COORDENAÇÃO GERAL DE RECURSOS LOGISTICOS MCID

Estudo Técnico Preliminar 28/2025

1. Informações Básicas

Número do processo: 80000.000344/2024-33

2. Descrição da necessidade

Trata-se de Estudo Técnico Preliminar da contratação que objetiva identificar a mais eficaz solução para a aquisição de ativos de infraestrutura de TIC visando atender às necessidades presentes e futuras do Ministério das Cidades.

Com a promulgação da Lei nº 14.600/2023, que deu origem ao Ministério das Cidades (MCID), mediante o desmembramento do Ministério do Desenvolvimento Regional (MDR), houve a necessidade de transferir competências e incumbências previamente atribuídas ao órgão extinto /transformado.

De acordo com o Decreto nº 11.468, de 5 de abril de 2023, o Ministério das Cidades (MCID) tem como áreas de competência os seguintes assuntos:

I - política de desenvolvimento urbano e ordenamento do território urbano;

II - políticas setoriais de habitação e de saneamento ambiental, incluídas as políticas para os pequenos Municípios e a zona rural;

III - política setorial de mobilidade e trânsito urbano;

IV - promoção de ações e programas de habitação e de saneamento básico e ambiental, incluída a zona rural;

V - promoção de ações e programas de urbanização, de desenvolvimento urbano, de transporte urbano e de trânsito;

VI - política de financiamento e subsídio ao desenvolvimento urbano, à habitação popular, ao saneamento e à mobilidade urbana;

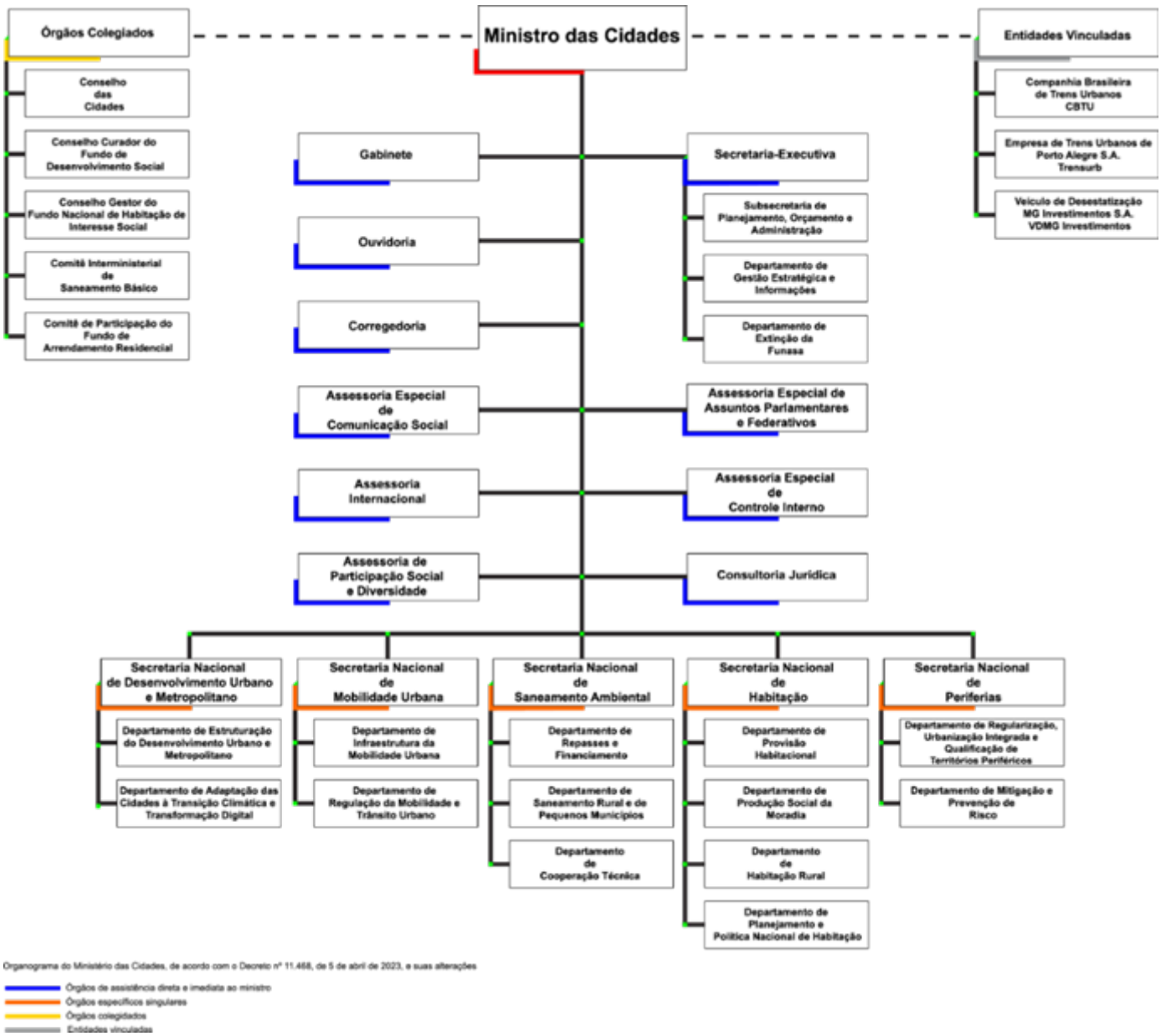
VII - planejamento, regulação, normatização e gestão da aplicação de recursos em políticas de urbanização, habitação e saneamento básico e ambiental, incluída a zona rural;

VIII - planejamento, regulação, normatização e gestão da aplicação de recursos em políticas de desenvolvimento urbano e de mobilidade e trânsito urbanos; e

IX - participação na formulação das diretrizes gerais para conservação dos sistemas urbanos de água e para adoção de bacias hidrográficas como unidades básicas do planejamento e da gestão do saneamento.

Atualmente a Estrutura Organizacional do Ministério das Cidades (MCID) compõe-se por:

IMAGEM 1 - ESTRUTURA ORGANIZACIONAL DO MCID



No âmbito governamental, a Tecnologia da Informação desempenha um papel fundamental na execução de políticas, no atendimento às demandas da população e na eficácia das operações.

Nesse contexto, torna-se imperativa uma seleção minuciosa de ferramentas tecnológicas que não devem apenas atender às necessidades imediatas, mas também criar um ambiente versátil, colaborativo e eficaz.

A Coordenação Geral de Tecnologia da Informação (CGTI) desempenha um papel essencial como provedor de tecnologias computacionais e sistemas de informação. Sua responsabilidade principal é oferecer soluções de informática eficientes e confiáveis, com o objetivo de aprimorar consideravelmente a qualidade dos serviços oferecidos à população. Adicionalmente, a CGTI é encarregada de gerenciar e supervisionar as iniciativas de informatização destinadas aos sistemas internos do Ministério das Cidades.

A Coordenação-Geral de Tecnologia da Informação (CGTI) é a responsável por desenvolver, aperfeiçoar, manter e dar suporte aos sistemas informatizados e aos bancos de dados no âmbito do MCID, administrando os recursos de informação e informática do órgão. Todas as áreas desse Ministério dependem de serviços específicos de Tecnologia da Informação para o desempenho de suas atividades.

As demandas da Tecnologia da Informação exigem métodos e ferramentas que garantam o nível de qualidade para atender às expectativas dos clientes e usuários, ao mesmo tempo em que acompanham a constante evolução de suas necessidades.

O projeto tem como principal escopo o fornecimento de uma infraestrutura de conectividade robusta e moderna para o Ministério das Cidades. A necessidade de aquisição dos ativos decorre da mudança de sede, que demanda uma atualização tecnológica capaz de suportar as operações essenciais e garantir conectividade eficiente em todas as áreas do novo edifício.

O escopo do projeto inclui a implementação de soluções de rede local (LAN) e rede sem fio (WLAN), com a seguinte infraestrutura:

1. **Switches Core**: Equipamentos de alta capacidade que formam o núcleo da rede. Esses switches proporcionam a interconexão entre os switches de acesso, garantindo máxima performance, resiliência e eficiência no tráfego de dados. São responsáveis pela agregação de tráfego e pela conexão com os servidores e outras redes.

2. **Switch Acesso - Tipo 01**: Switches de acesso de primeira linha que atendem a áreas com menor densidade de dispositivos ou com necessidades específicas de conectividade. Eles podem oferecer características diferenciadas, como menor número de portas ou opções de gerenciamento simplificado.

3. **Switch Acesso - Tipo 02**: Switches de acesso de segunda linha que fornecem conectividade a dispositivos finais, como computadores e impressoras. Estes switches oferecem suporte a uma variedade de portas e recursos, adequados para ambientes com alta demanda de largura de banda e alta densidade de dispositivos.

4. **Ponto de Acesso Sem Fio - Indoor**: Dispositivos destinados a fornecer conectividade sem fio dentro de ambientes internos. Estes pontos de acesso garantem uma cobertura de sinal eficiente e estável para dispositivos móveis, laptops e outros equipamentos que necessitam de conexão wireless.

5. **Sistema de Gerenciamento em Nuvem**: Plataforma baseada na nuvem que permite a administração e monitoramento centralizado da rede. Facilita a configuração, a atualização de firmware e o gerenciamento de dispositivos de rede, oferecendo relatórios e análises detalhadas sobre o desempenho e a segurança da rede.

6. **Controladora WLAN**: Equipamento responsável pela gestão centralizada dos pontos de acesso sem fio. A controladora WLAN assegura a integração eficiente dos pontos de acesso, otimiza o desempenho da rede sem fio e garante uma cobertura uniforme e segura.

7. **Rack**: Estrutura física utilizada para montar e organizar os equipamentos de rede, como switches, controladoras e servidores. O rack proporciona um espaço ordenado e acessível para a instalação e manutenção dos componentes de rede, garantindo uma melhor gestão do cabeamento e a ventilação adequada dos equipamentos.

A implementação desta infraestrutura é crucial para assegurar que o Ministério das Cidades continue a desempenhar suas funções com eficiência e segurança, atendendo às demandas crescentes por serviços digitais e comunicação interna. Além de atender às necessidades imediatas, esta atualização permitirá que o Ministério se prepare para futuras expansões e inovações tecnológicas.

Este estudo tem como objetivo identificar o melhor cenário para a implementação de uma solução integrada de rede local (LAN) e rede sem fio (WLAN) no Ministério das Cidades. Essa iniciativa é motivada pela iminente mudança de sede deste órgão, o que requer a aquisição de uma solução moderna e eficiente para garantir a conectividade tanto local quanto sem fio. Além disso, há a necessidade de atualizar o parque de ativos existente na Esplanada dos Ministérios Bloco E, atualmente equipado com dispositivos sem garantia e com mais de 10 anos de uso. Este cenário foi detalhado na pesquisa realizada por e-mail (SEI nº 5065707) ao Ministério da Integração e do Desenvolvimento Regional (MIDR), que atualmente é o órgão provedor, conforme estabelecido na Portaria MGI nº 43, de 31 de janeiro de 2023.

A infraestrutura de rede é fundamental para o funcionamento eficiente das operações internas, abrangendo a comunicação de dados em ambientes cabeados e sem fio, incluindo salas, departamentos e setores administrativos. Grande parte dos processos de trabalho é conduzida através de sistemas informatizados que dependem da rede de dados para a troca segura e confiável de informações sensíveis.

Portanto, o portfólio de serviços de infraestrutura de TI do Ministério deve incorporar soluções robustas para redes cabeadas e sem fio, garantindo o suporte necessário para atividades essenciais e administrativas. A implementação de uma rede que seja tanto confiável quanto segura é crucial para assegurar a continuidade dos negócios e otimizar a eficiência operacional.

Outro fator a ser mencionado é que Ministério das Cidades ocupa um prédio que é da FUNASA, e já possui pedido de desocupação para isso foi realizado um levantamento junto ao projeto do prédio que foi projetado a mudança do Ministério e realizado os levantamentos necessários para tal mudança, conforme consta nos anexos com previsões e o o projeto do novo prédio. (5065707, 5249125, 5249128, 5250399).

Neste sentido, considerando que durante os últimos 6 (seis) anos naõ houveram investimentos relevantes em infraestrutura de tecnologia da informaçaõ no âmbito do Ministério, é papel fundamental da área de tecnologia da informaçaõ, atuar na elaboraçaõ de projetos de soluçoẽs de tecnologia da informaçaõ que contemplem todo o cenário de recriaçaõ do Ministério com o foco no alcance das metas institucionais, principalmente aquelas relacionada à transformaçaõ digital, renovaçaõ do parque tecnológico, ampliaçaõ da rede de dados e otimizaçaõ da infraestrutura de tecnologia da informaçaõ, com implementaçaõ de soluçoẽs de segurança da informaçaõ e adaptaçaõ às normas.

Conforme detalha no documento 5065707, todos os ativos de rede não possuem suporte e/ou garantia, os mesmos já encerraram o EoL (não permitem atualizações), significa dizer que o Ministério trabalha com um risco alto de paralisação de sua estrutura, sistematizada da seguinte forma (Operação Switches do fabricante Enterasys):

- 9 Andar: pilha de 7 switches, 5 unidades B5K125-48P2 e 2 unidades B5G125-48P2 com 175 portas ativas de 346
- 8 Andar: pilha de 7 switches, 4 unidades B5K125-48P2 e 3 unidades B5G125-48P2 com 185 portas ativas de 344
- 7 Andar: pilha de 7 switches, 2 unidades B5K125-48P2 e 5 unidades B5G125-48P2 com 138 portas ativas de 340
- 6 Andar: pilha de 7 switches, 7 unidades B5K125-48P2 e 0 unidades B5G125-48P2 com 167 portas ativas de 350
- Térreo: 1 unidades B5K125-48P2 com 25 portas ativas de 50 Com relação aos Access Points é utilizado uma solução corporativa do fabricante Aerohive, ao qual encontrasse habilitado 70 Access Points do modelo AP250 Dual Band PoE de comunicação 802.11 g/n e 802.11a/n/ac, dos quais estão alocados 28 unidades no Bloco E.

Com o novo projeto serão contemplados 10 andares, na NOVA SEDE DO MCID - Antiga PF, com todo projeto descritivo no documento 5250399.

Alinhamento estratégico

O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

ID PCA PNCP: 05465986000199-0-000001/2025

Data de publicação no PNCP: 10/06/2024

Id do item no PCA: 125

Classe/Grupo: 162 - SERVIÇOS DE GERENCIAMENTO EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC)

Identificador da Futura Contratação: 560010-63/2025

O objeto da contratação também está alinhado com a Estratégia Nacional de Governo Digital para o período de 2024 a 2027 disponível no link (https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional), e em consonância com o Plano Diretor de Tecnologia da Informação - PDTI MIDR 2023/2026 (SEI nº 4781512), aprovado pelo Comitê de Governança Digital do Ministério das Cidades, em concordância com a Nota nº 00231/2023/CONJUR-MCID, e a consulta à Secretaria de Governo Digital do MGI.

Objetivos da Estratégia Nacional de Governo Digital:

OBJETIVO	ID	RECOMENDAÇÃO
6 - INFRAESTRUTURA DIGITAL	6.3.	Prover opções de conectividade pública, para acesso gratuito e facilitado a soluções de prestação de serviço digital pela sociedade, especialmente utilizando estrutura de canais de atendimento presencial e outros prédios e equipamentos públicos.
6 - INFRAESTRUTURA DIGITAL	6.4.	Estabelecer iniciativas para prover e qualificar o acesso a infraestruturas de rede, especialmente as de grande tráfego, para maior eficiência de trabalho em prédios e equipamentos públicos, considerando inclusive parcerias e programas nacionais voltados para essa finalidade.

Alinhamento ao Plano Diretor de Tecnologia da Informação - PDTI MIDR 2023/2026:

ALINHAMENTO AO PDTIC 2023-2026	
Id	**Ação**
NC04	Prover melhorias em soluções corporativas de TIC.
A64	Adquirir Ativos de Rede.
A65	Adquirir Solução de WiFi.

Em face da abrangência e da capilaridade dos resultados a serem alcançados, no sentido de propiciar o aumento de produtividade e o crescimento da maturidade funcional do MCID, a Coordenação-Geral de Tecnologia da Informação (CGTI) busca, de forma contínua, a atualização da infraestrutura tecnológica desta Pasta, com vistas a garantir o alto índice de disponibilidade das aplicações e dos serviços com desempenho, qualidade e segurança, o que para a manutenção desse grau de excelência, implica na constante procura ou pesquisa por novas tecnologias e pela manutenção e a sustentação adequada das Soluções de TIC já implantadas, em consonância com os avanços tecnológicos disponíveis no mercado especializado, as necessidades organizacionais e as disposições legais vigentes.

Motivação/Justificativa

O Ministério das Cidades apresenta uma carência crítica de infraestrutura de rede lógica, o que torna indispensável a aquisição de uma solução abrangente e integrada para garantir conectividade eficiente, segura e contínua. A ausência de uma infraestrutura pré-existente capaz de suportar as operações diárias do Ministério sublinha a urgência dessa iniciativa.

