1. INTRODUÇÃO

# A presente Especificação Técnica visa a implantação da INFRAESTRUTURA DE REDE ÓPTICA MUNICIPAL DA PREFEITURA DO MUNICÍPIO DE BRAGANÇA PAULISTA, COM FORNECIMENTO DE SERVIÇOS, MATERIAIS E EQUIPAMENTOS.

# Trata-se da instalação de uma rede de telecomunicações com alta capacidade de tráfego (velocidade e banda) composta de um conjunto de camadas física (hardware), de controle operacional (software) e de serviços que propicia a infraestrutura de operação em ambiente de comunicações baseado nos protocolos da Internet, tendo um caráter universalizante e de multi-serviços. Isso significa que ela possibilita a distribuição de todos os serviços oferecidos separadamente pelos sistemas atuais de telecomunicações, sendo, portanto capaz de tratar com igual eficiência tanto o tráfego de dados como os de telefonia, vídeo e áudio.

# A Infovia Municipal almeja dotar a Prefeitura de uma moderna rede integrada de telecomunicações englobando escolas, unidades de saúde, unidades administrativas e de atendimento da população.

1. DO OBJETO

A contratação de que trata o presente Pregão Presencial tem como objeto a instalação de um moderno sistema de comunicação que se caracteriza por alta disponibilidade, alta performance, redundância, contingência, segurança e convergência em consonância com as especificações e exigências técnicas contidas nesse e demais anexos. Este moderno Sistema de Comunicação possibilitará redução de custos com comunicação (voz e dados) em longo prazo, bem como enorme melhoria na prestação de serviços que dependem de informatização nas unidades atendidas. Futuramente, permitirá também a inclusão de dispositivos que melhorarão inclusive a segurança pública, como câmeras de vídeo-monitoramento.

As premissas básicas centrais se referem à qualidade dos serviços disponibilizados através da utilização de protocolo TCP/IP trafegando em Backbone Óptico Gigabit Ethernet e Conectividade de última milha no padrão de rede óptica passiva - GPON interligando os próprios da Prefeitura.

# Os serviços, materiais e equipamentos a serem fornecidos englobam:

### O fornecimento dos materiais e a instalação da Rede de Comunicação Óptica;

### A instalação e a configuração dos equipamentos ativos da Rede;

### A configuração do Centro de Operação e Gestão da Rede;

### O fornecimento, a instalação da infraestrutura e a configuração dos Pontos de Presença (POP na sigla inglesa derivada de “point of presence”).

### O fornecimento, a instalação das unidades de acesso (Sites).

### O fornecimento, a instalação da infraestrutura e a configuração dos Hot Spot (Ponto de acesso a população).

# Está prevista a instalação de 03 POP’s e a interconexão de 43 localidades (sites) e 13 Hot Spots.

# O Anexo V – Concepção Geral da Infovia – apresenta um resumo da concepção da Infovia definindo o contexto geral do projeto a ser implementado.

1. DETALHAMENTO

# Aspectos Gerais

# Todos os serviços deverão ser realizados com o máximo de esmero e ótimo acabamento, utilizando-se de materiais e acessórios de primeira linha, novos, não sendo aceitos componentes improvisados ou usados.

# A CONTRATADA deverá assegurar a correta integração e funcionalidade dos serviços, tendo em vista as especificações técnicas constantes desse Termo de Referência.

# As exigências aqui formuladas são mínimas de acordo com cada caso, devendo prevalecer sempre as Normas Brasileiras, Regulamentos, Posturas Municipais, Estaduais, Federais, Normas dos Fabricantes e das operadoras de eletricidade e de telecomunicações que apresentarem exigências mais rigorosas que as aqui constantes.

# A Vistoria Técnica é imprescindível e obrigatória: A vistoria técnica deverá ser realizada até a data anterior à abertura da sessão em horário de expediente, das 08:00 às 14:00, mediante agendamento prévio através do telefone (11) 4034-7032 com um colaborador da Diretoria de Tecnologia da Informação.

# O atestado de vistoria deverá ser apresentado junto à documentação solicitada no edital, sob pena de inabilitação.

# Neste termo são descritas as quantidades estimadas para execução da solução licitada, mais é obrigação da empresa licitante prever todo o quantitativo e serviço necessário para atendimento da necessidade dessa administração, por isso é obrigatória a visita técnica para a licitante obter todas as informações relevantes a execução dos serviços

# Todos os modelos de produtos e materiais ofertados devem estar em linha de produção, sem previsão de encerramento, na data da entrega da proposta.

# Dos Serviços

# A execução dos serviços deverá obedecer às especificações constantes dessa Especificação Técnica e todos os seus anexos.

# A FISCALIZAÇÃO dos serviços ficará a cargo da equipe técnica da Prefeitura.

# Quando, durante o desenvolvimento dos serviços, surgirem necessidades de modificações no projeto aprovado, elas deverão ser submetidas à apreciação da CONTRATANTE, podendo ser implementadas somente após sua aprovação.

# Todos os serviços devem ser executados de acordo com as posturas municipais e obedecendo às normas técnicas adequadas.

# Fazem parte dos serviços a remoção e reposição de forros, divisórias, piso elevado e vidros, bem como as adequações necessárias, desde que interfiram diretamente no objeto deste Edital.

# Deverá ser realizada a limpeza dos locais afetados pelos serviços incluindo a remoção, para locais apropriados, de possíveis entulhos.

# Ficará a CONTRATADA obrigada a desfazer instalações executadas inadequadamente, quando rejeitadas pela FISCALIZAÇÃO, refazendo-as corretamente, ficando por sua conta as despesas decorrentes desses serviços.

# Ocorrendo atraso, o prazo do cronograma será aumentado na mesma proporção, devendo a CONTRATADA notificar a CONTRATANTE dos motivos do atraso, a qual deverá analisar a solicitação, autorizando ou não a prorrogação.

# Serão impugnados pela CONTRATANTE todos os trabalhos que não satisfizerem plenamente as condições contratuais.

# No período de garantia a disponibilidade dos serviços on site deverá ser de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

# A contratada deverá possuir uma Central de Gerenciamento de rede para atendimento 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana com equipe técnica especializada para realizar intervenções remotas em casos de pane ou falha;

# A Contratada deverá disponibilizar uma Central de Gerenciamento de Rede remota para fazer o gerenciamento remoto da rede facilitando a detecção de falhas e aplicação de ações preventivas.

# A Central de Gerenciamento de Rede deverá ser 24 horas por dia x 7 dias por semana e deverá possuir telefone 0800 para atendimento e abertura de chamado, software de gerencia SNMP para os equipamentos que forem instalados e software de chamados Web ITIL;

# A Central deverá possuir profissionais qualificados para prestação de serviços de suporte telefônico.

# A proponente deve obrigatoriamente indicar em sua proposta comercial, sob pena de desclassificação, endereço de sua central de gerenciamento de rede, nome do profissional responsável pelo gerenciamento da rede, técnico/engenheiro com registro no CREA.

# Antes da assinatura do contrato a Prefeitura realizará visita técnica as instalações da proponente para verificar e validar a disponibilidade da Central de Gerenciamento de Rede.

# Dos Materiais e Equipamentos

# Todos os materiais e equipamentos a serem utilizados nos serviços deverão ser novos, comprovadamente de primeira qualidade, devendo atender rigorosamente às condições estipuladas no Anexo II – Requisitos Mínimos de Materiais e Equipamentos.

# A CONTRATANTE poderá, a qualquer momento, solicitar o exame dos materiais utilizados e impugnar o seu emprego, quando em desacordo com as Especificações do Anexos III e /ou com as amostras previamente aprovadas.

# Obriga-se a CONTRATADA a retirar do local de execução dos serviços, os materiais ou equipamentos porventura impugnados, dentro de 03 (três) dias úteis, ficando expressamente proibido manter no local de execução dos serviços quaisquer materiais que não satisfaçam a estas Especificações.

# Materiais adicionais (Ex.: buchas e parafusos, fita adesiva, fita isolante, rebites, pregos, etc.) necessários aos serviços de instalação integral do sistema, a partir da infraestrutura oferecida e que não estejam claramente especificados e cotados na proposta, serão considerados como parte integrante da proposta.

# Da Mão de Obra

# Toda a mão-de-obra necessária aos serviços de instalação, a partir da infraestrutura oferecida pela CONTRATANTE, será de responsabilidade única e exclusiva da CONTRATADA, que deverá fornecer equipe técnica suficiente para atender às necessidades do objeto contratado.

# Antes do início da execução dos serviços, a CONTRATANTE apresentará o responsável da CONTRATADA à chefia dos locais onde os mesmos serão executados.

# A CONTRATADA deverá apresentar às chefias dos órgãos envolvidos a relação do pessoal que permanecerá nas dependências dos prédios onde serão executados os serviços.

# Todos os funcionários da CONTRATADA deverão portar identificação quando da execução dos serviços.

# Todos os funcionários da CONTRATADA deverão usar equipamento de segurança e atender as normas técnicas pertinentes.

# A CONTRATANTE poderá exigir da CONTRATADA, a qualquer tempo, a substituição de qualquer profissional desde que verificada incompetência na execução das tarefas a seu cargo ou no caso do profissional apresentar hábitos de conduta inadequados ao bom andamento dos trabalhos.

# A substituição de qualquer profissional deverá ser processada em no máximo 48 (quarenta e oito) horas após a comunicação, por escrito, pela CONTRATANTE.

# Qualquer dano causado pela CONTRATADA ou seus prepostos, seja por imperícia, acidente ou negligência, deverá ser reparado de imediato, ficando suspensos os pagamentos das faturas pendentes até a execução dos reparos.

# Das Instalações, Configurações e dos Testes.

# Antes da execução dos serviços a empresa vencedora deverá elaborar um Plano de Instalação (PI) com base no projeto básico que será disponibilizado à CONTRATADA após a contratação, devendo atender às especificações mínimas contidas neste item e seus subitens.

# Seguindo o cronograma descrito no ANEXO V, após a execução Plano de Instalação (PI) a CONTRATADA deverá elaborar um Plano de Configuração (PC) com base nos equipamentos da rede Metro Ethernet e Gpon, devendo atender às especificações mínimas contidas neste item e seus subitens.

# O PI deverá conter, no mínimo:

# O cronograma detalhado de execução das atividades,

# A planta do município com todos os pontos (locais) que serão atendidos, detalhando o caminho exato de passagem do cabo óptico e como serão atendidas as premissas deste TR,

# As entradas dos cabos em todos os POP’s e seu retorno para dar continuidade ao seu caminho pelos pontos de passagem, detalhando como serão atendidas as premissas deste TR,

# O projeto de abertura do cabo e instalação completa de todos os POP’s, detalhando como serão atendidas as premissas deste TR.

# O PC deverá contemplar, ainda, os seguintes aspectos mínimos de configuração:

# Configuração do switch CORE instalado no Data Center da CONTRATANTE

# Tipo de protocolo de roteamento utilizado nos POP;

# Tipo de protocolo de roteamento utilizado nos switches COREs;

# Tipo de protocolo de roteamento utilizado nas unidades (sites) e hot spot`s;

# Tabela de roteamento entre redes existentes;

# Plano de endereçamento para rede local levando em consideração a rede atual;

# Endereçamento IP dos ativos;

# Configuração de trunking (agregação de links);

# Configuração de porta redundante nos POP;

# Programação de controle de broadcast inclusive fixando limite máximo de broadcasts por porta;

# Configuração de priorização de tráfego filas por porta;

# Configuração de VLAN’s levando em consideração as existentes na rede atual;

# Criação de rotina para envio de mensagem de correio eletrônico via SNMP, em caso de queda de links específicos, ativação de link resilientes e ciclo de Power up do switch;

# Criação de listas de controles de acesso visando à segurança;

# Configuração de roteamento entre VLAN’s;

# Criação de listas de controle de acesso e política de segurança.

# O PI e o PC poderão conter sugestões de melhorias no projeto geral da Infovia.

# O PI e o PC deverão obedecer a todas as especificações, requisitos e exigências contidas nesta Especificação Técnica e todos os seus anexos.

# O PI e o PC somente poderão ser executados após o seu aceite da equipe responsável da CONTRATANTE.

# Durante a instalação e testes, a CONTRATADA deverá se responsabilizar pelo fornecimento e segurança do ferramental de instalação e instrumental de testes.

# Deverão ser executados todos os testes necessários para o funcionamento dos produtos solicitados.

# A instalação deverá, obrigatoriamente, ser efetuada de forma a não afetar o funcionamento dos serviços já em operação, garantindo a continuidade dos serviços de voz e dados aos seus atuais usuários.

# No caso de necessidade de interrupção de outros serviços ou equipamentos, em decorrência da instalação a ser efetuada, esta deverá estar devidamente planejada e ser acordada com antecedência junto à CONTRATANTE.

# A CONTRATADA poderá propor modificações nas instalações de maneira a facilitar sua operação, manter a integridade física das pessoas e das instalações e proteger equipamentos, observando as normas técnicas e de segurança de seus funcionários.

1. REDE DE COMUNICAÇÃO ÓPTICA

# Aspectos Gerais

# As malhas de fibra óptica são as principais vias para escoamento do tráfego digital gerado, devendo ser dispostas em forma de anéis e em formato estrela, conforme apresentado no Anexo V – Concepção Geral da Infovia.

