Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em: -Grupo do usuário no Active Directory -Protocolo de autenticação utilizado -Tipo de dispositivo utilizado -Localização ou região do AP em que se conectou	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim
201	Solução de Gerenciamento	Deve implementar os serviços de autenticação, profiling, provisionamento e autorização para 4.000 mil usuários/dispositivos simultâneos	A solução deverá permitir o estabelecimento de critérios de segurança de acesso, como a identificação do usuário, sua autenticação e a atribuição de diferentes níveis de autorização de acordo com regras (perfis de acesso) predefinidas pela gerência da rede. Para isso, dentre outros itens, deverá ser ofertado um portal de autenticação acessível por navegadores de internet (Captive Portal)	Sim

Anexo II – Requisitos técnicos da Solução

1.1 Access Points – características comuns a todos os modelos

1.1.1 Os equipamentos devem ser do tipo Ponto de Acesso (Access Point ou AP) e possuírem estrutura que permita fixação em superfícies sólidas na horizontal (teto/forro) ou vertical (paredes ou similares) de ambientes internos.

1.1.2 Ser novos e de primeiro uso, de modelo em linha de produção sem anúncio ou previsão de encerramento da produção na data da entrega das propostas.

1.1.3 Todas as unidades devem ser do mesmo modelo, contando com a mesma revisão de hardware e software e sendo identificados pelo mesmo código junto ao fabricante (PartNumber).

1.1.4 Deverá suportar operar na faixa de temperaturas de 5 a 40°C e umidade de até 95% (não condensada).

1.1.5 Possuir luz/luzes (LED) capazes de indicar os status de ligado, conectado à LAN e de atividade de rede WLAN.

1.1.6 Suportar fonte de alimentação DC direta externa, para alimentação elétrica, com entrada AC bivolt automática.

1.1.7 Possuir suporte a alimentação pelo padrão Power over Ethernet (PoE) IEEE 802.3af ou 802.3at por meio de pelo menos uma das interfaces de rede, de forma que essa alimentação seja suficiente para o pleno funcionamento de todas as características do equipamento sem nenhuma perda de desempenho ou funcionalidades na interface pela qual é alimentado.

1.1.8 Possuir arquitetura com memória não volátil para armazenamento do software e configurações, de maneira a restabelecer automaticamente seu funcionamento com a última configuração ativa após eventuais falhas de alimentação elétrica.

1.1.9 Possuir pelo menos 2 rádios independentes que possam operar simultaneamente nas frequências de 2.4 e 5 GHz e compatibilidade de transmissão e recepção segundo os padrões IEEE 802.11 a/b/g/n/ac/ax (em suas respectivas frequências de operação).

1.1.10 Todas as antenas devem ser integradas e internas ao equipamento.

1.1.11 Possuir configuração com memória e CPU dimensionados de forma a permitir a utilização simultânea e constante de todas as características descritas neste item.

1.1.12 Possuir suporte para instalação de trava antifurto do tipo “Kensingtonsecure point”.

1.1.13 Ser fornecido com a versão mais recente do software interno (firmware) disponível na data da entrega.

1.1.14 Implementar a tecnologia Wi-Fi 6 (802.11ax) e permitir conectar simultaneamente dispositivos que se comuniquem em qualquer dos padrões IEEE 802.11: b, g, a, n, ac, ax.

1.1.15 O modelo ofertado deve possuir Certificado de Conformidade Técnica de produto do tipo Transceptor de Radiação Restrita homologado pela ANATEL, com vigência válida pelo menos até a data do certame.

1.1.16 O modelo ofertado deve ser certificado pela Wi-Fi Alliance na categoria Routers, subcategoria "Enterprise/Service ProviderAcess Point, Switch/ControllerorRouter" e, no sumário de certificações, apresentar as certificações:

1.1.16.1 2.4 GHz Spectrum Capabilities

1.1.16.2 5 GHz Spectrum Capabilities

1.1.16.3 Wi-Fi Certified a, b, g, n, ac, ax

1.1.16.4 WMM

1.1.16.5 WPA 3 Enterprise, Personal

1.1.16.6 WPA 2 Enterprise, Personal

1.1.16.7 Protected Management Frames

1.1.17 Possuir antenas com padrão de radiação omnidirecional com potência máxima de pelo menos 20dBm para transmissão e sensibilidade mínima de -92 dBm para recepção.

1.1.18 As antenas devem oferecer ganhos mínimos de 3 dBi em 2.4 GHz e de 4 dBi em 5 GHz.

1.1.19 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80/160MHz para os padrões IEEE 802.11ac/ax.

1.1.20 Operar com modulações de frequência OFDMA, BPSK, QBPSK, 16-QAM, 64-QAM, 256-QAM e 1024-QAM em IEEE 802.11ax.

1.1.21 Implementar o método CSMA/CA para controle de acesso ao meio de transmissão.

1.1.22 Implementar, suportar ou ser compatível com as seguintes especificações da família de protocolos IEEE 802.11: a, b, g, n, ac, ax, d, h, i, k, v, r, w, u.

1.1.23 Suportar operar em modo gerenciado por Controladora WLAN ou independente dela (autogerenciado), e poder ter todas suas características de funcionamento configuradas remotamente pela Controladora WLAN ou diretamente no próprio equipamento por meio de interface de navegador Web padrão HTTP/HTTPS.

1.1.24 Deve permitir o bloqueio de configuração por rede sem fios.

1.1.25 Deve ser capaz de estar conectado à Controladora que o gerencia, diretamente ou remotamente via roteamento de camada 3 com tráfego de gerenciamento protegido por túnel criptografado (IEEE 802.11w, Protected Management Frames).

1.1.26 Implementar seleção automática de canal e ajuste automático de potência do sinal, visando o melhor desempenho.

1.1.27 Ser capaz de prover 8 SSIDs simultâneos por rádio.

1.1.28 Permitir escolher entre habilitar e desabilitar a divulgação de qualquer SSID.

1.1.29 Deve permitir implementar pelo menos 8 VLANs e suportar o protocolo IEEE 802.1Q.

1.1.30 Permitir a associação dinâmica de usuário a VLAN de acordo com parâmetros da etapa de autenticação.

1.1.31 Implementar Short GuardInterval.

1.1.32 Deve implementar técnica de TransmitBeamforming (TxBF) para melhora do desempenho da transmissão.

1.1.33 Deve implementar o recurso de Target Wake Time (TWT) para otimizar o uso de energia dos dispositivos clientes.

1.1.34 Deve suportar BSS Coloring para minimizar conflitos de uso de canais.

1.1.35 Implementar MaximumRatioCombining (MRC) para melhorar o desempenho de recepção.

1.1.36 Deve implementar mecanismo para prevenção ou minimização do impacto da interferência de redes celulares (CelullarCoexistence).

1.1.37 Deve permitir a formação de conjuntos de Pontos de Acesso que se comuniquem e compartilhem as mesmas configurações (Mesh).

1.1.38 Possuir capacidade de realizar análise de espectro de RF em 2.4 e 5 GHz para a detecção e identificação de outros pontos de acesso no perímetro de alcance, intrusos ou não autorizados (rogue), além de detectar interferências nos canais habilitados no ponto de acesso. A análise de espectro deve ser realizada sem interferir no funcionamento do ponto de acesso nem afetar a conexão dos usuários

1.1.39 Permitir a conexão de usuários utilizando os protocolos IPv4 e IPv6 simultaneamente no equipamento (dual-stack).

1.1.40 Deve implementar cliente DHCP e possibilitar configuração inicial de modo que toda configuração seja baixada do Controlador WLAN automaticamente.

1.1.41 Implementar os protocolos NTP ou SNTP em modo cliente para sincronização do relógio interno com fonte externa de tempo.

1.1.42 Permitir a configuração de VLans, criptografia e QoS independentes por SSID.

1.1.43 Implementar WIDS e WIPS, com recursos de assintaturas de ataques, detecção de dispositivos intrusos e aplicação de contramedidas de proteção.

1.1.44 Permitir autenticação pelo protocolo 802.1x com EAP-TLS e EAP-PEAP/MSCHAPv2.

1.1.45 Implementar solução de autenticação e gerenciamento de usuários da rede sem fios interna e independente da Controladora WLAN.

1.1.46 A solução de autenticação e gerenciamento de usuários de rede interna deve contar com as opções de autenticação: MAC Address, servidores RADIUS e Captive Portal.

1.1.47 Possibilitar os métodos de autenticação de clientes: aberta (sem criptografia), através de MAC Address, WPA/WPA2/WPA3 em modos Personal e Entreprise com suporte a PSK, TKIP, AES, por 802.1x em base de dados local, por 802.1x por via de servidor Radius, por 802.1x em base LDAP externa e por Captive Portal, e permitir o método de autenticação com base no SSID.

1.1.48 Permitir a comutação de tráfego local sem necessidade de intervenção de Controladora WLAN, exceto para a fase de autenticação de usuários e estabelecimento da conexão inicial.

1.1.49 Suportar smart roaming (802.11k e 802.11v) e fast roaming (802.11r).

1.1.50 Ser gerenciável via protocolo SNMP v1/2c/3 e implementar MIB-II (RFC 1213).

1.1.51 Deverá ser acompanhado de todas as licenças, em caráter perpétuo, que permitam a utilização das características descritas para este item, inclusive aquelas necessárias para que seja gerenciado pela Controladora WLAN, do mesmo fabricante, a ser adquirida para compor o conjunto da solução.

1.1.52 Contar com garantia de 60 (sessenta) meses com envio de peças/equipamentos de reposição em até 5 dias úteis após registro do chamado.

1.2 Access Point Modelo 1

1.2.1 Possuir pelo menos 1 interface Gigabit Ethernet com conectores RJ-45 e operando em modo autosense para detecção de velocidade e auto MDI/MDIX para detecção de polaridade.

1.2.2 Suportar throughput combinado de, no mínimo, 1,45 Gbps.

1.2.3 Operar, pelo menos, em MIMO 2x2 com 2 fluxos espaciais SU-MIMO e MU-MIMO (2x2:2) em 2,4GHz e 5GHz.

1.2.4 Ser capaz de suportar pelo menos 250 conexões simultâneas de dispositivos clientes associados por rádio (250 em 2.4GHz e 250 em 5GHz) e não deve possuir restrição por software ou licença para a quantidade de usuários conectados simultaneamente.

1.3 Access Point Modelo 2

1.3.1 Possuir pelo menos 2 interfaces Gigabit Ethernet ou 1 interface Mutigigabit Ethernet, ou uma combinação destas, e todas com conectores RJ-45 e operando em modo autosense para detecção de velocidade e auto MDI/MDIX para detecção de polaridade.

1.3.2 Suportar throughput combinado de, no mínimo, 3,5 Gbps.

1.3.3 Operar, pelo menos, em MIMO 2x2 com 2 fluxos espaciais SU-MIMO e MU-MIMO (2x2:2) em 2,4GHz e em 2,4GHz e MIMO 4x4 com 4 fluxos espaciais SU-MIMO e MU-MIMO (4x4:4) em 5GHz.

1.3.4 Ser capaz de suportar pelo menos 512 conexões simultâneas de dispositivos clientes associados por rádio (512 em 2.4GHz e 512 em 5GHz) e não deve possuir restrição por software ou licença para a quantidade de usuários conectados simultaneamente.

1.4 Injetor de energia PoE

1.4.1 Deve prover, por meio do cabo de rede, o fornecimento de energia capaz de alimentar os Access Points aqui descritos.

1.4.2 Deve possuir 2 portas RJ-45 fêmea, uma (entrada) para ser conectada à porta de dados do switch não PoE, outra (saída) para fornecer energia e dados para o Access Point. Ambas as portas devem operar sob o padrão Gigabit Ethernet.

1.4.3 Deve sem compatível com os padrões IEEE 802.3af e 802.3at.

1.4.4 Deve acompanhar cabos e acessórios para o seu perfeito funcionamento.

1.4.5 Deve ser fornecido com fonte de alimentação com capacidade para operar em tensões de 110V ou 220V com comutação automática e frequência de 60Hz. Deve ser incluído cabo para conexão à rede elétrica no padrão brasileiro.

1.4.6 Garantia de 60 (sessenta) meses com envio de peças/equipamentos de reposição em até 3 dias úteis.

1.4.7 Este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

1.5 Controladora Wireless

1.5.1 A Controladora Wireless (ou WLAN), seja física (appliance) ou virtualizada (virtual appliance), deverá ser do mesmo fabricante, ser totalmente compatível com todas as funcionalidades e tecnologias e capaz de centralizar o controle, manutenção e distribuição das configurações dos Pontos de Acesso (Access Points) que compõem a solução.

1.5.2 Deve poder ser instalada em Centro de Dados, juntamente com outra unidade idêntica, compor um cluster e suportar operar em modo de redundância e alta disponibilidade na forma ativo/ativo ou ativo/stand-by (Hot Stand-by), possibilitando total redundância de configurações e replicação de sessões de usuários entre os equipamentos, de forma que se um dos nós sofra indisponibilidade, o outro assuma integralmente a provisão de serviços, assegurando que não haja interrupção de funcionamento dos dispositivos controlados. Não serão aceitas soluções baseadas em nuvem.

1.5.3 Deve suportar e ser capaz de gerenciar todas as características e protocolos

para os quais os Access Points adquiridos conjuntamente foram certificados, em especial:

1.5.3.1 Wi-Fi Certified a, b, g, n, ac, ax

1.5.3.2 WMM

1.5.3.3 WPA 3 Enterprise, Personal

1.5.3.4 WPA 2 Enterprise, Personal

1.5.3.5 Protected Management Frames

1.5.4 Independentemente da Controladora wireless ser oferecida em appliance físico ou virtual, deverá ser composta de todos os softwares e licenças, de caráter perpétuo, necessários e suficientes ao perfeito funcionamento da solução. Para efeito de contabilização de licenças, deve ser considerada a possibilidade de controlar de até 250 Pontos de Acesso.

1.5.5 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.

1.5.6 No caso da Controladora wireless ser oferecida em appliance físico, o hardware deverá ser composto de pelo menos 2 interfaces de rede 10Gb Ethernet com porta SFP+ e respectivos transceivers 10GBASE-SR multimodo com conectores LC e 4 interfaces 10/100/1000 Mbps com conectores RJ-45, 1 porta de console física para gerenciamento via linha de comando (CLI – CommandLine Interface) com conector RJ-45 ou USB com seu respectivo cabo, além de ser acompanhado, ainda, de fonte de alimentação com seleção automática de tensão (100-240 VAC), LEDs para a indicação do status das portas e atividade, e todos os acessórios e componentes necessários à sua instalação em rack de 19".

1.5.7 Ainda no caso de a Controladora ser oferecida em appliances físico, este equipamento deve ser entregue em configuração de CPU e memória suficiente e adequada para a execução simultânea de todas as funcionalidades exigidas nesta especificação e oferecer throughput mínimo de tráfego de rede de 20Gbps.

1.5.8 No caso da Controladora wireless ser oferecida em appliance virtualizado, este deve ser compatível e homologado para operação com VMwareESXi 6 ou superior, KVM ou Microsoft Hyper-V e ser compatível com as funcionalidades VMwarevMotion, VMware Snapshot e VMwareDistributedResourceScheduler (DRS), sem impacto ao funcionamento.

1.5.9 Deve suportar a adição e gerenciamento de Pontos de Acesso que operem nos padrões WiFi 802.11ac e 802.11ax.

1.5.10 A solução deverá operar com os padrões IEEE 802.11a/b/g/n/ac/ax, com diferentes rádios de diferentes padrões, em quaisquer combinações desses padrões.

1.5.11 Deve ser capaz de gerenciar, no mínimo, a quantidade de 250 Pontos de Acesso simultaneamente, com centralização das funcionalidades de autenticação.

1.5.12 Permitir gravação de múltiplas configurações no próprio equipamento, em memória não volátil.

1.5.13 Suportar, no mínimo, 4000 VLANs

1.5.14 Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento

1.5.15 Permitir operação dos Pontos de Acesso em modo mesh (WMN), com suporte ao protocolo de roteamento Hybrid Wireless MeshProtocol (HWMP).

1.5.16 Permitir a configuração e o uso de múltiplos SSIDs simultaneamente em cada Access Point, associando parâmetros de segurança distintos para cada SSID.

1.5.17 Ser capaz limitar o número de dispositivos conectados em cada Access Point com base em parâmetro definido pelo administrador.

1.5.18 Permitir o envio ou a gravação em tempo real de registros de eventos e erros do sistema (logs) em servidor externo por meio do protocolo syslog ou equivalente.

1.5.19 Oferecer a capacidade de ser gerenciado através de navegador padrão (HTTP/HTTPS), SSH, e interface console.

1.5.20 Suportar protocolos de transferência de arquivos como FTP (File TransferProtocol) ou TFTP (Trivial File TransferProtocol) ou SFTP (Secure File TransferProtocol) ou SCP (SecureCopyProtocol).

1.5.21 Implementar protocolo de autenticação para controle do acesso administrativo à Controladora baseado em mecanismos de AAA (Authentication, Authorization and Accounting).

1.5.22 Ajustar dinamicamente canais e potência de radiofrequência dos Pontos de Acesso para otimizar a cobertura de rede e seu desempenho baseado na cobertura de APs vizinhos e interferências e implementar função de DFS e controle de TPC, conforme indicado no draft IEEE802.11h. Deve ser possível desabilitar o ajuste de potência e ajuste de canal automático.

1.5.23 Implementar, por meio dos Pontos de Acesso, varredura de RF periódica e automática, classificando fontes de interferência e APs não autorizados (rogues), evitando problemas de cobertura e controle da propagação indesejada de RF.

1.5.24 Deve permitir tráfego IPv4, IPv6 e Multicast através do controlador (camada 2).

1.5.25 Implementar opções de comutação de tráfego central e comutação de tráfego local. Neste último modo não é necessário que todo o tráfego seja direcionado para 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)

1.5.26 Deve operar Pontos de Acesso em redes remotas, mesmo acessados por NAT ou através de túnel (VPN ou semelhante). Desta forma, deve ser possível definir o IP público da Controladora e fazer com que Pontos de Acesso remotos conectem-se automaticamente à Controladora através da Internet. Em caso de falha na comunicação entre Controladora e ponto de acesso, este deve continuar sua operação de transferência de dados aos clientes já conectados.

1.5.27 Caso haja falha de comunicação entre os APs 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.

1.5.28 Deve permitir balanceamento da carga de usuários entre os Pontos de Acesso fazendo a redistribuição de usuários entre os APs próximos de forma automática e sem intervenção humana e, no caso da inoperância de algum Ponto de Acesso, redistribuir automaticamente os usuários conectados a ele para os APs adjacentes, dentro da área de alcance. Deve ser possível escolher em qual WLAN (SSID) será permitido executar tal ação.

1.5.29 Deve implementar funcionalidades de wIDS com intuito de controlar e identificar tentativas de ataques a rede WLAN. Deve implementar mecanismos contra-ataques tipo AuthFlood, DeauthFlood, EAPOL Flood e Broadcast Deauth.

1.5.30 Deve permitir implementar todos os recursos e mecanismos de segurança previstos no item Pontos de Acesso.

1.5.31 Deve implementar listas de controle de acesso (ACLs) para cada SSID dos Pontos de Acesso com restrições de endereço IP, tipos de protocolos, portas, QoS, VLAN e direção do fluxo de dados, com base nos parâmetros da etapa de autenticação. Deve ser possível a criação de ACLspara SSIDs de APs conectados local e remotamente.

1.5.32 Deve ser possível determinar, por SSID, se os usuários conectados a determinado SSID poderão ou não trocar pacotes entre si.

1.5.33 Implementar segurança baseada nos padrões WPA/WPA2/WPA3 e 802.11i.

1.5.34 Possuir suporte a autenticação IEEE 802.1x, com pelo menos três dos seguintes métodos EAP: EAP-MD5, PEAP/EAP-GTC, EAP-PEAP, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo.

1.5.35 Deve possuir funcionalidade de autenticação web (Captive Portal), sendo possível indicar um captive portal externo e, também, implementar um Captive Portal interno, caso em que todo o mecanismo de autenticação deve ser interno a Controladora (website, lista de usuários, políticas), sendo que a criação destes

usuários deverá se dar 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 a criação de páginas personalizadas com imagem e texto, e especificar o tempo que um determinado usuário (login) ficará válido para ter acesso a rede através da autenticação web.

1.5.36 Deve permitir o cadastramento de usuários visitantes na base interna da Controladora.

1.5.37 Deve implementar o mecanismo de mudança de autorização dinâmica para 802.1x, conhecido como RADIUS CoA (ChangeofAuthorization) conforme RFC 3576 ou RC 5176.