Cabe registrar que a Coordenação-Geral de Tecnologia da Informação realizou um levantamento do quadro de pessoal que tem acesso a desktops deste Ministério, abrangendo todas as modalidades de vínculo empregatício (servidores, terceirizados, estagiários, consultores e temporários), conforme processo de levantamento nº 80000.012620/2023-25, considerando a situação atual e previsão futura:

CONSOLIDADO												
UNIDADE	TOTAL DE SERVIDORES			QUANTIDADE DE TERCEIRIZADOS			QUANTIDADE DE ESTAGIÁRIO			QTDE. DE USUÁRIOS QUE TEM ACESSO AO COMPUTADOR DO MINISTÉRIO		
	ATUAL	PREVISÃO FUTURA	PERCENTUAL DE CRESCIMENTO	ATUAL	PREVISÃO FUTURA	PERCENTUAL DE CRESCIMENTO	ATUAL	PREVISÃO FUTURA	PERCENTUAL DE CRESCIMENTO	ATUAL	PREVISÃO FUTURA	PERCENTUAL DE CRESCIMENTO
Total MCID	552	884	≈ 60.14	244	698	≈ 186.06	0	68	-	740	1527	≈ 106.35

Ocorre que todos os equipamentos que compõem a rede lógica do Ministério, como por exemplo: switches, access points, roteadores e controladoras de rede sem fio estão obsoletos, apresentando constantemente problemas físicos que causam indisponibilidades, colocando em risco a continuidade do negócio do Ministério uma vez que até mesmo os switches cores encontra-se obsoletos e sem cobertura contratual para suporte com reparos e substituição de peças e componentes. Desta forma, em caso de falhas destes equipamentos há o risco de que vários sistemas fiquem indisponíveis, por horas e até dias dependendo da gravidade do problema.

Ressalta-se ainda que, por suas condições de obsolescência, atualmente todos os switches do Ministério são pontos de vulnerabilidade colocando em risco a disponibilidade dos serviços, além de impossibilitar a implementação de soluções de segurança de rede mais adequadas às necessidades do Ministério uma vez que não há garantia de compatibilidade dos recursos de segurança atuais com os equipamentos defasados.

A nova sede está com projeto pronto conforme descritivo documento: 5250399, que contempla 10 andares, e toda uma topologia de rede deverá ser confeccionada nesse prédio, diante disso vem a necessidade desse projeto, pois sem os ativos necessários o novo prédio não terá a conectividade necessária para o funcionamento, assim paralisando os serviços do Ministério.

Com o crescimento do quantitativo de pontos de acesso físicos e lógicos para equipamentos de tecnologia da informação em uso na rede do Ministério, verifica-se ainda a necessidade de garantir a capacidade em quantitativos de pontos lógicos, assim com a compatibilidade da rede com os novos recursos de telefonia VoIP (voz sob IP), uma vez que há processo de aquisição de tal tecnologia no âmbito do Ministério.

A continuidade dos serviços ofertados pelo Ministério é um dos pilares fundamentais que deve ser preservado. Qualquer interrupção nos serviços prestados pode resultar em sérios transtornos, comprometendo a eficiência dos processos internos e impactando negativamente servidores e colaboradores. Dessa forma, assegurar uma rede robusta e confiável é essencial para manter a operação fluida e eficaz das atividades administrativas e essenciais do Ministério.

Para alcançar esses objetivos, é imprescindível adquirir uma infraestrutura de rede que inclua tanto conectividade cabeada quanto sem fio. A solução deve englobar serviços de implantação, configuração, garantia e suporte técnico, proporcionando uma transição suave para a nova sede e garantindo que todas as necessidades operacionais e de comunicação sejam plenamente atendidas. Tal investimento não só reforçará a capacidade tecnológica do Ministério, mas também assegurará a continuidade e a qualidade dos serviços prestados à população.

Registra-se a intenção de que a Ata de Registro de Preços a ser formalizada terá natureza interna e será destinada exclusivamente ao atendimento das necessidades presentes e futuras do Ministério das Cidades. Essa previsão se fundamenta no planejamento estratégico atualmente em curso, voltado à implantação da infraestrutura de TIC nas unidades já alocadas no Setor Bancário Norte, bem como na futura sede institucional, localizada no Setor de Autarquias Sul, na Antiga sede da Policia Federal em Brasília/DF. A manutenção da ata em caráter interno tem por objetivo resguardar as diretrizes administrativas em desenvolvimento, especialmente no que se refere à validação do projeto arquitetônico (Processo SEI nº 5250399), à definição dos locais de instalação dos equipamentos e à adequação ao cronograma de reformas em andamento.

3. Área requisitante

Área Requisitante	Responsável
COORDENAÇÃO-GERAL TECNOLOGIA DA INFORMAÇÃO	BRUNO LUCENA DE SÁ FREIRE

4. Necessidades de Negócio

Conforme as características da rede de computadores do Ministério das Cidades, já descritas na seção sobre a necessidade, a solução deve atender aos seguintes requisitos para satisfazer as necessidades de negócio da Pasta:

Conectividade Integral: Garantir a conectividade das redes internas dos edifícios Sede e Anexos do Ministério das Cidades. A solução deve permitir a implantação de conectividade eficaz entre sites, serviços e usuários localizados nas diversas unidades do Ministério, possibilitando também a implantação de serviços de telefonia VoIP e soluções de videoconferência.

Infraestrutura Física e Sem Fio: A solução deve contemplar a conectividade da rede física e sem fio, disponibilizando equipamentos que atendam tanto a conectividade cabeada quanto o acesso à rede sem fio. Deve garantir perfeita integração entre os equipamentos, permitindo que os usuários se mantenham conectados com segurança, tendo acesso aos recursos necessários para suas atividades laborais.

Desempenho Otimizado: A solução deve proporcionar a melhor performance de conectividade possível, utilizando os recursos de INFOVIA e acesso à internet para que os usuários acessem os sistemas e serviços do datacenter do Ministério de maneira adequada às suas necessidades.

Projeto de Instalação: A solução deve incluir a elaboração de um projeto de instalação e configuração, permitindo a análise prévia pela equipe técnica do Ministério das Cidades. Isso deve incluir o planejamento de janelas de indisponibilidade e um plano de comunicação para garantir transparência no processo de implementação.

Serviços de Instalação e Operação Assistida: Todos os serviços de instalação e configuração devem ser executados pela CONTRATADA, incluindo um período de operação assistida. Isso evitará sobrecarga da equipe de servidores e colaboradores do Ministério, que deverão acompanhar as atividades para garantir a correta operação da solução após a entrega.

Transferência de Conhecimento: A solução deve incluir treinamento para garantir a transferência de conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do Ministério das Cidades.

Modernização de Equipamentos: A solução deve contemplar todos os equipamentos e serviços necessários para a modernização do parque de switches e redes sem fio nas unidades do Ministério, incluindo a Sede, Anexos e outros, caso venha a existir.

Garantia e Suporte Técnico: A solução deve prever garantia de atualização de softwares e componentes, assistência e suporte técnico por um período mínimo de 60 meses, em regime 24x7. Isso garantirá que, em casos de problemas com os equipamentos críticos, o suporte seja acionado em tempo hábil, reduzindo o risco de indisponibilidade de serviços de conectividade.

Compatibilidade com VoIP: Deve-se garantir que os ativos de rede adquiridos sejam compatíveis com serviços de telefonia VoIP, permitindo a implantação de comunicação eficiente com economia, através da redução do uso de telefonia convencional.

Segurança de Rede: A implementação de uma solução de controle de acesso a rede fortalece a segurança ao autenticar rigorosamente todos os dispositivos que tentam se conectar, garantindo que apenas usuários e equipamentos autorizados tenham acesso. Ele possibilita a segmentação da rede em diferentes níveis de acesso, isolando dispositivos críticos e limitando a propagação de ameaças.

5. Necessidades Tecnológicas

Para garantir a disponibilidade e evitar que falhas em um equipamento causem a indisponibilidade dos serviços, a solução deverá ser baseada em hardware e software projetados especificamente para o roteamento e tráfego de dados. É necessário adotar redundância de equipamentos e links nos locais críticos da rede, como switches core e switches de distribuição, para garantir a continuidade das operações.

Alta Disponibilidade: A solução deve incluir pelo menos dois equipamentos idênticos como switches concentradores (core) para prover alta disponibilidade, a serem instalados na sala cofre do Ministério das Cidades localizada no subsolo do Bloco E da Esplanada dos Ministérios.

Gerenciamento Centralizado: Para garantir o gerenciamento eficiente dos ativos de rede e proporcionar recursos de monitoramento e atualização contínua dos equipamentos, a solução deve contemplar um sistema de gerenciamento centralizado.

Compatibilidade com IPv6: Com a evolução da infraestrutura de rede global e a escassez de endereços IPv4, a solução deve ser totalmente compatível com o protocolo IPv6. Esta compatibilidade garante diversas vantagens, como um espaço de endereçamento maior e segurança aprimorada.

Transição IPv4 para IPv6: Considerando que ainda há serviços em IPv4 no Ministério, é essencial que os novos equipamentos de rede sejam compatíveis com ambos os protocolos IPv4 e IPv6. Isso permitirá que as redes funcionem simultaneamente com ambos durante o período de transição, garantindo conectividade para todos os dispositivos.

Segurança com IPv6: O IPv6 oferece recursos de segurança aprimorados, incluindo autenticação e integridade dos pacotes, dificultando a interceptação e manipulação de dados na rede. Garantir compatibilidade com o IPv6 é vital para manter a segurança da rede do Ministério.

Suporte a Novas Tecnologias: Com o iminente encerramento do IPv4, novas aplicações e tecnologias, como Internet das Coisas (IoT), realidade virtual /aumentada e streaming de alta qualidade, dependerão do IPv6. Portanto, toda aquisição de equipamentos de rede deve ser compatível com IPv6.

Telefonia VoIP: A modernização da rede lógica deve possibilitar a implantação de telefonia VoIP, otimizando a largura de banda, priorizando tráfego, reduzindo latência e jitter, implementando medidas de segurança, e garantindo alta disponibilidade e compatibilidade de equipamentos.

Análise de Site (Site Survey): Para garantir a melhor topologia e distribuição de equipamentos da rede sem fio, será necessário realizar uma análise minuciosa do ambiente de rede (Site Survey), identificando a capacidade de transmissão de dados e possíveis obstruções e gargalos a serem corrigidos.

Redundância de Fontes de Energia: Para minimizar o tempo de indisponibilidade dos switches de acesso e reduzir o risco de falhas devido a problemas elétricos, é exigido que os switches sejam fornecidos com duas fontes de energia redundantes, permitindo conexão a mais de um circuito.

Rede Local Definida por Software (SD-LAN): A solução deve seguir o padrão SD-LAN, que utiliza software para gerenciar e controlar elementos da rede local, tornando-a mais flexível, escalável e ágil. Isso permitirá que o Ministério das Cidades atenda às demandas de crescimento e adaptação contínua de pontos de conexão.

Gerenciamento e Monitoramento: A solução deve incluir recursos de gerenciamento para switches e access points, atendendo às necessidades de monitoramento da rede, permitindo atualizações remotas, especialmente em locais sem profissionais de TI disponíveis.

Alta Disponibilidade: Os equipamentos da rede cabeada e sem fio devem garantir alta disponibilidade, como fontes redundantes, ou serem dimensionados para que os escritórios regionais não dependam de um único equipamento para conectividade com a internet e outras unidades.

Expansão de Equipamentos: Poderão ocorrer substituição dos switches e roteadores existentes no parque de ativos de rede do Ministério das Cidades, será necessário fornecer equipamentos para localidades ainda não atendidas, como nova sede do Ministério.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Requisitos de Negócio

Conforme as características da rede de computadores do Ministério das Cidades, a solução deve atender aos seguintes requisitos:

Conectividade Integral: Garantir a conectividade das redes internas dos edifícios Sede e Anexos do Ministério das Cidades. A solução deve permitir a implantação de conectividade eficaz entre sites, serviços e usuários localizados nas diversas unidades do Ministério, possibilitando também a implantação de serviços de telefonia VoIP e soluções de videoconferência.

Infraestrutura Física e Sem Fio: A solução deve contemplar a conectividade da rede física e sem fio, disponibilizando equipamentos que atendam tanto a conectividade cabeada quanto o acesso à rede sem fio. Deve garantir perfeita integração entre os equipamentos, permitindo que os usuários se mantenham conectados com segurança, tendo acesso aos recursos necessários para suas atividades laborais.

Desempenho Otimizado: A solução deve proporcionar a melhor performance de conectividade possível, utilizando os recursos de INFOVIA e acesso à internet para que os usuários acessem os sistemas e serviços do datacenter do Ministério de maneira adequada às suas necessidades.

Projeto de Instalação: A solução deve incluir a elaboração de um projeto de instalação e configuração, permitindo a análise prévia pela equipe técnica do Ministério das Cidades. Isso deve incluir o planejamento de janelas de indisponibilidade e um plano de comunicação para garantir transparência no processo de implementação.

Serviços de Instalação e Operação Assistida: Todos os serviços de instalação e configuração devem ser executados pela CONTRATADA, incluindo um período de operação assistida. Isso evitará sobrecarga da equipe de servidores e colaboradores do Ministério, que deverão acompanhar as atividades para garantir a correta operação da solução após a entrega.

Transferência de Conhecimento: A solução deve incluir treinamento para garantir a transferência de conhecimento para os servidores e colaboradores que atuam na infraestrutura de TI do Ministério das Cidades.

Modernização de Equipamentos: A solução deve contemplar todos os equipamentos e serviços necessários para a modernização do parque de switches e redes sem fio nas unidades do Ministério, incluindo a Sede, Anexos e outros, caso venha a existir.

Garantia e Suporte Técnico: A solução deve prever garantia de atualização de softwares e componentes, assistência técnica e suporte técnico por um período mínimo de 60 meses, em regime 24x7. Isso garantirá que, em casos de problemas com os equipamentos críticos, o suporte seja acionado em tempo hábil, reduzindo o risco de indisponibilidade de serviços de conectividade.

Compatibilidade com VoIP: Deve-se garantir que os ativos de rede adquiridos sejam compatíveis com serviços de telefonia VoIP, permitindo a implantação de comunicação eficiente com economia, através da redução do uso de telefonia convencional.

Requisitos de Capacitação

A CONTRATADA é responsável pela contínua reciclagem e aprimoramento do conhecimento de seus técnicos, de modo a capacitá-los a atender às demandas atuais e futuras do CONTRATANTE, bem como às atualizações tecnológicas e/ou produtos que vierem a ser implementados durante a vigência contratual. Isso inclui garantir que os técnicos estejam atualizados com as qualificações técnicas mínimas previstas no contrato.

O CONTRATANTE não custeará cursos e/ou treinamentos para os profissionais da CONTRATADA. Toda a responsabilidade por treinamento e atualização contínua recai sobre a CONTRATADA.

Embora não haja requisitos específicos de capacitação para os usuários finais, a CONTRATADA deve promover a divulgação periódica (ou quando solicitado) de informações relacionadas ao acesso, triagem, avaliação e consulta. Isso deve ser feito por meio de publicações ou e-mails institucionais, contendo orientações didáticas e de linguagem simples, como cartilhas, checklists e tutoriais passo a passo.

Requisitos Legais

O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Decreto nº 10.024/2019 (Pregão Eletrônico), Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

Deve-se observar, no que couber, os seguintes normativos:

Lei 12.305/ 2010 - Institui a Política Nacional de Resíduos Sólidos;

Decreto nº 11.462/2023 - Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional;

Decreto nº 11.246/2022 - Regulamenta o disposto no § 3º do art. 8º da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre as regras para a atuação do agente de contratação e da equipe de apoio, o funcionamento da comissão de contratação e a atuação dos gestores e fiscais de contratos, no âmbito da administração pública federal direta, autárquica e fundacional;

Decreto-Lei 200/67 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

Decreto nº 7.174/10 - Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;

Resolução nº 717/2019 - Aprova o Regulamento de Qualidade dos Serviços de Telecomunicações – RQUAL;

Instrução Normativa SGD/MGI nº 6, de 29 de março de 2023 - Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC;

Instrução Normativa SEGES/ME nº 81/2022 - Dispõe sobre a elaboração do Termo de Referência - TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital;

Instrução Normativa SEGES/ME nº 58, de 8 de agosto de 2022 - Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

Portaria SEGES/ME nº 8.678/2021 - Dispõe sobre a Governança das Contratações Públicas no âmbito da Administração Pública federal direta, autárquica e fundacional.

Requisitos de Manutenção

Manutenção Preventiva:

A CONTRATADA deverá realizar manutenções preventivas nos switches adquiridos com uma periodicidade mínima semestral. Estas manutenções devem incluir inspeções de hardware, atualizações de firmware e software, verificação de logs de eventos e execução de testes de desempenho para garantir o funcionamento eficiente e contínuo dos equipamentos.

Manutenção Corretiva:

A CONTRATADA deve garantir a prestação de serviços de manutenção corretiva para os switches, com atendimento técnico disponível 24 horas por dia, 7 dias por semana. O tempo máximo de resposta para o início do atendimento é de 4 horas após a abertura do chamado técnico pela CONTRATANTE.

Substituição de Equipamentos:

Em caso de falhas que impossibilitem o reparo imediato dos switches, a CONTRATADA deverá fornecer equipamentos de substituição equivalentes ou superiores em até 24 horas, para assegurar a continuidade das operações do CONTRATANTE.

Atualizações de Firmware e Software:

A CONTRATADA é responsável por garantir que todos os switches recebam atualizações de firmware e software regularmente, de acordo com as recomendações do fabricante, para corrigir vulnerabilidades de segurança, melhorar o desempenho e introduzir novas funcionalidades.

Documentação de Manutenção:

A CONTRATADA deverá fornecer relatórios detalhados após cada intervenção de manutenção, incluindo descrição das atividades realizadas, peças substituídas, atualizações aplicadas e recomendações para melhorias. Esses relatórios devem ser entregues à CONTRATANTE no prazo de até 5 dias úteis após a execução dos serviços.

Acordo de Nível de Serviço (SLA):

A manutenção dos switches deve estar sujeita a um Acordo de Nível de Serviço (SLA) que especifique claramente os tempos de resposta e resolução, bem como as penalidades aplicáveis em caso de descumprimento dos prazos estabelecidos.

Treinamento em Manutenção:

A CONTRATADA deverá oferecer, sem custos adicionais, treinamentos periódicos para a equipe técnica da CONTRATANTE, capacitando-os na operação e na resolução de problemas básicos dos switches, visando a redução do tempo de inatividade e o aumento da eficiência operacional.