# O escopo de contratação engloba:

# O lançamento dos cabos ópticos;

# A instalação dos pontos de telecomunicações e de links ópticos;

# O fornecimento de todo o material necessário, incluindo os ativos de rede e racks’s;

# O fornecimento de toda a mão de obra necessária.

# Entende-se por lançamento de cabos ópticos, no mínimo:

# A fixação dos cabos de fibras ópticas em postes;

# A passagem eventual dos cabos ópticos em dutos e sub-dutos subterrâneos;

# A passagem dos cabos ópticos com travessia aérea;

# A passagem dos cabos ópticos em eletrodutos, eletrocalhas, mangueiras ou similares no interior de prédios;

# O tensionamento dos cabos ópticos;

# A fixação ou enrolamento na cordoalha;

# A instalação de suportes, conjuntos de ancoragem e outras ferragens;

# A identificação dos cabos ópticos e das caixas de emendas.

# Entende-se por instalação de pontos de telecomunicações e de links ópticos, no mínimo:

# A instalação dos DIO´s – Distribuidores Internos Ópticos – em conformidade com os tipos de fibras e conectores definidos;

# A instalação de caixas de passagem, inspeção e emenda, de acordo com os tipos definidos;

# A instalação de armários (racks) e sub-bastidores (sub-racks);

# A instalação dos ativos de rede necessários (a serem fornecidos pela CONTRATANTE);

# A instalação de cordões ópticos;

# As derivações em redes de fibras ópticas;

# A configuração dos equipamentos ativos presentes na INFOVIA;

# A fusão das fibras ópticas.

# Características Básicas

# A lista de materiais para a infraestrutura e passagem de fibra deve seguir os padrões dos itens referentes no Anexos III.

# Durante os serviços não será permitida qualquer alteração no Projeto Básico existente, que não seja oficializada por escrito, com, pelo menos, 5 (cinco) dias de antecedência da execução e devidamente validada pela FISCALIZAÇÃO.

# O encaminhamento do backbone óptico deverá ser de modo aéreo através dos postes da Concessionária de Energia.

# A negociação quanto à aprovação por parte da Concessionária de Energia Elétrica para utilização desta infraestrutura será de responsabilidade da Prefeitura, ficando a CONTRATADA com a responsabilidade de apresentar plantas, desenhos e locais dos postes a serem utilizados, bem como o cálculo de esforços neles aplicados com as novas instalações.

# Toda a infraestrutura para ancoragem dos cabos deverá ser executada antes do início de lançamento pela CONTRATADA.

# Antes de desenrolar as bobinas com os cabos ópticos, deverá ser feita verificação visual e com equipamentos OTDR se as mesmas encontram-se em ordem, ou seja, se não foram danificadas durante o embarque, transporte e desembarque.

# Os cabos ópticos não devem ser estrangulados, torcidos, prensados e deve-se evitar que sejam “pisados”, com o risco de provocar alterações nas características originais do cabo.

# Caso seja verificado pela FISCALIZAÇÃO presença de cabos ópticos estrangulados, torcidos ou prensados e que estão provocando alterações nas características originais do cabo, eles deverão ser substituídos sem ônus para a CONTRATANTE.

# Na ocasião do puxamento do cabo óptico, a CONTRATADA deverá tomar o cuidado de monitorar a carga de tracionamento do cabo, através do dinamômetro e respeitando-se a carga máxima de tracionamento permitida para cada tipo de cabo.

# Os tracionamentos e curvas realizadas em todo percurso na instalação da fibra ótica deverão seguir as normas técnicas, garantindo que:

# As curvaturas não excedam 90 graus;

# Os tracionamentos não sejam com folgas e não excedam 11,3 Kg de tensão.

# As sobras dos cabos ópticos deverão ser acomodadas, considerando-se sempre sua fixação e seu raio de curvatura.

# Se houver a necessidade de utilização do percurso aéreo, considerando poda parcial de árvores e/ou fechamento temporário de ruas e avenidas, deverá ser comunicado antecipadamente por escrito à CONTRATANTE, com no mínimo 3 (três) dias úteis.

# Os cabos ópticos deveram ser lançados no percurso com fibras auto-sustentáveis.

# Não serão permitidas fusões ou emendas nos lances de fibras ópticas, salvo as necessárias para a conectorização nos DIO´s e nas caixas de fusão.

# Os cabos terão uma identificação única com plaquetas que deverão obedecer ao modelo e layout solicitados em edital.

# As plaquetas de identificação referidas no item anterior deverão ser fixadas a cada lance de 20 metros, em cada poste, nas caixas de passagem e nos rack’s em todo o percurso da Infovia.

# Todo poste deverá conter uma abraçadeira ajustável, uma armação “press bow” com 1 (um) isolador.

# Em todas as esquinas onde não são viáveis os lançamentos de um cabo óptico de poste a poste, o lançamento do cabo será feito através de duas cordoalhas, instaladas de modo a formar um ângulo de 90º envolvendo outros 2 postes.

# Deverão ser respeitadas as normas de passagem de cabeamento nos postes, ou seja, a faixa de altura entre cada poste e a rede elétrico-telefônica e altura mínima necessária para pontos de travessias.

# Na travessia de avenidas e estradas, ou seja, em travessias longas, a fibra ótica deverá ser lançada em altura superior com a utilização de cabo de aço, evitando acidentes com o trânsito de veículos de grande porte.

# Está prevista uma margem de segurança de 30% para as travessias, entradas de POP´s e sites, sobras, entre outras, já incluso na estimativa de metragem de fibra ótica e outros materiais adjuntos.

# Na entrada de cada prédio (sites contemplados, abrigando ou não algum POP), o cabo óptico deverá ser lançado até o poste ou a caixa subterrânea mais próximo, onde será encaminhado até a fachada da localidade que terá uma armação “press bow” com 1 (um) isolador para a fixação do cabo (no caso de instalação aérea) ou na caixa de passagem da entrada do prédio (no caso de instalação subterrânea), ficando a definição dependente da logística de cada unidade, onde os quesitos facilidade de acesso e segurança física da instalação serão as variáveis analisadas.

# A infraestrutura da entrada do cabo de fibra ótica em cada prédio até o rack interno deverá ser instalada pela CONTRATADA, ou seja, deverá ser construída uma tubulação de eletroduto de 2” (duas polegadas) prensado e galvanizado a fogo para o encaminhamento do cabo até o armário de telecomunicações do prédio, observando que todas as tubulações para o encaminhamento de fibra óptica não podem ter curvas com raios menores que 60mm, não sendo permitido o uso de conduletes em pontos de curva.

# A CONTRATADA poderá realizar alguns serviços simples de alvenaria, principalmente quanto à construção de caixas de passagens e possíveis perfurações em paredes dos imóveis (Sites e POP´s) para passagem de eletrodutos, ficando responsável pela realização de todos os reparos, reconstruções e acabamentos que se fizerem necessários.

# No caso de construção de caixas de passagem, elas deverão obedecer ao código de obras do município, principalmente no aspecto de drenagem, devendo a tubulação subterrânea deverá ser envelopada com concreto.

# Dentro das caixas de fusão e DIO’s, os cabos deverão ser desencapados e a fusão feita com extensões ópticas, os pigtails fornecidos pela CONTRATADA.

# Deverão ser instaladas caixas de fusão de até 24 FO’s nos Anéis na passagem de fibra ótica, a cada término de bobina de fibra e quando for necessário por algum motivo técnico do percurso.

# Nas caixas de passagem deve ser deixado pelo menos uma volta de cabo óptico contornando as laterais da caixa de passagem, para ser utilizado como folga estratégica para uma eventual manutenção do cabo óptico.

# Nos pontos de emendas, deverão ser deixados, no mínimo, cinco metros de cabo óptico, com o objetivo de se ter sobra suficiente para as emendas ópticas.

# Deverá ser evitado o fracionamento (fusão) em demasia nas passagens das fibras.

# Não deverão ser instaladas caixas de passagem e fusão próximas a caixas de terceiros.

# As perdas de potência ótica deverão atender aos limites máximos apresentados a seguir:

# Conector: máximo de 0,5 dB;

# Emenda: máximo de 0,2 dB;

# Fibra ótica instalada: máximo de 0,5 dB/km.

# A CONTRATANTE poderá, sempre que julgar necessário, solicitar à CONTRATADA o relatório de medição de perdas de potência.

1. EQUIPAMENTOS ATIVOS DE REDE

# Ativos de Rede

# A CONTRATADA deverá executar a instalação, adequação e configuração dos equipamentos ativos de rede tanto novos quanto os já existentes que necessitarem de mudanças e/ou reconfigurações em conformidade com o detalhado no Plano de Configuração (vide item 3.5.4 e subitens).

# Todos os ativos de rede previstos no projeto básico e necessários para o perfeito funcionamento da Infovia fazem parte do escopo de fornecimento desse certame e deverão ser fornecidos pela CONTRATADA.

# A lista completa com descrição dos ativos a serem fornecidos no item anterior, com as características necessárias consta no Anexo II – Requisitos Mínimos.

# Deverão ser instalados, 2 (dois) equipamentos do tipo Switch Core, ambos na SMTI ;.

# Ambos os equipamentos referidos no item anterior deverão ser instalados e configurados de tal forma que quando um deles falha o outro assume a rede automaticamente.

# Nos POP’s a CONTRATADA deverá instalar e configurar switches que façam o fechamento dos anéis com protocolo de redundância de rede, ou seja, quando ocorrer falha no link de um dos trechos do anel, o equipamento reconhece a falha e reestabelece automaticamente a conexão utilizando outro caminho, conforme especificado no item 2.10 do Anexo I – POP – Ponto de Presença.

# Nas unidades a CONTRATADA deverá instalar e configurar, os equipamentos para receber o sinal enviado pelos POP’s.

# Todos equipamentos a serem fornecidos deverão ser compatíveis com os equipamentos existentes.

# A empresa terá acesso às informações dos equipamentos existentes durante a Visita Técnica, conforme prevista em 3.1.4 acima.

# Todos os equipamentos deverão ser configurados por profissionais qualificados, estando previstas todas as funcionalidades no Anexos III.

# Racks

# A CONTRATADA deverá instalar e adequar fisicamente os racks nos locais indicados pela CONTRATANTE e detalhados no PI.

# Todos os racks previstos no projeto básico e necessários para o perfeito funcionamento da Infovia fazem parte do escopo de fornecimento desse certame, devendo ser fornecidos pela CONTRATADA.

# A lista completa dos racks referidos no item anterior, com as características relevantes consta do Anexo II – Requisitos Mínimos Materiais e Equipamentos.

# A infraestrutura para lançamento do cabo óptico até o rack deverá ser construída pela CONTRATADA com eletrodutos galvanizados.

# POP´s, OLT´s, Localidades e ONU´s

# Os POP´s da Infovia deverão ser fornecidos e instalados pela CONTRATADA conforme especificações e exigências contidas no Anexo I – POP – Ponto de Presença..

# Nos POP’s deverão ser instalados OLT (“Optical Line Terminal”) para fazer a conexão com as localidades (sites).

# Nos sites deverão ser instalados ONU (“Optical Network Unit”) para fazer as conexões com os respectivos OLT dos POP´S.

# Todos os equipamentos deverão ser configurados por profissionais qualificados, estando previstas todas as funcionalidades no Anexos III.

# Instalações Elétricas

# A CONTRATADA deverá fornecer relatório com o dimensionamento das cargas de todos os POP´s levando em consideração os equipamentos que serão instalados em cada localidade atendendo as especificações contidas no Anexo I – POP – Ponto de Presença.

# Todos os POP´s deverão ter alimentação elétrica exclusiva de modo que a rede de entrada de cada localidade deverá alimentar diretamente um quadro elétrico de distribuição (QDG) específico em conformidade com as normas da ABNT.

# O quadro elétrico e o circuito deverão estar dimensionados para suportar a carga gerada pelos equipamentos que serão instalados no POP.

# Toda a infraestrutura de alimentação dos POP´s é de responsabilidade da CONTRATADA.

# Nas localidades (sites) a CONTRATADA deverá instalar um circuito independente para alimentação do rack local com um disjuntor específico e diretamente ligado na rede de entrada do prédio.

# No-break’s

# Nos POP’s deverão ser instalados, No-breaks dentro dos gabinetes outdoor de no mínimo 1,2 kVA, com capacidade de gerenciamento e conectados ao Sistema de supervisão e Telecomando.

# Em todos os gabinetes a CONTRATADA deverá considerar a instalação e fornecimento de Nobreak para garantir a disponibilidade em caso de falha de fornecimento de energia elétrica.

1. CENTRO DE OPERAÇÃO E GESTÃO DA INFOVIA MUNICIPAL

# Aspectos Gerais

# O Centro de Operação e Gestão da Infovia Municipal tem por objetivo garantir a qualidade dos serviços, objetivando alta disponibilidade, alta performance e segurança das informações e das instalações.

# O escopo de contratação engloba:

# Preparação de uma equipe técnica da CONTRATANTE que tenha condições de oferecer serviços qualificados para atendimento preventivo e corretivo, com o compromisso de manter a rede funcionando 24 horas;

# Instalação dos ativos de rede em conformidade com o especificado no Anexos III;

# Fornecimento e instalação dos pontos de acesso para os Hot Spot conforme especificado no Anexo II.

# Fornecimento de todo o software conforme especificado no Anexos III.

# Características Básicas

# Deverá ser configurado no software de gerenciamento da rede toda a gestão dos ativos de rede da Prefeitura.

# O software deve garantir o monitoramento, mapeamento e ação para o funcionamento do NOC (Centro de Operação da Rede) da Prefeitura.