1.5.38 Deve ser possível, de forma integrada ao software da Controladora, localizar usuários, 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)

1.5.39 Deve possuir funcionalidade baseada em reconhecimento de aplicações através da técnica de DPI (DeepPacketInspection) 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

1.5.40 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.

1.5.41 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.

1.5.42 Deve implementar recurso que evite automaticamente a conexão de usuários wireless em Pontos de Acesso classificados como maliciosos ou não autorizados.

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

1.5.44 Deve permitir implementar configurações distintas por SSID nos Pontos de Acesso, locais ou remotos, tais como regras de autenticação, QoS, criptografia, SSID e VLAN para cada domínio. Deve ser possível especificar em quais APs/Grupos de APs cada SSID será aplicado.

1.5.45 Para fins de controle, deve permitir a restrição da quantidade de usuários conectados em um determinado SSID.

1.5.46 Implementar SGI – Short Guard Interval.

1.5.47 Possibilitar fast roaming, melhorando a performance de aplicações em tempo real (802.11r).

1.5.48 Implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente Pontos de Acesso próximos disponíveis para roaming.

1.5.49 Deve implementar SNTP ou NTP para sincronização de tempo com outros dispositivos de rede.

1.5.50 Deve permitir a atualização do software (firmware) da Controladora e do software (firmware) dos Pontos de Acesso (APs), mesmo quando conectado remotamente.

1.5.51 Implementar SNMP v2c e v3 incluindo a geração de traps, a criptografia do tráfego de dados de gerência e suportar MIB vII (conforme RFC 1213), que permitam coletar dados de uso pelo menos dos seguintes componentes da Controladora e dos Pontos de Acesso: interfaces de rede, CPU e memória.

1.5.52 Deve permitir o gerenciamento da Controladora e dos Pontos de Acesso através de IPv6.

1.5.53 Deve suportar Wireless Multimedia Extensions (WMM), Unscheduled Automatic Power Save Delivery (U-APSD) e Call Admission Control (CAC).

1.5.54 Oferecer detecção e proteção integrada de ataques de negação de serviços TCP, ICMP.

1.5.55 Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede.

1.5.56 Permitir o controle de banda disponível (bandwithcontracts) por usuário ou através de perfis de usuários.

1.5.57 Possuir capacidade de gerar alarmes e executar contramedidas no caso de detecção de um ataque.

1.5.58 Possuir mecanismo automático de QoS para protocolos de voz utilizando inspeção e realizando o taggingautomatico dos pacotes (SVP).

1.5.59 Implementar o protocolo 802.1w (RapidSpanningTree)

1.5.60 Oferecer suporte a roteamento e switching de camadas L2 e L3 na rede sem fio wireless e nas portas cabeadas do controlador

1.5.61 Poder atuar como Proxy Arp

1.5.62 Implementar servidor DHCP, oferecer suporte a DHCP Relay e DHCP Snooping ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede.

1.5.63 Oferecer os recursos de mobilidade entre VLANs para roaming de camada L2.

1.5.64 Implementar tagging de VLANs através do protocolo 802.1Q.

1.5.65 Ser capaz de realizar a descoberta automática dos APs na infraestrutura wireless.

1.5.66 Ser capaz de estabelecer conexão tunelada entre Access Points e Controladora de maneira segura.

1.5.67 Qualquer das funcionalidades acima pode ser considerada suprida caso esteja disponível na Solução de Gerenciamento.

1.5.68 Garantia de 60 (sessenta) meses com envio de peças/equipamentos de reposição em até 5 dias úteis.

1.5.69 Deve possuir firewall do tipo Stateful. Caso a solução não possua um firewall Stateful integrado, poderão ser fornecidas soluções externas (dispositivos ou appliances), do mesmo fabricante e cujo emprego não impacte no desempenho da solução, de forma a contemplar as características de segurança aqui exigidas.

1.5.70 Deve reconhecer e ser capaz de aplicar pelo menos 3000 políticas de QoS para otimização de tráfego de aplicações.

1.5.71 Este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos deste grupo (lote).

1.6 Solução de Gerenciamento

1.6.1 A Solução de Gerenciamento e Controle de Acesso à Rede (doravante chamada de Solução de Gerenciamento) deverá ser do mesmo fabricante, ser totalmente compatível e ter capacidade de gerenciar, de maneira unificada, todas as funcionalidades e tecnologias da Controladora Wireless e dos Pontos de Acesso (Access Points) que compõem a Solução de Rede Wi-Fi, devendo poder ser utilizada como única interface gráfica de administração de toda solução descrita neste documento.

1.6.2 Será aceito que a Solução de Gerenciamento seja física (appliance) ou virtualizada (virtual appliance), software instalável em servidor Microsoft Windows Server 2019 ou GNU Linux, ou, ainda, conjunto de funcionalidades de gerenciamento existentes na Controladora Wireless, ativas e disponíveis por padrão ou ativáveis por licenciamento. Não serão aceitas soluções baseadas em nuvem.

1.6.3 Caso a Controladora Wireless a ser ofertada ofereça todas as funcionalidades de gerenciamento exigidas neste item, sem custo ou necessidade de licenciamento adicional, o proponente deve mencionar explicitamente isso em sua proposta e cotar este item com o custo R$ 0,00.

1.6.4 Deve suportar e ser capaz de gerenciar todas as características e protocolos para os quais a Controladora Wireless os Access Points adquiridos conjuntamente foram certificados, em especial:

1.6.4.1 Wi-Fi Certified a, b, g, n, ac, 6

1.6.4.2 WMM

1.6.4.3 WPA 3 Enterprise, Personal

1.6.4.4 WPA 2 Enterprise, Personal

1.6.4.5 Protected Management Frames

1.6.5 Independentemente da Solução de Gerenciamento ser oferecida em appliance físico ou virtual, deverá ser composta de todos os softwares e licenças, de caráter perpétuo, necessários e suficientes ao perfeito funcionamento da solução. Para efeito de contabilização de licenças, deve ser considerada a possibilidade de gerenciamento de até 250 Pontos de Acesso, 5.000 dispositivos e 5.000 usuários registrados, dentre os quais até 1.000 poderiam ser usuários visitantes (ou não registrados).

1.6.6 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.

1.6.7 No caso da Solução de Gerenciamento ser oferecida em appliance físico, o hardware deverá ser composto de pelo menos 1 interface de rede Multigigabit Ethernet 2.5Gb e 2 interfaces 10/100/1000 Mbps com conectores RJ-45, 1 porta de console física para gerenciamento via linha de comando (CLI – CommandLine Interface) com conector RJ-45 ou USB com seu respectivo cabo, além de ser acompanhado, ainda, de fonte de alimentação com seleção automática de tensão (100-240 VAC), LEDs para a indicação do status das portas e atividade, e todos os acessórios e componentes necessários à sua instalação em rack de 19".

1.6.8 Ainda no caso de a Controladora ser oferecida em appliances físico, este equipamento deve ser entregue em configuração de CPU e memória suficiente e adequada para a execução simultânea de todas as funcionalidades exigidas nesta especificação e oferecer throughput mínimo de tráfego de rede de 2Gbps.

1.6.9 No caso da Controladora wireless ser oferecida em appliance virtualizado, este deve ser compatível e homologado para operação com VMwareESXi 6 ou superior, KVM ou Microsoft Hyper-V e ser compatível com as funcionalidades VMwarevMotion, VMware Snapshot e VMwareDistributedResourceScheduler (DRS), sem impacto ao funcionamento.

1.6.10 Deve permitir que todos os eventos da Controladora Wireless e dos Access Points sejam redirecionados para uma console de gerência central.

1.6.11 Possuir a capacidade de gerência de configuração, com armazenamento de diferentes versões e suporte a "rollback".

1.6.12 Toda a interface de gerenciamento deverá ser gráfica e o acesso ao sistema deverá ser por meio de cliente com browser padrão, compatível com Google Chrome e Mozilla Firefox em suas versões mais recentes, utilizando o protocolo HTTPS.

1.6.13 . Implementar protocolo de autenticação para controle do acesso

administrativo à solução utilizando servidor Radius e auditoria de comandos com mecanismos de AAA.

1.6.14 . Deve possibilitar a importação de plantas baixas dos andares/pavimentos nos formatos GIF ou JPG e a organização hierárquica de equipamentos em andares, de andares em prédios e de prédios em cidades.

1.6.15 Permitir a visualização do mapa lógico da rede, com a representação gráfica dos equipamentos e sinalização por cor de seu estado operacional.

1.6.16 Possuir visualização dos mapas de calor (heatmaps) dos andares de cada prédio, apresentando, em tempo real, posição dos pontos de acesso, dos clientes conectados, dos rogue APs e a cobertura do sinal de radiofrequência tanto em 2,4 GHz como em 5 GHz.

1.6.17 Permitir a visualização de eventuais áreas sem cobertura de radiofrequência (áreas de sombra).

1.6.18 Permitir a monitoração do desempenho, em tempo real, das redes WLAN, reportando os seguintes parâmetros: falhas de autenticação, relação sinal-ruído, interferência, potência de sinal, utilização da rede por cliente, consumo de CPU e memória nas Controladoras e APs.

1.6.19 Deve implementar a listagem em tempo real das informações dos usuários conectados nas redes WLAN contendo os seguintes parâmetros: endereço IP, endereço MAC, banda utilizada pelo cliente, nível de potência de recepção, relação sinal-ruído, parâmetros de associação, autenticação e nome do usuário.

1.6.20 Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que causam interferência na rede sem fio.

1.6.21 Possuir capacidade de gerenciamento hierárquico com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento.

1.6.22 Implementar modelos de configuração (templates) de forma a possibilitar a replicação de configuração entre equipamentos.

1.6.23 Realizar a descoberta automática dos dispositivos individuais da infraestrutura wireless.

1.6.24 Fornecer a visualização de alertas da rede em tempo real, com indicação do nível de severidade por cor.

1.6.25 Ser capaz de detectar, em conjunto com a Controladora Wireless e os Pontos de Acesso, pelo menos, os seguintes ataques: flood de frames de gerenciamento dos clientes wireless, respostas de nullprobe, flood de autenticação, ataque de deauthentication, flood de EAP handshake.

1.6.26 Implementar mecanismos para detecção, localização e bloqueio de pontos de acesso não autorizados (rogues) e redes ad-hoc.

1.6.27 Deve possuir ferramenta para de ajuste automático de configurações de espectro, onde configure, no mínimo, os seguintes parâmetros, baseados em dados colhidos dos próprios Pontos de Acesso:

1.6.27.1 Potência do rádio

1.6.27.2 Canal de difusão

1.6.28 Possuir capacidade de geração de relatórios dos seguintes tipos: Listagem de clientes wireless por período informado, Inventário, Informações de configuração das Controladoras Wi-Fi, utilização da rede, detalhes dos pontos de acesso não autorizados (rogues) detectados.

1.6.29 Deve possuir relatório de inventário da rede capaz de identificar a versão de software instalada e o número serial de todos os equipamentos monitorados na plataforma.

1.6.30 A plataforma deve ser capaz de analisar, a nível de protocolo, falhas no momento de autenticação, ajudando a identificar a etapa da autenticação em que houve a falha

1.6.31 A plataforma deve ser capaz apresentar em tempo real a quantidade de usuários conectados em um determinado andar.

1.6.32 A plataforma deve ser capaz de identificar e apresentar dados analíticos de usuários que tiveram baixa qualidade de serviços dentro da rede.

1.6.33 Deve ser capaz de apresentar painel com as aplicações que estão sendo executadas na rede e mostrar o consumo de banda por aplicação.

1.6.34 A plataforma deve ser capaz de identificar interferências WiFi e não-WiFi, aplicar contramedidas, e mostrar na planta do pavimento a posição da ameaça/interferência, identificando o tipo de dispositivo (ad-hoc, rogue, controles sem-fio, etc)

1.6.35 Deve ser possível acessar o terminal de comando dos Pontos de Acesso gerenciados através da plataforma de gerência

1.6.36 Deve permitir a criação de perfis de administradores, criando visões administrativas independentes como, por exemplo, administradores (acesso completo à plataforma), operadores (acesso a configurações de usuários e Pontos de Acesso) e monitores (acesso apenas de leitura a consultas, painéis e relatórios).

1.6.37 Deve permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados nos Pontos de Acesso, Controladoras Wireless a partir da Solução de Gerência

1.6.38 Deve realizar a atualização de software do conjunto de Controladoras Wireless e Pontos de Acesso de forma agendada e gradual (em grupos), sem causar indisponibilidade do respectivo serviço.

1.6.39 Deve implementar autenticação 802.1x para os usuários da rede sem fios, podendo utilizar os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2, PEAP-

GTC e EAP-MD5.

1.6.40 Deve permitir a integração com RADIUS Server com suporte aos métodos EAP citados no item anterior.

1.6.41 Deve implementar autenticação RADIUS baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes.

1.6.42 Deve implementar autenticação via portal web (captive portal) para os usuários da rede que não puderem se autenticar via 802.1x. O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo.

1.6.43 Para redes abertas (guest VLAN) utilizadas em eventos e para visitantes, o cliente deverá poder se conectar sem senha à infraestrutura de rede e ter seu acesso redirecionado para o portal de autenticação.

1.6.44 O Captive Portal deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes.

1.6.45 O Captive Portal deve possuir suporte aos idiomas Português do Brasil ou Inglês, quando não houver em idioma Português, a plataforma deve permitir que seja realizado a tradução.

1.6.46 Deve suportar diferentes tipos de servidores de AAA (Authentication, Authorization and Accounting) de retaguarda (“BackendAuthentication Servers”), como RADIUS, LDAP e Microsoft Active Directory (sem alteração no Schema do AD).

1.6.47 Deve implementar funcionalidades de Classificação Automática de Dispositivos (“Deviceprofiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso.

1.6.48 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

1.6.48.1 Grupo do usuário no Active Directory

1.6.48.2 Protocolo de autenticação utilizado

1.6.48.3 Tipo de dispositivo utilizado

1.6.48.4 Localização ou região do AP em que se conectou

1.6.49 Deve implementar os serviços de autenticação, profiling, provisionamento e autorização para 1.500 mil usuários/dispositivos simultâneos.

1.6.50 Qualquer das funcionalidades acima pode ser considerada suprida caso esteja disponível Controladora Wireless.

1.6.51 Solução de autenticação de usuários e dispositivos para controle de acesso a

rede baseada em appliance físico ou Virtual Appliance, sendo compatível com os seguintes Hypervisors:

1.6.51.1 VmWareESXi 5.5 ou superior;

1.6.51.2 Microsoft Hyper-V Server 2012 R2/2016 e Windows Server 2012 R2 com Hyper-V;

1.6.51.3 Amazon EC2;

1.6.51.4 CentOS KVM;

1.6.52 Para soluções virtualizadas, deverão fazer parte do fornecimento os servidores necessários, obedecendo as especificações mínimas recomendadas pelo fabricante, assim como sistemas operacionais e software para a completa instalação do sistema, atendendo a todas as características solicitadas

1.6.53 Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas / de dispositivo e elementos condicionais em um conjunto de políticas.

1.6.54 Suporte a seguintes fontes para autenticação:

1.6.54.1 Microsoft Active Directory

1.6.54.2 Kerberos

1.6.54.3 LDAP-compliantdirectory

1.6.54.4 ODBC-compliant SQL server

1.6.54.5 Token servers

1.6.54.6 Base SQL interna

1.6.54.7 Radius

1.6.54.8 Microsoft Azure Active Directory

1.6.54.9 Google G Suite

1.6.54.10 HTTP

1.6.54.11 Lista estática de endereços MAC

1.6.55 Deve suportar "Single Sign-on" (SSO) através de SAML v2.0

1.6.56 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

1.6.56.1 Atributos do usuário autenticado,

1.6.56.2 Hora do dia, dia da semana,

1.6.56.3 Tipo de dispositivo utilizado,

1.6.56.4 Localização do usuário;

1.6.56.5 Tipo de autenticação utilizado

1.6.57 Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, MAC Address 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 utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise

1.6.58 Deve possuir dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:

1.6.59 - Lista com os últimos Alertas do sistema;

1.6.60 - Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication.

1.6.61 - Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;

1.6.62 - Para soluções compostas por mais de um servidor/appliance, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados

1.6.63 - Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação.

1.6.64 - Últimas falhas de autenticação;

1.6.65 - Lista com as últimas autenticações

1.6.66 - Lista com as últimas autenticações com sucesso

1.6.67 - Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

1.6.68 Deve implementar funcionalidade de classificação automática de dispositivos (“Deviceprofiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

1.6.69 Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartphone, impressora, etc), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

1.6.70 Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

1.6.71 Deve possuir base de regras e categorias de dispositivos pré-configurada;

1.6.72 Deve suportar mecanismo de atualização das regras e categorias pré-configuradas;

1.6.73 Deve implementar os serviços de autenticação, profiling e autorização para

1.500 usuários/dispositivos;

1.6.74 Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados.

1.6.75 Deve suportar a integração nativa com soluções de MDM de mercado, com no mínimo os seguintes fabricantes:

1.6.75.1 Airwatch

1.6.75.2 JAMF

1.6.75.3 MaaS360

1.6.75.4 MobileIron

1.6.75.5 SAP Afaria

1.6.75.6 SOTI

1.6.75.7 XenMobile

1.6.76 Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.

1.6.77 Suporte a RADIUS CoA, Web authentication e SAML v2.0

1.6.78 Deve suportar no mínimo os seguintes métodos de autenticação:

1.6.78.1 EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)

1.6.78.2 PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)

1.6.78.3 TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)

1.6.78.4 EAP-TLS

1.6.78.5 PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5

1.6.78.6 Windows machineauthentication

1.6.78.7 SMB v2/v3

1.6.78.8 WPA3 - MPSK

1.6.78.9 RADSec

1.6.78.10 Online Certificate Status Protocol (OCSP)

1.6.78.11 TACACS+

1.6.78.12 WEB Authentication

1.6.79 Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP)

1.6.80 Suporte a aplicação de políticas em ambiente multivendor de Wireless, cabeado e VPN.

1.6.81 Deve suportar integração com no mínimo Brocade, Palo Alto, Splunk, Juniper, Fortinet e Check Point, ServiceNow, Mcafee, Twilio

1.6.82 Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptacaoda comunicacao.

1.6.83 Deve suportar EDUROAM

1.6.84 Suporte a integração com plataforma de terceiros usando HTTP/RESTful API.

1.6.85 Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários.

1.6.86 Suporte aos seguintes recursos através de IPv6:

1.6.86.1 - Administração via WEB e CLI

1.6.86.2 - Servidores de autenticação e autorização com endereçamento IPv6;

1.6.86.3 - IPv6 Accounting Proxy;

1.6.86.4 - Acesso a servidores com endereçamento IPv6 para contexto de endpoints;

1.6.86.5 - Syslog, DNS, NTP;

1.6.86.6 - Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;

1.6.86.7 - Fontes de Syslog para processamento de eventos

1.6.86.8 Validações e conformidades:

1.6.86.9 - FIPS 140-2

1.6.86.10 - Common CriteriaNDcPP + Servidor de autenticação

1.6.87 A solução deve permitir configuração em alta disponibilidade com no minimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições;

1.6.88 A solução deve permitir a configuração centralizada de politicas em ambientes distribuídos, na qual as politicas serão configuradas em um único elemento para serem distribuidas aos demais que pertençam a mesma "zona"

1.6.89 A solução deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos as seguintes atividades anormais detectadas na rede:

1.6.89.1 - Autenticações

1.6.89.2 - Acesso a dispositivos de rede

1.6.89.3 - Tentativa de execução de comandos em dispositivos de rede por

usuários sem privilégios

1.6.89.4 - Atividades irregulares nos servidores da solução

1.6.90 A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, peritindo o agendamento e envio por e-mail em formato HTML e PDF.

1.6.91 Gerenciamento de Convidados

1.6.92 Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;

1.6.93 Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

1.6.94 Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

1.6.95 Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;

1.6.96 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.6.97 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.6.98 Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

1.6.99 Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através do portal web, sem a necessidade de um autorizador;

1.6.100 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;

1.6.101 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 e números para compor a senha;

1.6.102 Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;

1.6.103 Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e impressão local

1.6.104 Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de sponsorship;

1.6.105 Deve permitir bilhetagem e integração com provedor de pagamento;

1.6.106 Deve prover serviço de propaganda, por exemplo, exibir video antes de liberar o acesso, promoções e propagandas;

1.6.107 Deve permitir o gerenciamento das credenciais de visitantes;

1.6.108 Deve permitir a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;

1.6.109 Deve realizar o caching de endereço MAC dos usuários visitantes;

1.6.110 Deve permitir o login automático de usuários que realizem o auto-registro;

1.6.111 Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;

1.6.112 Deve permitir a criação de token de acesso;

1.6.113 Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;

1.6.114 Deve permitir a desconexão de múltiplas sessões ativas;

1.6.115 Deve possuir página que exibe estatística de sessão após realizar login para que os usuários possam monitorar sua utilização e cota atribuída;

1.6.116 Deve permitir autenticação através de social login nativa na solução;

1.6.117 Deve ser capaz de modificar ou desconectar uma sessão ativa de visitante através de RADIUS Dynamic Authorization.