Requisitos Temporais

O prazo de vigência da contratação será de 60 (sessenta) meses contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.

Os bens/produtos devem ser entregues em até 45 (quarenta e cinco) dias corridos após a emissão da Ordem de Serviço ou de Fornecimento de Bens. Os bens/serviços entregues poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações ou critérios de aceitação, devendo ser substituídos às suas custas, sem prejuízo da aplicação das penalidades cabíveis. A instalação e configuração da solução devem ocorrer em até 15 (quinze) dias úteis.

A reunião inicial de alinhamento com a Contratada, deverá ocorrer em no máximo 5 (cinco) dias corridos, posteriormente à assinatura do instrumento contratual.

A Contratada deverá cumprir todos os prazos descritos neste Termo de Referência, respeitando os prazos máximos estabelecidos e zelando pelo cumprimento dos Níveis Mínimos de Serviço Exigidos.

O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia deverá estar de acordo com o especificado no acordo de nível de serviço do Termo de Referência;

O prazo de entrega e instalação deverá estar de acordo com o especificado no Termo de Referência, caso não seja especificado um prazo diferente na ordem de serviço.

Os serviços e itens a qual se refere este projeto, devem ser entregues em Brasília.

A entrega deverá acontecer no horário compreendido entre as 09:00 as 17:00 e poderá ser agendada em data e hora previamente com a CONTRATANTE;

Caberá ao CONTRATANTE rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Termo de Referência.

O recebimento dos serviços e itens desse projeto, será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

Requisitos de Segurança e Privacidade

Obedecer a todas as normas e procedimentos de segurança implementados no ambiente de TI do CONTRATANTE;

As pessoas envolvidas na execução das atividades terão acesso às instalações do CONTRATANTE por meio de credenciais emitidas pela Administração e deverão executar as atividades em ambiente definido pelo órgão, estando sujeitas, além do uso de crachás, a todas as formas de controle de acesso às dependências da instituição, tais como atendimento aos horários de expediente, vistoria de objetos que estejam portando etc.;

O acesso a áreas restritas, por técnicos das eventuais empresas CONTRATADAS, obedecerá ao previsto na POSIC do CONTRATANTE e suas Normas Complementares;

A execução das atividades deverá observar os princípios básicos de Segurança da Informação e Comunicações – SIC;

Além do que está descrito acima, deverão ser observados os requisitos de segurança e privacidade especificados nos requisitos tecnológicos da solução.

Vistoria

A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 08:00 horas às 18:00 horas.

Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

Caso o licitante opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

Para agendar a vistoria, o licitante deverá entrar em contato com a equipe técnica da Coordenação-Geral de Tecnologia da Informação de segunda à sexta-feira, das 08:00 horas às 18:00 horas:

Coordenação-Geral de Tecnologia da Informação

Tel.: (61) 3314 – 6575 / 6417

E-mail: cgti@cidades.gov.br

O licitante que optar por realizar a vistoria deverá preencher o Termo de Vistoria. Caso decida não realizar a vistoria, deverá preencher o Termo de Renúncia à Vistoria.

Requisitos Sociais, Ambientais e Culturais

Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

Requisitos Sociais:

Responsabilidade Social: a contratada deve demonstrar compromisso com a responsabilidade social, cumprindo as leis trabalhistas, respeitando os direitos humanos e adotando práticas éticas de negócios.

Qualidade no atendimento: a contratada deve oferecer atendimento de qualidade, com prontidão nas respostas, comunicação eficaz, empatia e respeito aos usuários.

Requisitos Ambientais:

Exigência que os profissionais realizem o uso eficiente de energia, práticas de descarte adequadas e conformidade com regulamentações ambientais aplicáveis.

Requisitos Culturais:

Conhecimento da cultura e ambiente local: Consideração da compreensão da cultura local e dos desafios específicos da região, para garantir uma adaptação adequada dos serviços de TI à realidade do Ministério das Cidades (MCID).

Sensibilidade cultural:

Avaliação da capacidade das empresas licitantes em lidar com a diversidade cultural e tratar os colaboradores e usuários com respeito e igualdade, promovendo um ambiente de trabalho inclusivo.

Requisitos de Arquitetura Tecnológica

Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos no item 9 deste ETP.

Requisitos de Projeto e de Implementação

Desenho de Arquitetura de Rede:

A CONTRATADA deve fornecer um projeto detalhado de arquitetura de rede, incluindo a topologia proposta, localização dos switches, diagramas de conectividade e especificações técnicas dos equipamentos, garantindo que todos os requisitos de desempenho e escalabilidade sejam atendidos.

Capacidade e Escalabilidade:

Os switches adquiridos devem suportar a capacidade de tráfego atual da rede da CONTRATANTE, com possibilidade de escalabilidade para acomodar um aumento de pelo menos 50% no volume de dados, sem degradação de desempenho.

Redundância e Alta Disponibilidade:

A solução deve incluir mecanismos de redundância, como switches em configuração de failover e links de comunicação redundantes, para assegurar alta disponibilidade e continuidade de serviço em caso de falhas.

Compatibilidade e Interoperabilidade:

Os switches devem ser compatíveis com os equipamentos de rede existentes e suportar protocolos de comunicação padrão da indústria, como IEEE 802.1 Q para VLANs, Spanning Tree Protocol (STP), e Link Aggregation Control Protocol (LACP).

Configuração e Integração:

A CONTRATADA deve realizar a configuração inicial e a integração dos switches na rede da CONTRATANTE, seguindo as melhores práticas de segurança e desempenho. Isso inclui a configuração de VLANs, QoS, e ACLs conforme necessário.

Teste de Aceitação:

Antes da aceitação final, a CONTRATADA deve executar uma série de testes para verificar a funcionalidade, desempenho, e segurança dos switches instalados. Os resultados dos testes devem ser documentados e submetidos à CONTRATANTE para revisão.

Documentação Técnica:

A CONTRATADA deve fornecer documentação completa e detalhada, incluindo manuais de configuração, guias de usuário, e procedimentos de manutenção para todos os switches e equipamentos associados.

Treinamento para Equipe Técnica:

A CONTRATADA deve oferecer treinamento técnico à equipe da CONTRATANTE, cobrindo aspectos de configuração, operação e manutenção dos switches, para garantir que o pessoal interno esteja capacitado a lidar com o novo sistema.

Plano de Gerenciamento de Projeto:

Um plano de gerenciamento de projeto detalhado deve ser desenvolvido e acordado com a CONTRATANTE, incluindo cronograma de implementação, recursos necessários, e responsabilidades das partes envolvidas.

Conformidade com Normas e Regulamentos:

O projeto e a implementação devem estar em conformidade com todas as normas e regulamentos aplicáveis, incluindo requisitos de segurança, privacidade, e sustentabilidade ambiental.

Requisitos de Implantação

A CONTRATADA deverá observar integralmente os requisitos de implantação, instalação e fornecimento descritos no item 9 deste ETP.

A instalação e configuração deverão ser executadas por técnicos da CONTRATADA, certificados pelo fabricante dos equipamentos fornecidos. É necessária a apresentação de documentação original que comprove a validade dessas certificações enquanto durar o contrato, podendo ser solicitada a qualquer momento.

A CONTRATADA deverá manter o local de execução dos serviços em perfeitas condições de limpeza e uso.

Requisitos de Garantia, Manutenção e Assistência Técnica

O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

A garantia será prestada com o objetivo de manter os equipamentos e itens de software fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o CONTRATANTE.

A garantia abrange a realização da Manutenção Preventiva e Corretiva dos bens, realizada pelo próprio CONTRATADO ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

Entende-se por Manutenção Preventiva os serviços que compreendem verificações frequentes em relação ao bom funcionamento do hardware e à atualização de drivers, softwares e firmwares necessários para todos os itens que compõem os equipamentos. Quando necessário, haverá a substituição de peças e componentes, que deverão ser novos, originais e não recondicionados. Os serviços deverão ser realizados mediante cronograma de execução previamente aprovado pelo CONTRATANTE.

As verificações preventivas ocorrerão pelo menos trimestralmente, em datas a serem definidas pelo CONTRATANTE. A manutenção preventiva poderá ser solicitada pela CONTRATANTE, que definirá o nível de severidade, por meio de chamado registrado junto à CONTRATADA.

A CONTRATADA deverá emitir um relatório de atendimento de manutenção preventiva, que deverá evidenciar os parâmetros de desempenho do equipamento, as versões de software e as recomendações, quando for o caso.

Uma vez identificados vícios ou defeitos nos equipamentos, a CONTRATADA deve prover todas as manutenções corretivas necessárias para a normalização do ambiente, corrigindo todos os defeitos, mensagens de erro ou qualquer tipo de mau funcionamento apresentado em qualquer um dos equipamentos e seus componentes internos.

Entende-se por Manutenção Corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos, atualizações e correções necessárias.

As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento, sem custo adicional para o CONTRATANTE.

Uma vez notificado, o CONTRATADO realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo máximo de 1 (um) dia útil, contados a partir da data de retirada do equipamento das dependências da Administração pelo CONTRATADO ou pela assistência técnica autorizada.

O prazo indicado no subitem anterior poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do CONTRATADO, aceita pelo CONTRATANTE.

Na hipótese do subitem acima e seu predecessor, o CONTRATADO deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo CONTRATANTE, de modo a garantir a continuidade dos serviços e trabalhos administrativos durante a execução dos reparos.

Decorrido o prazo para reparos e substituições, ou violados os NÍVEIS MÍNIMOS DE SERVIÇO, sem o atendimento da solicitação do CONTRATANTE ou a apresentação tempestiva de justificativas pelo CONTRATADO, fica o CONTRATANTE autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do CONTRATADO o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do CONTRATADO.

A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo a eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

Dos requisitos específicos de assistência técnica:

Este serviço compreende o apoio técnico à distância e/ou presencial (on-site) fornecido pela assistência técnica do fabricante dos equipamentos e da CONTRATADA para solucionar problemas de ordem sistêmica, problemas em equipamentos desta marca e problemas decorrentes de mau funcionamento de software, bem como solucionar dúvidas quanto à correta operação e configuração dos equipamentos.

Deverá existir acesso ao serviço de assistência técnica do fabricante e da CONTRATADA por telefone gratuito, e-mail ou acesso seguro ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. No site do fabricante, deverão existir ferramentas de autosserviço que permitam o diagnóstico e sugestões de solução do problema, quando possível.

Deverá existir acesso ao serviço de assistência técnica da CONTRATADA, por telefone gratuito, e-mail ou acesso ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. A indisponibilidade da comunicação por parte da CONTRATADA não afetará a contagem de tempo relativa aos prazos de atendimento.

Os chamados junto à CONTRATADA deverão ser atendidos por profissionais da CONTRATADA, em português, e serão usados para abrir solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos e soluções fornecidos.

Dos requisitos específicos de acesso à documentação:

Este serviço compreende o acesso remoto, por parte da CONTRATANTE, às documentações técnicas dos equipamentos do fabricante.

A CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante dos equipamentos, que contenha especificações técnicas, informações, assistência e orientação para instalação, desinstalação, configuração e atualização de firmware e software, aplicação de correções (patches), diagnósticos, avaliações e resolução de problemas, além de demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

Dos requisitos específicos de garantia técnica do fabricante:

A CONTRATADA deverá descrever, em sua proposta, os termos da garantia técnica oferecida pelo fabricante, incluindo o Part Number da garantia ofertada e fornecendo também, em momento oportuno, o número de contrato individual (em nome da CONTRATANTE) junto ao fabricante.

O Termo de Garantia Técnica terá duração mínima de 60 (sessenta) meses.

Dos requisitos de reposição de equipamento defeituoso:

Este serviço compreende o envio de equipamento(s), componente(s), acessório(s) e dispositivo(s) novos, de primeiro uso e de modelo igual ou superior ao(s) danificado(s), às expensas do fabricante, às dependências da CONTRATANTE.

O contrato de reposição de equipamento, peças ou acessórios deverá ser na modalidade 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, devendo o equipamento substituto (definitivo ou provisório) ser entregue na CONTRATANTE até o próximo dia útil (Next Business Day - NBD) após a abertura do chamado.

Para determinação do horário de início de cada chamado referente à substituição de equipamento defeituoso, devem ser levadas em consideração as seguintes condições: caso a determinação de falha do hardware pelo fabricante tenha ocorrido antes das 15h, horário local de Brasília-DF, de segunda a sexta-feira (excluindo os feriados), o equipamento deverá ser enviado no mesmo dia para chegar no próximo dia útil. Para as solicitações feitas depois das 15h, o fabricante deverá entregar o equipamento substituto até o segundo dia útil após a determinação da falha.

O equipamento substituto passará à propriedade da CONTRATANTE, devendo ser imediatamente incluído no contrato de manutenção vigente em substituição ao equipamento danificado. O equipamento substituído deverá ser devolvido ao fabricante às expensas do mesmo, em até 5 (cinco) dias úteis.

A CONTRATANTE deverá ter acesso à Central de Assistência Técnica (TAC) do fabricante para abertura dos chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, através de login/senha individual. A CONTRATANTE deverá ter a opção de abrir os chamados junto ao fabricante com o intermédio da CONTRATADA.

Os requisitos de Garantia, Manutenção e Assistência Técnica deverão observar os NÍVEIS MÍNIMOS DE SERVIÇO exigidos, descritos no capítulo Modelo de Gestão de Contrato deste Termo.

Requisitos de Experiência Profissional

Os serviços de assistência técnica, suporte, garantia, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

Requisitos de Formação da Equipe

Não serão exigidos requisitos de formação da equipe para a presente contratação.

Requisitos de Metodologia de Trabalho

O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Ordem de fornecimento de Bens (OFB) emitida pela Contratante.

A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 8 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 7 dias por semana por via telefônica.

O andamento do fornecimento dos equipamentos dever ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Requisitos de Segurança da Informação e Privacidade

Os serviços contratados deverão ser prestados em conformidade com as leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal relacionadas à Segurança da Informação e Comunicações (SIC), com especial atenção à Lei Federal n° 13.709/2018 (LGPD).

Conformidade com Normas e Políticas:

A CONTRATADA deverá adotar a Política de Segurança da Informação e Comunicações (POSIC) do Ministério das Cidades, bem como as normas relativas à Segurança da Informação do Governo Federal.

Credenciamento e Seleção de Profissionais:

A CONTRATADA deverá credenciar junto à CONTRATANTE todos os seus profissionais que venham a ser designados para prestar serviços, independentemente do formato de execução (presencial, remoto e/ou híbrido).

A CONTRATADA deverá adotar critérios rigorosos no processo seletivo dos profissionais que irão atuar diretamente na execução do contrato, a fim de evitar a incorporação de perfis que possam comprometer a segurança ou credibilidade da CONTRATANTE.

Gestão de Acesso:

A CONTRATADA deverá comunicar à CONTRATANTE, com antecedência mínima, qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do contrato, para que sejam revogados imediatamente todos os privilégios de acesso aos sistemas, informações e recursos da CONTRATANTE.

Treinamento e Qualificação:

A CONTRATADA deve garantir que sua equipe profissional seja treinada, qualificada e esteja disponível para executar os serviços atribuídos, conforme aplicável às características dos serviços contratados.

Identificação e Confidencialidade:

Todos os funcionários da CONTRATADA envolvidos na prestação dos serviços deverão utilizar crachá.

Todas as informações acessadas pela CONTRATADA em função da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada sua reprodução, utilização ou divulgação a terceiros.

Sigilo e Proteção de Dados:

Os representantes, empregados e colaboradores da CONTRATADA deverão zelar pela manutenção do sigilo de dados, informações, documentos e especificações técnicas de que tenham conhecimento em razão dos serviços executados.

A CONTRATADA deverá adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações tratadas no âmbito da prestação dos serviços.

Prevenção de Acesso Não Autorizado:

A CONTRATADA deverá implementar medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade, prevenindo acesso não autorizado às informações disponibilizadas para prestação dos serviços.

Proibição de Transferência de Dados:

A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo de informação de propriedade da CONTRATANTE sem autorização.

Cumprimento de Normas de Segurança:

A CONTRATADA deverá submeter-se aos procedimentos contidos nas normas de segurança corporativa do Ministério das Cidades (MCID) e da Administração Pública em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários nas dependências do órgão.

Identificação de Equipamentos:

A CONTRATADA deverá identificar qualquer equipamento de sua propriedade que venha a ser instalado nas dependências da CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança, etc.

Termos de Compromisso e Ciência:

A CONTRATADA deverá assinar o Termo de Compromisso, e seus funcionários alocados na prestação de serviços deverão assinar o Termo de Ciência, conforme modelos anexos ao Termo de Referência:

- TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO;
- TERMO DE CIÊNCIA.

Sustentabilidade

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

- questionamento inicial quanto à necessidade do consumo;

- redução do consumo;
- análise do ciclo de vida do produto (produção, distribuição, uso e disposição) para determinar a vantajosidade econômica da oferta;
- estímulo para que os fornecedores assimilem a necessidade premente de oferecer ao mercado, cada vez mais, obras, produtos e serviços sustentáveis;
- fomento da inovação, tanto na criação de produtos com menor impacto ambiental negativo, quanto no uso racional destes produtos, minimizando a poluição e a pressão sobre os recursos naturais;
- fomento a soluções mais sustentáveis, as quais foquem na função que se almeja com a contratação e que gerem menor custo e redução de resíduos;
- fomento à contratação pública compartilhada entre órgãos, por intenção de registro de preço (contratações compartilhadas sustentáveis).

Só será admitida a oferta de ativos de infraestrutura de TIC (Switch Core; Switch Acesso; Ponto de acesso sem fio; Sistema de Gerenciamento em Nuvem; Controladora WLAN e Instalação de Rack) que cumpra os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 304, de 2023 do INMETRO.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021)

Na presente contratação, não será admitida a indicação da marca/fabricante;

Da exigência de carta de solidariedade

Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Subcontratação

Não é admitida a subcontratação do objeto contratual.