# A empresa deverá dar respaldo técnico e treinamento, para a implantação do Centro de Operação e Gestão da Infovia Municipal.

# Deverão ser configuradas todas as funcionalidades responsáveis por visualização e ajuste, para o perfeito funcionamento do equipamento com os POP´s e sites, visando atender a contento, a transmissão de dados, voz e imagem, nas unidades da PMU.

# A cada 3 (três) meses da data de instalação, no primeiro ano, deverá a CONTRATADA, através de amparo técnico do fabricante, realizar manutenção preventiva na rede (CORE e outros equipamentos) para melhor desempenho, confiabilidade e correção de erros, com o devido acompanhamento técnico da PMU.

# O conceito de redundância deverá ser respeitado e garantido, ou seja, a implementação lógica deve espelhar a topologia física da rede, garantindo que a rede não pare por um único rompimento de parte de um anel, resolvendo automaticamente, até o devido conserto da parte de fibra rompida.

1. NORMAS

# Para os serviços de instalação, deverão ser seguidas as normas e determinações abaixo, além de outras especificações, citadas neste termo de referência:

### **EIA/TIA 568A**: Commercial Building Telecommunications Wiring Standard.

### **EIA/TIA 569**: Commercial Building Standard for Telecommunications Pathways and Spaces.

### **EIA/TIA 607**: Commercial Building Grounding / Bonding Requirements.

### **EIA/TIA BULLETIN TSB-67**.

### **ABNT NBR 5410:2004** Versão Corrigida: 2008: Instalações Elétricas de Baixa Tensão;

### **ABNT NBR 5419:2005**: Proteção de Estruturas Contra Descargas Atmosféricas;

### **ABNT NBR 13570:1996**: Instalações Elétricas em Locais de Afluência de Público – Requisitos Específicos;

### **ABNT NBR 14136:2002** Versão Corrigida: 2007: Plugues e Tomadas para Uso Doméstico e Análogo até 20A/250 v em Corrente Alternada – Padronização;

### **ABNT NBR 14306:1999**: Proteção Elétrica e Compatibilidade Eletromagnética em Redes Internas de Telecomunicações em Edificações – Projeto.

### Normas da Concessionária de Energia Elétrica local, última revisão em vigor.

### Normas da Concessionária de Telefonia local, última versão em vigor.

1. TESTES

# Do Testes

# O sistema de backbone óptico deverá ser devidamente certificado com equipamento homologado e aferido OTDR (Optical Time Domain Reflectrometer).

# Ao final da execução dos serviços a CONTRATADA fornecerá relatório de todos os testes realizados em todos os pontos.

# O relatório referido no item anterior deverá ser aprovado pela equipe técnica da CONTRANTE que acompanhou os serviços.

# O sistema de óptico deverá ser devidamente certificado com equipamento homologado e aferido e com o fornecimento dos relatórios de aferição do equipamento e certificação das fibras.

# Cada seguimento deverá ser identificado individualmente conforme norma EIA/TIA 606 considerando a aplicação de etiquetas:

# Nas portas dos DIO’s,

# No cabeamento em todo o trajeto com plaquetas (conforme modelo descrito no anexo V)

# No inter-connect (nas duas extremidades do patch cord).

1. DOCUMENTAÇÃO E “AS BUILT”

# Do Encerramento dos Serviços

# Após a implantação do backbone óptico e conexão dos pontos finais, além da ativação dos mesmos, a CONTRATADA deverá fornecer em mídia digital e cópia heliográfica a documentação de “As Built” do sistema implantado composta por:

# Mapa base com os encaminhamentos das fibras atualizadas;

# Poligonal das fibras ópticas;

# Mapa de topologia da rede;

# Iidentificação dos cabos ópticos no mapa base;

# Diagramas unifilares do backbone;

# Diagrama unifilares das conexões com as unidades;

# Diagramas unifilares e de conexões das OLT;

# Diagramas de conexões nos DIOS;

# Diagramas das caixas de fusão;

# Backup das configurações finais das OLTs instaladas nos POPs

# Backup das configurações das ONUs instaladas nas localidades;

# Manual de instalação das OLTs;

# Manual de instalação das ONUs;

# Plano de face dos Armários de Telecomunicações instalados no backbone;

# Documentação completa dos gabinetes outdoor instalados nos POP’s;

# Planilha constando modelo dos equipamentos, número de serie, versão do software instalado, versão do firmware instalado.

# A documentação referida no item anterior deverá ser aprovada pela equipe técnica da CONTRATADA que acompanhou os serviços.

1. GARANTIA E PÓS-IMPLANTAÇÃO

# Aspectos Gerais

# Todos os itens deste Edital deverão ser instalados com garantia “on site” dos serviços, materiais e equipamentos de no mínimo 12 meses, ressalvadas as especificidades assinaladas ao longo desse Termo de Referência.

# Os serviços de manutenção, no período de garantia, deverão ser executados pela CONTRATADA.

# Durante o período de garantia a CONTRATADA compromete-se a executar os serviços de manutenção corretiva sem quaisquer ônus para a CONTRATANTE, inclusive de transporte e despesas acessórias.

# Não estarão cobertos pela garantia:

# Atos de vandalismo,

# Mau uso,

# Incêndio,

# Inundações ou

# Descargas atmosféricas.

# No período de garantia a disponibilidade dos serviços on site deverá ser de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

# A contratada deverá possuir uma Central de Gerenciamento de rede para atendimento 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana com equipe técnica especializada para realizar intervenções remotas em casos de pane ou falha;

# A Contratada deverá disponibilizar uma Central de Gerenciamento de Rede remota para fazer o gerenciamento remoto da rede facilitando a detecção de falhas e aplicação de ações preventivas.

# A Central de Gerenciamento de Rede deverá ser 24 horas por dia x 7 dias por semana e deverá possuir telefone para atendimento e abertura de chamado, software de gerencia SNMP para os equipamentos que forem instalados;

# A Central deverá possuir profissionais qualificados para prestação de serviços de suporte telefônico.

# A proponente deve obrigatoriamente indicar em sua proposta comercial, sob pena de desclassificação, endereço de sua central de gerenciamento de rede, nome do profissional responsável pelo gerenciamento da rede, técnico/engenheiro com registro no CREA.

# Antes da assinatura do contrato a PMU realizará visita técnica as instalações da proponente para verificar e validar a disponibilidade da Central de Gerenciamento de Rede.

# Atendimento

# Os chamados técnicos para serviços de manutenção de switches e equipamentos, no período de garantia, incluindo aqui no-breaks e cabos de conexão, deverão atender aos seguintes requisitos:

# Tempo de chegada do técnico ao local de instalação e reparo dos equipamentos, a partir da chamada, de no máximo 12 (doze) horas, dentro do período de disponibilidade.

# Período de disponibilidade de atendimento telefônico: 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

# Os chamados técnicos deverão ser abertos através de um telefone da central de atendimento a suporte técnico da CONTRATADA, sendo que o Suporte NÍVEL 1 deverá ser realizado por um profissional que identificará inicialmente a possível pane/falha no sistema e através de suporte telefônico prestará imediata assistência técnica para solução da pane/falha.

# Caso o Suporte Nível 1 não solucione a pane/falha, será acionado o Suporte NÍVEL 2, que deverá ser prestado por profissional que solucionará a pane/falha com intervenção on-site, e no caso de falha na operação em algum dos equipamentos indicados, este profissional deverá substituir o equipamento por um igual ou superior.

# Caso o Suporte Nível 1 exceda o atendimento de um chamado em 1 (uma) hora sem solucionar a pane/falha, o Suporte Nível 2 (on-site) deve ser acionado imediatamente.

# Nos casos extremos de remoção para manutenção, o equipamento deverá ser substituído por equipamento equivalente ou mais avançado até o próximo dia útil.

# É de responsabilidade da CONTRATANTE o fornecimento de switches na eventual necessidade de substituição em decorrência de problemas.

# É de responsabilidade da CONTRATANTE o fornecimento de OLTS e ONU na forma de backup, na eventual necessidade troca ou envio para garantia na decorrência de problemas.

# É de responsabilidade da CONTRATADA a substituição e configuração dos passivos instalados nos sites e POPs na eventual necessidade troca em decorrência de problemas.

# É de responsabilidade da CONTRATADA a substituição e configuração dos switches instalados nos sites e POPs na eventual necessidade de ocorrência de problemas.

# Quando da necessidade de instalação de equipamento IP para a substituição, ele deverá ser configurado e instalado seguindo as seguintes atividades:

# Instalação dos equipamentos nos racks envolvidos;

# Atribuição de endereçamento IP aos switches;

# Configuração de trunking (agregação de links);

# Programação de Controle de Broadcast, inclusive fixando limite máximo de Broadcasts por porta;

# Configuração de priorização de tráfego filas por porta;

# Configuração de VLAN’s (gerenciamento – dados – voz);

# Criação de links resilientes (redundantes) e implementação de protocolos Spanning Tree e Rapid Spanning Tree (IEEE 802.1w);

# Criação de rotina para envio de mensagem de correio eletrônico, via SNMP, em caso de queda de links específicos, ativação de link resiliente e ciclo power up do switch;

# Criação de listas de controle de acesso visando a segurança;

# Configuração de roteamento entre VLAN’s;

# Criação de Listas de Controle de Acesso e política de segurança;

# Configuração de network login.

# A CONTRATANTE deverá ser notificada sempre que se tornarem disponíveis atualizações de software para os produtos incluídos no contrato, devendo a referida notificação ser enviada no prazo máximo de 2 (duas) semanas contadas da data de disponibilidade do software.

# Não estará coberto neste contrato:

# Furto,

# Efeitos decorrentes da natureza, tais como: relâmpago, chuva, inundação;

# Mau uso,

# Erro operacional da CONTRATANTE,

# Incêndio,

# Explosão,

# Rompimento de fibra;

# Catástrofe ou

# Danos quando em trânsito;

# Anel Óptico

# Os chamados técnicos para serviços de manutenção de anel óptico, no período de garantia, deverão atender aos seguintes requisitos:

# Tempo de chegada do técnico ao local de instalação e reparo, a partir da chamada de no máximo 12 (doze) horas, dentro do período de disponibilidade.

# Período de disponibilidade de atendimento telefônico: 24 (vinte e quatro) horas por dia, 7 dias por semana.

# Os chamados técnicos deverão ser abertos através de um telefone da central de atendimento a suporte técnico da CONTRATADA, sendo que o atendimento NÍVEL 1 deverá ser realizado por um profissional, o qual identificará inicialmente a possível pane/falha no sistema e através de suporte telefônico prestará imediata assistência técnica para solução da pane/falha .

# Caso o Suporte Nível 1 não solucione a pane/falha, será acionado o Suporte NÍVEL 2, que deverá ser prestado por profissional, o qual solucionará a pane/falha com intervenção on site, e no caso de rompimento da fibra.

# Caso o Suporte Nível 1 exceda o atendimento de um chamado em 1 (uma) hora sem solucionar a pane/falha, o Suporte Nível 2 (on site) deve ser acionado imediatamente.

# Deverá ser considerado pela CONTRATADA em caso de rompimento da fibra, materiais adicionais como Caixa de Fusões, lances de fibra, patch cord óptico, extensões ópticas, alinhadores, a Contratada deverá relacionar os itens a serem utilizados para envio e aprovação por parte da Contratante.

# Para todo e qualquer rompimento da fibra, deverá ser feita fusão no cabo óptico.

# Toda infraestrutura para ancoragem dos cabos será executada antes do início de lançamento dos mesmos.

# No caso de rompimento do cabo de aço o mesmo deverá ser substituído e devidamente espinado por todo o percurso poste a poste.

# Em caso de problema com conectores, patch cords ópticos, alinhadores, cordões e Distribuidores Internos Ópticos o mesmo deverá ser substituído pela CONTRATADA.

# Após a fusão do cabo óptico, deverá ser efetuado teste de OTDR em todos os cabos ópticos envolvidos (em cada cabo óptico o teste deverá ser feito em ambas as extremidades, ou seja, dois testes de OTDR para cada fio óptico), com acompanhamento de um funcionário da CONTRATANTE e entrega de Relatório de Certificação.

# Quando da necessidade de fusão de fibra óptica rompida, a mesma não poderá ser efetuada a uma distância inferior a 200 metros de outra fusão, devendo ser trocado o lance de fibra neste caso.

1. TREINAMENTO

# Do Treinamento

# Deverá ser ministrado um treinamento da operação da rede implantada de no mínimo 2 dias sendo 8 horas diárias para até 5 técnicos da Prefeitura do Município de Ubatuba.

# A CONTRATADA deverá fornecer pelo menos 5 cópias das apostilas e todo o material didático relativo ao conteúdo apresentado durante o treinamento.