1.6.118 Serão aceitas soluções/softwares adicionais para compor a solução completa, desde que entregue em conjunto com a solução do próprio fabricante.

1.6.119 Análise de postura

1.6.120 Deve possuir funcionalidade para verificação das políticas de segurança implementadas nos dispositivos conectados a rede, através de agentes instalados ou temporários.

1.6.121 Deve suportar a verificação, nos mínimos nos sistemas operacionais:

1.6.121.1 Windows 7, Windows 8 e Windows 10;

1.6.121.2 Mac OSX 10.10 e superior;

1.6.121.3 Linux (RedHat, Ubuntu, CentOS, Fedora e Suse).

1.6.122 Permitir a execução do agente como serviço quando instalado em sistemas Windows;

1.6.123 Permitir o uso de agentes instalados nos dispositivos, ou agente temporários para o uso em dispositivos de terceiros que necessitem acesso a rede.

1.6.124 Permitir o gerenciamento centralizado das políticas, e permitir que os usuários/dispositivos que estiverem fora das políticas de segurança, sejam

direcionados para um segmento de rede específico ou determinação de uma política de acesso restritiva, permitindo ainda que estes consigam se adequar a respectiva política (remediação).

1.6.125 Permitir que a solução realize a adequação da política (remediação) de forma automática, sem necessidade de intervenção do usuário.

1.6.126 Deve suportar a verificação de pelos menos os seguintes serviços:

1.6.126.1 Firewall

1.6.126.2 Conexões de rede

1.6.126.3 Windows Hotfixes

1.6.126.4 Máquinas Virtuais

1.6.126.5 Aplicações instaladas

1.6.126.6 Serviços

1.6.126.7 Dispositivos USB

1.6.126.8 Processos

1.6.126.9 Checagem de arquivos

1.6.126.10 Criptografia de disco

1.6.126.11 Aplicações peer-to-peer

1.6.127 Deve suportar a verificação de Anti-virus com pelos menos os seguintes parâmetros:

1.6.127.1 Produto instalado

1.6.127.2 Versão instalada

1.6.127.3 Data da última atualização

1.6.127.4 Data da última verificação

1.6.128 A plataforma deve suportar a integração com SCCM ou WSUS.

1.6.129 Deve permitir a verificação de postura de dispositivos Windows 10 sem a necessidade de instalação prévia de agentes, executando todas as operações de verificação em "background", ou seja, transparente ao usuário final;

1.6.130 A solução deve suportar a avaliação de postura e saúde para 1.500 dispositivos.

1.6.131 Serão aceitas soluções/softwares adicionais para compor a solução completa, desde que entregue em conjunto com a solução do próprio fabricante.

1.7 Entrega e instalação

1.7.1 Todos os equipamentos e softwares descritos nos itens 1.2, 1.3, 1.4, 1.5 e 1.6 acima deverão ser entregues no Complexo Sede do Tribunal Regional do Trabalho

da 23ª Região.

1.7.2 O prazo de entrega para os bens referidos no item 1.7.1 é de 120 dias após a emissão da Nota de Empenho ou Ordem de Fornecimento.

1.7.3 Para fins de planejamento, provisionamento de recursos e estimativa de custos, fica determinado que os serviços de instalação consistirão de ativação lógica e configuração dos primeiros 50 (cinquenta) Pontos de Acesso instalados no(s) prédio(s) da Sede do Tribunal contratante (ou até este limite). Fica esclarecido, ainda, que a instalação física, provimento de cabeamento de rede e eventual alimentação elétrica dos Pontos de Acesso serão de inteira responsabilidade do Tribunal contratante e deverão ser realizados até a data prevista para a ativação lógica desses mesmos Pontos de Acesso.

1.7.4 Até a data de entrega dos equipamentos e softwares a empresa deverá entregar também o cronograma de atividades, que contemple o planejamento da instalação e as datas previstas para a realização de cada etapa, contendo pelo menos: Site Survey prévio, instalação e ativação da controladora e solução de gerenciamento, instalação e ativação do grupo piloto de pontos de acesso, validação das configurações e operação, ativação dos demais pontos de acesso, Site Survey posterior, validação da instalação.

1.7.5 O prazo de entrega da implantação em pleno funcionamento é de 60 dias após a entrega dos bens referidos no item 1.7.1.

1.8 Transferência de conhecimento "*handson*"

1.8.1 A transferência de conhecimento na modalidade "*handson*" deverá ocorrer de maneira presencial, no momento da instalação dos componentes de hardware e software da Controladora Wireless e Solução de Gerenciamento, juntamente com a instalação do primeiro conjunto de Pontos de Acesso do Complexo Sede deste Tribunal.

1.8.2 A capacitação aqui descrita deverá contar com uma carga-horária mínima de 16h de atividades práticas.

1.8.3 A capacitação deverá contar com material de apoio orientativo contendo a relação das atividades, seus objetivos e descrição, e ser elaborado pelo instrutor ou organização promovente, e ser entregue aos alunos em formato eletrônico ou impresso.

Anexo III – Site Surveys realizados

Ao longo dos trabalhos que serviram de base para e elaboração deste documento, foram realizados, a pedido da CITM e desta EPC, diversos levantamentos do tipo Site Survey preliminar ou preditivo, como meio de estimar a quantidade de Access Points necessários para prover uma cobertura de sinal satisfatória nos ambientes do Regional. Em razão da extensão dos documentos em número de páginas e quantidade de imagens ilustrativas, entendeu-se ser mais adequado juntar a íntegra desses documentos ao processo administrativo que este estudo instrui.

Anexo IV – Pesquisa de preços públicos

Para estimar os custos totais da solução aqui pretendida foram realizadas pesquisas de preços em contratações públicas com objetos similares. Em razão da extensão dos documentos, entendeu-se ser mais adequado juntar a íntegra desses documentos ao processo administrativo que este estudo instrui, e colar aqui apenas a página que contenha o resumo dos valores de cada contratação pública:

ZOOM TECNOLOGIA

AO

BANCO CENTRAL DO BRASIL - BACEN

PREGÃO ELETRÔNICO Nº 78/2021

PROPOSTA COMERCIAL

Apresentamos nossa proposta, para a contratação de empresa especializada em tecnologia da informação para aquisição e instalação de uma solução de rede sem fio (rede wireless) para todas as localidades do Banco Central do Brasil, conforme quantidades e exigências estabelecidas no Edital e seus anexos, conforme abaixo:

Item	Descrição	Qtd	Valor do Hardware	Valor do Software	Valor da Garantia e Suporte Técnico	Valor da Instalação	Total
01	Controladora Wi-Fi para até 200 pontos de acesso **Marca:** Huawei **Modelo:** AC6805	8	R$ 291.181,61	R$ 225.229,75	R$ 262.992,36	R$ 57.724,30	R$ 837.128,02
02	Controladora Wi-Fi para até 50 pontos de acesso **Marca:** Huawei **Modelo:** AC6805	16	R$ 582.363,23	R$ 450.459,51	R$ 219.160,30	R$ 115.448,97	R$ 1.367.432,01
03	Ponto de acesso Wi-Fi 6 **Marca:** Huawei **Modelo:** AirEngine 5760-51	650	R$ 618.214,45	R$ 203.498,90	R$ 274.074,90	R$ 327.130,47	R$ 1.422.918,72
04	Software de Gerenciamento **Marca:** Huawei **Modelo:** iMaster NCE-Campus	1	R$ 62.882,58	R$ 25.129,75	R$ 11.456,11	R$ 11.071,89	R$ 110.540,33
05	Software de Controle do Acesso à Rede **Marca:** Huawei **Modelo:** iMaster NCE-CampusInsight	1	R$ 77.263,00	R$ 30.159,01	R$ 11.456,11	R$ 13.102,81	R$ 131.980,93

Valor Total Global: R$ 3.870.000,00. Por extenso: três milhões, oitocentos e setenta mil reais.

Validade da Proposta: 60 (sessenta) dias.

Prazo de Garantia: 48 (quarenta e oito) meses.

Declaramos que nos preços contidos estão inclusos todos os custos e despesas diretas e indiretas, encargos sociais, previdenciários, trabalhistas e comerciais, taxa de administração

SERVIX

Ao
Ministério do Meio Ambiente
Instituto Chico Mendes de Conservação da Biodiversidade
Divisão de Licitações

Pregão Eletrônico nº 41/2021
Processo nº 02070.006158/2020-47

Objeto: Contratação de solução de rede sem fio (Wi-Fi) para a Sede, ACADEBio e Regionais do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

PROPOSTA

A empresa Servix Informática Ltda., inscrita no CNPJ sob o nº 01.134.191/0002-28, estabelecida na SIG, Quadra 04, Lote 125, Bloco A, Salas 01 e 02, Cruzeiro, Brasília - DF, por intermédio do seu Representante Legal, o Sr. Cleber Augusto Calejon, portador do RG nº 25.127.646-6-SSP/SP, e inscrito no CPF sob o nº 286.718.678-11, apresenta sua proposta comercial nas condições que seguem.

LOTE	ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO	VALOR TOTAL
01	1	Controladora Física	Und	2	R$ 100.459,00	R$ 200.918,00
	2	Serviços de Instalação de Controladora Física (presencial)	Serviço	2	R$ 10.647,00	R$ 21.294,00
	3	Access Point Indoor	Und	307	R$ 4.030,00	R$ 1.237.210,00
	4	Serviços de Instalação de Access Point Indoor (presencial)	Serviço	58	R$ 533,00	R$ 30.914,00
Valor Total					**R$ 1.490.336,00**	

Valor total da proposta: R$ 1.490.336,00 (Um milhão e quatrocentos e noventa mil e trezentos e trinta e seis reais).

Validade da proposta: 60 (sessenta) dias, contados de sua apresentação.

Nos valores propostos estão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

Declaro que o produto ofertado possui a garantia técnica solicitada no termo de referência.

Filial Brasília
SIG, Quadra 04, Lote 125, Bloco A, Salas 01 e 02, Capital Financial Center, 70610-440, Brasília - DF, Brasil
+55 61 3031 2960
www.servix.com

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

ATA DE REGISTRO DE PREÇOS - TRF1-SEATA

PROCESSO N. 6165902019401/8000 - PREGÃO ELETRÔNICO N. 0020/2021

ATA DE REGISTRO DE PREÇOS N. 0009/2021

A União, por intermédio do **TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO,** com sede Praça dos Tribunais Superiores, Bloco "A" – Brasília/DF, inscrito no CNPJ/MF n. 03.658.507/0001-25, representado pelo Diretor - Geral, **CARLOS FREDERICO MAIA BEZERRA**, CPF n. 480.325.571-72 nos termos das Leis n. 8.666, de 21 de junho de 1993, e n. 10.520, de 17 de julho de 2002, e dos Decretos n. 10.024, de 20 de setembro de 2019, n. 7.892, de 23 de janeiro de 2013, e demais normas legais aplicáveis, obedecidas as disposições contidas no instrumento convocatório e em face da classificação da proposta apresentada no Pregão Eletrônico n. 0020/2021, RESOLVE registrar o preço ofertado pelo Fornecedor Beneficiário, **LETTEL DISTRIBUIDORA DE TELEFONIA LTDA**, estabelecido na Rua Osni Joao Vieira, 205, Bairro Campinas, São Jose/SC, CEP: 88101-270, telefone/fax: (51) 2123-2300/2355, (51) 99326-1977, email: everson@lettel.com.br; felipe@lettel.com.br, inscrito no CNPJ sob o n. 07.789.113/0001-67, representado pelo Sr. Everson Silva Leite, CPF n. 291.823.360-91, conforme abaixo. Demais especificações, conforme Edital.

GRUPO 01				
ITEM	QUANTIDADE	UNIDADE	PREÇO UNITÁRIO R$	PREÇO TOTAL R$
1	1	LICENCA	28.081,00	28.081,00
ESPECIFICAÇÕES: SOLUÇÃO DE GERÊNCIA DE REDE SEM FIO (WLAN). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL-LUCENT. MODELO: OmniVista 2500 NMS + LICENÇAS OV NM EX + SUPORTE 5 ANOS.				
2	320	UN	2.405,00	769.600,00
ESPECIFICAÇÕES: PONTO DE ACESSO SEM FIO, COM GARANTIA DE 60 (SESSENTA MESES). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniAccess OAW-AP1221- RW + OAW- AP1221-SW + OAW-AP-MNT- W + PP5N- OAWAP1221 (GARANTIA 5 ANOS) + LICENÇAS E ACESSÓRIOS.				
3	35	UN	4.959,00	173.565,00
ESPECIFICAÇÕES: SWITCH DE ACESSO PoE DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniSwitch OS6350-P24-US + OS6350-P24 - SW + PP5N OS6350 (GARANTIA 5 ANOS) + 2 SFP-GIG-SX + LICENÇAS E ACESSÓRIOS.				
4	2	UN	53.169,00	106.338,00
ESPECIFICAÇÕES: CONTROLADORA WIRELESS. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS + 1 OmniSwitch OS6860E-24-US + 2 FONTE REDUNDANTE OS6860-BP-US + PP5N-OS6860 (GARANTIA 5 ANOS) + SFP-10G-SR + LICENÇAS OV-AP + SUPORTE 5 ANOS.				
5	2	LICENCA	4.462,03	8.924,06
ESPECIFICAÇÕES: PACOTE DE LICENÇAS PARA USUÁRIOS VISITANTES (500 USUÁRIOS). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS MODULO OV-GA-500-N + PW5N- OVGA500N (SUPORTE 5 ANOS).				
6	1	LICENCA	32.497,00	32.497,00
ESPECIFICAÇÕES: SOLUÇÃO DE CONTROLE DE ACESSO. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS MODULO OV-GA-1K-N + PW5N- OVGA1KN (SUPORTE 5 ANOS).				
7	1	SERVICO	7.877,00	7.877,00
ESPECIFICAÇÕES: SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS ITENS 1, 4, 5 E 6. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
8	320	SERVICO	297,00	95.040,00
ESPECIFICAÇÕES: SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS ITENS 2 E 3. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
9	2	TURMA	6.024,00	12.048,00
ESPECIFICAÇÕES: TREINAMENTO TELEPRESENCIAL (COM ATÉ 5 ALUNOS POR TURMA). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
10	6	SERVICO	6.024,00	36.144,00
ESPECIFICAÇÕES: SITE SURVEY. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
TOTAL REGISTRADO PARA O GRUPO 01				**1.270.114,06**

Este Registro de Preços terá validade de 12 (doze) meses, contados da data da sua assinatura pelas partes, instante a partir do qual o instrumento será considerado apto a produzir seus jurídicos efeitos. O extrato desta Ata será publicado em órgão oficial da Administração.

As especificações técnicas e demais exigências constantes do Decreto n. 7.892/2013, no Processo Administrativo n. 6165902019401/8000 e Pregão Eletrônico n. 0020/2021 integram esta Ata de Registro de Preços, independentemente de transcrição.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais do Tribunal Regional Federal da Primeira Região e do Fornecedor Beneficiário.

CARLOS FREDERICO MAIA BEZERRA
Diretor - Geral

EVERSON SILVA LEITE
Lettel Distribuidora de Telefonia Ltda

Documento assinado eletronicamente por **Everson Silva Leite**, **Usuário Externo**, em 23/07/2021, às 15:42 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Frederico Maia Bezerra**, **Diretor-Geral da Secretaria**, em 26/07/2021, às 09:27 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf1.jus.br/autenticidade informando o código verificador **13523289** e o código CRC **B72E04A7**.

Anexo V – Propostas comerciais recebidas

Ao longo dos trabalhos que serviram de base para e elaboração deste documento, foram solicitados, pela CITM e desta EPC, como consequência dos levantamentos do tipo Site Survey, orçamentos estimados de custos totais da implantação de uma infraestrutura completa de rede sem fios neste Regional. Em razão da extensão dos documentos, entendeu-se ser mais adequado juntar a íntegra desses documentos ao processo administrativo que este estudo instrui, e colar aqui apenas a página que contenha o resumo dos valores de cada proposta:

Proposta da empresa TELTEC para rede Wi-Fi 5, em 26/07/2019:

teltec SOLUTIONS

1. **Solução**

Validade da ATA	Item ATA	QTD registrada	Descrição	Valor unit.	ADESÃO ATA UTFPR – TRT23 QTD	ADESÃO ATA UTFPR – TRT23 Valor Total
09/04/2020	5	2	Controladora Wireless Virtual Cisco licenciada para 5 APs com suporte para até 200 Aps. Garantia de 5 anos.	R$ 3.600,00	1	R$ 3.600,00
	6	390	Licença para expansão de controladora wireless virtual para 1 AP. Garantia de 60 meses.	R$ 720,00	107	R$ 77.040,00
	7	224	Access Point Cisco 1852I 802.11ac Wave2 Dual Band MIMO 4x4 com 3 spatial streams - Mobility Express para até 50 Aps. Garantia de 5 anos.	R$ 5.200,00	112	R$ 582.400,00
	8	120	Injetor PoE Cisco	R$ 420,00	60	R$ 25.200,00
	9	2	Serviço de configuração da solução wireless	R$ 20.000,00	1	R$ 20.000,00
					Total	R$ 708.240,00

2. **Condições gerais da proposta**
   a. Forma de pagamento
      i. Pagamento dos produtos (equipamentos e licenças) em até 15 dias após o recebimento
      ii. Pagamento dos serviços em até 15 dias após a execução
   b. Validade da proposta
      i. Proposta válida por 30 dias
   c. Prazo de entrega dos produtos
      i. Produtos serão entregues em até 75 dias corridos após o recebimento da ordem de compra
   d. Prazo de entrega dos serviços
      i. Os serviços terão seu início em até 30 dias corridos após o recebimento total dos produtos (equipamentos e licenças)

3. **Dados cadastrais da Teltec Solutions**

Razão social: Teltec Solutions Ltda
Nome fantasia: Teltec Solutions
Endereço: R. Miguel Daux, 100 - Coqueiros - Florianópolis/SC - CEP 88080-220
Telefone: 48 3031-3450 | Email: teltec@teltecsolutions.com.br
CNPJ: 04.892.991/0001-15 | I.E: 254.353.290
Dados Bancários – Banco do Brasil | Agência: 3077-5 |Conta: 7555-8

Proposta da empresa TELTEC para uma rede Wi-Fi 6, em 11/06/2021:

teltec SOLUTIONS

1) INVESTIMENTO

ITEM	PN/DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	ACCESS POINT Cisco Catalyst 9105 • WiFi 6 • MIMO 2x2 • Licença software de gerenciamento • Licença para a controladora • Garantia de 36 meses	75	R$ 5.400,00	R$ 405.000,00
2	ACCESS POINT Cisco Catalyst C9115 • WiFi 6 • MIMO 4x4 • Licença software de gerenciamento • Licença para a controladora • Garantia de 36 meses	45	R$ 9.940,00	R$ 447.300,00
	ACCESS POINT Cisco Catalyst C9120 • WiFi 6 • MIMO 4x4 • Licença software de gerenciamento • Licença para a controladora • Garantia de 36 meses	30	R$ 13.200,00	R$ 396.000,00
3	Injetor PoE 802.3at	150	R$ 790,00	R$ 118.500,00
4	CONTROLADORA VIRTUAL Cisco Catalyst 9800-CL com Suporte e Garantia de 36 Meses	2	R$ 5.750,00	R$ 11.500,00
5	SOFTWARE DE GERENCIAMENTO – Cisco Prime Infrastructure com Suporte e Garantia de 36 Meses	1	R$ 1.500,00	R$ 1.500,00
VALOR TOTAL DA PROPOSTA				R$ 1.379.800,00

2) CONDIÇÕES GERAIS DESTA PROPOSTA:

- **Condições gerais:** Os valores apresentados são válidos somente para o quantitativo e cliente final descrito nesta proposta. Qualquer ajuste no quantitativo e/ou cliente final pode requerer uma atualização na proposta e seus valores;
- Os valores apresentados acima contêm todos os impostos, taxas, frete e demais despesas que venham a incidir sobre o valor da proposta;
- Todos os itens apresentados estão em REAIS BRASILEIRO (R$), exceto se especificado individualmente;

- **Prazo de entrega dos produtos e serviços:** Os produtos cotados possuem prazo de entrega padrão de 120 dias, contados a partir da assinatura/recebimento de ordem de fornecimento ou instrumento equivalente, podendo vir a ser reduzido conforme disponibilidade nos estoques. Consulte o representante de vendas para maior detalhamento;

- **Validade da proposta:** Esta proposta é válida por 30 dias. Em caso de a taxa câmbio do dólar americano ultrapassar R$ 5,30, esta proposta perde automaticamente sua validade;

- **Pagamento:** em até 30 dias após a emissão da Nota Fiscal;

- **Confidencialidade:** Garantimos a confidencialidade das informações, dados, senhas e documentos que venha a ter acesso em razão da execução dos produtos/serviços adquiridos.