Da verificação de amostra do objeto

Não será exigida a verificação de amostra do objeto

Garantia da Contratação

Será exigida a garantia da contratação a que se referem os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e nas condições descritas nas cláusulas do contrato.

Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-lo, no máximo, até a data de assinatura do contrato.

A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

O CONTRATANTE poderá utilizar o valor da garantia prestada para descontar os valores referentes a eventuais glosas e multas aplicadas à CONTRATADA, além da satisfação de prejuízos causados ao CONTRATANTE ou a terceiros na execução do objeto contratual por culpa ou dolo da CONTRATADA.

Se o valor da garantia, ou parte dele, for utilizado em pagamento de qualquer obrigação ou em decorrência de penalidade imposta, inclusive indenização a terceiros, a CONTRATADA se obriga a efetuar a respectiva reposição ou complementação no prazo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação feita pelo CONTRATANTE.

Caso a CONTRATADA não cumpra o disposto nos itens anteriores dentro do prazo estipulado, ficará sujeita às penalidades contratuais cabíveis.

Em caso de aditamento do contrato, por motivos previstos na Lei, a CONTRATADA fica obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e nas modalidades constantes desta Seção.

O contrato poderá oferecer maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

Informações relevantes para o [dimensionamento E/OU apresentação] da proposta

A proposta de preços deverá ser apresentada de acordo com o Modelo de Proposta de Preço (Anexo II - SEI nº 5302936). A proposta de preços deverá ser apresentada com descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas neste Termo de Referência e no Edital.

A proposta técnica de preços deverá ter prazo de validade não inferior a 60 (sessenta) dias corridos, a partir da data da sessão pública.

A licitante deverá declarar, no momento de sua proposta, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis de serviço exigidos, cumprindo os requisitos especificados para a presente contratação.

A proposta deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no Termo de Referência.

O LICITANTE é o único responsável pelas informações sobre tributos. Não caberá qualquer reivindicação para majoração de preço em virtude de possíveis equívocos cometidos. Efetuar-se-á a devida correção quando houver alteração da respectiva legislação tributária que rege a operação objeto do instrumento contratual, após a data estabelecida para apresentação da PROPOSTA.

Se houver indícios de que as propostas de preços apresentadas pelas Licitantes tornem o contrato inexequível em todas ou em parte das exigências de cumprimento de obrigações contratuais, ou em caso da necessidade de esclarecimentos complementares, caberá à CONTRATANTE, ao longo do processo licitatório ou a qualquer tempo, solicitar às mesmas Licitantes a demonstração de exequibilidade do contrato. Estas deverão apresentar justificativas e comprovações em relação aos custos do projeto, embasando, portanto, a decisão da contratante a respeito da desclassificação da proposta.

A CONTRATADA deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objetivo da licitação exceto quando ocorrer algum dos eventos arrolados no Art. 57 da Lei n° 14.133/2021.

7. Estimativa da demanda - quantidade de bens e serviços

Conforme citado no capítulo de descrição da necessidade, este projeto contempla a atualização de todo o parque de switches e roteadores do Ministério das Cidades, incluindo a troca e instalação dos equipamentos localizados na nova sede e no Bloco E.

Diante dessas considerações, para o dimensionamento da demanda, foram realizados os seguintes levantamentos:

Apresentamos a relação detalhada dos switches atualmente em uso no edifício do Ministério das Cidades, localizado no Bloco E da Esplanada dos Ministérios. Esta lista abrange exclusivamente os andares ocupados pelo Ministério das Cidades, conforme (Documento SEI nº 5065707). As informações foram consolidadas e estão organizadas no quadro a seguir:

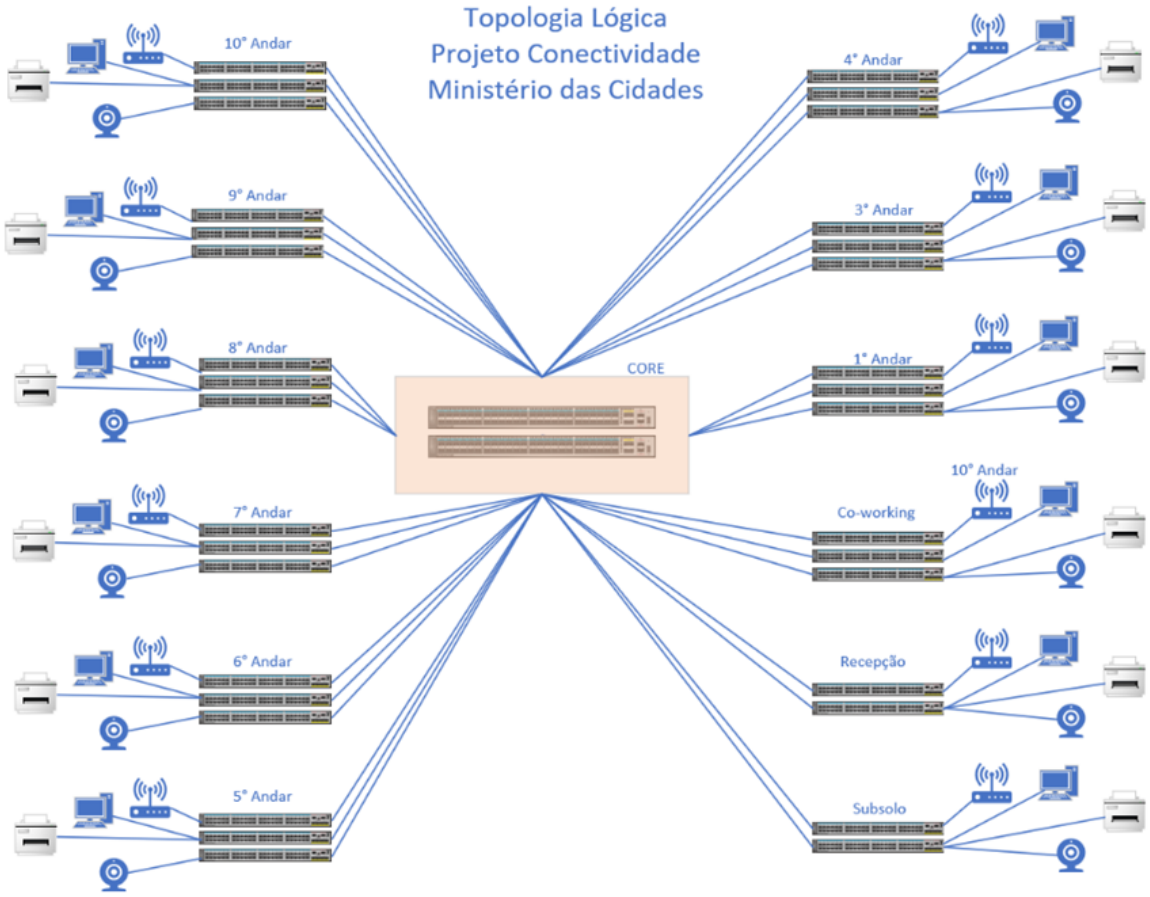
Switches Bloco E		
Andar	Qtde. Switches	Qtde. Portas
7°	7 switches enterasys, 2 unidades B5K125-48P2 e 5 unidades B5G125-48P2	138 portas ativas de 346
9°	7 switches enterasys, 5 unidades B5K125-48P2 e 2 unidades B5G125-48P2	175 portas ativas de 340
Sala Cofre Bloco E	2 unidades SWITCH HUAWEI 59706 - CORE	**por unidade:** Módulo 1 - 8 portas 10gbps Módulo 2 - 24 portas 1gbps Módulo 3 - duas portas 40gbps Módulo 4 - 48 portas 1gbps Módulo 5 - 48 portas 1gbps Módulo 6 - 16 portas 10gbps Módulo 7 - system Control master Módulo 8 - system Control slave

Análise e Planejamento da Infraestrutura de Conectividade para a Nova Sede do Ministério das Cidades

Em relação à nova sede, conforme o estudo do projeto arquitetônico apresentado no Documento SEI nº 5250399, foram identificados e mapeados os pontos críticos, que exigem uma cobertura adequada pela nova infraestrutura. Esta avaliação foi realizada pelo responsável da CGSL/MCID, conforme os Documentos SEI nº 5249125e 5249128.

A equipe de planejamento para a contratação analisou essas necessidades e estruturou a distribuição dos recursos da infraestrutura da seguinte forma:

Topologia Lógica do Projeto de Conectividade do Ministério das Cidades:



Detalhamento do Projeto para a Edificação Sede do Ministério das Cidades:

Projeto Conectividade - Ministério das Cidades - Ed. Sede									
Pavimento	Pontos (usuários)	Câmeras	Impressoras	Access Point	Catracas/ Leitores	Outros	Total - Portas	SW-24 T1	SW-48T2
10° Andar	82	8	4	6	6	12	118	1	3
9° Andar	82	8	4	6	6	12	118	1	3
8° Andar	82	8	4	6	6	12	118	1	3
7° Andar	82	8	4	6	6	12	118	1	3
6° Andar	82	8	4	6	6	12	118	1	3
5° Andar	82	8	4	6	6	12	118	1	3
4° Andar	82	8	4	6	6	12	118	1	3
3° Andar	82	8	4	6	6	12	118	1	3
2° Andar	82	8	4	6	6	12	118	1	3
1° Andar	82	8	4	6	6	12	118	1	3
Co-working/Restaurante	60	12	4	8	12	12	108	2	2
Recepção	15	8	4	6	12	12	57	1	1
Subsolo	20	8	0	4	6	12	50	1	1
TOTAIS	915	108	48	78	90	156	1395	14	34

Detalhamento do Projeto para o Bloco E do Ministério das Cidades:

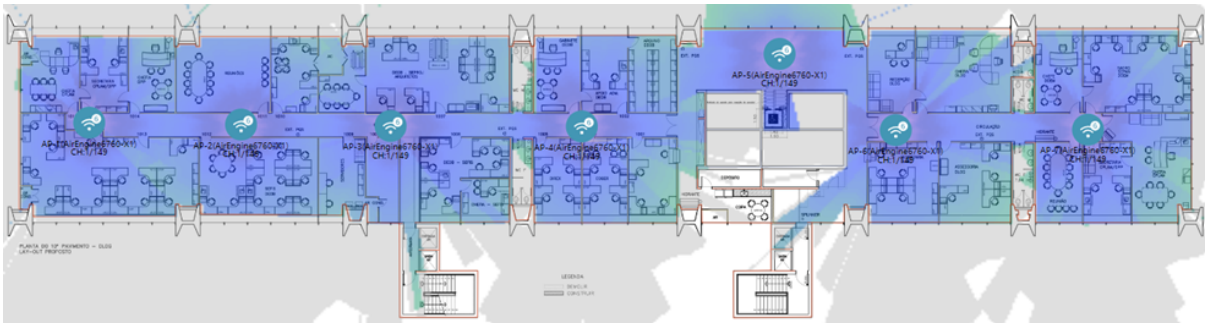
Projeto Conectividade - Ministério das Cidades - Bloco E									
Pavimento	Pontos (usuários)	Câmeras	Impressoras	Access Point	Catracas/ Leitores	Outros	Total - Portas	SW-24T1	SW-48T2
9° Andar	85	4	4	6		7	106	1	3
7° Andar	100	4	4	6		7	121	1	3
TOTAIS	185	8	8	12	0	14	227	2	6

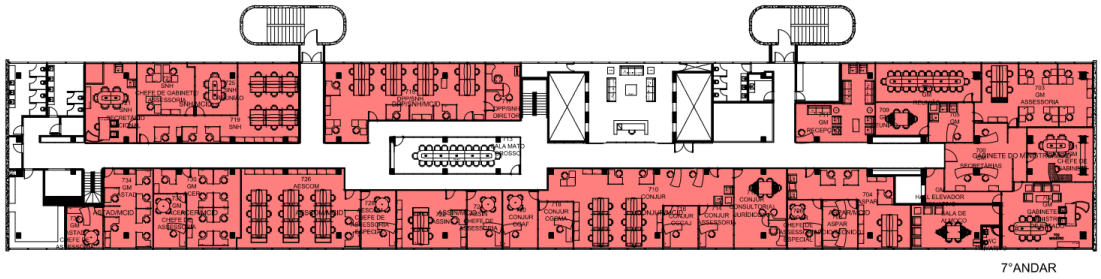
Componentes e Características Principais da Infraestrutura:

- Switches full PoE
- Uplinks - SFP+ 10GE
- Alta largura de banda /Alta simultaneidade
- Gerenciamento em nuvem

Mapa de Calor da Edificação Sede e Bloco E (5250399 e 5365032**):**

Este mapa ilustra a cobertura e o posicionamento dos Access Points (APs), evidenciando:





Destacando:

- Cobertura completa em 2.4ghz e 5ghz;
- Hand over transparente entre ambientes do Ministério das Cidades

Detalhamento do resumo projeto de conectividade do Ministério das Cidades:

Projeto Conectividade - Ministério das Cidades - Resumo Projeto					
Edificio (Localidade)	Switch Core	Acesso - Tipo 01	Acesso - Tipo 02	Access Point	Controlador - WLAN
Ed. Sede	1	13	34	78	1
Bloco E	1	3	6	14	
TOTAIS	2	16	40	92	1

A estrutura proposta visa garantir que todas as áreas críticas da nova sede estejam bem suportadas pela infraestrutura de conectividade, proporcionando um ambiente de trabalho eficiente e tecnologicamente avançado.

ESPECIFICAÇÃO TÉCNICA

SWITCH DE CORE COM 48 PORTAS SFP

ESPECIFICAÇÕES GERAIS

Deve permitir instalação em rack de 19” padrão Telco EIA;

Deve possuir altura máxima 1 (um) rack unit (RU);

Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

Deve possuir fonte de alimentação redundante interna e hot-swappable;

Deve possuir capacidade de processamento igual ou superior a 670 (seiscentos e setenta) Mpps;

Deve possuir capacidade de switching igual ou superior a 900 (novecentos) Gbps;

Deve possuir 48 (quarenta e oito) portas SFP, sendo que no mínimo 12 (doze) dessas portas devem operando 1G/10GbE compatíveis com SFP/SFP+ e o restante das portas devem operar em 1GbE SFP;

Deve permitir empilhamento de até 10 (dez) unidades outros equipamentos em topologia linear e em anel, e permitir gerenciar a pilha com um único endereço IP;

Deve possuir banda agregada de empilhamento mínima de 160 (cento e sessenta) Gbps ,podendo ser através de 2 (duas) portas de 40 (quarenta) Gbps operando em full-duplex. As portas de empilhamento deverão ser fornecidas nesse certame;

O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;

Deve suportar expansão futura de pelo mínimo 1 (uma) porta 100Gbps QSFP28 adicional as portas solicitadas nesse certame;

Deve suportar expansão futura de pelo no mínimo 2 (duas) portas 40Gbps QSFP+ adicionais as portas solicitadas nesse certame;

Deve suportar expansão futura de pelo menos 4 (quatro) portas 1/10Gbps SFP+ adicionais as portas solicitadas nesse certame;

Deve ser compatível com SFP 1000BASE-SX, 1000BASE-LX e 1000Base-T;

Deve ser compatível com SFP+ 10GBASE-SR,10GBASE-LR, 10GBASE-ER;

Deve ser compatível com QSFP+ 40GBASE-SR4, 40GBASE-LR4 e 40G-BiDi;

Deve ser compatível com QSFP28 100GBASE-SR4, 100GBASE-LR4 e 100GBASE-CWDM4;

Deve possuir pelo menos 8MB de buffer de pacotes;

Deve possuir, no mínimo, 4GB de memória DRAM e 4GB de memória NVRAM (flash);

Deve possuir ventilação front to back, isto é, o fluxo de ar deve seguir no sentido das portas de interface para as fontes de energia;

Deve suportar a inversão do fluxo de ar de ventilação para o modo “back to front” através de pelo menos um dos seguintes métodos: troca de ventiladores e fontes, atualização de firmware ou alteração do arquivo de configuração;

Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;

Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;

Possui slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;

Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

Deve possuir botão de reset voltar a para configuração default de fábrica;

O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;

A proposta comercial deve discriminar o fabricante e o modelo do equipamento ofertado bem como seus respectivos “P/Ns”;

Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;

Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet

FUNÇÕES DE CAMADA 2

Deve possuir capacidade de no mínimo 110.000 (cento e dez mil) endereços MAC;

Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad.

Deve permitir a configuração de pelo menos 250 (duzentos e cinquenta) grupos de LACP com pelo menos 16 (dezesseis) portas dentro de um mesmo grupo;

Deve permitir a configuração de grupos de portas agregadas (LAGs) com balanceamento simétrico, garantindo que o tráfego de um mesmo origem e destino passe pela mesma porta de um LAG de forma bidirecional;

Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);

Deve ser compatível com o protocolo PVST+;

Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

Deve implementar BPDU Guard e Root Guard;

Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

Deve permitir a criação VLANs privadas;

Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

Deve implementar selective QinQ;

Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

Deve permitir a configuração de endereços MAC de unicast multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

Deve implemenetar MLD snooping v1 e v2;

Deve implementar MVRP (Multiple VLAN Registration Protocol);

Deve possuir funcionalidade de refletir o tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;

Deve implementar protocolo de proteção de topologia em anel;

FUNÇÕES DE CAMADA 3

Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;

Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;

Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;

Deve implementar roteamento usando o protocolo BGP4 e BGP4+;

Deve implementar criação de túneis GRE;

Deve implementar VRF ou VRF-lite, com suporte a pelo menos 32 (trinta e duas) instâncias;

Deve implementar os protocolos VRRP e VRRPv3;

Deve implementar ECMP com no mínimo 8 (oito) caminhos;

Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;

Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.