1. DAS OUTRAS EXIGÊNCIAS

**A proponente deverá apresentar ainda os seguintes documentos técnicos junto ao envelope “Documentação”:**

* 1. Certidão de Registro de Pessoa Jurídica, dentro de seu prazo de validade, junto ao CREA - Conselho Regional de Engenharia e Agronomia e/ou CAU (Conselho de Arquitetura e Urbanismo).
     1. Caso a empresa pertença a outra Região e vier a ser contratada pela PMU, deverá obrigatoriamente apresentar, ANTES da assinatura do Contrato, o Registro da empresa e de seus Responsáveis Técnicos com o competente visto do CREA-SP
  2. Certidão de Registro do profissional responsável, dentro de seu prazo de validade, junto ao CREA - Conselho Regional de Engenharia e Agronomia e/ou CAU (Conselho de Arquitetura e Urbanismo).
  3. Qualificação Operacional: Atestado(s) ou Certidão (ões) fornecido(s) por pessoa jurídica de direito público ou privado, necessariamente em nome da empresa licitante, devidamente registrado(s) no órgão competente CREA/CAU, (súmula 24 do TCESP e art. 30 da Lei); que comprove a execução dos seguintes serviços:
     1. Fornecimento e implantação de serviços de fibra óptica GPON, cabos de fibra óptica:

1. Fibra óptica – tipo I
2. Fibra óptica – tipo II
   * 1. Instalação e configuração de rede óptica passiva GPON (Gigabit passive optical network) ITU-T-G.984:
3. OLT (Optical Line Terminal)
4. ONU (Optical Network unit)
5. Instalação de switch Core 10 Gigabit
6. Instalação de switch de link
   * 1. Prestação de garantia on site da instalação com atendimento 24h x 7 dias x 6 horas com central de gerenciamento de rede e suporte telefônico.
     2. Fornecimento e implantação de soluções de serviços de fibra óptica GPON com no mínimo 15Km em postes de Concessionária de Energia Elétrica
   1. Comprovação do vínculo do profissional para atendimento do item descrito acima, mediante Contrato Social, registro na Carteira Profissional, Ficha de Empregado ou Contrato de Trabalho, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços.
      1. O(s) profissional(ais) detentor(es) do(s) atestado(s) para atendimento ao item 9.1.2. (b) deverá (ão) participar da obra objeto da licitação, como responsável (eis)pelos Serviços, nos termos do Inciso I do § 1º do art. 30 da LF 8.666/93, admitindo-se a substituição por profissional(ais) de experiência equivalente ou superior, desde que aprovada pela Administração.
   2. A proponente deverá declarar junto ao envelope documentação que caso seja a vencedora do certame, comprovará em até 48 horas após o encerramento da sessão os documentos solicitados abaixo:

* + 1. Comprovação de possuir em seu quadro de funcionários, no mínimo 02 técnicos que participarão da execução dos serviços, certificados no curso de NR10 - Norma regulamentadora do ministério do trabalho, relativo à prevenção de acidentes com eletricidade no ambiente de trabalho (anexar atestado que realizou o treinamento).
    2. Comprovação de possuir em seu quadro de funcionários, no mínimo 02 técnicos que participarão da execução dos serviços, certificados no curso de NR35 - Norma regulamentadora do ministério do trabalho, relativo à trabalho em altura (anexar atestado que realizou o treinamento).
    3. A proponente deverá comprovar que possuí pelo menos um equipamento homologado e aferido OTDR (Optical Time Domain Reflectrometer). Poderá haver diligenciamento para comprovar tal informação.
    4. A proponente deverá comprovar que possuí pelo menos um equipamento de fusão de fibra óptica. A comprovação poderá se dar através de declaração própria de que possui tal equipamento. Poderá haver diligeciamento para comprovar tal declaração.
    5. A proponente deverá comprovar possuir em seu quadro de funcionários pelo menos 2 técnicos com Certificado de Curso de Rede Óptica Passiva. A, comprovação se dará anexando junto a Documentação de habilitação os certificados. A comprovação do vínculo empregatício deverá ser feita através da apresentação de cópia autenticada do Contrato Social da empresa, em caso de sócio, da Carteira de Trabalho ou do contrato de prestação de serviços, assinados pela proponente;
    6. Os documentos poderão ser apresentados em original, cópia autenticada por Cartório ou cópia simples, para autenticação por membro da Comissão de Licitação, neste caso acompanhado dos originais, não sendo aceitos fac-símiles (fax).

1. DA PROPOSTA COMERCIAL
   * 1. A proponente deve anexar em sua proposta comercial sob pena de desclassificação catálogos, manuais, folhetos, sites impressos da WEB, com suas respectivas URL’s para conferência, ou qualquer outro tipo de documento técnico do fabricante, que efetivamente comprove a existência e aderência ao quesito ou padrão exigido ao longo dessas especificações de todos os produtos ofertados descritos na planilha de materiais e quantitativos.
     2. Informar código FINAME dos equipamentos finamizáveis indicados no Anexo I Proposta Comercial, sob pena de desclassificação.
     3. No caso da cotação de equipamentos produzidos no exterior, a Prefeitura poderá solicitar a qualquer momento a 4ª (quarta) via de importação;
     4. Os equipamentos ativos de rede (switches Core, switches de distribuição switches de acesso, acess point e aplliance de gerenciamento de rede) deverão ser obrigatoriamente do mesmo fabricante, garantindo a compatibilidade da rede instalada.
     5. Os produtos da rede passiva óptica GPON OLT, ONT, deverão ser obrigatoriamente do mesmo fabricante, garantindo a compatibilidade da rede instalada.
     6. As características técnicas obrigatórias dos principais equipamentos ópticos (OLT, ONT ) e também dos ativos de rede (Switch Core Switch de Distribuição) deverão estar grifadas ou destacadas na documentação entregue, para sua comprovação, de forma a garantir uma rápida e melhor análise.
     7. O vencedor do certame deverá apresentar amostra de quaisquer dos itens ofertados, objetivando análise técnica, em caso de dúvidas em relação ao atendimento de qualquer requisito técnico, em até 05 (cinco) dias a contar da data da licitação. A(s) amostra(s) entregue(s) ficarão de posse da Prefeitura até a execução dos serviços contratados, visando comparação com o material a ser entregue pela vencedora.
     8. Serão desclassificadas as proponentes que não atenderem à solicitação de apresentação de documentação técnica que comprove todas as características técnicas exigíveis neste edital.
     9. A proponente deverá permitir que uma equipe técnica da Prefeitura realize, a seu critério, diligências, visitas técnicas e entrevistas, de modo a certificar-se da veracidade dos documentos apresentados.
2. PLANILHA DE MATERIAIS E QUANTITATIVOS





1. DA GARANTIA GERAL DE EQUIPAMENTOS
   1. Todos os itens deste Edital deverão ser instalados com garantia de equipamentos e serviços de no mínimo 12 meses, ressalvadas as especificidades assinaladas ao longo desse Termo de Referência.
   2. Não deverão estar cobertos pela garantia: atos de vandalismo, mau uso, incêndio, inundações ou descargas atmosféricas.
   3. Durante o período de garantia o fornecedor compromete-se a executar os serviços de manutenção corretiva sem quaisquer ônus para a Contratante, inclusive de transporte e despesas acessórias.
2. ESPECIFICAÇÃO DOS SERVIÇOS
   1. A prestação dos serviços e o fornecimento dos materiais deverão ser feitos mediante abertura de ordem de serviço feita pela Prefeitura, conforme especificado abaixo.
   2. Deverá ser previsto um Técnico ou Engenheiro Responsável para acompanhamento de reuniões e definições das O.S. em todo o período de vigência do contrato. O nome e o número do registro no CREA do Técnico ou Engenheiro Responsável deverá obrigatoriamente constar na proposta comercial;
   3. Todos os serviços deverão ser realizados com o máximo de esmero e ótimo acabamento, utilizando-se de materiais e acessórios de primeira linha, novos, não sendo aceitos componentes improvisados ou usados.
   4. A Contratada deverá providenciar a Anotação de Responsabilidade Técnica (ART) de projeto e execução de acordo com a complexidade e solicitação do contratante, junto ao órgão competente e, se necessário, o Alvará expedido pela Contratante.
   5. Não serão solicitadas ART de serviços de remanejamentos, manutenção e serviços de pequena complexidade.
   6. A Contratada deverá assegurar a correta integração e funcionalidade dos serviços, dentro da boa prática da Engenharia, tendo em vista as especificações técnicas constantes desse Termo de Referência.
   7. As exigências aqui formuladas são mínimas de acordo com cada caso, devendo prevalecer sempre as Normas Brasileiras, Regulamentos, Posturas Municipais, Estaduais, Federais, Normas dos Fabricantes e das operadoras de eletricidade e de telecomunicações que apresentarem exigências mais rigorosas que as aqui constantes.
3. DOS MATERIAS
   1. Todos os materiais e equipamentos a empregar nas obras serão novos, comprovadamente de primeira qualidade e deverão satisfazer rigorosamente às condições estipuladas neste termo de referência;
   2. A CONTRATANTE poderá solicitar o exame dos materiais a serem utilizados a qualquer momento e impugnar o seu emprego, quando em desacordo com as Especificações do Anexo II e/ou com as amostras previamente aprovadas.
   3. Obriga-se a empresa vencedora a retirar do recinto das obras os materiais porventura impugnados, dentro de 03 (três) dias úteis. Fica expressamente proibido manter no recinto das obras quaisquer materiais que não satisfaçam a estas Especificações.
   4. Materiais adicionais (Ex.: buchas e parafusos, fita adesiva, fita isolante, rebites, pregos, etc.) necessários aos serviços de instalação integral do sistema, a partir da infraestrutura oferecida e que não estejam claramente especificados e cotados na proposta, serão considerados como parte integrante da proposta.
   5. A empresa vencedora deverá apresentar no ato de cada entrega catálogos, manuais, folhetos, sites impressos da WEB, com suas respectivas URL’s para conferência, ou qualquer outro tipo de documento técnico do fabricante, que efetivamente comprove a existência e aderência ao quesito ou padrão exigido ao longo das especificações aos produtos de cabeamento óptico (cabos ópticos, patch cords, e distribuidores internos ópticos e terminadores ópticos), racks, ativos rede (switches, módulos, software e acessórios) ofertados pela licitante vencedora.
4. DA MÃO DE OBRA
   1. Toda a mão-de-obra necessária aos serviços de instalação, a partir da infraestrutura oferecida pela Contratante, será de responsabilidade única e exclusiva da Contratada, que deverá fornecer equipe técnica suficiente para atender às necessidades da Prefeitura.
   2. Antes do início da execução dos serviços, a Contratante apresentará o responsável da Contratada pela obra à chefia dos locais onde os mesmos serão executados.
   3. A empresa contratada deverá apresentar às chefias dos órgãos envolvidos a relação do pessoal que permanecerá nas dependências do prédio onde serão executados os serviços.
   4. Todos os funcionários da empresa contratada deverão portar identificação quando da execução dos serviços.
   5. Todos os funcionários da empresa contratada deverão usar equipamento de segurança.
   6. A SMTI poderá exigir da empresa vencedora, a qualquer tempo, a substituição de qualquer profissional alocado na execução dos trabalhos pela empresa vencedora desde que verificada incompetência na execução das tarefas a seu cargo ou no caso do profissional apresentar hábitos de conduta inadequados ao bom andamento dos trabalhos;
   7. A substituição de qualquer profissional deverá ser processada em no máximo 48 (quarenta e oito) horas após a comunicação, por escrito, para Prefeitura.
   8. Qualquer dano causado pela empresa contratada ou seus prepostos, seja por imperícia, acidente ou negligência, deverá ser reparado de imediato. Sem a execução do reparo, as faturas pendentes não serão pagas.
5. DAS INSTALAÇÕES E DOS TESTES
   1. Durante a instalação e testes, a empresa vencedora deverá se responsabilizar pelo fornecimento e segurança do ferramental de instalação e instrumental de testes.
   2. Deverão ser executados todos os testes necessários para o funcionamento dos produtos solicitados.
   3. A instalação deverá, obrigatoriamente, ser efetuada de forma a não afetar o funcionamento dos serviços já em operação, garantindo a continuidade dos serviços de voz e dados aos seus atuais usuários.
   4. Deve-se levar em consideração que as atividades de configuração, instalação e ativação provavelmente ocorrerão em dias úteis e horário comercial.
   5. No caso de necessidade de interrupção de outros serviços ou equipamentos, em decorrência da instalação a ser efetuada, esta deverá estar devidamente planejada e ser acordada com antecedência junto à Secretaria Municipal de Tecnologia da Informação.
   6. A empresa vencedora poderá propor modificações nas instalações de maneira a facilitar sua operação, manter a integridade física das pessoas e das instalações e proteger equipamentos, observando as normas técnicas e de segurança de seus funcionários.
6. CRITÉRIOS DE JULGAMENTO
   1. No julgamento das propostas, a classificação se dará em ordem crescente dos preços apresentados, sendo considerada vencedora a proposta que ofertar o menor lance observadas as especificações técnicas definidas no edital e seus anexos.
7. DOS PRAZOS
   1. O prazo de vigência do presente contrato é 12 (doze) meses, a partir da data da assinatura, e será gerenciada pela Secretaria Municipal de Tecnologia da Informação – SMTI/PMU
   2. A empresa vencedora será convocada para assinar o contrato, no prazo de até 05 (cinco) dias contados da data do recebimento da convocação.
   3. Os prazos de execução total dos serviços contratados deverá ser de 180 (cento e oitenta) dias, sendo como referência o prazos estabelecidos no cronograma financeiro Anexo IV.
8. OBRIGAÇÕES DA EMPRESA CONTRATADA:
   1. Constituem obrigações da contratada:
   2. Executar fielmente o ajustado, efetuando os serviços no local, prazo e condições descritos neste termo de referência.
   3. Não transferir, no todo ou em parte, o objeto deste Edital
   4. Manter durante toda a execução do contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
   5. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da execução dos serviços, que incidam ou venham a incidir, direta e indiretamente, sobre o material /serviço contratado, necessários ao fiel cumprimento do objeto a ser contratado.
   6. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da Contratante.
   7. Responsabilizar-se por qualquer prejuízo causado ao Município, a seus prepostos ou a terceiros, provocados por ação ou omissão da contratada, em decorrência de falhas ou imperfeições na execução dos serviços.
   8. Responsabilizar-se por eventuais danos ou desvios causados aos bens que lhe forem confiados, devendo efetuar o ressarcimento correspondente, imediatamente após o recebimento da notificação expressa da Administração, sob pena de glosa de qualquer importância que tenha direito a receber.
   9. Comunicar à Prefeitura, qualquer fato extraordinário ou anormal que ocorra durante a vigência do contrato.
   10. Prestar os serviços nas condições e prazos estabelecidos pelo Município.
   11. Fornecer os equipamentos de acordo com as especificações técnicas determinadas pelo Município no Anexo II (Requisitos Mínimos de materiais).
   12. Refazer os serviços que venham a ser executados de maneira incorreta ou insatisfatória, sem qualquer novo ônus para o Município.
   13. Arcar com todas as despesas decorrentes da execução dos serviços e encargos fiscais, previdenciários, sociais, seguros obrigatórios, seguro contra roubo, furto, danos materiais e pessoais, inclusive de terceiros.
   14. Manter em serviço somente profissionais capacitados, portando crachás de identificação individuais, do qual deverá constar o nome da contratada, nº de registro, função e fotografia do empregado portador.
   15. Assegurar que todo o empregado que cometer falta disciplinar qualificada como de natureza grave não será mantido em serviço.
   16. Atender as solicitações do Município quanto às substituições de empregados não qualificados ou entendidos como inadequados para a prestação dos serviços. A substituição de qualquer profissional deverá ser processada em no máximo 48 (quarenta e oito) horas após a comunicação, por escrito, pela Prefeitura.
   17. Todos os funcionários da contratada deverão usar Equipamento de Segurança (EPIs), seguindo as Normas Reguladoras de Segurança do Trabalho (NRs) vigentes.
   18. Responsabilizar-se civil e criminalmente pelos danos causados ao Município ou a terceiros, decorrentes da execução do contrato.
   19. Prestar os esclarecimentos desejados, bem como comunicar o Município, quaisquer fatos ou anormalidades que porventura possam prejudicar o bom andamento ou o resultado final dos serviços.
   20. A contratada deverá indicar uma pessoa como coordenador/supervisor responsável por todas as equipes que estiverem execultando o contrato, sendo o mesmo o canal entre a contratada e o Município.
   21. A contratada, após o recebimento da Ordem de Execução de Serviço celebrado, deverá apresentar à chefia/coordenadoria/responsáveis dos órgãos envolvidos a relação de pessoal que permanecerá nas dependências do prédio onde serão executados os serviços.
   22. Responder por qualquer dano causado por si ou seus prepostos, seja por imperícia, acidente ou negligência, deverá ser reparado de imediato.
   23. Responsabilizar-se pelo fornecimento e segurança do ferramental de instalação e instrumental de testes, durante a instalação dos mesmos.
   24. Cumprir a legislação vigente relativa à segurança e higiene do trabalho no que se refere ao pessoal colocado à disposição dos serviços contratados, fiscalizando, inclusive, a utilização pelos funcionários do uso dos equipamentos individuais de segurança. A contratada ainda tomará todas as providências necessárias para prevenir possíveis acidentes que possam ocorrer por falta ou deficiência de sinalização e/ou proteção dos serviços, assumindo total responsabilidade sobre eventuais falhas.
   25. Reparar quaisquer danos causados ao Município ou a terceiros em decorrência da execução dos serviços contratados.
   26. Recolher taxa correspondente a A.R.T. do serviço exigida pelo CREA e entregar cópia à Prefeitura.
   27. Exigir a apresentação dos funcionários adequadamente trajados, não sendo permitido o uso de bermudas, camisas sem manga, camisetas e chinelos.
   28. Responsabilizar-se por seus empregados e auxiliares, no concerne ao cumprimento da legislação trabalhista, previdência social, seguro de acidentes de trabalho ou quaisquer outros encargos previstos em lei, em especial no que diz respeito às normas de segurança do trabalho, prevista na legislação Federal( Portaria nº 3.214 de 08/07/1978, do Ministério do Trabalho) , sendo que o seu descumprimento poderá motivar a aplicação de multas por parte da Prefeitura ou a rescisão contratual com a aplicação das sanções cabíveis.