- **Faturamento em notas fiscais distintas:** Em consonância com a legislação tributária vigente, a Teltec Solutions adota o mesmo formato de faturamento praticado por seus fornecedores, sejam eles fabricantes, desenvolvedores, licenciantes ou importadores, fornecendo os itens de hardware como

TELTEC 30 ANOS. TRANSFORMAR É O NOSSO DESAFIO!

Proposta da empresa ZOOM para uma rede Wi-Fi 6, em 13/07/2021:

TRT 23ª

ZOOM tecnologia

SOLUÇÃO A SER IMPLEMENTADA

Item	Modelo	Descrição	Quantidade	Valor Unitario	Valor Total
1	ZoomCloud-MGT	Licença para Sistema de Gerenciamento NCE-IMaster Campus em Nuvem para Ponto de Acesso AirEngine 5760-51, por 5 anos.	144	R$ 320,57	R$ 46.162,08
2	ZoomCloud-MGT	Licença para Sistema de Gerenciamento NCE-IMaster Campus em Nuvem para Controladora AC6508, por 5 anos.	2	R$ 5.187,20	R$ 10.374,40
3	ZoomCloud-NAC	Licença para Sistema de Autenticação NCE-IMaster Campus em Nuvem para para 1.000 usuarios simultaneos, por 5 anos.	1000	R$ 4,46	R$ 4.456,33
4	ZoomCloud-Analytics	Licença para Sistema analitico NCE-IMaster Insight para configuração automatica de rede através de IA, com localicação geografica de terminais e dispositivos RFID com identificação de aplicação de camada 3 a 7 sendo executadas na rede, por 5 anos.	1	R$ 248.339,52	R$ 248.339,52
5	AC6508	Controladora AC6508 para até 256 pontos de acesso, com capacidade de atuar em alta disponibilidade, com 5 anos de garantia.	2	R$ 9.490,97	R$ 18.981,94
6	AirEngine 6760-51	Ponto de Acesso indoor WiFi 6 (802.11ax) mid-end, capacidade de comutação de 5.37 Gbps, MiMo 4x4, suporte de 1024 usuarios simultaneos e garantia de 5 anos.	144	R$ 2.605,24	R$ 375.154,56
7	W0ACP8E11	Injeto PoE++ para ponto de acesso AirEgine, com 5 anos de garantia	144	R$ 942,07	R$ 135.658,08
				Valor Total Geral	R$ 839.126,91

Condições Comerciais

- Os valores que porventura forem apresentados em US$ (dólares americanos) deve ser convertidos em R$ (reais), e será utilizada a cotação do dólar (PTAX = 5,3)

- Os valores devem ser expressos em reais, fixos por 12 meses, considerando todos os impostos e frete:

- Os valores poderão ser pauta de renegociação no caso da Ptax informada na proposta varie + ou - 10%.

- Os equipamentos serão faturados e entregues nas lojas.

- A ZOOM Tecnologia poderá rever a validade desta Proposta sempre que ocorrer um fato ou ato superveniente que resulte na imposição de um ônus excessivo refletido nos valores e preços apresentados.

- A ZOOM Tecnologia poderá rever a validade desta proposta sempre que ocorrer um fato ou ato superveniente que resulte na imposição de um ônus excessivo refletido nos valores e preços apresentados.

Proposta da empresa TELTEC, em 31/08/2021:

teltec SOLUTIONS

1) INVESTIMENTO

		Q	A	B	C=A+B	Q*C
ITEM	PN/DESCRIÇÃO	QTD	VALOR UNITÁRIO NF PRODUTO	VALOR UNITÁRIO NF SOFTWARE/SERVIÇO	VALOR UNITÁRIO CONJUGADO	VALOR TOTAL CONJUGADO
WLAN SECURITY						
1	CONTROLADORIA/FIREWALL PEQUENO PORTE PARA UNIDADES REMOTAS COM SUPORTE E GARANTIA DE 60 MESES. Modelo: FOTINET FG-40F	24	R$ 933,26	R$ 2.828,43	R$ 3.761,69	R$ 90.280,58
2	CONTROLADORIA/FIREWALL PARA UNIDADE CENTRAL COM SUPORTE E GARANTIA DE 60 MESES. Modelo: FOTINET FG-200F	1	R$ 7.870,39	R$ 22.269,55	R$ 30.139,94	R$ 30.139,94
3	ACCESS POINT INDOOR – FORTINET FAP-231F-N • WiFi 6 • Tri radio, 802.11 a/b/g/n/ac/ax 2x2 MU-MIMO • 2x 10/100/1000 RJ45 port, BT/BLE • 1x Type A USB • 1x RS-232 RJ45 Serial Port • Kit de montagem incluso Garantia de 60 meses	150	R$ 5.361,17	R$ 1.571,69	R$ 6.932,86	R$ 1.039.928,65
4	ACCESS POINT INDOOR – FORTINET FAP-431F-N • WiFi 6 • Tri radio (2x 802.11 a/b/g/n/ac/ax, 4x4 MIMO e 1x 802.11 a/b/g/n/ac Wave 2, 2x2 MU-MIMO) • 1x 10/100/1000/2500 Base-T RJ45 • 1x 10/100/1000 Base-T RJ45 • 1x Type A USB • 1x RS-232 RJ45 Serial Port. • Kit de montagem incluso Garantia de 60 meses	20	R$ 7.791,47	R$ 2.284,05	R$ 10.075,52	R$ 201.510,39
5	Injetor PoE Gigabit 802.3at	50	R$ 1.121,23		R$ 1.121,23	R$ 56.061,55
VALOR TOTAL WLAN SECURITY						R$ 1.417.921,12

Proposta da empresa YSSY, em 01/09/2021:

YSSY

CLIENTE: TRT 23ª Região
PROPOSTA: AY-2021-03-17454
DATA: 1-set-21
CONTATO: Rogério M. Pimenta
E-MAIL: rogeriopimenta@trt23.jus.br
FONE: -

Rede WiFi

Item	Part Number	Descrição	Qtde.	Tipo	IPI %	ICMS %	ISS %	Valor unitário	Valor Total
1	ITEM 1 - Solução de Controle e Gerência da Rede Wifi								
1.1	OV-AP-NM-100-N	OV-AP-NM-100-N OV2500 NM R4 Lic - Lic. 100 AP-NEW for 10 ALU-E Stellar	2	SFW			2%	42.181,40	84.362,80
1.2	OV-GA-1K-N	OV-GA-1k-N - OV2500 GA R4 Lic. - Lic. 1000 GA-NEW for Guest Access	1	SFW			2%	62.102,86	62.102,86
1.3	OV-BYOD-1K-N	OV2500 BYOD R4 Lic. - Lic 1000 BOYD-NEW for BYOD Access Policy Manager	1	SFW			2%	62.102,86	62.102,86
1.4	PW3N-OVAPNM100	5YR 24X7 Partner SUPPORT for OV2500 NMS - RELEASE 4 OV-AP-NM-100-N.	2	SFW			2%	33.949,20	67.898,40
1.5	PW3N-OVBYOD1KN	5YR 24X7 Partner SUPPORT Software for OV2500 NMS - R4 OV-BYOD-1K-N	1	SFW			2%	43.812,83	43.812,83
1.6	PW3N-OVGA500N	5YR 24X7 Partner SUPPORT Software OV2500 NMS - RELEASE 4 OV-GA-500-N	1	SFW			2%	36.644,02	36.644,02
2	ITEM 2 - Pontos de Acesso da Rede Sem Fio								
2.1	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	HW		17%		6.281,06	1.256.212,00
2.2	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	SFW			2%	3.138,92	627.784,00
2.3	OAW-AP-MNT-W10	10 Pack. Mounting kit, Type A ceiling/wall mount	20	HW		17%		1.634,23	32.684,60
2.4	PW3R-OAWAP1301	5 Yr Renew Partner Support Software for OAWAP1301	200	SFW			2%	347,72	69.544,00
								SUB-TOTAL HW:	1.288.896,60
								SUB-TOTAL SOFTWARES E LICENÇAS:	1.054.251,79
								SUB-TOTAL SERVIÇOS:	-
								TOTAL Rede WiFi:	2.343.148,39

R$ 2.343.148,39 dois milhões, trezentos e quarenta e três mil, cento e quarenta e oito reais e trinta e nove centavos

CONDIÇÕES COMERCIAIS

PRAZO DE ENTREGA:	Em até 60 dias, contados a partir da data de confirmação do pedido com aceite formal. (O prazo está sujeito a alteração sem prévio aviso, conforme disponibilidade de estoque.)
VALIDADE DA PROPOSTA:	60 dias.
PAGAMENTO:	30 dias após aceite definitivo.
IMPOSTOS:	Inclusos de acordo com a legislação vigente. (Serão repassados aos valores ainda não faturados quaisquer variações que venham ocorrer nas alíquotas existentes.)
FRETE E SEGURO:	Inclusos.
GARANTIA:	60 meses

Atenciosamente,

Abilio Cardoso Chaves Filho
Gerente de Contas
(61) 99921-4427
abilio.chaves@yssy.com.br

yssy

CLIENTE: TRT 23ª Região
PROPOSTA: AY-2021-03-17454
DATA: 9-mai-22
CONTATO: Rogério M. Pimenta
E-MAIL: rogeriopimenta@trt23.jus.br
FONE: -

Rede WiFi

Item	Part Number	Descrição	Qtde.	Tipo	IPI %	ICMS %	ISS %	Valor unitário	Valor Total
1	ITEM 1 - Controladora Wireless + Solução de Gerenciamento e Controle de Acesso a Rede Wifi								
1.1	OV-AP-NM-100-N	OV-AP-NM-100-N OV2500 NM R4 Lic - Lic. 100 AP-NEW for 10 ALU-E Stellar	2	SFW			2%	32,311.04	64,622.08
1.2	OV-GA-1K-N	OV-GA-1k-N - OV2500 GA R4 Lic. - Lic. 1000 GA-NEW for Guest Access	1	SFW			2%	51,031.84	51,031.84
1.3	OV-BYOD-1K-N	OV2500 BYOD R4 Lic. - Lic 1000 BOYD-NEW for BYOD Access Policy Manager	4	SFW			2%	52,733.75	210,935.00
1.4	PW5N-OVAPNM100	5YR 24X7 Partner SUPPORT for OV2500 NMS - RELEASE 4 OV-AP-NM-100-N.	2	SFW			2%	24,574.97	49,149.94
1.5	PW5N-OVBYOD1KN	5YR 24X7 Partner SUPPORT Software for OV2500 NMS - R4 OV-BYOD-1K-N	4	SFW			2%	33,844.15	135,376.60
1.6	PW5N-OVGA500N	5YR 24X7 Partner SUPPORT Software OV2500 NMS - RELEASE 4 OV-GA-500-N	1	SFW			2%	27,107.38	27,107.38
2	ITEM 2 - Pontos de Acesso da Rede Sem Fio								
2.1	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	HW		17%		6,846.92	1,369,384.00
2.2	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	SFW			2%	3,105.01	621,002.00
2.3	OAW-AP-MNT-W10	10 Pack. Mounting kit, Type A ceilling/wall mount	20	HW		17%		1,612.52	32,250.40
2.4	PW5R-OAWAP1301	5 Yr Renew Partner Support Software for OAWAP1301	200	SFW			2%	326.76	65,352.00
2.5	Power Injector	Power Injector (802.3at) for Access Points	1	HW				660.08	660.08
								SUB-TOTAL HW:	1,402,294.48
								SUB-TOTAL SOFTWARES E LICENÇAS:	1,224,576.84
								SUB-TOTAL SERVIÇOS:	-
								TOTAL Rede WiFi:	2,626,871.32

R$ 2,626,871.32 dois milhões, seiscentos e vinte e seis mil, citocentos e setenta e um reais e trinta e dois centavos

CONDIÇÕES COMERCIAIS

PRAZO DE ENTREGA:	Em até 90 dias, contados a partir da data de confirmação do pedido com aceite formal. (O prazo está sujeito a alteração sem prévio aviso, conforme disponibilidade de estoque.)
VALIDADE DA PROPOSTA:	60 dias.
PAGAMENTO:	conforme edital
IMPOSTOS:	Inclusos de acordo com a legislação vigente. (Serão repassados aos valores ainda não faturados quaisquer variações que venham ocorrer nas aliquotas existentes.)
FRETE E SEGURO:	Inclusos.
GARANTIA:	60 meses

Atenciosamente,

Abilio Cardoso Chaves Filho
Gerente de Contas
(61) 99921-4427
abilio.chaves@yssy.com.br

Anexo II – Requisitos técnicos da Solução

Item	Descrição
1	Pontos de Acesso Sem Fios (Wireless Access Points) Modelo 1
2	Pontos de Acesso Sem Fios (Wireless Access Points) Modelo 2
3	Injetores de Energia PoE (PoEinjectors)
4	Controladora de Rede Sem Fios (Wireless Controller)
5	Solução de Controle de Acesso a Redes (Network Access Control)
6	Pacote de licenças adicionais para usuários/dispositivos internos (500 usuários por pacote)
7	Pacote de licença para usuários visitantes (500 usuários por pacote)
8	Serviços de instalação e configuração
9	Transferência de conhecimento “handson” presencial para até 5 pessoas, por turma

1.1 Características comuns a todos os itens de fornecimento

1.1.1 Todos os equipamentos devem ser novos e de primeiro uso, de modelo em linha de produção e sem anúncio ou previsão de encerramento da produção na data da entrega das propostas.

1.1.2 Não serão aceitos equipamentos remanufaturados (*refurbished*).

1.1.3 Todos os equipamentos deverão ser acompanhados de todos os componentes e acessórios necessários à sua instalação e funcionamento, o que inclui, eventualmente, cabos e/ou fontes de alimentação, suportes e parafusos.

1.1.4 Todos os equipamentos deverão ser entregues em caixas originais do fabricante, lacradas e íntegras, sem sinais de rasgos, amassados ou outras imperfeições que possam denotar comprometimento do conteúdo.

1.1.5 Todos os equipamentos a ser fornecidos ter certificado homologação válida pela ANATEL na data da entrega das propostas etais certificados devem estar disponíveis para consulta eletrônica on-line e o caminho para acesso a eles deve ser fornecido pelo proponente.

1.1.6 Todas as unidades de equipamentos do mesmo item devem ser do mesmo modelo, contando com a mesma revisão de hardware e software e sendo identificados pelo mesmo código junto ao fabricante (PartNumber) e ser fornecidos com a versão mais recente do software interno (firmware) disponível na data da

entrega.

1.1.7 No caso de itens que venham ser fornecidos como dispositivos físicos do tipo *hardware appliances*, deverão suportar operar em faixas de temperatura de 0°C a 45°C, ser acompanhados de fonte de alimentação com seleção automática de tensão (100-240 VAC), LEDs para a indicação do status das portas e atividade, e todos os acessórios e componentes necessários à sua instalação em rack de 19", além de 1 porta de console física para gerenciamento via linha de comando (CLI – CommandLine Interface) com conector RS232, RJ-45 ou USB com seu respectivo cabo.

1.1.8 No caso de itens que venham ser fornecidos como dispositivos físicos do tipo *hardware appliances*, devem 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.Devem, ainda ser entregues em configurações de CPU e memória suficiente e adequada para a execução simultânea de todas as funcionalidades exigidas para o equipamento em questão.

1.1.9 No caso de itens que venham ser fornecidos como dispositivos virtualizados do tipo *virtual appliances*, estes deverão ser este compatíveis e homologados para operação com servidores de virtualização VMwareESXi 6 ou superior, KVM ou Microsoft Hyper-V, haja vista que a infraestrutura de virtualização utilizada será a do órgão contratante. Caso seja necessária alguma licença adicional, esta deverá ser fornecida juntamente com a solução, com a mesma garantia, suporte e o mesmo prazo de vigência da solução que suporta.

1.1.10 Todos as unidades de todos os itens, equipamentos e softwares aplicativos, deverão ser fabricados pelo mesmo fornecedor, salvo quando explicitamente admitida exceção, e deverão vir acompanhados de toda a documentação necessária ao seu funcionamento e operação. Esta documentação pode ser impressa ou eletrônica/digital, neste último caso devendo ser fornecida gravada em mídia eletrônica a ser entregue juntamente com os itens a que se refere ou, ainda, no caso de estar disponível on-line, ter seu caminho de acesso (atalho/link) fornecido em documento que acompanhe o item a que se refere.

1.1.11 Deverão ser fornecidas quaisquer outras licenças necessárias ao perfeito funcionamento da solução em atendimento aos requisitos destedocumento, e deverá ser acompanhado de todos os itens necessários para operacionalização, tais como sistemasoperacionais, softwares de apoio e licenças de software.

1.1.12 Todos os itens devem ser fornecidos de forma que possam ser instalados e executados nas dependências do contratante (*onpremises*), mesmo na eventual ausência de conexão com a internet. Não serão aceitos itens cujas soluções sejam baseadas em nuvem do fabricante (*Software as a Service - SaaS* ou *Network as a Service –NaaS*) ou que tenham modelo de fornecimento como serviço por assinatura (*subscription*), exceto para o caso de licenciamento de funcionalidades.

1.1.13 Todos os itens deverão contar com garantia de funcionamento e suporte

técnico pelo período mínimo de 60 meses.

1.1.14 Todos os itens de software deverão ser entregues com licenças de uso perpétuo.

1.1.15 A comprovação de atendimento aos requisitos técnicos aqui presentes deverá ser explícita e apresentada na forma de tabela onde constem as informações a seguir: número do item de requisito técnico, confirmação de atendimento (Sim ou Não),descrição do requisito técnico, referência (com endereço eletrônico/link de acesso) de comprovação de atendimento pelo fabricante e observações (campo livre para informações adicionais). Será fornecida planilha com modelo padrão a ser adotado.

1.1.16 Todos os itens a serem fornecidos deverão ser de fabricante queconste em um dos quatro Quadrantes Mágicos da pesquisa “Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure” (“Quadrante Mágico para Infraestrutura de LAN com fio e sem fio corporativa” em tradução livre) da edição de 21/12/2022, a saber: Alcatel-Lucent Enterprise, Arista Networks, Cambium Networks, Cisco, CommScope (RUCKUS), Extreme Networks, Fortinet, HPE (Aruba),Huawei, Juniper e TP-Link.

1.2 Pontos de Acesso (*Access Points*) – características comuns a todos os modelos

1.2.1 O equipamento deve ser do tipo Ponto de Acesso (*Access Point* ou AP) e vir acompanhado de estrutura que permita fixação em superfícies sólidas na horizontal (teto/forro) e suportar sua eventual instalação na vertical (paredes ou similares) de ambientes internosmediante uso de estruturas de fixação próprias para este fim.

1.2.2 Deverá suportar operar na faixa de temperaturas de 5 a 40°C e umidade de até 95% (não condensada).

1.2.3 Possuir luz/luzes (LED) capazes de indicar os status de ligado, conectado à LAN e de atividade de rede WLAN.

1.2.4 Vir acompanhado de fonte de alimentação DC externa, para alimentação elétrica, com entrada AC bivolt automática (100-240V). Caso não haja possibilidade de fornecimento do item com fonte de alimentação externa, será aceito em substituição e sem custo adicional, que seja acompanhado de adaptador de energia PoE nos padrões descritos no item 1.4 deste documento.

1.2.5 Suportar alimentação pelo padrão Power over Ethernet (PoE) IEEE 802.3af ou 802.3at por meio de pelo menos uma das interfaces de rede, de forma que essa alimentação seja suficiente para o pleno funcionamento de todas as características do equipamento sem nenhuma perda de desempenho ou funcionalidades.