Deverá possuir no mínimo 500 (quinhentas) interfaces virtuais para roteamento entre VLANs

Deve permitir a configuração de pelo menos 2.000 (duas mil) rotas estáticas IPv4;

Deve permitir a configuração de pelo menos 1.000 (mil) rotas estáticas IPv6;

Deverá suportar a capacidade pelo menos 97.000 (noventa e sete mil) entradas em sua tabela de roteamento IPv4;

Deverá suportar a capacidade de pelo menos 17.000 (dezessete mil) entradas em sua tabela de roteamento IPv6;

Deve possuir DHCP Server para IPv4 e IPv6;

Deve permitir a configuração de DHCP Relay;

Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;

Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para a escolher a rota default apropriada pelo host IPv6;

SEGURANÇA

Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

Implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuirem suplicantes 802.1X;

Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

Deve implementar “Change of Authorization” de acordo com a RFC 5176;

Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

Deve implementar ACLs de entrada e ACLs de saída para IPv4;

Deve implementar ACLs de entrada e ACLs de saída para IPv6;

Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

Deve permitir a criação de filtros de endereço MAC de origem e destino;

Deve possuir protocolos para proteção de ataques de Denial of Service;

Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

Deve possuir funcionalidade de proteção contra ataques do tipo “ARP Poisoning”;

Deve permitir a configuração de Dynamic ARP Inspection em pelo menos 500 vlans;

Deve implementar IP Source Guard;

Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;

Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;

Deve implementar IPv6 RA guard e IPv6 ND inspection;

Deve implementar RADsec conforme RFC6614;

Deve implementar unicast Reverse Path Forwarding (uRPF) como ferramenta para evitar ataques do tipo source IP spoofing;

GERENCIAMENTO

Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

Deve implementar gerenciamento usando SSH v2 utilizando os algoritimos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

Deve implementar pelo menos 4 (quatro) grupos de RMON;

Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

Deve possuir suporta a automação com Ansible;

Deve implementar RESTCONF;

Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

QUALIDADE DE SERVIÇO

Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

Deve implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

Deve permitir a configuração de Rate Limiting de entrada;

Deve permitir a configuração de Rate Shaping de saída;

Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

TIPO 01 - SWITCH DE ACESSO COM 24 PORTAS

ESPECIFICAÇÕES GERAIS

Deve permitir instalação em rack de 19” padrão Telco EIA;

Deve possuir altura máxima 1 (um) rack unit (RU);

Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

Deve possuir 24 (vinte e quatro) portas 10/100/1000 Mbps, usando conectores RJ-45;

As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP/SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

Deve possuir capacidade de processamento igual ou superior a 98 (noventa e oito) Mpps;

Deve possuir capacidade de switching igual ou superior a 132 (cento e trinta e dois) Gbps;

Deve possuir, pelo menos, 2 MB de buffers de pacotes;

Deve possuir, pelo menos, 1 GB de memória DRAM;

Deve possuir, pelo menos, 2 GB de memória flash;

Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;

Deve ser do tipo fanless ou permitir operação com os ventiladores internos desligados;

Deve permitir empilhamento de até 8 (oito) unidades com outros equipamentos em topologia linear e em anel;

Deve permitir o empilhamento com switches da mesma série, sendo switches 24 portas, switches 48 portas, switches multi-gigabit e switches PoE+, e permitir gerenciar a pilha com um único endereço IP;

Deve suportar banda agregada de empilhamento de no mínimo 80Gbps fullduplex, podendo ser através de agregação de portas de 10G. Essas portas podem ser formadas pelas portas do item 2.1.6;

O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;

Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;

Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;

Deve possuir slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;

Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

Deve possuir botão de reset para voltar a para configuração default de fábrica;

Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242 com documentos disponíveis publicamente no sítio público dessa agência na Internet;

FUNÇÕES DE CAMADA 2

Deve possuir capacidade de no mínimo 16.000 (dezesseis mil) endereços MAC;

Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad.

Deve permitir configuração de pelo menos 120 (cento e vinte) grupos de LACP copelo menos 8 (oito) portas dentro de um mesmo grupo;

Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatro mil) vlans ativas;

Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);

Deve ser compatível com o protocolo PVST+;

Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias de Spanning Tree;

Deve implementar BPDU Guard e Root Guard;

Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

Deve permitir a criação VLANs privadas;

Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

Deve implementar selective QinQ;

Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet

Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

Deve implmenetar MLD snooping v1 e v2;

Deve implementar MVRP (Multiple VLAN Registration Protocol);

Deve implementar MVP (Multicast VLAN Registration);

Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste permitindo medir a continuidade da rede e o desempenho da porta ethernet;

Deve implementar protocolo de proteção de topologia em anel.

FUNÇÕES DE CAMADA 3

Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;

Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;

Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;

Deve implementar os protocolos VRRP e VRRPv3;

Deve implementar ECMP com no mínimo 8 caminhos;

Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;

Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.

Deverá possuir no mínimo 350 (trezentos e cinquenta) interfaces virtuais para roteamento entre VLANs;

Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv4;

Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv6;

Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas na sua tabela de roteamento IPv4;

Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas em sua tabela de roteamento IPv6;

Deve possuir DHCP Server para IPv4 e IPv6;

Deve permitir a configuração de DHCP Relay;

Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;

Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para a escolher a rota default apropriada pelo host IPv6;

SEGURANÇA

Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

Deve implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.: Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

Deve implementar “Change of Authorization” de acordo com a RFC 5176;

Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

Deve implementar ACLs de entrada e ACLs de saída para IPv4;

Deve implementar ACLs de entrada e ACLs de saída para IPv6;

Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

Deve permitir a criação de filtros de endereço MAC de origem e destino;

Deve possuir protocolos para proteção de ataques de Denial of Service;

Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

Deve possuir funcionalidade de proteção contra ataques do tipo “ARP Poisoning”;

Deve implementar IP Source Guard em IPv4 e IPv6;

Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;

Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;

Deve implementar IPv6 RA guard e IPv6 ND inspection;

Deve implementar RADsec conforme RFC6614;

GERENCIAMENTO

Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES.

Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

Deve implementar pelo menos 4 (quatro) grupos de RMON;

Deve permitir o monitoramento dos transceivers ópticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

Deve implementar o protocolo OpenFlow 1.3 com suporte para portas híbridas em Camada 2 e Camada 3;

Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos. Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

Deve possuir suporte a automação com Ansible;

Deve suportar RESTCONF ou RESTful API;

QUALIDADE DE SERVIÇO

Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

Deve implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

Deve permitir a configuração de Rate Limiting de entrada;

Deve permitir a configuração de Rate Shaping de saída;

Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

Deve suportar SDVoE (Software Defined Video over Ethernet);

TIPO 02 - SWITCH DE ACESSO COM 48 PORTAS

ESPECIFICAÇÕES GERAIS

Deve permitir instalação em rack de 19” padrão Telco EIA;

Deve possuir altura máxima 1 (um) rack unit (RU);

Deve possuir fonte de alimentação interna, do tipo auto-sense, para operar de 100 a 240 VAC;

Deve possuir 48 (quarenta e oito) portas 10/100/1000 Mbps, usando conectores RJ-45;

As portas 10/100/1000 BASE-T devem ser do tipo MDI/MDIX automático;

Deve possuir, no mínimo, 4 (quatro) portas 1/10 Gbps SFP/SFP+, as quais não devem operar em modo “combo” com as portas 10/100/1000 BASE-T em par trançado;

Deve possuir capacidade de processamento igual ou superior a 130 (cento e trinta) Mpps;

Deve possuir capacidade de switching igual ou superior a 180 (cento e oitenta) Gbps;

Deve possuir, pelo menos, 4 MB de buffers de pacotes;

Deve possuir, pelo menos, 1 GB de memória DRAM;

Deve possuir, pelo menos, 2 GB de memória flash;

Deve implementar os protocolos IEEE 802.3af Power over Ethernet (PoE) e IEEE 802.3at Power over Ethernet Plus (PoE+);

Deve possuir PoE power budget de pelo menos 370 (trezentos e setenta) watts;

Deve ser do tipo fanless ou permitir operação com os ventiladores internos desligados;

Deve permitir empilhamento de até 8 (oito) unidades com outros equipamentos em topologia linear e em anel;

Deve permitir o empilhamento com switches da mesma série, sendo switches 24 portas, switches 48 portas, switches multi-gigabit e switches PoE+, e permitir gerenciar a pilha com um único endereço IP;

Deve suportar banda agregada de empilhamento de no mínimo 80Gbps full-duplex, podendo ser através de agregação de portas de 10G. Essas portas podem ser formadas pelas portas do item 3.1.6;

O equipamento deve permitir empilhamento através de cabos de fibra óptica com distância de pelo menos 10 (dez) km entre cada uma das unidades da pilha;

Deve possuir porta de gerenciamento “out-of-band” operando a 10/100/1000 Mbps;

Deve possuir porta de console para gerenciamento utilizando conector RJ-45, USB, mini-USB ou USB Tipo C;

Deve possuir slot USB para inserção de uma mídia de armazenamento removível para fazer upgrade de imagem do switch e backup da configuração;

Deve possuir LEDs indicativos de energização, status de slot USB, atividade do link e velocidade das portas;

Deve permitir realizar troubleshooting visual da unidade na pilha, identificando através de LEDs se o switch é master ou slave da pilha, e sua identificação na pilha;

Deve permitir identificar através de sinalização visual onde o switch está localizado no rack através de comandos para ligar e desligar os LEDs do equipamento;

Deve possuir botão de reset para voltar a para configuração default de fábrica;

Deve implementar o padrão IEE 802.3az (Energy-Efficient Ethernet);

Deve possuir certificado de homologação junto à ANATEL de acordo a resolução 242com documentos disponíveis publicamente no sítio público dessa agência na Internet;

FUNÇÕES DE CAMADA 2

Deve possuir capacidade de no mínimo 16.000 (dezesseis mil) endereços MAC;

Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad. Deve permitir a configuração de pelo menos 120 (cento e vinte) grupos de LACP com pelo menos 8 (oito) portas dentro de um mesmo grupo;

Deve implementar o protocolo IEEE 802.1Q para criação de pelo menos 4000 (quatromil) vlans ativas;

Deve implementar o protocolo IEEE 802.1s (Multiple Spanning Tree), IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1D (Spanning Tree);

Deve ser compatível com o protocolo PVST+;

Deve permitir a configuração de pelo menos 250 (duzentas e cinquenta) instâncias deSpanning Tree;

Deve implementar BPDU Guard e Root Guard;

Deve permitir a configuração de VLANs “trunking” de acordo com o protocolo 802.1Q e VLANs nativas (sem tag) simultaneamente na mesma porta;

Deve permitir a criação VLANs privadas;

Deve permitir a configuração de VLAN Q-in-Q Tagging de acordo com o padrão IEEE802.1ad ou IEEE802.1QinQ;

Deve implementar selective QinQ;

Deve implementar para o protocolo UDLD (Uni-Directional Link Detection) ou DLDP (Device Link Detection Protocol) ou similar;

Deve implementar jumbo frames até 9000 bytes nas portas Gigabit Ethernet;

Deve implementar mecanismos para controle do tráfego broadcasts, multicast e unknown unicast;

Deve implementar mecanismo de detecção ativa de loops através do envio frames de detecção. Na detecção de um evento de loop, deve ser capaz de realizar o bloqueio da porta (port shutdown);

Deve permitir a configuração de endereços MAC unicast e multicast estáticos em múltiplas portas ethernet simultaneamente, para permitir a configuração de “clusters” de firewalls;

Deve implementar IGMP Snooping para IGMPv1, IGMPv2 e IGMPv3;

Deve implementar MLD snooping v1 e v2;

Deve implementar MVRP (Multiple VLAN Registration Protocol);

Deve implementar MVP (Multicast VLAN Registration);

Deve possuir funcionalidade de refletir a tráfego de entrada de uma porta Ethernet, retornando para um gerador de teste para permitindo medir a continuidade da rede e o desempenho da porta ethernet;

Deve implementar protocolo de proteção de topologia em anel.

FUNÇÕES DE CAMADA 3

Deve permitir roteamento local entre VLANs utilizando interfaces virtuais ou SVIs;

Deve permitir a configuração de rotas estáticas usando endereços IPv4 e IPv6;

Deve permitir a configuração de endereço IPv6 com prefixo de 127 bits para links point-to-point;

Deve implementar roteamento IP usando os protocolos RIPv1/v2 e RIPng;

Deve implementar roteamento IP usando os protocolos OSPFv2 e OSPFv3;

Deve implementar os protocolos VRRP e VRRPv3;

Deve implementar ECMP com no mínimo 8 caminhos;

Deve implementar os protocolos de roteamento de multicast PIM-S, PIM-SSM e PIM-DM;

Deve suportar PIM-Passive para reduzir e minimizar tráfego de controle.

Deverá possuir no mínimo 350 (trezentos e cinquenta) interfaces virtuais para roteamento entre VLANs

Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv4;

Deve permitir a configuração de pelo menos 500 (quinhentas) rotas estáticas IPv6;

Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas na sua tabela deroteamento IPv4;

Deverá suportar a capacidade de pelo menos 1.000 (mil) entradas em sua tabela de roteamento IPv6;

Deve possuir DHCP Server para IPv4 e IPv6;

Deve permitir a configuração de DHCP Relay;

Deve implementar PBR (Policy-Based Routing) para IPv4 e IPv6;

Deve implementar IPv6 router advertisement (RA) preference na mensagem de RA com informações de múltiplos routers para escolher a rota default apropriada pelo host IPv6;

SEGURANÇA

Deve permitir autenticação de usuários usando o padrão IEEE 802.1x, permitindo associação dinâmica de VLANs e ACLs usando profiles definidas por um servidor RADIUS externo;

Deve permitir a associação de VLANs restritas para usuários que falhem durante a autenticação 802.1X;

Deve implementar método de autenticação baseado em endereço MAC para os dispositivos que não possuírem suplicantes 802.1X;

Deve possuir capacidade de autenticação 802.1x com atribuição de VLAN, regras de acesso de segurança e QoS individuais para, no mínimo, 02 (dois) dispositivos (Ex.:Telefone IP e PC) conectados em uma única porta e usando VLANs distintas;

Deve permitir, no mínimo e em cada porta, os seguintes tipos de autenticação usando VLANs distintas:

2 (dois) dispositivos que suportam o padrão IEEE 802.1x;

2 (dois) dispositivos MAC que não suportam o padrão IEEE 802.1x;

1 (um) dispositivo que suporta o padrão IEEE 802.1x e 1 (um) dispositivo MAC que não suporta o padrão IEEE 802.1x;

O equipamento deve permitir a configuração de reautenticação 802.1x periódica;

O equipamento ofertado deve permitir a autenticação via Web Authentication para usuários que não possuem 802.1x;

Deve implementar “Change of Authorization” de acordo com a RFC 5176;

Deve permitir a autenticação de usuários para acesso às funções de gerenciamento usando-se os protocolos RADIUS, TACACS ou TACACS+;

Deve permitir a criação de ACLs para a filtragem de tráfego IPv4 baseado no endereço IP de origem e destino, portas TCP e UDP de origem e destino, bits do protocolo 802.1p e campo DSCP do protocolo Diffserv;

Deve permitir a criação de ACLs para a filtragem de tráfego IPv6 baseado no endereçoIP de origem e destino, portas TCP e UDP de origem e destino, campo PCP do protocolo 802.1p e campo DSCP do protocolo Diffserv;

Deve implementar ACLs de entrada e ACLs de saída para IPv4;

Deve implementar ACLs de entrada e ACLs de saída para IPv6;

Permitir a filtragem do tráfego através de pelo menos 500 (quinhentas) regras de ACL (Access Control List);

Deve implementar segurança de acesso baseada em endereços MAC de origem, com a possibilidade de bloqueio permanente ou temporário das portas onde for detectada uma violação de segurança;

Deve permitir a criação de filtros de endereço MAC de origem e destino;

Deve possuir protocolos para proteção de ataques de Denial of Service;

Deve possuir funcionalidade de proteção contra servidores DHCP não autorizados DHCPv4 snooping e DHCPv6 snooping;

Deve possuir funcionalidade de proteção contra ataques do tipo “ARP Poisoning”;

Deve implementar IP Source Guard em IPv4 e IPv6;

Deve implementar proteção contra ataques do tipo TCP SYN e ataques do tipo Smurf;

Deve permitir o monitoramento da movimentação de um endereço MAC de uma porta para outra, facilitando a distinção entre um movimento legítimo com um movimento malicioso de um ataque de MAC spoofing;

Deve implementar IPv6 RA guard e IPv6 ND inspection;

Deve implementar RADsec conforme RFC6614;

GERENCIAMENTO

Deve permitir monitoração e configuração usando SNMP v1, v2 e v3;

Deve permitir o gerenciamento via SNMPv3 com as seguintes opções: sem autenticação e sem privacidade, com autenticação e sem privacidade e com autenticação e com privacidade;

Deve ser possível enviar “traps” e realizar o gerenciamento via SNMP através das redes IPv4 e IPv6;

Deve permitir a configuração de porta para espelhamento de tráfego, para a coleta de pacotes em analisadores de protocolo ou detecção de intrusão;

Deve permitir espelhamento de tráfego baseado em Porta, VLAN, Filtro MAC e ACL;

Deve permitir a configuração de porta para espelhamento de tráfego para uma porta em um switch remoto;

Deve implementar gerenciamento usando SSH v2 utilizando os algoritmos de criptografia 3DES e AES. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

Deve implementar gerenciamento via Telnet. Deve ser permitido a utilização de endereços IPv4 e IPv6 para a funcionalidade solicitada;

Deve implementar pelo menos 4 (quatro) grupos de RMON;

Deve permitir o monitoramento dos transceivers óticos, retornando informação de temperatura, potência de transmissão (dBm), potência de recepção (dBm) e status;

Deve implementar funcionalidade de diagnóstico do cabo de par trançado, retornando informação de comprimento do cabo, status do link;

Deve permitir a atualização de arquivos de configuração e imagens de firmware usando TFTP ou FTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir a atualização de imagens de firmware dos equipamentos de uma pilha sem a necessidade de reinicialização simultânea de todos os equipamentos da pilha, permitindo a continuidade do tráfego de dados durante o processo de atualização;

Deve permitir configuração automática do seu próprio endereço IP e a seguir carga automática de um arquivo de configuração pré-definido, usando um servidor DHCP e um servidor TFTP ou FTP;

Deve implementar o protocolo LLDP conforme o padrão IEEE 802.1AB, bem como LLDP-MED;

Deve permitir o monitoramento de tráfego através dos protocolos sFlow, NetFlow ou IPFIX. Deve ser possível exportar o tráfego de redes IPv4 e IPv6;

Deve permitir a configuração de seu relógio interno de forma automática através do protocolo NTP. Em ambos os casos deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir armazenamento simultâneo de duas imagens de firmware em memória flash.