**ANEXO I**

**POP – Ponto de Presença**

Esse anexo descreve detalhadamente a solução a ser fornecida para abrigar os POP´s (Ponto de Presença) da Infovia e as demais exigências para sua instalação e configuração.

1. INTRODUÇÃO

A solução aqui apresentada é baseada em abrigos padronizados de telecomunicações utilizando gabinetes para locais abertos com os respectivos equipamentos de energia, climatização, segurança, aterramento, entre outros, que serão implantados para suportar um POP completo.

Trata-se de uma solução de infraestrutura básica de estações de telecomunicações com fornecimento dos gabinetes outdoor e materiais, necessários para o funcionamento, acomodação e proteção dos equipamentos dos sistemas ópticos, ativos de rede IP e demais materiais e equipamentos a serem utilizados nos POP’s da Infovia e que ficarão na parte externa dos edifícios onde serão instalados.

1. DETALHAMENTO
   1. **Definições**
      1. Está sendo chamado de “**gabinete outdoor**” o abrigo padronizado de telecomunicações utilizando gabinetes metálicos para locais abertos, obedecendo ás especificações contidas neste Termo de Referência.
      2. Está sendo chamando de “**estação de telecomunicação**” a área de terreno do próprio municipal que acomodará o gabinete outdoor com toda a infraestrutura adequada para seu funcionamento em alta disponibilidade.
   2. **Requisitos Gerais**
      1. O fornecimento dos gabinetes outdoor deverá ser totalmente integrado, ou seja, deve contemplar a instalação do:
      2. Sistema de Corrente Contínua (Fonte e Banco de Baterias) – “no-break”,
      3. Rack’s de 19 polegadas,
      4. Sistema de Ar Condicionado,
      5. Iluminação,
      6. Sistema de Abertura de Porta,
      7. Tomadas
      8. Aterramento
      9. Os gabinetes deverão possuir acessos laterais para manutenção da totalidade dos equipamentos.
      10. A CONTRATADA tem a responsabilidade de fornecer e instalar os gabinetes outdoor perfeitamente preparados para acolher todos os equipamentos.
      11. Os sistemas de energia CC e banco de baterias (“no-break”) devem ser de 1.2 kVA.
      12. Todos os equipamentos ópticos e IP serão alimentados por tensão de 127V AC.
      13. A CONTRATADA deverá definir a alocação do gabinete outdoor em cada um dos sites escolhidos para funcionamento dos POP’s em locais previamente acordados com a FISCALIZAÇÃO e os responsáveis pelo site.
      14. A CONTRATADA deverá prever toda a instalação de infraestrutura de instalação do armário incluindo (fixação da base, tubulação subterrânea de entrada do cabo óptico e elétrico).
      15. O sistema de aterramento do gabinete outdoor deve seguir as informações contidas no item 2.6 abaixo.
      16. Caberá à CONTRATADA apresentar desenhos em dwg, padrão AutoCAD, com detalhamento dos seguintes elementos:
      17. Base do gabinete outdoor;
      18. Instalações elétricas;
      19. Aterramento;
      20. Entrada de energia;
      21. Tubulação para entrada de fibra óptica;
      22. Medição e emissão de laudo de aterramento;
      23. Caberá a CONTRATADA, registrar em uma via do projeto as alterações que ocorrerem durante a instalação para execução do “AS BUILT”.
      24. A CONTRATADA deverá entregar toda a documentação técnica referente aos materiais e equipamentos utilizados na instalação.
      25. Os equipamentos e materiais deverão ter garantia integral contra defeitos de projeto, fabricação, instalação e desempenho inadequado.
      26. A CONTRATADA deverá fornecer equipamentos com certificado de homologação na ANATEL.
      27. Será de total responsabilidade da CONTRATADA:
      28. a realização das vistorias;
      29. a elaboração do detalhamento técnico e croquis das estações;
      30. o fornecimento de todos os materiais;
      31. a execução de todos os serviços pertinentes à construção das estações para os gabinetes outdoor.
   3. **Características Mecânicas do Gabinete Outdoor**
      1. O gabinete outdoor deverá possuir dimensões suficientes para acomodar 1 bastidor padrão 19” com 22 U’s disponíveis para os equipamentos ópticos e de IP.
      2. O gabinete deverá possuir camadas duplas de alumínio, para proteção contra vandalismo.
      3. Deverá possuir no mínimo 3 portas sendo 1 frontal e 2 laterais para maior facilidade de instalação de equipamentos.
      4. Suporte para base.
      5. Paredes com isolamento térmico.
      6. Sistema de Ar Condicionado.
      7. Sistema de proteção com duas chaves e indicação de abertura de porta.
      8. Trilho para suporte de equipamento.
   4. **Sistema de Energização dos Gabinetes Outdoor**
      1. O sistema de energia deverão ser do tipo Modular, acoplado ao Sistema de Supervisão e Telecomando.
      2. Cada gabinete deverá ser composto por Sistema de Baterias (Sistema “no break”) de, no mínimo 1.2 KVA.
      3. O sistema de bateria deverá ser instalado dentro dos Gabinetes Outdoor ou em Gabinete anexo na lateral do Gabinete outdoor.
      4. Conexão para baterias externas para adicionar ao nobreak um módulo externo de baterias, permitindo a expansão do tempo de autonomia.
      5. Detector de inversão entre fase e neutro.
      6. Sinalização audiovisual em display e alarmes sonoros
      7. Permite ser ligado na ausência de rede elétrica.
      8. Fusível rearmável, sem a necessidade de substituir o fusível.
      9. Modo econômico (ECO)
      10. Tempo Médio entre Falhas: 40.000 horas
      11. Tempo Médio para Reparos: 30 minutos
      12. Faixa de Temperatura: 0-40ºC
      13. Umidade Relativa 20 a 90% (sem condensação)
      14. Ruído Audível <50dB a 1metro
      15. Proteções: Contra a descarga total das baterias;
      16. Contra sobretensão e subtensão de rede elétrica;
      17. Proteção de Sobrecarga
      18. 100 a 110% - Aviso de sobrecarga.
      19. 110 a 130% - Desligamento em ate 30 segundos;
      20. 130% Desligamento imediato da saída.
      21. Contra sobreaquecimento no inversor.
      22. Contra a distorção harmônica da rede elétrica;
      23. Contra surtos de tensão, na entrada e saída.
   5. **Sistema de Refrigeração dos Gabinetes Outdoor**
      1. O sistema de refrigeração será do tipo ar condicionado, devendo ser garantidos os espaços internos necessários para os mesmos.
      2. O sistema de bateria deverá ser instalado dentro dos Gabinetes Outdoor ou em Gabinete anexo na lateral do Gabinete outdoor.
      3. Deve possuir Potencia de Frigorífica Útil de 1.000W
      4. Suportar alimentação 220V com bornes.
      5. Possuir Controlador com termostato eletrônico.
      6. Parâmentros:
      7. Temperatura de operação : 20 à +50°C
      8. Nível de proteção interna IP54
      9. Nível de proteção externa IP 34
      10. Nível de ruído 64dB
      11. Dimensões: 348mm x 783mm x 213mm
   6. **Aterramento dos Gabinetes Outdoor**
      1. O sistema deverá possuir barra ou borne para aterramento.
      2. O aterramento do equipamento deverá ser feito garantindo o mesmo potencial de aterramento do site.
      3. Todos os cabos e terminais deverão ter certificação, conforme Norma NBR5410 - Instalações Elétricas de Baixa Tensão.
      4. As distribuições de carga de consumidores (UDCs) do sistema deverão disponibilizar disjuntores para conexões dos negativos das cargas.
   7. **Iluminação interna dos Gabinetes Outdoor**
      1. Deverá ser através de lâmpada Led DC 42 a 58V e deverá proporcionar super brilho, com leds brancos e proteção transparente.
      2. Deverá ser resistente a choque, poeira e de baixa potência.
   8. **Içamento e Fixação em Fábrica dos Gabinetes Outdoor**
      1. O sistema deverá ser montado em um gabinete auto suportado.
      2. Cada gabinete deverá ser enviado com embalagem de plástico de alta resistência e fixado em palete de madeira.
      3. Deverão existir quatro olhais de içamento, sendo um em cada lado do gabinete.
   9. **Detectores de Abertura de Porta;**
      1. Os gabinetes outdoor deverão vir com detectores de abertura de porta.
2. PONTO DE PRESENÇA
   1. O POP – Ponto de Presença paço municipal será no próprio Data Center da Prefeitura.