1.2.6 Possuir pelo menos 2 rádios independentes que possam operar simultaneamente nas frequências de 2.4 e 5 GHz e compatibilidade de transmissão e recepção segundo os padrões IEEE 802.11 a/b/g/n/ac/ax (em suas respectivas frequências de operação).

1.2.7 Todas as antenas devem ser integradas e internas ao equipamento.

1.2.8 Possuir configuração com memória e CPU dimensionados de forma a permitir a utilização simultânea e constante de todas as características descritas neste item.

1.2.9 Possuir suporte para instalação de dispositivo antifurto.

1.2.10 Implementar a tecnologia Wi-Fi 6 (802.11ax) e permitir conectar simultaneamentedispositivosque se comuniquem em qualquer dos padrõestecnológicos anteriores (compatibilidade retroativa): IEEE 802.11: b, g, a, n, ac.

1.2.11 O modelo ofertado deve possuir Certificado de Conformidade Técnica de produto do tipo Transceptor de Radiação Restrita homologado pela ANATEL, com vigência válida pelo menos até a data do certame.

1.2.12 O modelo ofertado deve estar, na data da apresentação das propostas, certificado pela Wi-Fi Alliance na categoria Routers, subcategoria "Enterprise/Service ProviderAcess Point, Switch/ControllerorRouter" e, no sumário de certificações, apresentar as certificações:

1.2.12.1 2.4 GHz Spectrum Capabilities
1.2.12.2 5 GHz Spectrum Capabilities
1.2.12.3 Wi-Fi Certified a, b, g, n, ac, 6
1.2.12.4 WMM
1.2.12.5 WPA 3 Enterprise, Personal
1.2.12.6 WPA 2 Enterprise, Personal
1.2.12.7 Protected Management Frames

1.2.13 Possuir antenas com padrão de radiação omnidirecional,alcançar potência máxima de transmissão de, pelo menos, 21dBm em cada frequência (2,4 GHz e 5 GHz) (podendo ser combinada com o ganho da antena), e sensibilidade mínima de recepção de -92 dBm.

1.2.14 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80MHz para os padrões IEEE 802.11ac/ax.

1.2.15 Possuir pelo menos 2 interfaces Gigabit Ethernet ou 1 interface Mutigigabit Ethernet, ou uma combinação destas, todas com conectores RJ-45.

1.2.16 Ser capaz de suportar pelo menos 512 conexões simultâneas de dispositivos clientes associados por Ponto de Acesso e não deve possuir restrição por software ou licença para a quantidade de usuários internos conectados simultaneamente.

1.2.17 Implementar, suportar ou ser compatível com as seguintes especificações da família de protocolos IEEE 802.11: a, b, g, n, ac, ax, d, h, i, k, v, r, w, u.

1.2.18 Suportar operar em modo gerenciado por Controladora WLAN ou independente dela (autogerenciado), e poder ter todas suas características de funcionamento configuradas remotamente pela Controladora WLAN ou diretamente no próprio equipamento por meio de interface de navegador Web padrão HTTP/HTTPS.

1.2.19 Deve ser capaz de se conectar à Controladora que o gerencia, diretamente ou remotamente via roteamento de camada 3, com tráfego de gerenciamento protegido por túnel criptografado (IEEE 802.11w, Protected Management Frames).

1.2.20 Implementar seleção automática de canal e ajuste automático de potência do sinal, visando o melhor desempenho.

1.2.21 Ser capaz de prover 16SSIDs simultâneos por Ponto de Acesso.

1.2.22 Permitir escolher entre habilitar e desabilitar a divulgação de qualquer SSID.

1.2.23 Deve permitir implementar pelo menos 8 VLANs e suportar o protocolo IEEE 802.1Q.

1.2.24 Permitir a associação dinâmica de usuário a VLAN de acordo com parâmetros da etapa de autenticação.

1.2.25 Implementar Short GuardInterval.

1.2.26 Implementar MaximumRatioCombining (MRC) ou MU-MIMO para melhorar o desempenho de recepção.

1.2.27 Deve implementar mecanismo para detecção e prevenção ou minimização do impacto da interferência de sinais de radiofrequêncianão Wi-Fi na área de alcance do Ponto de Acesso.

1.2.28 Deve permitir a formação de conjuntos de Pontos de Acesso que se comuniquem e compartilhem as mesmas configurações mesmo sem a necessidade de uma controladora wireless (redes mesh).

1.2.29 Possuir capacidade de realizar análise de espectro de RF em 2.4 e 5 GHz para a detecção de outros pontos de acesso no perímetro de alcance, intrusos ou não autorizados (rogue), além de detectar interferências nos canais habilitados no ponto de acesso.

1.2.30 Permitir a conexão de usuários utilizando os protocolos IPv4 e IPv6 simultaneamente no equipamento (dual-stack).

1.2.31 Deve suportar atribuição de endereço IP de forma estática ou por meio de servidor DHCP.

1.2.32 Deve possibilitar a entrega automática de parâmetros de configuração a Pontos de Acessoque atendam critérios previamente definidos, de modo que toda configuração seja baixada do Controlador WLAN durante os processos de inicialização dos Pontos de Acesso.

1.2.33 Implementar os protocolos NTP ou SNTP em modo cliente para sincronização do relógio interno com fonte externa de tempo.

1.2.34 Permitir a configuração de VLans, criptografia e QoS independentes por SSID.

1.2.35 Implementar WIDS e WIPS, com recursos de assintaturas de ataques, detecção de dispositivos intrusos e aplicação de contramedidas de proteção.

1.2.36 Permitir autenticação pelo protocolo 802.1x com EAP-TLS.

1.2.37 Implementar solução de autenticação e gerenciamento de usuários da rede sem fios interna e independente da Controladora WLAN.

1.2.38 Possibilitar os métodos de autenticação de clientes: aberta (sem criptografia), através de MAC Address, WPA/WPA2/WPA3 em modos Personal e Entreprise com suporte a PSK, TKIP, AES, 802.1x por via de servidor Radius, 802.1x em base de dados local, 802.1x em base LDAP externa,Captive Portal.

1.2.39 Permitir a comutação de tráfego local (entre dispositivos da mesma sub-rede) sem necessidade de intervenção de Controladora WLAN, exceto para a fase de autenticação de usuários e estabelecimento da conexão inicial.

1.2.40 Ser gerenciável via protocolo SNMP v1/2c/3 e implementar MIB-II (RFC 1213).

1.2.41 Contar com garantia de 60 (sessenta) meses com remessa de peças/equipamentos de reposição em até 5 dias úteis após registro do chamado.

1.3 Ponto de Acesso (Access Point) Modelo 1

1.3.1 Suportar throughput combinado de, no mínimo, 1,45 Gbps.

1.3.2 Operar, pelo menos, em MIMO 2x2 com 2 fluxos espaciais SU-MIMO e MU-MIMO (2x2:2) em 2,4GHz e 5GHz.

1.3.3 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80MHz para os padrões IEEE 802.11ac/ax.

1.4 Ponto de Acesso (Access Point) Modelo 2

1.4.1 Suportar throughput combinado de, no mínimo, 3,5 Gbps.

1.4.2 Operar, pelo menos, em MIMO 2x2 com 2 fluxos espaciais SU-MIMO e MU-MIMO (2x2:2) em 2,4GHz e em 2,4GHz e MIMO 4x4 com 4 fluxos espaciais SU-MIMO e MU-MIMO (4x4:4) em 5GHz.

1.4.3 Operar em canais de 20MHz para os padrões IEEE 802.11a/b/g, 20/40MHz para o padrão IEEE 802.11n e 20/40/80/160MHz para os padrões IEEE 802.11ac/ax.

1.5 Injetor de energia PoE

1.5.1 Deve prover, por meio do cabo de rede UTP cat-5e ou cat-6, o fornecimento de energia capaz de alimentar os Access Points aqui descritos.

1.5.2 Deve possuir 2 portas RJ-45 fêmea, uma (entrada) para ser conectada à porta de dados do switch não PoE, outra (saída) para fornecer energia e dados para o Access Point. Ambas as portas devem operar sob o padrão Gigabit Ethernet.

1.5.3 Deve sem compatível com os padrões IEEE 802.3af e 802.3at e fornecer potência elétrica suficiente para que o dispositivo alimentado funcione com todas suas características ativas.

1.5.4 Deve acompanhar cabos e acessórios para o seu perfeito funcionamento.

1.5.5 Deve ser fornecido com fonte de alimentação com capacidade para operar em tensões de 110V ou 220V com comutação automática e frequência de 60Hz. Deve ser incluído cabo para conexão à rede elétrica no padrão brasileiro.

1.5.6 Garantia de 60 (sessenta) meses com envio de peças/equipamentos de reposição em até 3 dias úteis.

1.5.7 Este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos equipamentos dos itens 1.1 e 1.2 deste grupo (lote), ou ser homologado pelo fabricante deles.

1.6 Controladora Wireless (*WLAN Controller*)

1.6.1 A Controladora Wireless (ou *WLANController*) poderá ser ofertada em dispositivo físico (*hardware appliance*) ou virtualizado (*virtual appliance*), ou, ainda, em software aplicativo, deverá ser totalmente compatível com todas as funcionalidades e tecnologias e capaz de centralizar o controle, manutenção e distribuição das configurações dos Pontos de Acesso (Access Points) que compõem a solução.

1.6.2 Independentemente da arquitetura da Controladora Wireless (se dispositivo físico, virtualizado ou software aplicativo), esta deve poder ser instalada em Centros de Dados do Contratante juntamente com outra unidade idêntica, no mesmo local ou em local diverso, para compor um cluster e operar em modo de redundância e alta disponibilidade na forma ativo/ativo ou ativo/stand-by (Hot Stand-by) ou na proporção N+1 (onde sempre haja, além da quantidade mínima de nós necessária para suportar a demanda, mais uma unidade para prover redundância), possibilitando total redundância de configurações e replicação de sessões de usuários entre os equipamentos, de forma que se um dos nós sofra indisponibilidade, o outro assuma automática e integralmente a provisão de serviços, assegurando que não haja interrupção de funcionamento e da capacidade de gerenciamento dos dispositivos controlados.

1.6.3 Deve suportar e ser capaz de gerenciar todas as características e protocolos para os quais os Access Points adquiridos conjuntamente foram certificados, em especial:

1.6.3.1 Wi-Fi Certified a, b, g, n, ac, 6
1.6.3.2 WMM
1.6.3.3 WPA 3 Enterprise, Personal
1.6.3.4 WPA 2 Enterprise, Personal
1.6.3.5 Protected Management Frames

1.6.4 No caso da Controladora Wireless ser oferecida em dispositivo físico, o hardware deverá ser composto de pelo menos 2 interfaces de rede 10Gb Ethernet com porta SFP+ e respectivos transceivers 10GBASE-SR multimodo com conectores LC e 4 interfaces 10/100/1000 Mbps com conectores RJ-45 e oferecer throughput mínimo de tráfego de rede de 20Gbps.

1.6.5 A solução deverá poder controlar Pontos de Acesso que operemnos padrões IEEE 802.11a/b/g/n/ac/ax, com diferentes rádios, em quaisquer combinações desses padrões.

1.6.6 Cada Controladora Wireless deve ser capaz de gerenciar de forma nativa, simultaneamente, pelo menos 200Pontos de Acesso, com centralização das funcionalidades de autenticação. Esta capacidade deve poder ser expandida por meio da adição de licenças de Pontos de Acesso e/ou por meio da adição de novas Controladoras Wireless a um cluster de controladoras conforme descrito no item

1.6.2, cujo gerenciamento deve ocorrer por meio de plataforma e interface de gerenciamento única.

1.6.7 A quantidade de Controladoras Wireless a ser fornecida deve ser provisionada de acordo com o necessário e suficiente para gerenciar a todos os Pontos de Acesso previstos na contratação.

1.6.8 Possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e aplicação de alteração das características de configuração dos itens de todo o grupo sem a necessidade de configuração individual de cada equipamento.

1.6.9 Permitir operação dos Pontos de Acesso em modo de rede *wireless mesh*.

1.6.10 Permitir a configuração e o uso de múltiplos SSIDs simultaneamente em cada Ponto de Acesso, associando parâmetros de segurança distintos para cada SSID.

1.6.11 Ser capaz limitar o número de dispositivos conectados a cada Ponto de Acesso com base em parâmetro definido pelo administrador.

1.6.12 Permitir o envio ou a gravação em tempo real de registros de eventos e erros do sistema (logs) em servidor externo por meio do protocolo syslog ou equivalente.

1.6.13 Fornecer a visualização de alertas da rede em tempo real, com indicação do nível de severidade por cor.

1.6.14 Oferecer a capacidade de ser gerenciado através de navegador padrão (HTTP/HTTPS), SSH, e interface console (este último somente no caso da Controladora Wireless ser oferecida em dispositivo físico).

1.6.15 Suportar protocolos de transferência de arquivos como FTP (File TransferProtocol) ou TFTP (Trivial File TransferProtocol) ou SFTP (Secure File TransferProtocol) ou SCP (SecureCopyProtocol).

1.6.16 Implementar protocolo de autenticação para controle do acesso administrativo à Controladora baseado em mecanismos de AAA (Authentication, Authorization and Accounting).

1.6.17 Permitir a criação de, pelo menos, dois grupos com níveis diferentes de permissão de acesso à Controladora Wireless, sendo um com capacidade de gerenciar todas as funções (administrativo) e outro apenas com permissão para visualização e/ou consulta de informações (somente leitura).

1.6.18 Ajustar dinamicamente canais e potência de radiofrequência dos Pontos de Acesso para otimizar a cobertura de rede e seu desempenho baseado na cobertura de APs vizinhos e interferências e implementar função de DFS e controle de TPC, conforme indicado no draft IEEE802.11h. Deve ser possível desabilitar o ajuste de potência e ajuste de canal automático.

1.6.19 Implementar, por meio dos Pontos de Acesso, varredura de RF periódica e automática, classificando fontes de interferência e APs não autorizados (rogues), evitando problemas de cobertura e controle da propagação indesejada de RF.

1.6.20 Deve permitir tráfego IPv4, IPv6 e Multicast através do controlador (camada 2).

1.6.21 Suportar opções de comutação de tráfego central e comutação de tráfego local. Neste último modo não é necessário que todo o tráfego seja direcionado para 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 Wireless, otimizando a conexão em caso de Pontos de Acesso gerenciados sobre um link remoto (internet, WAN, MPLS).

1.6.22 Deve controlar Pontos de Acesso em redes remotas, mesmo acessados por NAT ou através de túnel (VPN ou semelhante). Desta forma, deve ser possível definir o IP público da Controladora Wireless e fazer com que Pontos de Acesso remotos conectem-se automaticamente à Controladora Wireless através da Internet. Em caso de falha na comunicação entre Controladora Wireless e Ponto de Acesso, este deve continuar sua operação junto aos clientes já conectados.

1.6.23 Caso haja falha de comunicação entre os APs e a Controladora Wireless, 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 Wireless e os Pontos de Acesso para que novos usuários possam se conectar à rede utilizando autenticação 802.1x mesmo que os Pontos de Acesso estejam sem comunicação com a Controladora Wireless.

1.6.24 Deve permitir realizar o balanceamento automático da carga de usuários entre Pontos de Acesso adjacentes, fazendo a redistribuição de usuários entre os APs próximos sem intervenção humana e, no caso da inoperância de algum Ponto de Acesso, redistribuir automaticamente os usuários conectados a ele para os APsremanescentes dentro da área de alcance. Deve ser possível escolher em qual WLAN (SSID) será permitido executar tal ação.

1.6.25 Deve implementar funcionalidades de wIDS com intuito de controlar e identificar tentativas de ataques de tipos conhecidos ou identificáveis por regras heurísticas, e manter mecanismos que permitam atualizar a biblioteca de assinaturas de ataques.

1.6.26 Deve permitir implementar e gerenciar todos os recursos, assim como os mecanismos de segurança previstos no item Pontos de Acesso.

1.6.27 Deve implementar listas de controle de acesso (ACLs) para cada SSID dos Pontos de Acesso com restrições de endereço IP, tipos de protocolos, portas, QoS, VLAN e direção do fluxo de dados, com base nos parâmetros da etapa de autenticação. Deve ser possível a criação de ACLs para SSIDs de APs conectados local e remotamente.

1.6.28 Deve ser possível determinar, por SSID, se os usuários conectados a determinado SSID poderão ou não trocar pacotes entre si.

1.6.29 Implementar segurança baseada nos padrões WPA/WPA2/WPA3 e 802.11i.

1.6.30 Possuir suporte a autenticação IEEE 802.1x, com pelo menos três dos seguintes métodos EAP: EAP-MD5, PEAP/EAP-GTC, EAP-PEAP, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo.

1.6.31 Deve possuir funcionalidade de portal de autenticação web (Captive Portal), sendo possível indicar um CaptivePortal externo e, também, implementar um Captive Portal interno, caso em que todo o mecanismo de autenticação deve ser interno à Controladora Wireless (website, lista de usuários, políticas). Além disso, deve ser possível a criação de páginas personalizadas com imagem e texto, e especificar o tempo que um determinado usuário (login) ficará válido para ter acesso a rede através da autenticação web.

1.6.32 Deve permitir o cadastramento de usuários visitantes na base interna da Controladora Wireless.

1.6.33 Deve permitir a criação, pelos administradores, de perfis de tráfego para aplicações de voz e vídeo e permitir a priorização deste tráfego com atribuição de QoS.

1.6.34 A solução deve ainda permitir a criação de regras para bloqueio e limite de banda de aplicações comuns de mercadoe que estas regras possam ser aplicadas por SSID ou grupos de usuários.

1.6.35 Deve implementar recurso que evite automaticamente a conexão de usuários wireless em Pontos de Acesso classificados como maliciosos ou não autorizados.

1.6.36 A solução deve permitir detectar e/ou mitigar interferências que impactem diretamente no funcionamento da rede.

1.6.37 Deve permitir implementar configurações distintas por SSID nos Pontos de Acesso, locais ou remotos, tais como regras de autenticação, QoS, criptografia, SSID e VLAN. Deve ser possível especificar em quais APs/Grupos de APs cada SSID será aplicado.

1.6.38 Para fins de controle, deve permitir a restrição da quantidade de usuários conectados em um determinado SSID.

1.6.39 Deve permitir o gerenciamento da disponibilidade de SSIDs por data/hora e dias da semana e horários previamente determinados.

1.6.40 Possibilitar fast roaming, melhorando a performance de aplicações em tempo real (802.11r).

1.6.41 Implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente Pontos de Acesso próximos disponíveis para roaming.

1.6.42 Deve implementar SNTP ou NTP para sincronização de tempo com outros dispositivos de rede.

1.6.43 Deve permitir a atualização do software (firmware) da Controladora Wireless e do software (firmware) dos Pontos de Acesso (APs), mesmo quando conectado remotamente.

1.6.44 Implementar SNMP v2c e v3 incluindo a geração de traps, a criptografia do tráfego de dados de gerência e suportar MIB vII (conforme RFC 1213), que permitam coletar dados de uso pelo menos dos seguintes componentes da Controladora e dos Pontos de Acesso: interfaces de rede, CPU e memória.

1.6.45 Deve permitir o gerenciamento da Controladora Wireless e dos Pontos de Acesso através de IPv6.

1.6.46 Deve suportar Wireless MultimediaExtensions (WMM).

1.6.47 Oferecer detecção e proteção integrada de ataques de negação de serviços.

1.6.48 Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede.

1.6.49 Deve reconhecer e ser capaz de aplicar pelo menos 1024 políticas de QoS para otimização de tráfego de aplicações.

1.6.50 Permitir o controle de banda disponível (bandwithcontracts) por usuário ou através de perfis de usuários.

1.6.51 Possuir capacidade de gerar alarmes e executar contramedidas no caso de detecção de um ataque.

1.6.52 Implementar o protocolo 802.1w (RapidSpanningTree) no caso da Controladora Wireless ser oferecida em dispositivo físico.

1.6.53 Poder atuar como Proxy Arp

1.6.54 Oferecer os recursos de roaming de camada L2.

1.6.55 Implementar tagging de VLANs através do protocolo 802.1Q.

1.6.56 Ser capaz de realizar a descoberta automática dos APs na infraestrutura wireless.

1.6.57 Ser capaz de estabelecer conexão tunelada entre Pontos de Acesso e Controladora Wireless de maneira segura.

1.6.58 Possuir capacidade de consulta em tela ou geração de relatórios dos seguintes tipos de informação: Listagem de Pontos de Acesso ativos, listagem de clientes wireless ativos por Ponto de Acesso, por grupos de Pontos de Acesso e por SSID, taxa de utilização de rede por Ponto de Acesso.