Deve permitir atualização de imagem de firmware através de mídia de armazenamento externa conectado ao slot USB;

Deve permitir o envio de mensagens de syslog à pelo menos 2 servidores distintos.

Deve ser permitido a utilização de redes IPv4 e IPv6 para a funcionalidade solicitada;

Deve permitir o envio de syslog com formato conforme RF5424 para prover mais informações no seu header;

Deve possuir suporte a automação com Ansible;

Deve suportar RESTCONF;

Deve implementar funcionalidade de rollback automático de configuração, permitindo que o switch retorne automaticamente para uma configuração estável prévio caso o administrador não confirmar a alteração realizada dentro de um prazo de tempo configurável.

QUALIDADE DE SERVIÇO

Deve permitir priorização de tráfego usando 8 (oito) filas de priorização por porta;

Deve permitir priorização de tráfego baseado no padrão IEEE 802.1p e no campo DSCP do protocolo Diffserv;

Deve implementar pelos menos os seguintes métodos para configuração das filas de priorização: ponderada, prioridade estrita e ambas combinadas;

Deve implementar priorização de tráfego baseado em porta física, protocolo IEEE 802.1p, endereços IP de origem e destino e portas TCP/UDP de origem e destino;

Deve permitir a configuração de Rate Limiting de entrada;

Deve permitir a configuração de Rate Shaping de saída;

Deve implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) e uma combinação entre os dois métodos SP e WRR;

Deve suportar SDVoE (Software Defined Video over Ethernet);

PONTO DE ACESSO INDOOR

ESPECIFICAÇÕES GERAIS

Deverá ser do mesmo fabricante do CONTROLADOR DE REDE SEM FIO - WLAN para fins de compatibilidade.

Deverá possuir estrutura metálica que permita a utilização do equipamento em locais internos, com fixação em teto.

Não serão aceitos equipamentos com padrão de instalação física em parede, conhecidos como “wall plate”, uma vez que a instalação física deverá ocorrer no teto.

Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

Deve visar a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO, Target Wake Time (TWT), se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 no programa da WiFi Alliance na data do pregão.

Deve possuir a certificação IEC 61373 para uso em ambientes sujeitos à vibração e impactos.

Deve ser compatível com o padrão UL 2043, o qual regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

Deve suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

Deve possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE IEEE 802.3at ou IEEE 802.3af. Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

Deve suportar temperatura de operação entre 0°C a 50°C.

O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

Deverá possuir 2 (duas) interfaces ethernet 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local.

Deverá possuir, no mínimo, um rádio embarcado para IoT, o qual deve ser compatível com BLE e ZigBee.

Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.

Deverá possuir LEDs para a indicação do status da alimentação do ponto de acesso, rádios de 2.4 GHz e 5 GHz, operação em Mesh e gerenciamento via controladora.

Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS, e Wi-Fi Mesh habilitadas, incluindo auto cura via Mesh.

Deve ser compatível com IPv4, IPv6 e dual-stack.

CARACTERÍSTICAS DOS RÁDIOS

O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

Deverá implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a 300 Mbps, IEEE 802.11ac: 6.5 Mbps a 867 Mbps e IEEE 802.11ax: 4 Mbps a 1200 Mbps.

Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11 a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 1.5 dBi para 2.4GHz e 2.5 dBi para 5GHz.

Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 25 dBm na frequência de 5 GHz e 26 dBm na frequência de 2.4 GHz.

Deverá suportar canalização de 20 MHz, 40 MHz e 80 MHz.

Deverá possuir mecanismo de rádio com suporte a 4 (quatro) fluxos espaciais, sendo 2x2:2 em 5 GHz e 2.4 GHz para SU-MIMO e MU-MIMO.

Deve possuir sensibilidade mínima de recepção de -97dBm considerando MCS0 HE20 (802.11ax) em 5GHz e 2.4GHz.

Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

SERVIÇOS, SEGURANÇA E GERENCIAMENTO

Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

Deve suportar auto cura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.

Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

Deve suportar a configuração de limite de banda por usuário ou por SSID.

Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services).

Deve implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

Deve suportar VLANs conforme o padrão IEEE 802.1Q.

Deve suportar atribuição dinâmica de VLAN por usuário.

Deve implementar balanceamento de usuários por ponto de acesso.

Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

Deve suportar HotSpot 2.0, Captive Portal e WISPr.

Deverá implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, PSK (Pre-Shared Key) única por dispositivo cliente em um mesmo SSID, IEEE 802.1X e IEEE 802.11i.

Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.

Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

Deve permitir habilitar e desabilitar a divulgação do SSID.

Deverá implementar autenticação de usuários usando portal de captura.

Deverá suportar funções para análise de espectro.

Deve suportar conversão de tráfego multicast para unicast.

Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.

Deve permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.

Deve permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

Deverá implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

Deve permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

SISTEMA DE GERENCIAMENTO EM NUVEM

ESPECIFICAÇÕES GERAIS

A solução deverá ser baseada nas premissas de computação em nuvem ofertada como serviço pelo fabricante e ser compatível com a plataforma de gerenciamento, os pontos de acesso e os switches propostos nesse certame;

A solução deverá ser baseada em algoritmos de inteligência artificial e nos conceitos de *machine learning* (aprendizagem de máquina);

A solução deverá atuar em conjunto com as funcionalidades do controlador LAN/WLAN desde que seja do mesmo fabricante dos controladores, pontos de acesso e switches utilizados na solução. Os dados de telemetria enviados pelo controlador LAN/WLAN para a nuvem devem estar criptografados.

Deve permitir seu acesso e gerenciamento através de navegador web padrão (HTTPS);

Deve possuir interface gráfica para visualização das informações, dashboards e relatórios;

O Dashboard deve mostrar um resumo da integridade da rede, incluindo os principais incidentes e recomendações de reparo;

Deve classificar automaticamente os incidentes de rede por nível de severidade em pelo menos 4 níveis.

Deve fornecer contagem total dos incidentes que ocorreram na rede e categorizá-los de acordo com a severidade, sendo possível analisar os incidentes dos últimos 90 dias.

Deve ser possível exportar a lista de incidentes, pelo menos no formato CSV.

Para cada incidente, deverá apresentar análise contendo: severidade, descrição detalhada do incidente, data e horário de início do incidente, duração, equipamentos e/ou clientes impactados, causa raiz e recomendações de reparo.

Para incidentes relacionados à conexão, deve identificar pelo menos os seguintes problemas:

Falhas elevadas de associação e autenticação 802.11;

Falhas elevadas com servidores de DHCP;

Falhas elevadas com EAP;

Falhas elevadas com servidores RADIUS;

Elevado tempo para conexão de dispositivos e/ou usuários;

Para incidentes relacionados à desempenho, deve identificar pelo menos os seguintes problemas:

Cobertura - Clientes com baixo nível de sinal (RSSI);

Condições do canal abaixo do ideal;

Alta utilização de CPU da controladora;

Alta utilização de memória dos switches;

Alta utilização do *Airtime* dos APs nas bandas de 2.4GHz, 5GHz e 6GHz, identificando se a alta utilização é devido à transmissão (TX), recepção (RX) ou interferências;

Para incidentes relacionados à infraestrutura, deve identificar pelo menos os seguintes problemas:

Erro de sincronismo de horários;

PoE – APs recebendo menos energia do que o necessário para o máximo desempenho;

Incompatibilidade de velocidade da interface do AP com o switch;

Incompatibilidade de VLAN ID entre AP e switch;

Falhas e alta latência na comunicação entre AP e Controladora;

Elevado número de reinicializações dos APs;

Através de análise de fatores dinâmicos e estáticos que influenciam o comportamento da rede, a solução deve fornecer recomendações de configurações que melhoram a experiência do usuário e aprimoram o desempenho da rede.

Cada recomendação deve apresentar descrição detalhada, contendo horário de criação, nível de prioridade, justificativa da recomendação e possíveis impactos de sua aplicação.

Deve possuir solução inteligente de gerenciamento de recursos de rádio (*RRM – Radio Resource Management*), a fim de reduzir ao máximo a interferência co-canal.

A solução deve analisar continuamente as condições da rede e informar via recomendação sempre que houver uma oportunidade para melhorar o ambiente de RF. A recomendação de RRM deve considerar os parâmetros de canal, canalização e potência de rádio.

Deve ser possível aceitar ou recusar a recomendação. Em caso de aceite, deve ser possível agendamento do horário de execução. A aplicação da recomendação dever ser executada diretamente pela solução de análise, sem necessitar que o administrador de rede tenha que fazer qualquer configuração na controladora WLAN.

Para cada recomendação, antes de seu aceite, deve ser possível visualizar quais alterações de canal, canalização e potência de rádio serão executadas em cada AP.

Deve fornecer informações sobre a saúde da rede através de indicadores de desempenho, que permitam analisar o comportamento da rede em linha de tempo. A linha de tempo deve permitir filtrar as últimas 24 horas, última semana, últimos 30 dias e customização de período com os últimos 90 dias. Deve apresentar no mínimo os seguintes indicadores:

Conexões realizadas com sucesso e conexões com falha;

Tempo para se conectar;

Porcentagem de autenticações 802.11 realizadas com sucesso;

Porcentagem de associações 802.11 realizadas com sucesso;

Porcentagem de tentativas EAP (4-way handshake) completadas com sucesso;

Porcentagem de tentativas de autenticação Radius realizadas com sucesso;

Porcentagem de tentativas de DHCP realizadas com sucesso;

Porcentagem de tentativas de Roaming realizadas com sucesso;

Throughput estimado de *downlink* para os clientes wi-fi;

Porcentagem dos usuários com nível de sinal (RSS) dentro de SLA definido. Por exemplo, mostrar a porcentagem de usuários com nível de sinal melhor do que -75dBm.

Deve monitorar e analisar alterações nos indicadores de desempenho da rede devido à alterações das configurações ou atualizações de firmware. Deve permitir a comparação dos indicadores antes e depois das alterações, e listar todas as alterações que foram realizadas na solução wi-fi entre esses dois períodos.

Deve proporcionar mecanismos de validação de serviço na rede, permitindo emular a conexão fim-à-fim de um cliente wi-fi em determinada WLAN. Devem ser analisados os parâmetros de EAP, Radius, Ping, DNS, Traceroute, DHCP, testes de velocidade e também validar a conexão via RF.

Os testes de validação de serviço, principalmente de validação de conexão via RF, podem ser realizados com os próprios Pontos de Acesso emulando clientes wi-fi ou com probes/sensores adicionais. No caso de utilização de probes/sensores extras, estes devem ser fornecidos junto com a solução de Análise e Visibilidade de Rede, e na quantidade de 1 sensor para cada 2 pontos de acesso.

Deve realizar testes para avaliar a qualidade de uma vídeo-chamada na rede wi-fi para pelo menos a plataforma Zoom;

Deve possuir mecanismos para investigação detalhada do processo de conexão para usuário individualmente, através do endereço MAC, IP ou nome do usuário. A solução deve permitir definir o período de tempo a ser investigado. Para o período definido, devem ser apresentadas as conexões com sucesso, causa de falhas, desconexões, roamings, qualidade do sinal e os incidentes relacionados com o usuário.

Deve gerar de relatórios dos seguintes tipos:

Informações com status dos APs, modelos e versões de firmware;

Informações com status dos switches, portas, modelos e versões de firmware;

Informações das WLAN;

Listagem de APs conectados, com histórico de usuários conectados e volume de tráfego por AP;

Informação de utilização de *airtime* (rx, tx, interferências) nas bandas de 2.4GHz, 5GHz e 6GHz.

Listagem das principais aplicações em uso por quantidade de usuários e por volume de tráfego.

Listagem de clientes, sistema operacional e fabricante dos dispositivos;

Deve suportar a criação de relatórios customizados.

Deve possuir retenção de dados de pelo menos 90 dias para gerar relatórios;

Deve permitir que os relatórios sejam convertidos em arquivos pdf e csv;

A solução ofertada deve suportar a capacidade de monitorar simultaneamente, no mínimo, 2.000 (dois mil) pontos de acesso, 400 (quatrocentos) switches e 2 (dois) controladores de rede;

LICENÇA OU SERVIÇO DE ASSINATURA

Deve adicionar licença de uso para cada ativo (ponto de acesso ou switch) monitorado no item Solução de Análise e Visibilidade da Rede.

Deve permitir expansão de ativos monitorados em incrementos unitários, permitindo aquisição de licenças para o número exato de ativos monitorados.

Deve ter validade de no mínimo 5 anos, incluindo suporte do fabricante.

ESPECIFICAÇÕES DE SEGURANÇA DE ACESSO

Deverá ser do mesmo fabricante dos controladores WLAN e Pontos de Acesso, visando garantir a interoperabilidade entre as soluções.

Deve ser fornecido para instalação em ambiente virtualizado VMware 5.5 ou superior ou Hyper-V versão 2012 ou superior.

Deve vir licenciado para permitir o cadastramento de, no mínimo de 1000 (mil) usuários visitantes simultâneos, com capacidade de expansão futura para, no mínimo, 20000 (vinte mil) usuários.

A solução deve suportar clusterização no modo ativo/ativo ou ativo/passivo para prover resiliência e alta disponibilidade. Permitir a criação de páginas personalizadas para o captive portal, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos clientes.

Deve suportar autenticação de usuários através de redes sociais suportando, no mínimo, integração com Facebook, LinkedIn e Google.

Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo visitante e em caso de autosserviço, especificando quais informações cadastrais dos visitantes são requisitadas.

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

Deve implementar um portal web seguro (HTTPS) a ser apresentado automaticamente aos usuários temporários durante o início de sua conexão com a rede.

Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail ou impressão local.

O portal de autenticação deve ser suportado, no mínimo, pelos seguintes navegadores de Internet: Microsoft Internet Explorer, Mozila Firefox, Safari e Chrome, operando em PCs e dispositivos móveis.

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 provisionar automaticamente um certificado digital para o dispositivo cadastrado e configurar o dispositivo com o certificado gerado e com as configurações de rede sem fio para que o usuário utilize autenticação segura via 802.1X na rede corporativa.

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 e deverá suportar, no mínimo, os seguintes sistemas operacionais: Apple iOS, Windows, Mac OSx e Android.

A solução deve guiar/instruir o usuário durante o procedimento de instalação do certificado digital e configuração do perfil da rede sem fio através de página web ou através de aplicativo.

Após a finalização do processo de autosserviço e configuração do suplicante, a solução deve desconectar o dispositivo do usuário da rede visitante (captive portal) e conectá-lo automaticamente na rede corporativa com autenticação 802.1X em dispositivos que suportem tal ação.

A solução deve instalar os certificados digitais através de CA (Certification Authority) interna na ferramenta (certificado digital auto assinado) e também permitir a utilização de certificados digitais de CA externas (Root CA do Active Directory, por exemplo).

A solução deve suportar autenticação de usuários via integração direta com Microsoft Active Directory, LDAP, SAML 2.0 e base de usuários local.

Deve suportar autenticação PEAP com um servidor RADIUS embutido.

Possuir capacidade de autenticação dos usuários visitantes através de senhas pré cadastradas ou vouchers, para cada usuário ou grupo de usuários, no caso de utilização em eventos.

Permitir a configuração do número máximo de conexões simultâneas realizadas por uma mesma conta, possibilitando que um usuário possua mais de um dispositivo na rede com a mesma senha e que contas coletivas sejam utilizadas em eventos. Esta funcionalidade deve ser aplicada para usuários visitantes autenticados pelo captive portal.

Deve oferecer visibilidade e controle sobre dispositivos na rede com a possibilidade de revogar o acesso.

Realizar verificação de postura dos dispositivos quando os mesmos se associam pela primeira vez, incluindo checagem de antivírus, configurações de registro, patches, proxy, firewall, entre outros, com a possibilidade de remediação.

Deve permitir a criação de conjunto de chaves PSK privadas (PPSK, DPSK, MPSK ou similar), para serem associadas individualmente para cada usuário. Essas chaves devem ser criadas na própria solução, ou seja, sendo externas à controladora WLAN.

Deve suportar OCSP (Online Certificate Status Protocol) com revogação automática.

Deve suportar integração com OAuth 2.0 e SAML 2.0 para autenticação externa.

Deve prover REST APIs para permitir integração com soluções de terceiros.

Deve suportar Radius CoA (Change of Authorization) para o servidor RADIUS interno.

O servidor Radius interno deve suportar RadSec, e deve ser possível visualizar os logs de autenticação do Radius.

Disponibilizar servidor SMTP interno ou possibilitar a configuração de servidor SMTP externo para envio de e-mails.

Deve ser possível solicitar ao usuário visitante, no passo de autenticação, a inserção do e-mail da pessoa responsável por aprovar o seu acesso à rede, sendo que essa pessoa se encarregará por aprovar ou rejeitar a requisição uma vez que o sistema a notifique via e-mail.

CONTROLADOR DE REDE SEM FIO - WLAN

ESPECIFICAÇÕES GERAIS

Deverá ser do mesmo fabricante dos pontos de acesso fornecidos pela CONTRATADA, para fins de compatibilidade e gerenciamento;

O hardware e o software deverão ser do mesmo fabricante para garantir desempenho e confiabilidade da solução.