**ANEXO II**

**Requisitos Mínimos de Materiais e Equipamentos**

Nesse anexo são apresentadas as características mínimas indispensáveis de todos os materiais que irão compor a solução proposta; complementarmente são apresentadas características de materiais e equipamentos em anexos aqui mencionados, a saber, Anexo I – POP – Ponto de Presença;

1. Organizador de Cabos Horizontal;
   1. Deve possuir estrutura metálica em aço espessura de 1,5 mm;
   2. Deve possuir largura padrão de 19, conforme requisitos da norma ANSI/TIA/EIA-310D;
   3. Deve possuir altura de 1U;
   4. Deve possuir uma tampa frontal de encaixe;
   5. Possuir pintura em epóxi de alta resistência a riscos;
   6. Deve ser fornecido na cor preta;
2. Porca Gaiola;
   1. Porca Gaiola, M4, M5 e M6 ou M8 temperada, com acabamento niquelado;
   2. Parafuso Panela Philips M5x 16 mm niquelado;
   3. Arruela niquelada;
3. Patch Cord RJ45/RJ45 2,5m Cat; 6;
   1. Deve atender às especificações contidas nas normas ANSI/TIA/EIA-568-A e ANSI/TIA/EIA-568-B categoria 6;
   2. Deve possuir características elétricas e desempenho testado em frequências de até 600 MHz;
   3. Deve possuir no minimo 2,5 metros de comprimento;
   4. Devem ser confeccionados em cabo par trançado, UTP (Unshielded Twisted Pair), 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina e capa externa em PVC não propagante a chama, na cor azul, conectorizados à RJ-45 macho Categoria 6 nas duas extremidades, com as características necessárias para atender as especificações contidas na norma ANSI/TIA/EIA-568-A-5 Categoria 6 e a FCC part; 68;5 (Interferência Eletromagnética), ter corpo em termoplástico de alto impacto não propagante a chama que atenda a norma UL 94 V-0 (inflamabilidade), possuir contatos em cobre-berílio e camada protetora com no mínimo 50 (cinquenta) micro polegadas de ouro, possuir terminação do tipo 110 IDC (conexão traseira) estanhados para a proteção contra oxidação, garra tripla para garantia de vinculação elétrica com as veias do cabo;
   5. Deverá ser utilizado para manobras entre painel de conexão (Patch Panel) e os equipamentos (2,5 m);
   6. Deve possuir certificações UL ou CSA;
   7. Devem ser confeccionados e testados em fábrica, sendo obrigatória à apresentação da certificação do fabricante, quando da Instalação dos mesmos;
   8. Deverá ser apresentado catálogo do produto na proposta comercial;
4. Tomada Elétrica Universal 2P+T
   1. Deverá apresentar polos 2P+T;
   2. Deve possiur Termoplásticoauto extinguível
5. Cabo Elétrico flexível 2,5mm² preto
   1. O Cabo Elétrico deverá ser flexível;
   2. Deverá apresentar seção nominal de 2,5 mm²;
   3. Deverá suportar tensão nominal de até 750 V;
   4. Deverá ser fornecido na cor preta;
6. Cabo Elétrico flexível 2,5 mm² azul
   1. O Cabo Elétrico deverá ser flexível;
   2. Deverá apresentar seção nominal de 2,5 mm²;
   3. Deverá suportar tensão nominal de até 750 V;
   4. Deverá ser fornecido na cor azul;
7. Cabo Elétrico flexível 2,5mm2 verde
   1. O Cabo Elétrico deverá ser flexível;
   2. Deverá apresentar seção nominal de 2,5 mm²;
   3. Deverá suportar tensão nominal de até 750 V;
   4. Deverá ser fornecido na cor verde;
8. Fita Isolante
   1. Deverá apresentar no minimo 10 metros de comprimento;
   2. Deverá ser fornecido na cor preta;
9. Terminal tipo agulha para cabo de 2,5mm²
   1. Deve possuir cobre com camada de estanho;
   2. Apresentar ranhuras no interior para melhorar o contato elétrico e aumentar a resistência ao deslizamento do condutor;
   3. Deverá ser fornecido para cabos de seção nominal de 2,5mm²;
   4. Deverá ser do tipo pino;
10. Terminal tipo olhal para cabo de 2,5mm²
    1. Deve possuir cobre com camada de estanho;
    2. Apresentar ranhuras no interior para melhorar o contato elétrico e aumentar a resistência ao deslizamento do condutor;
    3. Deverá ser fornecido para cabos de seção nominal de 2,5 mm²;
    4. Deverá ser do tipo olhal;
11. Caixa de Emenda para 24 FO
    1. Caixa dimensões máximas de 310 nm (altura) x 260mm (largura) x 100mm (profundidade);
    2. Deve possuir no minimo 04 entradas redondas para cabos com diâmentro de 10 a 17 mm;
    3. Deve possuir no minimo 01 entrada oval para 2 cabos com diâmetro minimo de 8 a 17mm;
    4. Deve possuir fechamento mecânico;
    5. Deve possuir fixação do membro de tração do cabo;
    6. Deve possuir válvula de teste de pressão;
    7. Deve possuir no minimo kit de bandeja para até 24 emendas de fibras ópticas;
    8. Deve possuir resistencia à corrosão e envelhecimento e proteção ultravioleta;
    9. Deve possuir certificado de homologação da Anatel.
12. Caixa Terminal Óptica
    1. Deve possuir capacidade para aplicação PON;
    2. A caixa Terminal Óptica deve possuir certificação Anatel Categoria III;
    3. A caixa Terminal deverá ter sistema de abertura e fechamento mecânico, de maneira que não apresente peças soltas, nem necessidade de ferramentas especiais para seu manuseio;
    4. A caixa deve permitir sangria de cabos da rede externa, bem como cabos drop, assegurando que não haja danos às fibras ópticas;
    5. A caixa deve ter capacidade para 16 saídas de cabos drop;
    6. Deve possuir sistema para fixação dos elementos de reforço mecânico “FRP” dos cabos ópticos, que não implique na utilização de ferramentas especiais;
    7. Deve possuir sistema de proteção contra poeira e umidade, além de ser resistente à corrosão e ter proteção UV;
    8. Deve permitir a instalação de até 2 splitters 1:8 conectorizados, ou 1 splitter 1:16, os quais devem ser acomodados na parte anterior da  bandeja onde são instalados os adaptadores ópticos;
    9. Deve ter disponibilidade para 16 adaptadores SC-APC;
    10. A caixa deve ter ambientes independentes para realização de emendas e ativação de assinantes, de modo que, uma vez que as emendas forem realizadas, elas fiquem totalmente isoladas da bandeja de conectores, impedindo o seu acesso no momento da ativação de novos assinantes;
    11. A entrada oval deve aceitar cabos multifibra de 7 a 12mm de diâmetro;
    12. Deve ter dimensões compactas aproximadas de:  Largura (300mm) x Altura (220mm) x Profundidade (100mm), sem contar eventuais itens adicionais de fixação;
    13. A caixa deve ter espaço adequado para abrigar reserva de fibra de pelo menos 1,5m;
    14. A bandeja de emenda fornecida juntamente com a caixa terminal óptica deve ter capacidade para realização de 16 emendas;
    15. Deve ser de mesma marca do cabo de fibra óptica fornecido na solução;
    16. Deverá ser apresentado catálogo do produto na proposta comercial.
13. Fibra Óptica do Tipo I
    1. Deverá possuir mínimo de 6 fibras ópticas (03 pares) monomodo , com filamentos de fibras dielétricas aplicadas ao redor da unidade básica;
    2. Deverá possuir tubo de proteção preenchido com geleia;
    3. Deverá possuir cordão de rasgamento;
    4. Deverá possuir camada externa termoplastica aplicada por processo de extrusão simultaneamente sobre o núcleo e fio de aço de sustentação;
    5. Deve ser um cabo de aplicação para acesso final as unidades da PMU;
    6. Deverá possuir fibras ópticas revestidas em acrilato;
    7. Deverá possuir elemento de sustentação com 1 fio de aço galvanizado para previnir esforços de tração e contração no cabo;
    8. Deve possuir uma capa interna de material termoplástico com cordão de rasgamento sob a capa interna;
    9. Deverá possuir vão mínimo de 80m;
    10. Deverá possuir atenuação óptica máxima (dB/Km) 0,37 @ 1310 mm e 0,25 @ 1550nm;
    11. Deverá possuir temperatura de operação minima de -20 a 65 graus Celsius;
    12. Deve possuir certificado de homologação da Anatel;
    13. Deverá possuir ser fornecido em bobinas de madeira com 500m de fibra;
    14. Apresentar Catálogo do Produto junto a proposta comercial
14. Fibra Óptica do Tipo II
    1. Deverá possuir mínimo de 12 fibras ópticas (06 pares) monomodo, com núcleo resistente a penetração de umidade e revestimento externo de material termoplástico;
    2. A fibra óptica deve ser do tipo Auto-Sustentável e não aérea por espinagem;
    3. Tubo de proteção tubo loose;
    4. Dois tubos devem ser identificados com cores, para facilitar o sangramento do cabo;
    5. Fibras ópticas revestidas em acrilato;
    6. Elemento de sustentação de material não metálico;
    7. Capa externa de material retardante a chama;
    8. Revestimento externo termoplástico na cor preta resistente a intempéries (diâmetro externo máximo de 8,3 mm);
    9. Vão mínimo de 80m;
    10. Atenuação óptica máxima (db/Km) 0,36 @ 1310mm e 0,21 @1550nm;
    11. Massa nominal do cabo (Kgf/Km) 65 Kgf/Km;
    12. Carga máxima durante a instalação de 2Kgf x peso do cabo/Km.
    13. Raio mínimo de curvatura durante a instalação 20mm x Diâmetro Externo;
    14. Temperatura de operação de -20 a 65 graus Celsus;
    15. Deve possuir certificado de homologação da Anatel.
15. Armação Press Bow
    1. Deve ser armação PRESS BOW com no máximo 1 (um) isolador;
    2. Armação press-bow deve ser de aço fundido galvanizado a fogo com 1 posição para 1 isolador de porcelana 72x72mm;
16. Abraçadeira ajustável para poste
    1. Deve ser abraçadeira ajustável para poste tipo BAP2;
    2. Deve ser fabricada em aço altamente resistente ao tempo, comprimento (esticada) 800 mm, com regulagem para diâmetros diferentes de postes;
17. Alça Pré-formada de Serviço
    1. Alça pré-formada de serviço deve ser fabricada em aço galvanizado, para aplicação na ancoragem de cabos revestidos e nús, sendo instalados em isoladores nos postes;
18. Cabo de Aço Galvanizado
    1. Deve ser cabo de aço galvanizado 3/16;
    2. Deve ser cabo de aço tipo cordoalha galvanizado, 7 fios;
19. Fio de Espinar
    1. Deve ser fio de Espinar tipo FEI-07;
    2. Deve possuir fio de aço isolado encapado de espinar;
    3. Deve estar preparado para uso em conjunto com o cabo de aço, nas grandes travessias;
20. Plaquetas de Identificação
    1. Deve ser de material plástico;
    2. Deve ser plaquetas próprias para fixação emcabos de fibra ópticos aéreos ou subterrâneos;
    3. Deve atender ao layout proposto conforme anexo V;
    4. Deverá possuir bom ajuste a superfícies irregulares, curvadas;
    5. Deve possuir uma durabilidade minima de 5 (cinco) anos em ambientes externos;
    6. Deve possuir as dimensões mínimas de largura 90 mm x altura 50 mm seguindo o layout proposto conforme anexo V;
    7. Deverá ser na cor amarela seguindo o layout proposto conforme anexo V;
21. Cruzeta e Armação Longa
    1. Deve possuir braço de extensão com isolador horizontal de no maximo 72x72mm;
22. Spiraduto
    1. Deve possuir Spiraduto 3/4branco;
23. OLT GPON (Optical Line Terminal)
    1. Deve operar em conformidade com a recomendação ITU-T G.984
    2. Ter capacidade de Downstream: 2.488Gbps @ 1490nm
    3. Ter capacidade de Upstream: 1.244 Gbps @ 1310nm
    4. Alcance de até 20Km através de módulo SFP com laser classe B+ e orçamento de link de 28dB.
    5. Possibilidade de operar com módulos SFP que permitam a funcionalidade PON Extended (Para até 60Km)
    6. Suportar até 64 TCONTs
    7. Possuir FEC: Forward Error Correction
    8. Suporte a alocação estática e dinâmica de banda: SBA e DBA
    9. Até 4096 port-IDs no downstream e upstream
    10. Até 1024 alloc-IDs no upstream
    11. O equipamento deve prover mecanismos que permitam a visibilidade entre usuários de portas PON distintas, bem como de usuários da mesma porta PON. Além disso, o equipamento deve permitir que esta facilidade seja desativada, provendo isolação entre os usuários.
    12. Deve possuir 8 interfaces GPON acompanhadas de transceptores ópticos (SFP) plenamente compatíveis com os equipamentos
    13. Deve possuir 8 interfaces 1Gbps via SFP
    14. Deve possuir 2 interfaces 10 Gbps 10BaseLR via SFP+
    15. Deve suportar 2 Interfaces 10 Gbps via XFP
    16. Possuir redundância permitindo espelhamento entre portas GPON e Porta GPON com Porta Active Ethernet;
    17. Possibilitar a agregação de portas via protocolo LACP;
    18. Possibilidade de atendimento de ONUs via Active Ethernet;
    19. Permitir as seguintes facilidade e configurações:
    20. Link aggregation estático e dinâmico nas portas LAN (LACP)
    21. IGMP snooping (v1,v2,v3)
    22. IGMP Proxy
    23. RSTP e ERPS
    24. Suporte a VLAN 802.1q (Q in Q)
    25. VLAN tagging por porta e por MAC
    26. VLAN trunking e VLAN mapping
    27. DHCP Relay Agent (Option 82)
    28. PPPoE Intermediante Agent (PPPoE tag)
    29. Suporte a QoS em camada 2 (802.1p) e em camada 3 com 8 filas distintas
    30. 8.2.1.12.11 Upgrade de Firmware com suporte a duas versões para maior segurança
    31. 8.2.1.12.12 ACL’s flexíveis (layer 2 e layer 3), podendo serem definidas por porta ou por VLAN.
    32. Alimentação: -48V ou AC, através de 2 fontes redundantes com ‘’hot swap’’.
    33. Temperatura de operação: 0 a 65 graus CELSIUS, umidade: até 90% não condensado (para permitir / suportar instalação em armários de rua).
    34. Gabinete para instalação em rack padrão EIA 19’’ com 1 (um) U de altura.
    35. Permitir as seguintes configurações de gerência:
    36. Configuração e gerência através do protocolo SNMP (v2,v3), RFC1213.
    37. Gerencia in-band e/ou através de porta Ethernet dedicada (out-of-band).
    38. Acesso à linha de comando de configuração através de porta serial RS 232, conexão segura SSH ou protocolo TELNET.
    39. Syslog local e remoto.
    40. Apresentar obrigatoriamente Certificado de homologação expedido pela Anatel junto a proposta comercial;
    41. Apresentar obrigatoriamente Certificado de Produto com PPB (Processo Produtivo Básico) junto a proposta comercial;
    42. Apresentar obrigatoriamente Certificado de produto com tecnologia nacional emitido pelo MCT junto a proposta comercial.
    43. Anexar obrigatoriamente catálogo do produto junto a proposta comercial:
24. ONU GPON (Optical Network Unit)
    1. Características Gerais: O equipamento deverá ser um CPE configurável em Router (Camada 3) ou Bridge (Camada 2) por software, com as seguintes características técnicas mínimas obrigatórias:
       1. Operação de acordo com a recomendação ITU-T G.984
       2. Possibilidade de operação em Serviços Ponto-Multiponto (GPON) e Ponto a Ponto (Active Ethernet)
       3. Ter capacidade de Downstream: 2.488 Gbps @ 1490nm
       4. Ter capacidade de Upstream: 1.244 Gbps @ 1310nm
       5. Deve permitir mapeamento individual entre as Vlans e as portas LAN, com retirada de tag de Vlan;
       6. Operação nos modos GPON e Active Ethernet, com auto detecção
       7. Single 9/125um fixed, nonremovable laser (single mode) com conector SC/APC
       8. Suporte para operação em IPV4 e IPV6;
       9. Suportar até 8 T-CONTs;
       10. Suporta até 32 GEM Port-Ids;
       11. Ativação por Serial Number descoberto ou configurado
       12. Possuir Certificado de Uso Eficiente de Energia;
       13. Suportar 5 (cinco) tipos de T-CONT: (fixed BW, Assured BW, Non-assured BW, Best-effort BW, Combination of others);
       14. Possibilitar a exibição do nível de sinal óptico recebido (1490nm) na interface GPON. O valor deve ser exibido em dB e possibilitar consulta via CLI e SNMP.
       15. Acesso à linha de comando CLI através de conexão segura SSH ou Telnet;
       16. Suporte a atualização remota de firmware
       17. Ter capacidade mínima de conectividade de:
       18. Uma interface óptica GPON (G.984) para conexão GPON ou Active Ethernet;
       19. No mínimo 1 (uma) interface Gigabit Ethernet (1000 Mbps), full-duplex, auto-negotiation, auto MDI/MDI-X (auto sense)
       20. Funcionalidade em Camada 2: Suporte a VLAN segundo IEEE 802.1Q com até 32 VID’s distintos;
       21. Permitir mapeamento individual entre as Vlans e as portas LAN, com retirada de tag de Vlan;
       22. Permitir operação com tabela MAC de até 1024 entradas;
       23. Suporte a Q-in-Q;
       24. IGMP Snooping
       25. Interface WEB que permita configuração do equipamento localmente e remotamente;
       26. Permitir alterar o login e senha dos usuários de acesso a interface de configuração;
       27. VLAN access e trunking
       28. Botão físico no equipamento que permita a restauração da configuração padrão de fábrica
       29. Suporte a multicast através de GEM port especifica
       30. Funcionalidade em Camada 3: Marcação e classificação de tráfego upstream de acordo com porta de entrada
       31. Priorização de tráfego através de filas para suporte a serviços de voz
       32. Permitir operação em PPoE
       33. Possuir NAT, NATP e DHCP (IPv4 e IPv6)
       34. Possuir OSPF e RIP
       35. Permitir mecanismos de QoS
       36. Desempenho de roteamento até 1Gbit/s com pacotes de 64 Bytes
       37. Características Mecânicas:
       38. Alimentação: Fonte externa 12V
       39. Temperatura de operação: 0 a 50 graus Celsius
       40. Certificado de homologação expedido pela Anatel;
25. Chassi de Splitter Modular Óptico 1:4
    1. Deve ser fornecido em Chassi para acomodação de até 4 Splitters na razão de 1:4, 1:2; 1:8;
    2. Deve possuir disponibilidade de 4 unidades de Splitters na razão de 1:4;
    3. Deve possuir full espectro 1260~1650nm com reduzidas perdas de inserção;
    4. Deve ser do tipo PLC ou FBT;
    5. Deve ser fornecido já conectorizados com conector do tipo SC e com polimento APC
    6. Deve ser homologado pela Anatel;
26. Splitter Óptico 1:2
    1. Deve possuir capacidade para aplicação em projetos PON;
    2. Deve possuir full espectro 1260~1650nm com reduzidas perdas de inserção;
    3. Deve ser fornecido na razão de 1:2
    4. Deve ser fornecido do tipo PLC: Planar Ligtwave Circuit;
    5. Deve possuir compatibilidade com bandejas de emenda ou módulos conectorizados;
    6. Deve possuir tamanho compacto que permite o acondicionamento em diversos tipos de bandejas e emenda ópticas;
    7. Deve possuir temperatura mínima de operação de -40°C a +75°C;
    8. Deve possuir umidade relativa mínima de operação 5~95% UR;
    9. Deve ser possuir característica para uso interno ou externo (acomodado em caixa apropriado);
    10. Deve ser homologado pela Anatel;
27. Splitter Óptico 1:4
    1. Deve possuir full espectro de 1260~1650nm com reduzidas perdas de inserção;
    2. Deve ser fornecido na razão de 1:4;
    3. Deve ser fornecido do tipo PLC: Planar Ligtwave Circuit;
    4. Deve possuir compatibilidade com bandejas de emenda e módulos conectorizados;
    5. Deve possuir tamanho compacto que permite o acondicionamento em diversos tipos de bandejas e emenda ópticas;
    6. Temperatura de operação de -40°C a +75°C;
    7. Umidade Relativa de Operação 5~95%UR;
    8. . Deve ser possuir característica para uso interno ou externo (acomodado em caixa apropriado);
    9. Deve ser homologado pela Anatel;
28. Splitter Óptico 1:8
    1. Deve possuir full espectro de 1260~1650nm com reduzidas perdas de inserção;
    2. Deve ser fornecido na razão de 1:8;
    3. Deve ser do tipo PLC: Planar Ligtwave Circuit;
    4. Deve possuir compatibilidade com bandejas de emenda e módulos conectorizados;
    5. Deve possuir tamanho compacto que permite o acondicionamento em diversos tipos de bandejas e emenda ópticas
    6. Deve possuir temperatura mínima de operação de -40°C a +75°C
    7. Deve possuir umidade relativa mínima de operação 5~95% UR
    8. Deve ser possuir característica para uso interno ou externo (acomodado em caixa apropriado);
    9. Deve ser homologado pela Anatel;
29. Splitter Óptico 1:16
    1. Deve possuir full espectro de 1260~1650nm com reduzidas perdas de inserção;
    2. Deve ser fornecido na razão de 1:16;
    3. Deve ser do tipo PLC: Planar Ligtwave Circuit;
    4. Deve possuir compatibilidade com bandejas de emenda e módulos conectorizados;
    5. Deve possuir tamanho compacto que permite o acondicionamento em diversos tipos de bandejas e emenda ópticas
    6. Deve possuir temperatura mínima de operação de -40°C a +75°C
    7. Deve possuir umidade relativa mínima de operação 5~95% UR
    8. Deve ser possuir característica para uso interno ou externo (acomodado em caixa apropriado);
    9. Deve ser homologado pela Anatel;
30. DIO DE 24