1.6.59 Qualquer das funcionalidades acima pode ser considerada suprida caso esteja disponível na Solução de Controle de Acesso à Rede (NAC).

1.7 Solução de Controle de Acesso à Rede (NAC)

1.7.1 A Solução de Controle de Acesso à Rede (NAC), doravante chamada de NAC, deverá ser totalmente compatível e ter capacidade de gerenciar, de maneira integrada, todas as funcionalidades e tecnologias da Controladora Wireless e dos Pontos de Acesso que compõem a Solução de Rede Wi-Fi, podendo ser utilizada como única interface gráfica de administração de toda solução descrita neste documento.

1.7.2 Será aceito que a Solução de Controle de Acesso à Rede (NAC) seja física (*hardware appliance*) ou virtualizada (*virtual appliance*) ou software aplicativo, instalável em servidor Microsoft Windows Server 2019 ou superior ou GNU Linux, ou, ainda, conjunto de funcionalidades de gerenciamento existentes na Controladora Wireless, ativas e disponíveis por padrão ou ativáveis por licenciamento.

1.7.3 Caso a Controladora Wireless a ser ofertada ofereça todas as funcionalidades de gerenciamento exigidas neste item, sem custo ou necessidade de licenciamento adicional, o proponente deve mencionar explicitamente isso em sua proposta e cotar este item com o custo simbólico R$ 1,00.

1.7.4 Deve suportar e ser capaz de gerenciar todas as características e protocolos para os quais a Controladora Wireless os Access Points adquiridos conjuntamente foram certificados, em especial:

1.7.4.1 Wi-Fi Certified a, b, g, n, ac, 6
1.7.4.2 WMM
1.7.4.3 WPA 3 Enterprise, Personal
1.7.4.4 WPA 2 Enterprise, Personal
1.7.4.5 Protected Management Frames

1.7.5 O software deve contar com um mínimo de 1.000 licenças de uso e autenticação para usuários/dispositivos internos à rede corporativa e mais 500 licenças de uso e autenticação para usuários/dispositivos visitantes e deve, ainda, poder ter a quantidade de usuários/dispositivos licenciados acrescida pela mera aquisição e registro de novas licenças, sem a necessidade de qualquer reinstalação ou alteração nos softwares instalados.

1.7.6 No caso da Solução de Controle de Acesso à Rede (NAC) ser oferecida em dispositivo físico, o hardware deverá ser composto de pelo menos 1 interface de rede Multigigabit Ethernet 2.5Gb e 2 interfaces 10/100/1000 Mbps com conectores RJ-45 e oferecer throughput mínimo de tráfego de rede de 2Gbps.

1.7.7 Deve permitir que todos os eventos da Controladora Wireless e dos Access Points sejam redirecionados para uma console de gerência central.

1.7.8 Toda a interface de gerenciamento deverá ser gráfica e o acesso ao sistema deverá ser por meio de cliente com browser padrão, compatível com Microsoft Edge, Google Chrome e Mozilla Firefox em suas versões mais recentes, utilizando o

protocolo HTTPS.

1.7.9 . Implementar protocolo de autenticação para controle do acesso administrativo à solução utilizando servidor Radius e auditoria de comandos com mecanismos de AAA.

1.7.10 Possuir visualização dos mapas de calor (heatmaps) dos andares de cada prédio, apresentando, em tempo real, posição dos pontos de acesso, dos clientes conectados, dos rogue APs e a cobertura do sinal de radiofrequência tanto em 2,4 GHz como em 5 GHz.

1.7.11 Permitir a visualização de eventuais áreas sem cobertura de radiofrequência (áreas de sombra).

1.7.12 Permitir a monitoração do desempenho, em tempo real, das redes WLAN, reportando os seguintes parâmetros: falhas de autenticação, relação sinal-ruído, interferência, potência de sinal, utilização da rede por cliente dos e APs e consumo de CPU e memória nas Controladoras Wireless.

1.7.13 Deve implementar a listagem em tempo real das informações dos usuários conectados nas redes WLAN contendo os seguintes parâmetros: endereço IP, endereço MAC, banda utilizada pelo cliente, nível de potência de recepção, relação sinal-ruído, parâmetros de associação, autenticação e nome do usuário.

1.7.14 Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que causam interferência na rede sem fio.

1.7.15 Possuir capacidade de gerenciamento hierárquico com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento.

1.7.16 Implementar modelos de configuração (templates) de forma a possibilitar a replicação de configuração aos equipamentos selecionados.

1.7.17 Realizar a descoberta automática dos dispositivos individuais da infraestrutura wireless.

1.7.18 Fornecer a visualização de alertas da rede em tempo real, com indicação do nível de severidade por cor.

1.7.19 Ser capaz de detectar, em conjunto com a Controladora Wireless e os Pontos de Acesso, pelo menos, os seguintes ataques: flood de frames de gerenciamento dos clientes wireless, respostas de nullprobe, flood de autenticação, ataque de deauthentication, flood de EAP handshake.

1.7.20 Implementar mecanismos para detecção, localização e bloqueio de pontos de acesso não autorizados (rogue) e redes ad-hoc.

1.7.21 Deve possuir ferramenta para de ajuste automático de configurações de espectro, onde configure, no mínimo, os seguintes parâmetros, baseados em dados colhidos dos próprios Pontos de Acesso:

1.7.21.1 Potência do rádio

1.7.21.2 Canal de difusão

1.7.22 Possuir capacidade de consulta em tela ou geração de relatórios dos seguintes tipos de informação: Listagem de clientes wireless por período informado, informações de configuração das Controladoras Wi-Fi, utilização da rede, detalhes dos pontos de acesso não autorizados (rogues) detectados.

1.7.23 Deve possuir consulta em tela ou relatório que permitaidentificar a versão de software instalada e o número serial de todos os equipamentos monitorados na plataforma.

1.7.24 A plataforma deve ser capaz de analisar, a nível de protocolo, falhas no momento de autenticação, ajudando a identificar a etapa da autenticação em que houve a falha

1.7.25 A plataforma deve ser capaz apresentar em tempo real a quantidade de usuários conectados a um agrupamento lógico de Pontos de Acesso, que possam representar uma determinada sala, andar ou localidade de interesse.

1.7.26 A plataforma deve ser capaz de identificar e apresentar dados analíticos de usuários que tiveram baixa qualidade de serviços dentro da rede.

1.7.27 Deve ser capaz de apresentar painel com as aplicações (em camada 7 do modelo OSI) que estão sendo executadas na rede e mostrar o consumo de banda por aplicação.

1.7.28 A plataforma deve ser capaz de detectar interferências, aplicar contramedidas, e identificar o Ponto de Acesso no qual a interferência foi detectada.

1.7.29 Deve ser possível, através da plataforma de gerência, acessar o terminal de comando ou determinar a execução de scripts CLI nos Pontos de Acessogerenciados.

1.7.30 Deve permitir a criação de perfis de administradores, criando visões administrativas independentes como, por exemplo, administradores (acesso completo à plataforma), operadores (acesso a configurações de usuários e Pontos de Acesso) e monitores (acesso apenas de leitura a consultas, painéis e relatórios).

1.7.31 Deve permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados nos Pontos de Acesso, Controladoras Wireless a partir da Solução de Gerência

1.7.32 Deve realizar a atualização de software do conjunto de Controladoras Wireless e Pontos de Acesso de forma gradual (em grupos), sem causar indisponibilidade do respectivo serviço.

1.7.33 Deve permitir implementar autenticação 802.1x para os usuários da rede sem fios utilizando, pelo menos, o método EAP-TLS.

1.7.34 Deve permitir a integração com RADIUS Server com suporte ao método EAP citado no item anterior.

1.7.35 Deve implementar autenticação RADIUS baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes.

1.7.36 Deve implementar autenticação via portal web (captive portal) para os usuários da rede que não puderem se autenticar via 802.1x. O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo.

1.7.37 Permitir a automatização do processo de conexão segura à rede sem fio através da instalação automática de certificado digital e configuração de perfil de rede sem fio em dispositivos móveis. A solução deve identificar automaticamente o tipo de dispositivo cadastrado e conectado à rede para provisionar o certificado digital e configurar o perfil da rede sem fio conforme o sistema operacional utilizado, no mínimo os seguintes sistemas operacionais: Android ,Apple iOS, Mac OS X e Windows, para que o usuário utilize autenticação segura via 802.1X na rede corporativa.

1.7.38 Para redes abertas (guest VLAN) utilizadas em eventos e para visitantes, o cliente deverá poder se conectar sem senha à infraestrutura de rede e ter seu acesso redirecionado para o portal de autenticação.

1.7.39 O Captive Portal deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes.

1.7.40 O Captive Portal deve possuir suporte aos idiomas Português do Brasil ou Inglês, quando não houver em idioma Português, a plataforma deve permitir que seja realizado a tradução.

1.7.41 Deve suportar diferentes tipos de servidores de AAA (Authentication, Authorization and Accounting) de retaguarda (“Backend Authentication Servers”), como RADIUS, LDAP e Microsoft Active Directory (sem alteração no Schema do AD).

1.7.42 Deve implementar funcionalidades de Classificação Automática de Dispositivos (“Deviceprofiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso.

1.7.43 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

1.7.43.1 Grupo do usuário no Active Directory

1.7.43.2 Protocolo de autenticação utilizado

1.7.43.3 Tipo de dispositivo utilizado

1.7.43.4 Localização ou região do AP em que se conectou

1.7.44 Deve implementar os serviços de autenticação, profiling, provisionamento e

autorização para 1.000 mil usuários/dispositivos simultâneos.

1.7.45 Possuir plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas / de dispositivo e elementos condicionais em um conjunto de políticas.

1.7.46 Suporte a seguintes fontes para autenticação:

1.7.46.1 Microsoft Active Directory

1.7.46.2 Kerberos

1.7.46.3 LDAP-compliantdirectory

1.7.46.4 Radius

1.7.46.5 Microsoft Azure Active Directory

1.7.46.6 Google G Suite

1.7.46.7 Lista estática de endereços MAC

1.7.47 Deve suportar "Single Sign-on" (SSO) através de SAML v2.0 ou NPS (Network Policy Server).

1.7.48 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

1.7.48.1 Atributos do usuário autenticado,

1.7.48.2 Hora do dia, dia da semana,

1.7.48.3 Tipo de dispositivo utilizado,

1.7.48.4 Localização do usuário;

1.7.48.5 Tipo de autenticação utilizado

1.7.49 Permitir a visualização de todas informações relativas a cada usuário conectado, como data e hora de autenticação, MAC Address do dispositivo, classificação do dispositivo, usuário, equipamento que requisitou a autenticação (origem), método de autenticação utilizado, fonte de autenticação utilizada para validação, status da autenticação e alertas em caso de falha.

1.7.50 Deve implementar funcionalidade de classificação automática de dispositivos (“Deviceprofiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

1.7.51 Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, Smartphone, impressora, etc), por sistema operacional (ex. Windows, Linux, MacOS, etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server, etc);

1.7.52 Deve suportar a coleta de informações, para classificação, usando no mínimo 2 dos métodos a seguir: DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting;

1.7.53 Deve possuir base de categorias de dispositivos pré-configuradas e suportar a criação de regras para os dispositivos de acordo com sua categoria;

1.7.54 Deve implementar os serviços de autenticação, profiling e autorização para 1.500 usuários/dispositivos;

1.7.55 Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados.

1.7.56 Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.

1.7.57 Suporte a RADIUS CoA, Web authentication e SAML v2.0 ou NPS (Network Policy Server).

1.7.58 Suporte a aplicação de políticas em ambiente multivendor de Wireless, cabeado e VPN.

1.7.59 Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptacao da comunicacao.

1.7.60 Deve suportar EDUROAM

1.7.61 Suporte a integração com plataforma de terceiros usando HTTP/RESTFUL API.

1.7.62 Permitir que a solução faça consultas em bases internas de usuários, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários.

1.7.63 A solução deve permitir configuração em alta disponibilidade com no minimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições.

1.7.64 A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, na qual as políticas serão configuradas em um único elemento para serem distribuidas aos demais que pertençam a mesma "zona".

1.7.65 Gerenciamento de Usuários Visitantes (Convidados)

1.7.65.1 Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;

1.7.65.2 Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

1.7.65.3 Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

1.7.65.4 Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;

1.7.65.5 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.7.65.6 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.7.65.7 Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

1.7.65.8 Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através do portal web, sem a necessidade de um autorizador;

1.7.65.9 Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;

1.7.65.10 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 e números para compor a senha;

1.7.65.11 Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login;

1.7.65.12 Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e impressão local

1.7.65.13 Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de sponsorship;

1.7.65.14 Deve permitir o gerenciamento das credenciais de visitantes;

1.7.65.15 Deve permitir a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;

1.7.65.16 Deve realizar o caching de endereço MAC dos usuários visitantes;

1.7.65.17 Deve permitir o login automático de usuários que realizem o auto-registro;

1.7.65.18 Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;

1.7.65.19 Deve permitir a criação de tokenou QR Codede acesso;

1.7.65.20 Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;

1.7.65.21 Deve permitir a desconexão de múltiplas sessões ativas;

1.7.65.22 Deve permitir autenticação através de social login nativa na solução;

1.7.65.23 Deve ser capaz de modificar ou desconectar uma sessão ativa de visitante através de RADIUS Dynamic Authorization.

1.7.66 Serão aceitas soluções/softwares adicionais para compor a solução completa, desde que entregue em conjunto com a solução do próprio fabricante.

1.7.67 Qualquer das funcionalidades acima pode ser considerada suprida caso esteja disponível Controladora Wireless.

1.8 Entrega e instalação

1.8.1 Todos os equipamentos e softwares descritos nos itens 1.3, 1.4, 1.5, 1.6 e 1.7 acima deverão ser entregues no Complexo Sede do Tribunal Regional do Trabalho da 23ª Região.

1.8.2 O prazo de entrega para os bens referidos no item 1.8.1 é de 90 dias após a assinatura do Contrato, emissão da Nota de Empenho ou Ordem de Fornecimento.

1.8.3 Imediatamente após a assinatura do Contrato ou emissão da Nota deEmpenho ou da Ordem de Fornecimento, a Contratada terá 20 dias para elaboração do projeto executivo de instalação da Rede Sem Fios, que contemplará todas as etapas do processo, desde o cronograma da instalação e as datas previstas para a realização de cada etapa, contendo pelo menos os seguintes eventos:

1.8.3.1 Site Surveypresencial prévio no SítioPiloto;

1.8.3.2 Apontamento dos locais de instalação dos Pontos de Acesso do Grupo Piloto

1.8.3.3 Instalação e ativação da controladora e Solução de Controle de Acesso à Rede (NAC);

1.8.3.4 Instalação e ativação dosPontos de Acesso do Grupo Piloto;

1.8.3.5 Validação das configurações e parâmetros de operação do Sítio Piloto;

1.8.3.6 Site Surveypresencial pós instalação no SítioPiloto;

1.8.3.7 Realização da capacitação “Hands-on”;

1.8.3.8 Site Survey virtual nos demais ambientes da contratante;

1.8.3.9 Apontamento dos locais de instalação dos demais Pontos de Acesso;

1.8.3.10 Ativação remota dos demais pontos de acesso;

1.8.3.11 Validação da instalação e funcionamento de toda a rede.

1.8.4 O projeto executivo de instalação da Rede Sem Fios deverá ser entregue ao Gestor do Contrato, que o submeterá à análise do Fiscal Técnico para aprovação em até 5 dias. Em caso de reprovação do projeto ou apontamento da necessidade de alterações, a contratada terá 5 dias após a notificação para promover as alterações demandadas e entregar a versão definitiva do projeto.

1.8.5 Para fins de planejamento, provisionamento de recursos e estimativa de custos, fica determinado que os serviços de instalação consistirão em:

1.8.5.1 Instalação das Controladoras Wireless (item 1.6);

1.8.5.2 Instalação da Solução de Controle de Acesso de Rede (item 1.7);

1.8.5.3 Realização de Site Survey presencial prévio no site piloto;

1.8.5.4 Instalação e/ouativação lógica e configuração dos primeiros 50 (cinquenta) Pontos de Acesso (itens 1.3 e/ou 1.4) instalados fisicamente no(s) prédio(s) da Sede do Tribunal contratante (ou até este limite);

1.8.5.5 Realização de Site Survey presencial pós instalação no site piloto;

1.8.5.6 Instalação e/ou ativação lógica e configuração dos demais Pontos de Acesso (itens 1.3 e/ou 1.4) adquiridos e instalados fisicamente no(s) prédio(s) do contratante.

1.8.6 Fica esclarecido que o SítioPiloto será definido pela equipe de Gestão do Contrato e abrangerá apenas os ambientes da sede da contratante que sejam suficientes e necessários para a instalação da Controladora Wireless, da Solução de Controle de Acesso de Rede e de um conjunto de até 50 Pontos de Acesso que comporão o assim chamado Grupo Piloto de ativação.

1.8.7 Fica esclarecido, ainda, que a instalação física, provimento de cabeamento de rede e eventual alimentação elétrica de todos os Pontos de Acesso serão de inteira responsabilidade do contratante e deverá ser realizada até a data prevista no projeto executivo para a ativação lógica desses mesmos Pontos de Acesso.

1.8.8 O prazo de entrega da implantação em pleno funcionamento do SítioPiloto é de até 30 dias após a entrega dos bens referidos no item 1.8.1.

1.8.9 O prazo de entrega da implantação em pleno funcionamento de toda a Rede Sem Fios deverá ser pactuado entre a contratante e a contratada na fase de elaboração do projeto executivo, em virtude da necessidade de provimento, pela contratante, da infraestrutura para a instalação física dos Pontos de Acesso, mas não poderá exceder 120 dias após a entrega dos bens referidos no item 1.8.1.

1.9 Transferência de conhecimento "*handson*"

1.9.1 A transferência de conhecimento na modalidade "*handson*" deverá ocorrer de maneira presencial, imediatamente após a instalação dos componentes de hardware e software da Controladora Wireless e Solução de Controle de Acesso à Rede (NAC), juntamente com a instalação do GrupoPiloto de Pontos de Acesso no ambiente.

1.9.2 A capacitação aqui descrita deverá contar com uma carga-horária mínima de 24h, dentre as quais, pelo menos 50% sejam compostas por atividades práticas.

1.9.3 A capacitação deverá ser conduzida por profissional certificado (com certificação de proficiência) oficialmente pelo fabricante da solução`, para todos os itens que a compõem (Pontos de Acesso, Controladora Wireless e Solução de Controle de Acesso). Caso um único profissional não possua certificação oficial de todos os componentes, será aceita a condução por uma equipe de profissionais com certificação em partes complementares da solução.

1.9.4 A capacitação deverá contar com material de apoio orientativo contendo a relação das atividades, seus objetivos e descrição, e ser elaborado pelo instrutor ou organização promovente, e ser entregue aos alunos em formato eletrônico ou impresso.

1.9.5 O conteúdo da capacitação deverá no mínimo abranger, mas não se restringir a, todos os aspectos fundamentais de instalação, configuração, ativação, operação, diagnóstico e resolução de problemas (troubleshooting) dos componentes adquiridos e que constituirão a Rede Sem Fios, em um nível de profundidade de conhecimento equiparável ao que a Biblioteca ITIL considera as habilidades de uma equipe de suporte de Nível 1.

1.9.6 Após a conclusão da capacitação, deverá ser realizada uma pesquisa de satisfação onde os participantes possam avaliar com notas objetivas e comentários discursivos a qualidade do conteúdo, dos materiais de apoio e do(s) instrutur(es). Caso o resultado geral apurado por média aritmética seja inferior a 75% de aprovação, a capacitação deverá ser reformulada considerando os pontos de menor nota na avaliação e realizada novamente em um prazo inferior a 30 dias.

1.9.7 A capacitação poderá ser realizada de forma presencial na sede da contratante, em ambiente fornecido por ela, ou em ambiente fornecido pela contratada na mesma cidade da sede da contratante. A capacitação também poderá ser realizada de forma telepresencial síncrona em ambiente virtual de aprendizagem com a participação simultânea do instrutor e dos treinandos.

1.9.8 A capacitação poderá ser realizada por profissionais diretamente vinculados à contratada ou por meio do fornecimento de vouchers de treinamentos oficiais do fabricante.

Anexo III – Site Surveys realizados

Ao longo dos trabalhos que serviram de base para e elaboração deste documento, foram realizados, a pedido da CITM e desta EPC, diversos levantamentos do tipo Site Survey preliminar ou preditivo, como meio de estimar a quantidade de Access Points necessários para prover uma cobertura de sinal satisfatória nos ambientes do Regional. Em razão da extensão dos documentos em número de páginas e quantidade de imagens ilustrativas, entendeu-se ser mais adequado juntar a íntegra desses documentos ao processo administrativo que este estudo instrui.