Deve possuir hardware dedicado com software de gerenciamento e administração já embarcado.

Não serão aceitas soluções baseadas nas premissas de computação virtual sem hardware dedicado, controladores baseados em computação em nuvem ou controladores agregados a outros equipamentos, tais como Firewalls ou Roteadores.

Deve possuir fonte de alimentação com seleção automática de tensão (100-240V AC).

Deve possuir porta de console para gerenciamento e configuração via linha de comando com conector RJ-45 ou RS-232 ou USB.

Deve possuir, no mínimo, 04 (quatro) portas do tipo 1000BASE-T com conectores RJ-45 e 04 (quatro) portas do tipo 10 GbE BASE-X compatíveis com transceivers SFP+.

Deve acompanhar 1 cabo do tipo DAC sfp+ para sfp+ de pelo menos 1 mt de comprimento.

Deve disponibilizar todos os acessórios necessários para fixação em rack padrão de 19 (dezenove) polegadas em 1RU de espaço.

Deve suportar temperatura de operação entre 0°C e 40°C.

Deve possuir sistema de ventilação interno redundante.

Deve ter disponível LEDs indicando o estado de operação do equipamento, do disco e das portas ethernet.

Deverá possuir a funcionalidade de operar como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores e expansível até 4 (quatro) controladores.

Deve vir acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, acessórios, cabo de energia elétrica, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução.

Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax/be

Deverá ter a capacidade para gerenciar, no mínimo, 1.020 (mil e vinte) Pontos de Acesso simultâneos. S

Deve suportar, no mínimo, 24.000 (vinte e quatro mil) dispositivos simultâneos

GERENCIAMENTO

Deve prover o gerenciamento centralizado dos Pontos de Acesso

Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Subredes pré-configuradas

Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF) O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;

Deve possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP; Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento. Permitir a visualização de alertas da rede em tempo real;

Implementar, no mínimo, dois níveis de acesso administrativo ao equipamento (apenas leitura e leitura/escrita) protegidos por senhas independentes.

Deve permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador. Permitir a configuração e gerenciamento através de navegador padrão (HTTPS);

Deve gerenciar de forma centralizada a autenticação de usuários. Deverá possuir base de dados de usuários interna com suporte a até 24 (vinte e quatro) mil usuários.

Deve permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS).

Deve permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;

A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:

24 horas por dia, 7 dias na semana;

Agendamento customizado permitindo escolher os dias da semana e horários;

Os horários definidos não precisam ser sequenciais, ou seja, a solução deve suportar que o administrador defina o horário de funcionamento das 08:00 às 12:00 e 14:00 às 18:00;

Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível;

Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede;

Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP;

Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede wireless;

Monitorar o desempenho da rede wireless, permitindo a visualização de informações de cada ponto de acesso;

Implementar cluster de controladores WLAN no modo ativo/ativo, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability);

Deverá efetuar compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster;

Deverá em caso de falha realizar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede;

Deverá possuir a capacidade de geração de informações ou relatórios de no mínimo os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;

Deverá suportar a identificação de aplicações dos clientes conectados ao ponto de acesso com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações;

Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;

Deverá possibilitar a importação de plantas baixas nos formatos .dwg ou .jpg ou .png, devendo permitir a visualização dos Pontos de Acesso instalados, com seu estado de funcionamento;

Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio;

Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados;

A solução deve suportar a adição de um serviço de SMS externo, tal como Twilio.

REDE

Deverá implementar suporte aos protocolos IPv4 e IPv6;

Deverá suportar tagging de VLANs; Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x;

Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação.

Deverá suportar, no mínimo, 2.000 (dois mil) SSIDs simultâneos no cluster.

Deverá possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fios devem continuar conectados com acesso à rede.

Deve permitir que novos usuários se associem à rede sem fios utilizando autenticação do tipo 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.

Deve ser possível evitar que dispositivos 802.11b se conectem a rede, visando melhorar o desempenho da rede sem fio. Deve suportar 802.11d e 802.11k.

Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz e 5 GHz, bem como na interface LAN.

SEGURANÇA

Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);

Implementar, pelo menos, os seguintes padrões de segurança wireless:

Wi-Fi Protected Access (WPA);

Wi-Fi Protected Access 2 (WPA2);

Temporal Key Integrity Protocol (TKIP);

Advanced Encryption Standard (AES);

Dynamic PSK;

IEEE 802.1x;

IEEE 802.11i;

IEEE 802.11w.

Implementar, pelo menos, os seguintes controles/filtros:

Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;

Baseado em endereço IP;

Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;

Baseado em porta de origem e/ou destino;

Baseado em tipo ou sistema operacional do dispositivo;

Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

MAC Address;

Autenticação Local;

Captive Portal;

Active Directory;

RADIUS;

IEEE 802.1x;

LDAP.

Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID

Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

A solução deverá suportar a criação de uma zona de visitantes, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso a rede wireless.

O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote).

Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável.

Deve permitir que o portal interno para usuários visitantes (guest) seja customizável, bem como ser compatível com o idioma português.

Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede.

Deverá permitir enviar a senha de usuários visitantes (guests), por e-mail ou por SMS.

Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa.

Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subnet, sendo possível adicionar exceções com base em endereços MAC e IP.

Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0

Implementar, mecanismos para detecção de pontos de acesso do tipo rogue com informações de, no mínimo:

SSID-Spoofing – APs não pertencentes ao controlador propagando o mesmo SSID;

MAC Spoofing – APs não pertencentes ao controlador propagando o mesmo MAC de um AP válido;

Rogue APs – APs não pertencentes ao controlador;

Same Network – APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;

Deve implementar varredura de RF para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues);

Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;

Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;

RECURSOS DE GERENCIAMENTO AUTOMÁTICO DE RÁDIO FREQUÊNCIA (RF)

Na ocorrência de inoperância de um Ponto de Acesso, o controlador WLAN deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

Deve ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;

Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar o desempenho. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso.

Deverá permitir que o serviço wireless seja desabilitado de determinado ponto de acesso.

Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado.

RECURSOS DE CONVERGÊNCIA E MULTIMÍDIA

Deve suportar 802.11e.

Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;

Deverá permitir a configuração de prioridade de um determinado SSID sobre os outros SSID’s.

Deve acompanhar suporte do fabricante por 5 (cinco) anos.

RACK E INSTALAÇÃO

Padrão 19”

Deve possuir altura mínima de 42U’s, profundidade mínima de 600mm e largura mínima de 600mm;

Deve ser fornecido com 2 ventiladores, kit rodizio e pés niveladores;

Deve possuir entrada e saída de cabos pelo teto ou pela base do rack;

Deve possuir longarinas ajustáveis em profundidade, confeccionadas em aço com perfurações de ½ em ½ Us e demarcações das unidades de altura, permitindo a instalação de equipamentos de rede e bandejas padrão 19";

Deve possuir porta frontal em vidro, que permita a visualização dos equipamentos e infraestrutura instalada. Esta porta deve ser removível, reversível e possuir fechadura;

Deve possuir porta traseira lisa em aço com fechadura;

Capacidade de carga estática de 600kg;

Deve possuir tampas laterais removíveis com sistema de encaixe e desencaixe rápido, sem o uso de ferramentas e perfuração preparada para instalação de fechadura tipo cilindro;

Todas as portas e a estrutura interna devem possuir ponto de aterramento;

Deve ser fornecido na cor preta com espessura mínima de chapa 1.2mm;

O rack deve ser fornecido desmontado, possibilitando o fácil transporte e permitindo que a montagem seja feita em qualquer local.

8. Levantamento de soluções

Levantamento de Soluções

Necessidades similares em outros órgãos da Administração Pública e as soluções adotadas:

Diversos Órgãos e entidades da Administração Pública Federal compartilham uma necessidade crítica de infraestrutura de rede sem fio, dado o caráter vital dessa tecnologia para a disponibilidade e segurança das informações. A rede sem fio tornou-se uma ferramenta essencial, amplamente utilizada tanto em setores públicos quanto em organizações privadas. Nesse contexto, ao consultar o "painel de preços" do governo por meio do link (https://paineldeprecos.planejamento.gov.br/), foi possível identificar várias soluções de redes sem fio baseadas em tecnologias diversas. No entanto, é crucial ressaltar que cada ambiente possui particularidades distintas que demandam abordagens específicas.

Alternativas de mercado:

As alternativas do mercado serão melhores descritas no item 10.2.

A existência de software público brasileiro:

Não se aplica, pois o processo trata de aquisição de hardware ou serviço.

Identificação das Soluções

Foram encontradas 3 (três) possibilidades de solução para o atendimento da demanda:

Solução 1: Contratação de Extensão de Garantia com Atualização do Parque de Equipamentos

Descrição: Esta solução envolve a extensão da garantia para os equipamentos existentes, mantendo o padrão atual e realizando atualizações no parque de equipamentos.

Solução 2: Locação de Equipamentos Ativos de Rede

Descrição: Consiste na locação dos equipamentos ativos de rede necessários para a nova sede.

Solução 3: Aquisição de Ativos de Rede com Sistema de Gerenciamento em Nuvem, Controladora WLAN, Suporte e Garantia de 60 Meses

Descrição: A aquisição dos ativos de rede inclui switches core, switches de acesso (Tipo 01 e Tipo 02), pontos de acesso sem fio (indoor), sistema de gerenciamento em nuvem, controladora WLAN, e racks, com suporte e garantia de 60 meses.

9. Análise comparativa de soluções

A instrução Normativa 94 de 23 dezembro de 2022/SGD/ME no inciso II do art. 11, estabelece a análise comparativa de soluções como obrigatório.

A solução a ser contratada não consta nos Catálogos de Soluções de TIC com Condições Padronizadas. (https://www.gov.br/governodigital/pt-br /contratacoes-de-tic/catalogos-de-solucoes-de-tic-com-condicoes-padronizadas-para-licenciamento-de-software).

Análise Comparativa das Soluções para Infraestrutura de TIC:

Examina-se nesta seção, para cada solução, os aspectos previstos na IN SGD-ME n. 94/2022 que devem ser avaliados em uma contratação de TIC:

Requisito	**Solução**	**Sim**	**Não**	**Não se aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X

	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

REQUISITOS		**Há compatibilidade técnica da solução para atender a demanda? (SIM / NÃO)**		
		SOLUÇÃO 1	**SOLUÇÃO 2**	**SOLUÇÃO 3**
NEGÓCIO	Conectividade Integral	NÃO	SIM	SIM
	Infraestrutura Física e Sem Fio	SIM	SIM	SIM
	Desempenho Otimizado	NÃO	SIM	SIM
	Projeto de Instalação	NÃO	SIM	SIM
	Serviços de Instalação e Operação Assistida	NÃO	SIM	SIM
	Transferência de Conhecimento	NÃO	SIM	SIM
	Modernização de Equipamentos	NÃO	SIM	SIM
	Garantia e Suporte Técnico	SIM	SIM	SIM
	Compatibilidade com VoIP	SIM	SIM	SIM
	Alta Disponibilidade	NÃO	SIM	SIM
	Gerenciamento Centralizado	NÃO	SIM	SIM
	Compatibilidade com IPv6	SIM	SIM	SIM
	Transição IPv4 para IPv6	SIM	SIM	SIM

	Segurança com IPv6	NÃO	SIM	SIM
	Suporte a Novas Tecnologias	NÃO	SIM	SIM
TECNOLÓGICO	Telefonia VoIP	SIM	SIM	SIM
	Análise de Site (Site Survey)	NÃO	SIM	SIM
	Redundância de Fontes de Energia	NÃO	SIM	SIM
	Rede Local Definida por Software (SD-LAN)	SIM	SIM	SIM
	Gerenciamento e Monitoramento	SIM	SIM	SIM
	Alta Disponibilidade	NÃO	SIM	SIM
	Expansão de Equipamentos	NÃO	SIM	SIM
Resultado da Análise		NÃO VIÁVEL	VIÁVEL	VIÁVEL

Após análise das soluções restou verificado que é viável a implementação das soluções 2 e 3, passando a ser verificado entre elas qual a mais vantajosa quanto as questões técnicas e econômicas para o Ministério das Cidades:

Solução 1: Contratação de Extensão de Garantia com Atualização do Parque de Equipamentos

Análise:

- **Adequação ao Projeto**: A solução não é adequada para o novo projeto da Nova Sede do Ministério das Cidades, que inclui 10 andares e requer uma infraestrutura de rede moderna e eficiente. Os ativos de rede existentes já estão fora do ciclo de vida útil (End of Life - EoL) e não suportam atualizações significativas ou novas demandas do projeto.
- **Suporte e Garantia**: Os equipamentos atuais não possuem suporte e garantia adequados, o que compromete a continuidade e a segurança operacional da rede.
- **Viabilidade**: Esta solução não atende às necessidades do projeto em termos de escalabilidade e modernidade. A infraestrutura existente não é capaz de suportar a expansão e as especificações do novo projeto.

Conclusão: Esta solução não é viável devido à falta de suporte, a obsolescência dos equipamentos e a inadequação para o novo projeto.

Solução 2: Locação de Equipamentos Ativos de Rede

Análise:

- **Controle e Gestão**: A locação pode reduzir o controle sobre a infraestrutura de rede, uma vez que a responsabilidade pela manutenção e atualização pode estar em mãos do locador.
- **Custos**: Embora a locação possa parecer uma alternativa de custo baixo inicialmente, os custos podem se acumular ao longo do tempo, especialmente com períodos prolongados ou alterações nas necessidades.
- **Expertise e Recursos**: A equipe da CGTI, com um quadro reduzido e pouca expertise em fiscalização contratual e gestão de equipamentos locados, pode enfrentar dificuldades significativas na administração e monitoramento dos equipamentos locados.
- **Personalização e Flexibilidade**: A locação pode limitar a personalização da rede e o ajuste fino das configurações necessárias para atender às demandas específicas do novo projeto.

Conclusão: Esta solução não é viável devido à falta de controle sobre a infraestrutura, custos potencialmente altos e limitações na personalização, além da capacidade reduzida da equipe para gerenciar a locação.

Solução 3: Aquisição de Ativos de Rede com Sistema de Gerenciamento em Nuvem, Controladora WLAN, Suporte e Garantia de 60 Meses

Análise:

- **Adequação ao Projeto**: Esta solução é totalmente compatível com o escopo do novo projeto, fornecendo a infraestrutura necessária para atender às exigências de 10 andares da nova sede. Inclui todos os componentes essenciais para uma rede moderna e eficiente.
- **Suporte e Garantia**: O suporte e a garantia de 60 meses garantem a continuidade operacional e a segurança da rede, reduzindo o risco de falhas e garantindo manutenção adequada.
- **Gerenciamento e Eficiência**: A inclusão de um sistema de gerenciamento em nuvem e uma controladora WLAN permite um gerenciamento centralizado e eficiente da rede, otimiza o desempenho e melhora a cobertura sem fio, proporcionando uma rede robusta e segura.
- **Economia e Eficiência**: A aquisição direta dos equipamentos é economicamente viável e oferece um controle completo sobre a infraestrutura, o que é crucial para a implementação bem-sucedida do projeto.

Conclusão: Esta solução é a mais adequada e viável, atendendo às necessidades do novo projeto em termos de eficácia, efetividade, eficiência e economia.

A solução mais adequada para a nova sede do Ministério das Cidades é a **Solução 3**: **Aquisição de Ativos de Rede com Sistema de Gerenciamento em Nuvem, Controladora WLAN, Suporte e Garantia de 60 Meses**. Esta abordagem proporciona uma infraestrutura de rede moderna, escalável e totalmente alinhada com as necessidades do projeto, garantindo suporte contínuo e otimização da gestão de rede.

10. Registro de soluções consideradas inviáveis

Registro de Soluções Consideradas Inviáveis

Para identificar soluções inviáveis, realizou-se uma análise de riscos com as soluções identificadas, conforme Tabela a seguir:

Solução 1: Contratação de Extensão de Garantia com Atualização do Parque de Equipamentos

Justificativa:

1. **Obsolescência dos Equipamentos**: Os equipamentos atuais já estão fora do ciclo de vida útil (End of Life - EoL) e não suportam atualizações significativas. Estes ativos não são capazes de atender às novas demandas do projeto, que exige uma infraestrutura moderna e robusta para a nova sede.
2. **Inadequação ao Novo Projeto**: O novo projeto contempla a expansão para 10 andares na nova sede do Ministério das Cidades, exigindo uma infraestrutura de rede escalável e atualizada. A extensão de garantia e atualização de equipamentos antigos não atenderia adequadamente às necessidades de alta capacidade, desempenho e segurança exigidas pela nova sede.
3. **Falta de Suporte e Garantia Adequados**: Os ativos existentes não possuem suporte e garantia apropriados. Isso compromete a continuidade e a segurança operacional da rede, resultando em potencial perda de funcionalidade e aumento do risco de falhas na infraestrutura de TI.
4. **Custo-Benefício**: Manter e atualizar equipamentos obsoletos pode não ser economicamente viável quando comparado à aquisição de novos equipamentos. A extensão de garantia não justifica o investimento, considerando que os novos requisitos do projeto demandam tecnologia avançada e maior eficiência.

Conclusão: A solução de contratação de extensão de garantia com atualização de equipamentos antigos não é viável devido à obsolescência dos equipamentos, inadequação às necessidades do novo projeto, falta de suporte adequado e questões de custo-benefício.

Solução 2: Locação de Equipamentos Ativos de Rede

Justificativa:

1. **Controle Reduzido sobre a Infraestrutura**: A locação de equipamentos pode levar a um menor controle sobre a infraestrutura de rede. A gestão dos equipamentos locados fica parcialmente nas mãos do locador, o que pode dificultar a administração eficaz e a personalização da rede conforme as necessidades específicas do novo projeto.
2. **Custos Potenciais Mais Altos**: Embora a locação possa apresentar custos iniciais mais baixos, os custos totais podem se acumular ao longo do tempo. A longo prazo, a locação pode resultar em um custo mais elevado comparado à aquisição, especialmente considerando o período necessário para o projeto e possíveis ajustes.