**DIO de 24 fibras para rede GPON para fibras Monomodo**

* 1. Distribuidor óptico para até 24 fibras para Rack de 19;
  2. Distribuidor óptico para até 24 fibras em uma única unidade de altura (1U);
  3. Deve ser fornecido completo com 24 conectores SC-APC;
  4. Deve suportar conectores Small Form Factory, para até 48 fibras com conectores SC;
  5. Deverá ter a função de acomodar e proteger as emendas de transição entre o cabo óptico e as extensões ópticas;
  6. Deve possuir altura máxima de 1U;
  7. Deve ser padrão 19”;
  8. Deve possuir áreas de armazenamento de excesso de fibras;
  9. Deve possuir áreas de acomodação, onde as emenda devem ficar interna à estrutura assim conferindo maior segurança ao sistema;
  10. Deve ser fornecido com gaveta deslizante, que facilita a instalação dos cabos ópticos e das extensões ópticas;
  11. Deve ser fornecido com os pigtails e adaptadores ópticos;
  12. Deve ser fabricado em aço SAE 1020;
  13. Deve ser utilizado pintura do tipo epóxi de alta resistência a riscos;
  14. Deve possuir painel frontal articulável, permitindo o acesso aos cordões sem expor as fibras conectorizadas internamente;
  15. Deve possibilitar terminação direta ou fusão, utilizando um mesmo módulo básico;
  16. Deve ser fornecido com suportes para adaptadores ópticos, para uma melhor distribuição dos adaptadores ópticos.