Anexo IV – Pesquisa de preços públicos

Para estimar os custos totais da solução aqui pretendida foram realizadas pesquisas de preços em contratações públicas com objetos similares. Em razão da extensão dos documentos, entendeu-se ser mais adequado juntar a íntegra desses documentos ao processo administrativo que este estudo instrui, e colar aqui apenas a página que contenha o resumo dos valores de cada contratação pública:

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

ATA DE REGISTRO DE PREÇOS - TRF1-SEATA

PROCESSO N. 6165902019401/8000 - PREGÃO ELETRÔNICO N. 0020/2021

ATA DE REGISTRO DE PREÇOS N. 0009/2021

A União, por intermédio do **TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO,** com sede Praça dos Tribunais Superiores, Bloco "A" – Brasília/DF, inscrito no CNPJ/MF n. 03.658.507/0001-25, representado pelo Diretor - Geral, **CARLOS FREDERICO MAIA BEZERRA**, CPF n. 480.325.571-72 nos termos das Leis n. 8.666, de 21 de junho de 1993, e n. 10.520, de 17 de julho de 2002, e dos Decretos n. 10.024, de 20 de setembro de 2019, n. 7.892, de 23 de janeiro de 2013, e demais normas legais aplicáveis, obedecidas as disposições contidas no instrumento convocatório e em face da classificação da proposta apresentada no Pregão Eletrônico n. 0020/2021, RESOLVE registrar o preço ofertado pelo Fornecedor Beneficiário, **LETTEL DISTRIBUIDORA DE TELEFONIA LTDA**, estabelecido na Rua Osni Joao Vieira, 205, Bairro Campinas, São Jose/SC, CEP: 88101-270, telefone/fax: (51) 2123-2300/2355, (51) 99326-1977, email: everson@lettel.com.br; felipe@lettel.com.br, inscrito no CNPJ sob o n. 07.789.113/0001-67, representado pelo Sr. Everson Silva Leite, CPF n. 291.823.360-91, conforme abaixo. Demais especificações, conforme Edital.

GRUPO 01				
ITEM	QUANTIDADE	UNIDADE	PREÇO UNITÁRIO R$	PREÇO TOTAL R$
1	1	LICENCA	28.081,00	28.081,00
ESPECIFICAÇÕES: SOLUÇÃO DE GERÊNCIA DE REDE SEM FIO (WLAN). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL-LUCENT. MODELO: OmniVista 2500 NMS + LICENÇAS OV NM EX + SUPORTE 5 ANOS.				
2	320	UN	2.405,00	769.600,00
ESPECIFICAÇÕES: PONTO DE ACESSO SEM FIO, COM GARANTIA DE 60 (SESSENTA MESES). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniAccess OAW-AP1221- RW + OAW- AP1221-SW + OAW-AP-MNT- W + PP5N- OAWAP1221 (GARANTIA 5 ANOS) + LICENÇAS E ACESSÓRIOS.				
3	35	UN	4.959,00	173.565,00
ESPECIFICAÇÕES: SWITCH DE ACESSO PoE DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniSwitch OS6350-P24-US + OS6350-P24 - SW + PP5N OS6350 (GARANTIA 5 ANOS) + 2 SFP-GIG-SX + LICENÇAS E ACESSÓRIOS.				
4	2	UN	53.169,00	106.338,00
ESPECIFICAÇÕES: CONTROLADORA WIRELESS. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS + 1 OmniSwitch OS6860E-24-US + 2 FONTE REDUNDANTE OS6860-BP-US + PP5N-OS6860 (GARANTIA 5 ANOS) + SFP-10G-SR + LICENÇAS OV-AP + SUPORTE 5 ANOS.				
5	2	LICENCA	4.462,03	8.924,06
ESPECIFICAÇÕES: PACOTE DE LICENÇAS PARA USUÁRIOS VISITANTES (500 USUÁRIOS). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS MODULO OV-GA-500-N + PW5N- OVGA500N (SUPORTE 5 ANOS).				
6	1	LICENCA	32.497,00	32.497,00
ESPECIFICAÇÕES: SOLUÇÃO DE CONTROLE DE ACESSO. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL. MARCA: ALCATEL- LUCENT. MODELO: OmniVista 2500 NMS MODULO OV-GA-1K-N + PW5N- OVGA1KN (SUPORTE 5 ANOS).				
7	1	SERVICO	7.877,00	7.877,00
ESPECIFICAÇÕES: SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS ITENS 1, 4, 5 E 6. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
8	320	SERVICO	297,00	95.040,00
ESPECIFICAÇÕES: SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS ITENS 2 E 3. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
9	2	TURMA	6.024,00	12.048,00
ESPECIFICAÇÕES: TREINAMENTO TELEPRESENCIAL (COM ATÉ 5 ALUNOS POR TURMA). DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
10	6	SERVICO	6.024,00	36.144,00
ESPECIFICAÇÕES: SITE SURVEY. DEMAIS CARACTERÍSTICAS DE ACORDO COM O ANEXO I DO EDITAL.				
TOTAL REGISTRADO PARA O GRUPO 01				**1.270.114,06**

Este Registro de Preços terá validade de 12 (doze) meses, contados da data da sua assinatura pelas partes, instante a partir do qual o instrumento será considerado apto a produzir seus jurídicos efeitos. O extrato desta Ata será publicado em órgão oficial da Administração.

As especificações técnicas e demais exigências constantes do Decreto n. 7.892/2013, no Processo Administrativo n. 6165902019401/8000 e Pregão Eletrônico n. 0020/2021 integram esta Ata de Registro de Preços, independentemente de transcrição.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais do Tribunal Regional Federal da Primeira Região e do Fornecedor Beneficiário.

CARLOS FREDERICO MAIA BEZERRA
Diretor - Geral

EVERSON SILVA LEITE
Lettel Distribuidora de Telefonia Ltda

Documento assinado eletronicamente por **Everson Silva Leite**, **Usuário Externo**, em 23/07/2021, às 15:42 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Frederico Maia Bezerra**, **Diretor-Geral da Secretaria**, em 26/07/2021, às 09:27 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf1.jus.br/autenticidade informando o código verificador **13523289** e o código CRC **B72E04A7**.

ZOOM TECNOLOGIA

AO

BANCO CENTRAL DO BRASIL - BACEN

PREGÃO ELETRÔNICO Nº 78/2021

PROPOSTA COMERCIAL

Apresentamos nossa proposta, para a contratação de empresa especializada em tecnologia da informação para aquisição e instalação de uma solução de rede sem fio (rede wireless) para todas as localidades do Banco Central do Brasil, conforme quantidades e exigências estabelecidas no Edital e seus anexos, conforme abaixo:

Item	Descrição	Qtd	Valor do Hardware	Valor do Software	Valor da Garantia e Suporte Técnico	Valor da Instalação	Total
01	Controladora Wi-Fi para até 200 pontos de acesso **Marca:** Huawei **Modelo:** AC6805	8	R$ 291.181,61	R$ 225.229,75	R$ 262.992,36	R$ 57.724,30	R$ 837.128,02
02	Controladora Wi-Fi para até 50 pontos de acesso **Marca:** Huawei **Modelo:** AC6805	16	R$ 582.363,23	R$ 450.459,51	R$ 219.160,30	R$ 115.448,97	R$ 1.367.432,01
03	Ponto de acesso Wi-Fi 6 **Marca:** Huawei **Modelo:** AirEngine 5760-51	650	R$ 618.214,45	R$ 203.498,90	R$ 274.074,90	R$ 327.130,47	R$ 1.422.918,72
04	Software de Gerenciamento **Marca:** Huawei **Modelo:** iMaster NCE-Campus	1	R$ 62.882,58	R$ 25.129,75	R$ 11.456,11	R$ 11.071,89	R$ 110.540,33
05	Software de Controle do Acesso à Rede **Marca:** Huawei **Modelo:** iMaster NCE-CampusInsight	1	R$ 77.263,00	R$ 30.159,01	R$ 11.456,11	R$ 13.102,81	R$ 131.980,93

Valor Total Global: R$ 3.870.000,00. Por extenso: três milhões, oitocentos e setenta mil reais.

Validade da Proposta: 60 (sessenta) dias.

Prazo de Garantia: 48 (quarenta e oito) meses.

Declaramos que nos preços contidos estão inclusos todos os custos e despesas diretas e indiretas, encargos sociais, previdenciários, trabalhistas e comerciais, taxa de administração

SERVIX

Ao
Ministério do Meio Ambiente
Instituto Chico Mendes de Conservação da Biodiversidade
Divisão de Licitações

Pregão Eletrônico nº 41/2021
Processo nº 02070.006158/2020-47

Objeto: Contratação de solução de rede sem fio (Wi-Fi) para a Sede, ACADEBio e Regionais do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

PROPOSTA

A empresa Servix Informática Ltda., inscrita no CNPJ sob o nº 01.134.191/0002-28, estabelecida na SIG, Quadra 04, Lote 125, Bloco A, Salas 01 e 02, Cruzeiro, Brasília - DF, por intermédio do seu Representante Legal, o Sr. Cleber Augusto Calejon, portador do RG nº 25.127.646-6-SSP/SP, e inscrito no CPF sob o nº 286.718.678-11, apresenta sua proposta comercial nas condições que seguem.

LOTE	ITEM	DESCRIÇÃO	UND	QTD	VALOR UNITÁRIO	VALOR TOTAL
01	1	Controladora Física	Und	2	R$ 100.459,00	R$ 200.918,00
	2	Serviços de Instalação de Controladora Física (presencial)	Serviço	2	R$ 10.647,00	R$ 21.294,00
	3	Access Point Indoor	Und	307	R$ 4.030,00	R$ 1.237.210,00
	4	Serviços de Instalação de Access Point Indoor (presencial)	Serviço	58	R$ 533,00	R$ 30.914,00
Valor Total					**R$ 1.490.336,00**	

Valor total da proposta: R$ 1.490.336,00 (Um milhão e quatrocentos e noventa mil e trezentos e trinta e seis reais).

Validade da proposta: 60 (sessenta) dias, contados de sua apresentação.

Nos valores propostos estão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

Declaro que o produto ofertado possui a garantia técnica solicitada no termo de referência.

Filial Brasília
SIG, Quadra 04, Lote 125, Bloco A, Salas 01 e 02, Capital Financial Center, 70610-440, Brasília - DF, Brasil
+55 61 3031 2960
www.servix.com

AVANT TECNOLOGIA

55 (61) 4141.6425
55 (61) 98426.7545
www.avanttech.com.br

AO

DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL – DETRAN DF

PREGÃO ELETRÔNICO SRP Nº SRP 02/2023

Processo Administrativo nº 00055-00056232/2021-38

Tipo de Licitação: MENOR PREÇO GLOBAL

Data: 23/01/2023

Horário: 09:00 horas (horário de Brasília -DF)

Prezados Senhores,

Após examinar todas as cláusulas e condições estipuladas no Edital em referência, apresentamos nossa proposta nos termos consignados no mencionado ato convocatório e seus anexos, com os quais concordamos plenamente.

Nossa proposta é válida por 60 (sessenta) dias corridos, contados da data prevista para abertura da licitação.

Os equipamentos serão entregues no prazo de até 60 (sessenta) dias corridos decorridos da assinatura do contrato.

Declaramos que nos preços ofertados estão incluídas todas as despesas relativas à entrega do(s) bem(ns) tais como embalagens, encargos sociais, frete, seguro, tributos e encargos de qualquer natureza que, direta ou indiretamente, incidam sobre o objeto da licitação.

OBJETO: Registro de Preços, visando a eventual contratação de empresa para fornecimento de solução de rede WLAN e LAN, contemplando serviços de instalação, configuração e suporte técnico, com garantia pelo período de 60 (sessenta) meses on-site.

PLANILHA DE PROPOSTA DE PREÇOS

ITEM	DESCRIÇÃO	UNID.	QNT	VALOR UNIT.	VALOR TOTAL
1	Switch de Acesso 48 Portas 1G RJ45 POE+ **Fabricante: Commscope Ruckus** **Modelo: ICX7150-48PF-4X10GR**	Unid.	60	R$ 30.690,00	R$ 1.841.400,00

PartnerPRO NETWORK COMMSCOPE RUCKUS Lenovo

AVANT TECNOLOGIA

55 (61) 4141.6425
55 (61) 98426.7545
www.avanttech.com.br

2	Switch de Acesso 24 Portas 1G RJ45 POE+ **Fabricante: Commscope Ruckus** **Modelo: ICX7150-24P-4X10GR**	Unid.	40	R$	21.320,00	R$	852.800,00
3	Controlador/Gerenciador WLAN **Fabricante: Commscope Ruckus** **Modelo: Virtual Smartzone**	Unid.	1	R$	34.450,00	R$	34.450,00
4	Ponto de Acesso (AP) 802.11ax Interno **Fabricante: Commscope Ruckus** **Modelo: Ruckus R550**	Unid.	200	R$	6.110,00	R$	1.222.000,00
5	Serviço de Instalação W-Fi	Unid.	200	R$	590,00	R$	118.000,00
6	Solução de controle de acesso à rede (NAC) **Fabricante: Commscope Ruckus** **Modelo: Cloudpath Base On-Site Server As a Virtual Appliance**	Unid.	1	R$	15.500,00	R$	15.500,00
7	Licenciamento para solução de controle de acesso (NAC) **Fabricante: Commscope Ruckus** **Modelo: Cloudpath Per User On-Site License for Enterprises**	Unid.	1	R$	1.074.285,10	R$	1.074.285,10
8	Solução de gerência **Fabricante: Commscope Ruckus** **Modelo: Virtual Smartzone + Ruckus Analytics**	Unid.	1	R$	17.230,00	R$	17.230,00
9	Serviço de planejamento	Unid.	1	R$	200.000,00	R$	200.000,00
10	Serviço de migração/instalação SWITCHES	Unid.	100	R$	1.390,00	R$	139.000,00
11	Serviço de Configuração - Fase 2	Unid.	1	R$	39.900,00	R$	39.900,00
12	Serviço de Configuração - Fase 3	Unid.	1	R$	39.900,00	R$	39.900,00
13	Serviço de treinamento para switches e gerenciamento	Unid.	1	R$	22.234,90	R$	22.234,90
14	Serviço de treinamento para solução NAC	Unid.	1	R$	11.900,00	R$	11.900,00
15	Garantia e suporte	Meses	60	R$	9.190,00	R$	551.400,00
VALOR GLOBAL						R$ 6.180.000,00	

Valor total da proposta é de R$ 6.180.000,00 (Seis milhões cento e oitenta mil reais).

PartnerPRO NETWORK COMMSCOPE RUCKUS Lenovo

Anexo V – Propostas comerciais recebidas

Ao longo dos trabalhos que serviram de base para e elaboração deste documento, foram solicitados, pela CITM e desta EPC, como consequência dos levantamentos do tipo Site Survey, orçamentos estimados de custos totais da implantação de uma infraestrutura completa de rede sem fios neste Regional. Em razão da extensão dos documentos, entendeu-se ser mais adequado juntar a íntegra desses documentos ao processo administrativo que este estudo instrui, e colar aqui apenas a página que contenha o resumo dos valores de cada proposta:

Proposta da empresa TELTEC para rede Wi-Fi 5, em 26/07/2019:

teltec SOLUTIONS

1. **Solução**

Validade da ATA	Item ATA	QTD registrada	Descrição	Valor unit.	ADESÃO ATA UTFPR – TRT23 QTD	Valor Total
09/04/2020	5	2	Controladora Wireless Virtual Cisco licenciada para 5 APs com suporte para até 200 Aps. Garantia de 5 anos.	R$ 3.600,00	1	R$ 3.600,00
	6	390	Licença para expansão de controladora wireless virtual para 1 AP. Garantia de 60 meses.	R$ 720,00	107	R$ 77.040,00
	7	224	Access Point Cisco 1852I 802.11ac Wave2 Dual Band MIMO 4x4 com 3 spatial streams - Mobility Express para até 50 Aps. Garantia de 5 anos.	R$ 5.200,00	112	R$ 582.400,00
	8	120	Injetor PoE Cisco	R$ 420,00	60	R$ 25.200,00
	9	2	Serviço de configuração da solução wireless	R$ 20.000,00	1	R$ 20.000,00
					Total	R$ 708.240,00

2. **Condições gerais da proposta**
   a. Forma de pagamento
      i. Pagamento dos produtos (equipamentos e licenças) em até 15 dias após o recebimento
      ii. Pagamento dos serviços em até 15 dias após a execução
   b. Validade da proposta
      i. Proposta válida por 30 dias
   c. Prazo de entrega dos produtos
      i. Produtos serão entregues em até 75 dias corridos após o recebimento da ordem de compra
   d. Prazo de entrega dos serviços
      i. Os serviços terão seu início em até 30 dias corridos após o recebimento total dos produtos (equipamentos e licenças)

3. **Dados cadastrais da Teltec Solutions**

Razão social: Teltec Solutions Ltda
Nome fantasia: Teltec Solutions
Endereço: R. Miguel Daux, 100 - Coqueiros - Florianópolis/SC - CEP 88080-220
Telefone: 48 3031-3450 | Email: teltec@teltecsolutions.com.br
CNPJ: 04.892.991/0001-15 | I.E: 254.353.290
Dados Bancários – Banco do Brasil | Agência: 3077-5 |Conta: 7555-8

Proposta da empresa TELTEC para uma rede Wi-Fi 6, em 11/06/2021:

teltec SOLUTIONS

1) INVESTIMENTO

ITEM	PN/DESCRIÇÃO	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	ACCESS POINT Cisco Catalyst 9105 • WiFi 6 • MIMO 2x2 • Licença software de gerenciamento • Licença para a controladora • Garantia de 36 meses	75	R$ 5.400,00	R$ 405.000,00
2	ACCESS POINT Cisco Catalyst C9115 • WiFi 6 • MIMO 4x4 • Licença software de gerenciamento • Licença para a controladora • Garantia de 36 meses	45	R$ 9.940,00	R$ 447.300,00
	ACCESS POINT Cisco Catalyst C9120 • WiFi 6 • MIMO 4x4 • Licença software de gerenciamento • Licença para a controladora • Garantia de 36 meses	30	R$ 13.200,00	R$ 396.000,00
3	Injetor PoE 802.3at	150	R$ 790,00	R$ 118.500,00
4	CONTROLADORA VIRTUAL Cisco Catalyst 9800-CL com Suporte e Garantia de 36 Meses	2	R$ 5.750,00	R$ 11.500,00
5	SOFTWARE DE GERENCIAMENTO – Cisco Prime Infrastructure com Suporte e Garantia de 36 Meses	1	R$ 1.500,00	R$ 1.500,00
VALOR TOTAL DA PROPOSTA				R$ 1.379.800,00

2) CONDIÇÕES GERAIS DESTA PROPOSTA:

- **Condições gerais:** Os valores apresentados são válidos somente para o quantitativo e cliente final descrito nesta proposta. Qualquer ajuste no quantitativo e/ou cliente final pode requerer uma atualização na proposta e seus valores;
- Os valores apresentados acima contêm todos os impostos, taxas, frete e demais despesas que venham a incidir sobre o valor da proposta;
- Todos os itens apresentados estão em REAIS BRASILEIRO (R$), exceto se especificado individualmente;

- **Prazo de entrega dos produtos e serviços:** Os produtos cotados possuem prazo de entrega padrão de 120 dias, contados a partir da assinatura/recebimento de ordem de fornecimento ou instrumento equivalente, podendo vir a ser reduzido conforme disponibilidade nos estoques. Consulte o representante de vendas para maior detalhamento;

- **Validade da proposta:** Esta proposta é válida por 30 dias. Em caso de a taxa câmbio do dólar americano ultrapassar R$ 5,30, esta proposta perde automaticamente sua validade;

- **Pagamento:** em até 30 dias após a emissão da Nota Fiscal;

- **Confidencialidade:** Garantimos a confidencialidade das informações, dados, senhas e documentos que venha a ter acesso em razão de execução dos produtos/serviços adquiridos.

- **Faturamento em notas fiscais distintas:** Em consonância com a legislação tributária vigente, a Teltec Solutions adota o mesmo formato de faturamento praticado por seus fornecedores, sejam eles fabricantes, desenvolvedores, licenciantes ou importadores, fornecendo os itens de hardware como

TELTEC 30 ANOS. TRANSFORMAR É O NOSSO DESAFIO!