3. **Expertise e Recursos da CGTI**: A equipe da CGTI, que possui um quadro reduzido e limitada expertise em fiscalização contratual e gestão de equipamentos locados, pode enfrentar dificuldades significativas em garantir a conformidade e a qualidade dos serviços. Isso pode levar a problemas de gestão e manutenção que impactariam a eficiência da infraestrutura.

4. **Limitações na Personalização e Flexibilidade**: A locação pode limitar a capacidade de personalizar e ajustar a rede de acordo com as necessidades específicas do projeto. Além disso, a flexibilidade para atualizar ou modificar os equipamentos pode ser restrita, o que pode comprometer a adaptação a novas demandas ou tecnologias.

Conclusão: A locação de equipamentos ativos de rede não é viável devido ao controle reduzido sobre a infraestrutura, custos potenciais mais altos ao longo do tempo, desafios com a expertise e recursos da equipe da CGTI e limitações na personalização e flexibilidade da rede.

11. Análise comparativa de custos (TCO)

Composição da solução

A análise comparativa de custos foi elaborada considerando apenas as soluções técnica e funcionalmente viáveis, nos termos do inc. III art. 11 da IN-94 /2022/SGD, e inclui:

comparação de custos totais de propriedade (Total Cost Ownership – TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia, manutenção; e

memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Conforme determinado na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, deverá ser realizada a análise comparativa de custos envolvidos na contratação. Para isso, deverão ser consideradas somente as soluções **viáveis**, bastando o registro das soluções inviáveis no Estudo Técnico Preliminar da Contratação:

Art. 11

(...)

III - Análise comparativa de custos, que deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo:

a) Cálculo dos custos totais de propriedade (**Total Cost Ownership** - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento; e

b) Memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados;

IV - Estimativa do custo total da contratação; e

V - Declaração da viabilidade da contratação, contendo a justificativa da solução escolhida, que deverá abranger a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

§ 1º As soluções identificadas no inciso II consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

Como visto nos tópicos anteriores deste ETP, a **Solução 3**: **Aquisição de Ativos de Rede com Sistema de Gerenciamento em Nuvem, Controladora WLAN, Suporte e Garantia de 60 Meses** foi considerada a melhor alternativa dentre as opções elencadas, tratando-se da aquisição dos equipamentos por meio de recursos orçamentários de investimentos, proporcionando a substituição de todos os switches e roteadores da rede do Ministério das Cidades.

Após a definição da composição da solução de tecnologia da informação a ser adquirida, conforme registrado no item 9 das Especificações Técnicas deste estudo, verifica-se a necessidade da realização dos procedimentos relacionados ao levantamento das informações para a estimativa de custos para a aquisição da solução.

Neste sentido, verifica-se que o levantamento dos valores para a aquisição de bens e contratação de serviços em geral para os órgãos e entidades participantes do SISG - Sistema de Serviços Gerais, deve seguir os procedimentos administrativos definidos pela INSTRUÇÃO NORMATIVA SEGES /ME Nº 65, DE 7 DE JULHO DE 2021 da Secretaria de Gestão (SEGES) do Ministério da Economia. para tanto, este levantamento servirá para balizar a viabilidade financeira do projeto.

Em atendimento ao art. 5º da Instrução Normativa nº 65, de 07 de Julho de 2021:

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:
I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou

banco de preços em saúde, observado o índice de atualização de preços correspondente;
II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;
IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou
V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.
§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos.
§ 2º Quando a pesquisa de preços for realizada com fornecedores, nos termos do inciso IV, deverá ser observado:
I - prazo de resposta conferido ao fornecedor compatível com a complexidade do objeto a ser licitado;
II - obtenção de propostas formais, contendo, no mínimo:
a) descrição do objeto, valor unitário e total;
b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente;
c) endereços físico e eletrônico e telefone de contato;
d) data de emissão; e
e) nome completo e identificação do responsável.
III - informação aos fornecedores das características da contratação contidas no art. 4º, com vistas à melhor caracterização das condições comerciais praticadas para o objeto a ser contratado; e
IV - registro, nos autos do processo da contratação correspondente, da relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação, de que trata o inciso IV do caput.
§ 3º Excepcionalmente, será admitido o preço estimado com base em orçamento fora do prazo estipulado no inciso II do caput, desde que devidamente justificado nos autos pelo agente responsável e observado o índice de atualização de preços correspondente.

O custo da alternativa em questão foi elaborado considerando a necessidade mínima de atendimento, cujo valor unitário foi obtido considerando o levantamento constante na Pesquisa de Preços CGTI-MCID (5791725).

LOTE	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL POR ITEM
1	1	Switch Core - Instalação e configuração	Unidade	2	R$ 303.200,00	R$ 606.000,00
	2	Switch Acesso - Tipo 01 - Instalação e configuração	Unidade	16	R$ 87.070,00	R$ 1.393.120,00
	3	Switch Acesso - Tipo 02 - instalação e configuração	Unidade	40	R$ 79.000,00	R$ 3.160.000,00
	4	Ponto de acesso sem fio - Indoor	Unidade	92	R$ 28.520,00	R$ 2.623.840,00
	5	Sistema de Gerenciamento em Nuvem	Unidade	1	R$ 301.666,67	R$ 301.666,67
	6	Controladora WLAN	Unidade	1	R$ 426.300,00	R$ 426.300,00
	7	Rack - Instalação	Unidade	15	R$ 30.326,30	R$ 454.894,50
VALOR GLOBAL ESTIMADO						**R$ 8.965.821,17**

MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

DESCRIÇÃO DA SOLUÇÃO	ESTIMATIVA DE TCO AO LONGO DOS ANOS					TOTAL
	Ano 1	Ano 2	Ano 3	Ano 4	Ano 5	
Solução 3	**R$ 8.965.821,17**	-	-	-	-	**R$ 8.965.821,17**

12. Descrição da solução de TIC a ser contratada

Após análise das alternativas viáveis, considerando os aspectos técnicos e econômicos, a equipe de planejamento recomenda a adoção da estratégia delimitada na **solução 2.**

A solução escolhida foi a que melhor atende às necessidades do Ministério das Cidades, conforme às necessidades de negócio, tecnológicos e demais requisitos necessários e suficientes à escolha da solução de TIC, previstos nos itens 5, 6 e 7 deste ETP.

Diante do exposto, a solução será composta por 7 (sete) itens, conforme tabela a seguir:

ITEM	DESCRIÇÃO	CATMAT/CATSER	MÉTRICA OU UNIDADE DE MEDIDA	QUANTIDADE
1	Switch Core - Instalação e configuração	609690	Unidade	2
2	Switch Acesso - Tipo 01 - Instalação e configuração	618767	Unidade	16
3	Switch Acesso - Tipo 02 - instalação e configuração	618779	Unidade	40
4	Ponto de acesso sem fio - Indoor	486314	Unidade	92
5	Sistema de Gerenciamento em Nuvem	27472	Unidade	1
6	Controladora WLAN	486317	Unidade	1
7	Rack - Instalação	473605	Unidade	15

O prazo de vigência da contratação será de 60 (sessenta) meses contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

O objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º, 4º e 5º da IN SGD nº 94/2022:

Art. 3º Não poderão ser objeto de contratação:

I - mais de uma solução de TIC em um único contrato, devendo o órgão ou entidade observar o disposto nos §§ 2º e 3º do art. 12; e

II - os serviços dispostos no art. 3º do Decreto nº 9.507, de 2018, inclusive a gestão de processos de TIC e a gestão de segurança da informação.

Parágrafo único. O apoio técnico aos processos de gestão, de planejamento e de avaliação da qualidade das soluções de TIC poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do órgão ou entidade.

Art. 4º Nos casos em que a avaliação, mensuração ou apoio à fiscalização da solução de TIC seja objeto de contratação, a contratada que provê a solução de TIC não poderá ser a mesma que a avalia, mensura ou apoia a fiscalização.

Parágrafo único. A empresa ou o profissional contratado assumirá responsabilidade civil objetiva pela veracidade e pela precisão das informações prestadas, firmará termo de compromisso de confidencialidade e não poderá exercer atribuição própria e exclusiva de fiscal de contrato, conforme dispõe o art. 26, do Decreto nº 11.246, de 27 de outubro de 2022.

Art. 5º É vedado:

I - estabelecer vínculo de subordinação com funcionário de empresa prestadora de serviço terceirizado;

II - fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo contratado;

III - indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;

IV - demandar a funcionário de empresa prestadora de serviço terceirizado a execução de tarefas fora do escopo do objeto da contratação;

V - reembolsar despesas com transporte, hospedagem e outros custos operacionais, que devem ser de exclusiva responsabilidade da contratada;

VI - prever em edital exigências que constituam intervenção indevida da Administração na gestão interna do contratado;

VII - prever em edital exigência que os fornecedores apresentem, em seus quadros, funcionários capacitados ou certificados para o fornecimento da solução, antes da contratação;

VIII - adotar a métrica homem-hora ou equivalente para aferição de esforço, salvo mediante justificativa e sempre vinculada à entrega de produtos de acordo com prazos e qualidade previamente definidos;

IX - contratar por postos de trabalho alocados, salvo os casos justificados mediante a comprovação obrigatória de resultados compatíveis com o posto previamente definido;

X - fazer referências, em edital ou em contrato, a regras externas de fabricantes, fornecedores ou prestadores de serviços que possam acarretar na alteração unilateral do contrato por parte da contratada;

XI - nas licitações do tipo técnica e preço, incluir critérios de pontuação técnica que não estejam diretamente relacionados com os requisitos da solução de TIC a ser contratada ou que frustrem o caráter competitivo do certame;

XII - aceitar autodeclarações de exclusividade, ou seja, cartas ou declarações emitidas pela empresa proponente afirmando que seu próprio produto é exclusivo no mercado; e

XIII - definir forma de pagamento mediante exclusivo reembolso dos salários pagos.

13. Estimativa de custo total da contratação

Valor (R$): 8.965.821,17

A estimativa de custo total para a presente aquisição, de acordo com as necessidades do Ministério das Cidades, é de **R$ 8.965.821,17 (oito milhões, novecentos e sessenta e cinco mil oitocentos e vinte e um reais e dezessete centavos)**, conforme tabela detalhada abaixo:

LOTE	ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL POR ITEM
1	1	Switch Core - Instalação e configuração	Unidade	2	R$ 332.200,00	R$ 664.400,00
	2	Switch Acesso - Tipo 01 - Instalação e configuração	Unidade	16	R$ 87.070,00	R$ 1.393.120,00
	3	Switch Acesso - Tipo 02 - instalação e configuração	Unidade	40	R$ 79.000,00	R$ 3.160.000,00
	4	Ponto de acesso sem fio - Indoor	Unidade	92	R$ 28.520,00	R$ 2.623.840,00
	5	Sistema de Gerenciamento em Nuvem	Unidade	1	R$ 301.666,67	R$ 301.666,67
	6	Controladora WLAN	Unidade	1	R$ 426.300,00	R$ 426.300,00
	7	Rack - Instalação	Unidade	15	R$ 30.326,30	R$ 454.894,50

VALOR GLOBAL ESTIMADO	**R$ 8.965.821,17**

Sigilo Orçamentário

A equipe responsável pelo planejamento da contratação manifesta-se no sentido de que não há impedimento à divulgação do orçamento estimado para a presente contratação. Tal entendimento fundamenta-se no fato de que o valor orçamentário detalhado será oportunamente tornado público por meio de sua publicação no Diário Oficial da União (DOU), em conformidade com os procedimentos legais que regem o processo licitatório. Dessa forma, a exigência de transparência está devidamente assegurada pelos instrumentos oficiais de publicidade previstos na legislação vigente.

14. Justificativa técnica da escolha da solução

A escolha dos equipamentos e soluções propostos deve ser justificada com base em:

- **Desempenho e Capacidade**: A seleção de switches core e de acesso é fundamentada na necessidade de alta performance e capacidade para suportar o tráfego de dados e o número de dispositivos conectados.
- **Cobertura e Qualidade do Sinal**: Pontos de acesso sem fio foram selecionados para garantir uma cobertura eficiente e estável, atendendo às necessidades de conectividade dos dispositivos móveis e outros equipamentos sem fio.
- **Gerenciamento e Monitoramento**: A escolha de um sistema de gerenciamento em nuvem e de uma controladora WLAN é justificada pela necessidade de um controle centralizado e eficaz sobre a infraestrutura de rede.

DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

A contratação poderá ser parcelada com base em:

- **Complexidade dos Equipamentos**: A separação dos componentes (switches core, switches de acesso, pontos de acesso sem fio, etc.) permite um melhor gerenciamento e controle da execução do projeto.
- **Fases de Implementação**: A entrega e instalação dos equipamentos podem ser feitas em fases, começando pelos switches core e racks, seguidos pelos switches de acesso e, finalmente, pelos pontos de acesso sem fio e a controladora WLAN.

15. Justificativa econômica da escolha da solução

A escolha das soluções deve ser justificada economicamente com base em:

- **Custo-Benefício**: Análise dos custos envolvidos em relação ao desempenho e benefícios oferecidos pelos equipamentos e soluções propostas.
- **Eficiência Operacional**: A implementação de um sistema de gerenciamento em nuvem pode reduzir os custos operacionais com manutenção e suporte técnico a longo prazo.
- **Escalabilidade**: A escolha de equipamentos e soluções que permitam fácil expansão e atualização contribui para a eficiência econômica a longo prazo.

O PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

O parcelamento pode ser realizado com base em:

- **Orçamento Disponível**: Dividir a aquisição em parcelas que correspondem ao orçamento disponível em cada período.
- **Condiciones de Pagamento**: Negociar condições de pagamento com fornecedores para melhor adequação ao fluxo de caixa do ministério.

16. Benefícios a serem alcançados com a contratação

Os resultados a serem alcançados constam no Documento de Formalização de Demanda (DFD) SEI nº 4845666 e estão a seguir relacionados:

- Proporcionar conectividade eficiente e confiável em toda a nova sede do Ministério.
- Proporcionar escalabilidade de rede de comunicação na nova Sede.
- Cobertura de rede Wi-Fi abrangente em todas as áreas da nova sede, proporcionando acesso estável à rede sem fio em todos os ambientes.

- Recursos avançados de segurança nos ativos de redes adquiridos, fortalecendo a proteção contra ameaças cibernéticas.
- Redução de possíveis falhas e, consequentemente, diminuição do tempo de inatividade.
- Suportar tecnologias emergentes, como Internet das Coisas (IoT) e implementações futuras.
- Proporcionar uma infraestrutura de rede robusta e uma solução de Wi-Fi eficaz.
- Proporcionar a substituição de equipamentos defasados.

17. Providências a serem Adotadas

Providências a serem adotadas

Para avaliar a qualidade dos produtos entregues e garantir a aceitação dos mesmos, serão considerados os critérios abaixo:

Estado dos Equipamentos e Softwares:

Todos os equipamentos e softwares fornecidos devem ser novos, assegurando a qualidade e a eficiência dos componentes.

Compatibilidade e Funcionalidades:

Os componentes dos equipamentos e softwares, bem como suas funcionalidades, devem ser plenamente compatíveis entre si, garantindo a integração adequada do sistema.

Padrão de Aceitação:

Será adotado como padrão o processo de recebimento provisório e definitivo do objeto contratado, seguindo as condições acordadas.

Infraestrutura Pré-Instalada:

Os pontos lógicos e elétricos devem estar instalados previamente para permitir que a empresa execute a instalação dos pontos de acesso de forma eficiente.

Cadastramento e Qualificação dos Funcionários:

Todos os funcionários da empresa envolvidos nos serviços (instalação, configuração, manutenção e suporte) devem ser previamente cadastrados e qualificados.

Compromissos Documentados:

Após a contratação dos serviços, a empresa contratada é obrigada a assinar Termo de Compromisso, Termo de Ciência e Termo de Confidencialidade, formalizando seu comprometimento com as condições estabelecidas.

Cronograma de Implantação:

A empresa deverá apresentar um cronograma detalhado de implantação da solução, fornecendo transparência e clareza quanto aos prazos e etapas do processo de implementação.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Os estudos preliminares evidenciam que a realização da contratação pretendida é viável. Com o avanço tecnológico aliado ao fenômeno da globalização fez com que o setor produtivo buscasse alternativas para o aperfeiçoamento de bens e serviços produzidos, com redução de custos, e que essa busca culminou em um processo cada vez maior de especialização, e consequentemente com a contratação de terceiros para as atividades que não constituíssem a atividade principal da organização. Nesse caso, a Informática, ou Tecnologia da Informação, é uma área passível desse modelo de prestação de serviços. Tratando mais especificamente das Unidades do MCID, é cada vez mais relevante a capacidade da TI em suportar as atividades institucionais com novas soluções, serviços e implementações, portanto, faz-se necessária a contratação do serviço de TI para o atendimento das demandas e prestação de serviços, além de outras atividades afins da Tecnologia da Informação.A equipe técnica de planejamento da Contratação declara e justifica a viabilidade da contratação, considerando que a solicitação atende e está em conformidade com as necessidades do Ministério das Cidades.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

BRUNO LUCENA DE SA FREIRE

Equipe de Planejamento

Assinou eletronicamente em 12/08/2025 às 15:40:19.

EMERSON MOREIRA DE MORAIS

Equipe de Planejamento

Assinou eletronicamente em 12/08/2025 às 15:37:27.

LUCAS MENDES DOS SANTOS

Autoridade Maxima de TIC

Assinou eletronicamente em 12/08/2025 às 15:39:46.

HAROLDO RODRIGUES DA SILVA

Equipe de Planejamento