Proposta da empresa ZOOM para uma rede Wi-Fi 6, em 13/07/2021:

TRT 23ª

ZOOM tecnologia

SOLUÇÃO A SER IMPLEMENTADA

Item	Modelo	Descrição	Quantidade	Valor Unitario	Valor Total
1	ZoomCloud-MGT	Licença para Sistema de Gerenciamento NCE-IMaster Campus em Nuvem para Ponto de Acesso AirEngine 5760-51, por 5 anos.	144	R$ 320,57	R$ 46.162,08
2	ZoomCloud-MGT	Licença para Sistema de Gerenciamento NCE-IMaster Campus em Nuvem para Controladora AC6508, por 5 anos.	2	R$ 5.187,20	R$ 10.374,40
3	ZoomCloud-NAC	Licença para Sistema de Autenticação NCE-IMaster Campus em Nuvem para para 1.000 usuarios simultaneos, por 5 anos.	1000	R$ 4,46	R$ 4.456,33
4	ZoomCloud-Analytics	Licença para Sistema analitico NCE-IMaster Insight para configuração automatica de rede através de IA, com localicação geografica de terminais e dispositivos RFID com identificação de aplicação de camada 3 a 7 sendo executadas na rede, por 5 anos.	1	R$ 248.339,52	R$ 248.339,52
5	AC6508	Controladora AC6508 para até 256 pontos de acesso, com capacidade de atuar em alta disponibilidade, com 5 anos de garantia.	2	R$ 9.490,97	R$ 18.981,94
6	AirEngine 6760-51	Ponto de Acesso indoor WIFI 6 (802.11ax) mid-end, capacidade de comutação de 5.37 Gbps, MiMo 4x4, suporte de 1024 usuarios simultaneos e garantia de 5 anos.	144	R$ 2.605,24	R$ 375.154,56
7	W0ACP8E11	Injeto PoE++ para ponto de acesso AirEgine, com 5 anos de garantia	144	R$ 942,07	R$ 135.658,08
				Valor Total Geral	R$ 839.126,91

Condições Comerciais

- Os valores que porventura forem apresentados em US$ (dólares americanos) deve ser convertidos em R$ (reais), e será utilizada a cotação do dólar (PTAX = 5,3)

- Os valores devem ser expressos em reais, fixos por 12 meses, considerando todos os impostos e frete:

- Os valores poderão ser pauta de renegociação no caso da Ptax informada na proposta varie + ou - 10%.

- Os equipamentos serão faturados e entregues nas lojas.

- A ZOOM Tecnologia poderá rever a validade desta Proposta sempre que ocorrer um fato ou ato superveniente que resulte na imposição de um ônus excessivo refletido nos valores e preços apresentados.

- A ZOOM Tecnologia poderá rever a validade desta proposta sempre que ocorrer um fato ou ato superveniente que resulte na imposição de um ônus excessivo refletido nos valores e preços apresentados.

Proposta da empresa TELTEC, em 31/08/2021:

teltec SOLUTIONS

1) INVESTIMENTO

		Q	A	B	C=A+B	Q*C
ITEM	PN/DESCRIÇÃO	QTD	VALOR UNITÁRIO NF PRODUTO	VALOR UNITÁRIO NF SOFTWARE/SERVIÇO	VALOR UNITÁRIO CONJUGADO	VALOR TOTAL CONJUGADO
WLAN SECURITY						
1	CONTROLADORIA/FIREWALL PEQUENO PORTE PARA UNIDADES REMOTAS COM SUPORTE E GARANTIA DE 60 MESES. Modelo: FOTINET FG-40F	24	R$ 933,26	R$ 2.828,43	R$ 3.761,69	R$ 90.280,58
2	CONTROLADORIA/FIREWALL PARA UNIDADE CENTRAL COM SUPORTE E GARANTIA DE 60 MESES. Modelo: FOTINET FG-200F	1	R$ 7.870,39	R$ 22.269,55	R$ 30.139,94	R$ 30.139,94
3	ACCESS POINT INDOOR – FORTINET FAP-231F-N • WiFi 6 • Tri radio, 802.11 a/b/g/n/ac/ax 2x2 MU-MIMO • 2x 10/100/1000 RJ45 port, BT/BLE • 1x Type A USB • 1x RS-232 RJ45 Serial Port • Kit de montagem incluso Garantia de 60 meses	150	R$ 5.361,17	R$ 1.571,69	R$ 6.932,86	R$ 1.039.928,65
4	ACCESS POINT INDOOR – FORTINET FAP-431F-N • WiFi 6 • Tri radio (2x 802.11 a/b/g/n/ac/ax, 4x4 MIMO e 1x 802.11 a/b/g/n/ac Wave 2, 2x2 MU-MIMO) • 1x 10/100/1000/2500 Base-T RJ45 • 1x 10/100/1000 Base-T RJ45 • 1x Type A USB • 1x RS-232 RJ45 Serial Port. • Kit de montagem incluso Garantia de 60 meses	20	R$ 7.791,47	R$ 2.284,05	R$ 10.075,52	R$ 201.510,39
5	Injetor PoE Gigabit 802.3at	50	R$ 1.121,23		R$ 1.121,23	R$ 56.061,55
VALOR TOTAL WLAN SECURITY						R$ 1.417.921,12

Proposta da empresa YSSY, em 01/09/2021:

YSSY

CLIENTE: TRT 23ª Região
PROPOSTA: AY-2021-03-17454
DATA: 1-set-21
CONTATO: Rogério M. Pimenta
E-MAIL: rogeriopimenta@trt23.jus.br
FONE: -

Rede WiFi

Item	Part Number	Descrição	Qtde.	Tipo	IPI %	ICMS %	ISS %	Valor unitário	Valor Total
1	ITEM 1 - Solução de Controle e Gerência da Rede Wifi								
1.1	OV-AP-NM-100-N	OV-AP-NM-100-N OV2500 NM R4 Lic - Lic. 100 AP-NEW for 10 ALU-E Stellar	2	SFW			2%	42.181,40	84.362,80
1.2	OV-GA-1K-N	OV-GA-1k-N - OV2500 GA R4 Lic. - Lic. 1000 GA-NEW for Guest Access	1	SFW			2%	62.102,86	62.102,86
1.3	OV-BYOD-1K-N	OV2500 BYOD R4 Lic. - Lic 1000 BOYD-NEW for BYOD Access Policy Manager	1	SFW			2%	62.102,86	62.102,86
1.4	PW3N-OVAPNM100	5YR 24X7 Partner SUPPORT for OV2500 NMS - RELEASE 4 OV-AP-NM-100-N.	2	SFW			2%	33.949,20	67.898,40
1.5	PW3N-OVBYOD1KN	5YR 24X7 Partner SUPPORT Software for OV2500 NMS - R4 OV-BYOD-1K-N	1	SFW			2%	43.812,83	43.812,83
1.6	PW3N-OVGA500N	5YR 24X7 Partner SUPPORT Software OV2500 NMS - RELEASE 4 OV-GA-500-N	1	SFW			2%	36.644,02	36.644,02
2	ITEM 2 - Pontos de Acesso da Rede Sem Fio								
2.1	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	HW		17%		6.281,06	1.256.212,00
2.2	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	SFW			2%	3.138,92	627.784,00
2.3	OAW-AP-MNT-W10	10 Pack. Mounting kit, Type A ceiling/wall mount	20	HW		17%		1.634,23	32.684,60
2.4	PW3R-OAWAP1301	5 Yr Renew Partner Support Software for OAWAP1301	200	SFW			2%	347,72	69.544,00
								SUB-TOTAL HW:	1.288.896,60
								SUB-TOTAL SOFTWARES E LICENÇAS:	1.054.251,79
								SUB-TOTAL SERVIÇOS:	-
								TOTAL Rede WiFi:	2.343.148,39

R$ 2.343.148,39 dois milhões, trezentos e quarenta e três mil, cento e quarenta e oito reais e trinta e nove centavos

CONDIÇÕES COMERCIAIS

PRAZO DE ENTREGA:	Em até 60 dias, contados a partir da data de confirmação do pedido com aceite formal. (O prazo está sujeito a alteração sem prévio aviso, conforme disponibilidade de estoque.)
VALIDADE DA PROPOSTA:	60 dias.
PAGAMENTO:	30 dias após aceite definitivo.
IMPOSTOS:	Inclusos de acordo com a legislação vigente. (Serão repassados aos valores ainda não faturados quaisquer variações que venham ocorrer nas alíquotas existentes.)
FRETE E SEGURO:	Inclusos.
GARANTIA:	60 meses

Atenciosamente,

Abilio Cardoso Chaves Filho
Gerente de Contas
(61) 99921-4427
abilio.chaves@yssy.com.br

Proposta da empresa YSSY, em 09/05/2022:

yssy

CLIENTE:	TRT 23ª Região
PROPOSTA:	AY-2021-03-17454
DATA:	9-mai-22
CONTATO:	Rogério M. Pimenta
E-MAIL:	rogeriopimenta@trt23.jus.br
FONE:	-

Rede WiFi

Item	Part Number	Descrição	Qtde.	Tipo	IPI %	ICMS %	ISS %	Valor unitário	Valor Total
1	ITEM 1 - Controladora Wireless + Solução de Gerenciamento e Controle de Acesso a Rede Wifi								
1.1	OV-AP-NM-100-N	OV-AP-NM-100-N OV2500 NM R4 Lic - Lic. 100 AP-NEW for 10 ALU-E Stellar	2	SFW			2%	32,311.04	64,622.08
1.2	OV-GA-1K-N	OV-GA-1k-N - OV2500 GA R4 Lic. - Lic. 1000 GA-NEW for Guest Access	1	SFW			2%	51,031.84	51,031.84
1.3	OV-BYOD-1K-N	OV2500 BYOD R4 Lic. - Lic 1000 BOYD-NEW for BYOD Access Policy Manager	4	SFW			2%	52,733.75	210,935.00
1.4	PW5N-OVAPNM100	5YR 24X7 Partner SUPPORT for OV2500 NMS - RELEASE 4 OV-AP-NM-100-N.	2	SFW			2%	24,574.97	49,149.94
1.5	PW5N-OVBYOD1KN	5YR 24X7 Partner SUPPORT Software for OV2500 NMS - R4 OV-BYOD-1K-N	4	SFW			2%	33,844.15	135,376.60
1.6	PW5N-OVGA500N	5YR 24X7 Partner SUPPORT Software OV2500 NMS - RELEASE 4 OV-GA-500-N	1	SFW			2%	27,107.38	27,107.38
2	ITEM 2 - Pontos de Acesso da Rede Sem Fio								
2.1	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	HW		17%		6,846.92	1,369,384.00
2.2	OAW-AP1321-RW	OmniAccess Stellar Indoor AP1321. Dual radio	200	SFW			2%	3,105.01	621,002.00
2.3	OAW-AP-MNT-W10	10 Pack. Mounting kit, Type A ceilling/wall mount	20	HW		17%		1,612.52	32,250.40
2.4	PW5R-OAWAP1301	5 Yr Renew Partner Support Software for OAWAP1301	200	SFW			2%	326.76	65,352.00
2.5	Power Injector	Power Injector (802.3at) for Access Points	1	HW				660.08	660.08
								SUB TOTAL HW:	1,402,294.48
								SUB-TOTAL SOFTWARES E LICENÇAS:	1,224,576.84
								SUB-TOTAL SERVIÇOS:	-
								TOTAL Rede WiFi:	2,626,871.32

R$ 2,626,871.32 dois milhões, seiscentos e vinte e seis mil, oitocentos e setenta e um reais e trinta e dois centavos

CONDIÇÕES COMERCIAIS

PRAZO DE ENTREGA:	Em até 90 dias, contados a partir da data de confirmação do pedido com aceite formal. (O prazo está sujeito a alteração sem prévio aviso, conforme disponibilidade de estoque.)
VALIDADE DA PROPOSTA:	60 dias.
PAGAMENTO:	conforme edital
IMPOSTOS:	Inclusos de acordo com a legislação vigente. (Serão repassados aos valores ainda não faturados quaisquer variações que venham ocorrer nas aliquotas existentes.)
FRETE E SEGURO:	Inclusos.
GARANTIA:	60 meses

Atenciosamente,

Abilio Cardoso Chaves Filho
Gerente de Contas
(61) 99921-4427
abilio.chaves@yssy.com.br

yssy.com.br

Proposta da empresa SERVIX, em 06/04/2023:

SERVIX

SOLUÇÃO PROPOSTA

Cenário #1 – Solução de rede sem fio com Ruckus
A fim de endereçar uma solução, propomos o cenário abaixo.

Item	Part Number	Descrição	Quant.
01	901-R350-WW02	Access Point Ruckus R350 dual-band 802.11abgn/ac/ax Wireless Access Points, 2x2:2 streams (2.4GHz/5GHz) OFDMA, MU-MIMO, BeamFlex+	97
	902-0120-0000	Kit de suporte para montagem de Access Point Ruckus R-Series Indoor AP. Para parede, teto, poste ou treliça	97
02	901-R650-WW00	Access Point Ruckus R650 dual-band 802.11abgn/ac/ax Wireless Access Point com interface Multi-Gigabit Ethernet e backhaul, 4x4:4 + 2x2:2 streams, OFDMA, MU-MIMO, BeamFlex+, dual ports, PoH/uPoE/802.3at PoE support.	176
	902-0120-0000	Kit de suporte para montagem de Access Point Ruckus R-Series Indoor AP. Para parede, teto, poste ou treliça	176
03	L09-VSCG-WW00	Controladora Virtual Ruckus SmartZone software virtual appliance, para 1 instância, incluindo 1 licença de AP	01
04	L09-0001-5G00	Licenciamento para gerenciamento de AP para Ruckus Smartzone SZ-100/vSZ 3.X/SCG200/SZ300	273
05	S01-VSCG-3L00	Suporte e garantia End User WatchDog Support - VSZ-RTU, 3 YR	01
06	902-0162-BR00	Injetor PoE	97
07	S62-0001-3LSG	Suporte e garantia especializados da Ruckus	273
08	-	Treinamento	01
09	-	Serviço de configuração e instalação lógica - Configuração de controladora - Site survey preditivo detalhado com análise de requisitos para propagação de rádio 802.11 utilizando ferramenta Ekahau em 26 localidades (remoto) - Configuração de SSID para rede corporativa em 802.1x e rede visitantes com captive portal - Configuração de plano de canais e banda conforme site survey preditivo - Instalação física dos APs na sede com altura de até 3m - Documentação Asbuilt	01

Nota: Os injetores PoE estão sendo considerado apenas para unidades remotas. Estamos considerando instalação lógica dos equipamentos levando em consideração que o ambiente possui infraestrutura pronta para conectividade com a solução Wi-Fi e que não é necessário nenhum tipo de intervenção na estrutura ou nenhum tipo de obra civil.

servix.com 10 | Página

QUANTITATIVO ESTIMADO POR LOCALIDADE

LOCAL	QUANTIDADE	MODELO
Confresa	4	R350
Alta Floresta	5	R350
Alto Araguaia	4	R350
Barra do Garças	6	R350
Cáceres	6	R350
Campo Novo	4	R350
Colíder	4	R350
Colniza	4	R350
Água Boa	5	R350
Diamantino	5	R350
Jaciara	5	R350
Juara	4	R350
Mirassol	4	R350
Nova Mutum	4	R350
Peixoto de Azevedo	4	R350
Primavera do leste	4	R350
Rio Verde	4	R350
Sapezal	4	R350
Sorriso	5	R350
Várzea Grande	12	R350
Rondonópolis	8	R650
Sinop	7	R650
Prédio Administrativo	48	R650
Fórum Trabalhista	40	R650
Prédio Corte	33	R650
Sede	40	R650
	Total R350	**97**
	Total R650	**176**
	TOTAL	**273**

O TRT23 está divido em diversas localidades (varas) espalhadas pelo estado do Mato Grosso. As áreas possuem uma altura média de 3 a 5m. Estamos considerando conexão em frequências 2.4GHz e 5GHz com dispositivos variados de notebooks, smartphones e equipamentos coletores operando em ambas as frequências, podendo chegar em 250 dispositivos simultâneos por AP caso todos eles sejam de tecnologia 802.11ax ou superior com antenas 3X3:3 para cada dispositivo. A estimativa de Access Point foi feita utilizando a ferramenta considerando uma

avaliação de usuários, densidade de dispositivo e utilização básica de tráfego, não foi considerado apenas cobertura no mapa de calor para propagação de sinal.

INVESTIMENTO

Nosso compromisso é o de propor soluções com qualidade e eficiência, agregando valor ao seu negócio. Razão pela qual nos empenhamos para propor valores que acreditamos ser competitivos com o mercado.

Cenário #01: Venda Direta | Solução Ruckus com AP R650 & AP R350

Item	Categoria	Quant.	Valor Unitário	Valor total
01	901-R350-WW02	97	R$ 4.298,00	R$ 416.906,00
	902-0120-0000	97	R$ 221,00	R$ 21.437,00
02	901-R650-WW00	176	R$ 6.642,00	R$ 1.168.992,00
	902-0120-0000	176	R$ 221,00	R$ 38.896,00
03	L09-VSCG-WW00	01	R$ 3.537,00	R$ 3.537,00
04	L09-0001-SG00	273	R$ 356,00	R$ 97.188,00
05	S01-VSCG-3L00	01	R$ 3.636,00	R$ 3.636,00
06	902-0162-BR00	97	R$ 437,00	R$ 42.389,00
07	S62-0001-3LSG	273	R$ 367,00	R$ 100.191,00
08	Serviço - Treinamento	01	R$ 36.887,00	R$ 36.887,00
09	Serviço de configuração e instalação lógica.	01	R$ 182.706,00	R$ 182.706,00
			Total Global	**R$ 2.112.785,00**

O Valor de instalação dos Access Point está considerando ambientes de até 3m de altura com instalação apenas na capital em Cuiabá Mato Grosso

As informações acima podem não refletir exatamente a forma ou conteúdo das notas fiscais. Em caso de dúvida, solicite o envio de um "espelho de nota fiscal" para conferência das informações.

Proposta da empresa LETTEL, em 05/05/2023:

lettel
Cloud Enterprise

PROPOSTA DE PREÇOS

São José- SC, 05 de maio de 2023.
PROPOSTA LT-8-05/23

Ao
Tribunal Regional do Trabalho da 23ª Região – TRT23

A/C.: Sr. Rogério M. Pimenta
Secretaria de Tecnologia da Informação e Comunicações
E-mail: rogeriopimenta@trt23.jus.br

REF: Orçamento para aquisição de Solução de Rede WiFi

Prezados Senhores,

A **LETTEL DISTRIBUIDORA DE TELEFONIA LTDA**, inscrita no CNPJ sob o nº 07.789.113/0001-67, com sede na Rua Osni João Vieira, 205, Campinas, São José, SC, CEP: 88.101-270 vem respeitosamente apresentar a V.S, a proposta de preços para aquisição de solução de rede WiFi.

DESTACAMOS QUE A VALIDE DESTA PROPOSTA ESTA CONDICIONADA A ACEITAÇÃO DOS REQUISITOS TÉCNICOS APRESENTADOS ANTERIORMENTE POR E-MAIL, NO DIA 03 DE ABRIL DE 2023.

GRUPO	ITEM	DESCRIÇÃO	QTD.	VLR. UNITÁRIO	VLR. TOTAL
1	1.1	Ponto de Acesso Wi-Fi 6 Indoor Marca: **Alcatel-Lucent** Modelo: **OAW-AP1321-RW**	200	R$ 13.280,00	R$ 2.656.000,00
	1.2	Injetor de energia PoE Modelo: **PD-9001GR/AT/AC**	200	R$ 700,00	R$ 140.000,00
	1.3	Controladora Wireless Marca: **Alcatel-Lucent** Modelo: **OmniVista 2600**	2	R$ 120.000,00	R$ 240.000,00
	1.4	Solução de Gerenciamento e Controle de Acesso à Rede Marca: **Alcatel-Lucent** Modelo: **OmniVista 2600**	1	R$ 200.000,00	R$ 200.000,00
	1.5	Instalação	1	R$ 160.000,00	R$ 160.000,00
	1.8	Transferência de conhecimento "hands on"	1	R$ 170.000,00	R$ 170.000,00
VALOR TOTAL DO GRUPO					**R$ 3.688.000,00**

Lettel Distribuidora de Telefonia Ltda
CNPJ: 07.789.113/0001-67
+55 51 3223.2300
+55 51 3223.2300
marketing@lettel.com.br
www.lettel.com.br
Av. Dr. Carlos Barbosa, 293
Cep: 90880-001 | Porto Alegre/RS