1. Mini DIO de 06 Fibras Monomodo
   1. Deve possuir capacidade mínima de acomodar até 12 emendas ópticas em uma bandeja articulada;
   2. Deve possuir 4 portas ópticas SC/APC;
   3. Deve permitir inversão da fibra garantindo maior flexibilidade;
   4. Deve ser do tipo de parede ou bandeja;
   5. Deve ser feito em plástico de alta resistência mecânica;
   6. Deve permitir acomodação a reservas de fibra no interior do módulo principal;
   7. Deve permitir a utilização do protetor e emenda de 40 mm ou 60 mm;
   8. Deve ser preparado para receber qualquer tipo de conector óptico, sem a necessidade de adquirir qualquer placa extra de adaptadores;
   9. Dever possuir conector do tipo SC;
   10. Deve possuir medidas máxima de 153 mm x 129 mm x 55 mm (A x L x P)
   11. Deve suportar no máximo 12 fibras ópticas;
   12. Deve suportar fibras ópticas monomodo;
2. Cordão monofibra Tipo I
   1. Deve possuir compatibilidade com os equipamentos OLTs (Optical Line Terminal) ofertados;
   2. Deverá ser confeccionados e testados em fábrica;
   3. Deve ser pré-testados em fábrica nos três comprimentos de onda utilizados (1310nm, 1480nm e 1550nm) na rede GPON;
   4. Deve ser constituído por fibras ópticas monomodo ITU-T G 657;
   5. Deve ser em cabo optico em monofibra com os conectores ópticos instalados nas duas extremidades;
   6. Deve ser composto de conectores SC em ambas as pontas;
   7. Deve ser com polimento SPC em uma extremidade e APC não outra extremidade;
   8. Deve possuir revestimento primário em acrilato e revestimento secundário em PVC;
   9. Deve possuir revestimento secundário com elementos de tração e capa em PVC não propagante à chama;
   10. Deve possuir perda de inserção típica de no minimo 0,15 dB e Máxima de 0,30 dB;
   11. O fabricante deve possuir certificação da Anatel para os conectores ópticos SC;
   12. O cabo (cordão) óptico deverá possuir certificação ANATEL;
3. Cordão monofibra Tipo II
   1. Deve possuir compatibilidade com os equipamentos OLTs (Optical Line Terminal) ofertados;
   2. Deverá ser confeccionados e testados em fábrica;
   3. Deve ser pré-testados em fábrica nos três comprimentos de onda utilizados (1310nm, 1480nm e 1550nm) na redes GPON;
   4. Deve ser em cabo optico em monofibra com os conectores ópticos instalados nas duas extremidades;
   5. Deve ser constituído por fibras ópticas monomodo ITU-T G 657;
   6. Deve ser composto de conectores SC em ambas as pontas;
   7. Deve possuir polimento APC em ambas as extremidades;
   8. Deve possuir revestimento primário em acrilato e revestimento secundário em PVC;
   9. Deve possuir revestimento secundário com elementos de tração e capa em PVC não propagante à chama;
   10. Deve possuir perda de inserção típica de no minimo 0,15 dB e Máxima de 0,30 dB;
   11. O fabricante deve possuir certificação Anatel para os conectores ópticos SC;
   12. O cabo (cordão) óptico deverá possuir certificação ANATEL;
4. Patch Cord SC/LC monomodo
   1. Deve possuir conectores SC em uma das extremidades e LC na outra extremidade;
   2. Deve possuir no mínimo 2,5m de comprimento;
   3. Deverá ser constituído por um par de fibras ópticas monomodo 9/125 μm tipo “light“ com ITU-T G 657;
   4. Deverá ser fornecido na cor azul;
   5. Deve utilizar o padrão “zip-cord” de reunião das fibras para diâmetro de 2 mm;
   6. Deve possuir revestimento primário em acrilato e revestimento secundário em PVC;
   7. Deve possuir revestimento secundário com elementos de tração e capa em PVC não propagante à chama;
   8. As extremidades deste cordão óptico duplo devem vir devidamente conectorizadas e testadas de fábrica;
   9. Deverá possuir certificados ISO 9001 e ISO 14001;
   10. Deverá possuir impresso na capa externa nome do fabricante, identificação do produto e data de fabricação;
   11. O fabricante deve possuir certificação Anatel para os conectores ópticos SC e LC;
   12. Deverá possuir certificação ANATEL;
5. Eletrodutos Galvanizado 2”
   1. Deve ser do tipo Galvanizado a Fogo do tipo pesado;
   2. Deve possuir 2 “de diâmetro;
   3. Deve ser fornecido em barras de 3 metros;
   4. Devem ser fornecidos todos os acessórios necessários para instalação das tubulações;
   5. Curvas, Conduletes, Uniduts, Parafusos, Abraçadeiras;
6. Rack de 8 U`s
   1. Rack de 8 U`s padrão 19”;
   2. Deve possuir profundidade de 470mm;
   3. Deve possuir régua de 4 tomadas;
   4. Deve possuir kit de ventilação;
7. Nobreak 0.7KVA
   1. Caracteristicas de entrada:
   2. Tensão nominal:Bivolt automático 115/127/220v
   3. Variação de tensão:89 a 143V (rede 115V) e 175 a 264V (rede 220V)
   4. Frequencia de rede: 60 Hz (+-5%)
   5. Caracteristicas de Saída: Potencia 700VA/420W
   6. Fator de potencia de 0,7
   7. Tensão nominal 115V
   8. Regulação: +- 5% (para operação bateria) e +-6% -10% (para operação rede);
   9. Frequencia 60hz +-1% (para operação bateria);
   10. Forma de onda Senoidal por aproximação (retangular PWM)
   11. Numero de tomadas 5 tomadas no Padrão NBR 14136 sendo uma tomada espaçada ou em extensão para ligação de fonte de energia.
   12. Caracteristicas Gerais: Interativo de regulação on-line
   13. Microprocessador RISC/FLASH (Interativo – regulação on-line);
   14. Filtro de linha;
   15. Estabilizador interno com 4 estágios de regulação;
   16. DC Start: permite que o nobreak seja ligado na ausência de rede elétrica;
   17. Battery Saver: evita o consumo desnecessário das cargas da bateria;
   18. Auto diagnóstico de bateria: informa quando a bateria precisa ser substituida;
   19. Recarga automática das baterias em 4 estágios, mesmo com o nobreak desligado;
   20. Recarregador Strong Charger;
   21. Conector de módulo de bateria ao nobreak;
   22. True RMS;
   23. Auto teste: ao ser ligado, o nobreak testa os circuitos internos;
   24. Inversor sincronizado com a rede (sistema PLL);
   25. Circuito desmagnetizador;
   26. Acionamento do inversor menor 0,8 ms;
   27. Leds coloridos no painel frontal: indicam as condições de funcionamento do nobreak – modo rede, modo inversor/bateria, final de autonomia, subtensão, sobretensão.
   28. Alarme audiovisual: sinalização de eventos como queda de rede, subtensão e sobretensão, fim do tempo de autonomia e final de vida útil da bateria.
   29. Botão liga/desliga temporizado com função Mute: evita o acionamento ou desacionamento acidental, além de desabilitar o alarme sonoro após a sinalização de algum evento.
   30. Porta fusível externo com unidade reserva.
   31. Rendimento 95% (para operação rede) e 85% (para operação bateria)
   32. Proteções: Curto-circuito no inversor;
   33. Surtos de tensão entre fase e neutro;
   34. Sub/sobtensão da rede elétrica.
   35. Sobreaquecimento no inversor e no transformador;
   36. Potencia excedida com alarme e posterior desligamento;
   37. Descarga total das baterias.
8. Poste Metalico
   1. Poste para fixação de Ponto de acesso 7 metros de altura.
   2. Poste em metal galvanizado fabricado para instalação de ponto de acesso;
   3. Com furo de 2” para passagem de cabos numa distância de 2775 mm do topo;
   4. Deve possuir topo fechado;
   5. Com placa de identificação;
   6. Deve possuir traço de esgastamento em tinta preta a 2 (dois) metros do pé do poste;
   7. Diâmetro inicial (pé) de 320mm e final (topo) de 140mm;
   8. Com base de fixação de solo.
9. Caixa Hermetica Outdoor
   1. Caixa hermetica outdoor para ponto de acesso;
   2. Caixa hermetica outdoor para abrigo de fontes e equipamentos das localidades hot Spot;
   3. Caixa de aluminio shelter de aluminio com chapa de espessura de 2mm – 600mmx450mm;
   4. Para cada localidade de ponto hot Spot será instalado sum shelter de aluminio com chapa de espessura de 2mm nas dimensões de 600mmx450mm;
   5. Deve possuir no minimo três dobradiças com abertura de 90° em corpo cromado, bicromatizado;
   6. Deve possuir prateleira interna na altura de 200mm;
   7. A caixa deve possuir no minimo três furos com prensa cabos de diâmetro de 20mm para passagem dos cabos provenientes da rua;
   8. Deve possuir placa de montagem em L para fixação dos acessórios;
   9. Deve possuir ventilação forçada fixada na prateleita visando à troca de calor entre os dois compartimentos da caixa;
   10. Deve possuir possuir os seguintes acessórios instalados em seu interior: disjuntor para proteção elétrica, caixa de terminação óptica, regua de tomadas e canaletas tipo recorte aberto para acomodação do cabeamento interno;
   11. Deve possuir um chapéu na parte superior, com o obejetivo de evitar incidência de raios solares;
   12. Deve possuir vedação emborrachada na tampa;
   13. Deve possuir três suportes de fixação na parte traseira para fixação em poste através de braçadeiras do tipo BAP.
10. Gabinete Outdoor
    1. Conforme Anexo I – POP – Ponto de Presença.
11. Ponto de Acesso
    1. Fornecimento de Ponto de Acesso WiFi Interno, novo e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta.
    2. Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g , 802.11n draft 2.0 e 802.11ac ou superior.
    3. Deve ser homologado pela ANATEL.
    4. Deve ser capaz de operar simultaneamente nos padrões 802.11a/n/ac e 802.11b/g/n, através de rádios independentes (Dual Radio AP).
    5. Deve ser um equipamento ponto de acesso WiFi para rede local sem fio de uso interno, sem antenas aparentes, que atenda os padrões IEEE 802.11b/g/n na faixa de 2.4GHz e 802.11a/n/ac na faixa de 5GHz simultaneamente com configuração via software. O equipamento deve ter capacidade de análise espectral.
    6. Possuir funcionamento em modo autonomo sem a necessidade de controlador. Neste modo, permitir configuração e funcionamento do ponto de acesso sem a necessidade do controlador.
    7. Possuir funcionamento em modo gerenciado por Controlador WiFi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF.
    8. Deverá estar logicamente conectado a um Controlador WiFi, inclusive via roteamento da camada de rede OSI, através de rede pública ou privada.
    9. Deve implementar cliente DHCP, para configuração automática de rede.
    10. Possuir mecanismo de funcionamento para trabalhar com Controladores WiFi em redundância (principal e redundante).
    11. Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) WiFi - operação em modo de “chaveamento de tráfego local”.
    12. Operando no modo de “chaveamento de tráfego local”, o controlador WiFi e os pontos de acesso devem:
    13. O modo de operação de chaveamaneto de trafego local deve prever que se a comunicação entre o ponto de acesso WiFi e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WAN, LAN ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi deve continuar operando e permitindo que os usuários já autenticados na rede e associados aos pontos de acesso continuem a possuir acesso à rede. Deve permitir que os usuarios efetuem roaming rápido entre os pontos de acesso do mesmo site nesta situação;
    14. Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi em modo de chavemaento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que novos usuários se autentiquem de acordo com 802.1x e se associem à rede sem qualquer prejuízo de acesso aos mesmos;
    15. Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi em modo de chavemaento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que os usuarios efetuem roaming sem qualquer prejuízo de acesso aos mesmos;
    16. Deve permitir a operação de usuários configurados nos padrões IEEE 802.11b/g/n e 802.11a/n/ac simultaneamente.
    17. Atender os seguintes requisitos em 802.11n (faixas de 2.4GHz e 5GHz) e 802.11ac (faixas de 5GHz): 3x4 multiple-input multiple-output (MIMO).
    18. Operar em Canais de 20MHz para 2,4GHz e possibilitar channel bounding, canal de 40 MHz para 5GHz e canais de 80MHz para 5GHz.
    19. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps.
    20. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11n: MSC0 – MCS23 (6.5Mbps - 450Mbps).
    21. Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11ac: MSC0 – MCS9 para 1,2 e 3 Spatial Streams (6.5Mbps - 1,3Gbps).
    22. Possuir capacidade de selecionar automaticamente o canal de transmissão.
    23. Implementar o protocolo de enlace CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão.
    24. Operar nas modulações DSSS e OFDM.
    25. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.
    26. Possuir suporte a pelo menos 16 SSIDs e 16 VLANs.
    27. Permitir habilitar e desabilitar a divulgação do SSID.
    28. Possuir padrão WMM (Wi-Fi Multimedia) da Wi-Fi Alliance para priorização de tráfego.
    29. Não deve haver licença restringindo o número de usuários por ponto de acesso. O Ponto de Acesso deve permitir, no mínimo, 200 usuários por rádio.
    30. O Ponto de acesso deve permitir configuração de base de usuários local para utilização com protocólo 802.1X, com no mínimo 100 usuários.
    31. Deve possuir no mínimo 02 rádios (dual radio) operando simultâneamente em frequências distintas.
    32. Possuir potência máxima de transmissão de, no mínimo, 22 dBm para IEEE 802.11a/b/g/n/ac.
    33. Possuir antenas internas intergradas compatíveis com as freqüências de radio dos padrões 2.4GHz e 5GHz com ganho de, pelo menos, 4 dBi e 5,5 dBi, respectivamente, com padrão de irradiação omnidirecional.
    34. Possuir, no mínimo, duas interfaces IEEE 802.3 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX, com conectores RJ-45.
    35. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).
    36. Possuir no mínimo 01 LED indicativo do estado de operação.
    37. Deve possuir uma trava de segurança compatível à utilizada em desktops e notebooks (Kensington security lock) e que permita a instalação de um cabo de segurança com a finalidade de evitar o furto do equipamento. O equipamento deve vir acompanhado com o cabo de segurança.
    38. Deve implementar um mecanismo de controle de associação de banda, de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN.
    39. Implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso.
    40. Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados  usuários da rede WLAN. Deve perimitir a configuração desta formação de banda para clients legados do tipo 802.11a/g, e para cliente 802.11n;
    41. Possibilitar a alimentação via padrão PoE+ (IEEE 802.3at) utilizando apenas uma porta do switch onde estiver conectado.
    42. Possuir estrutura metálica que permita fixação do equipamento em teto e também em parede, devem ser fornecidos os acessórios metalicos para que possa ser feita a fixação.
    43. Deve ser entregue com todos os acessórios necessários para operacionalização do equipamento, tais como: kits de instalação, softwares, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.
    44. Possuir varredura de RF nas bandas 802.11 b/g/n e 802.11 a/n/ac para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado no ponto de acesso.
    45. Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:
    46. EAP-Transport Layer Security (EAP-TLS);
    47. EAP-TTLS/MSCHAPv2;
    48. PEAPv0/EAP-MSCHAPv2;
    49. PEAPv1/EAP-GTC;
    50. EAP Subscriber Identity Module (EAP-SIM).
    51. Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.
    52. Deve implementar suplicante 802.1x par identificar o pontos de acesso, ao ser conectado na estrutura de rede cabeada.
    53. Possuir modulo de criptografia em hardware.
    54. Implementar WEP (Wired Equivalent Privacy), chaves de 40 bits e 128 bits.
    55. Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check-MIC).
    56. Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES, 128 bits).
    57. Deve ser capaz de atender os usuários e realizar a função de “mesh indoor” ou modo “repetidor” de forma simultânea.
    58. Deve permitir a conexão de usuários em IPv4, IPv6 e Dual-stack.
    59. O equipamento deve ser capaz de implementar 802.11 dynamic frequency selection ( DFS ).
    60. Deve possuir suporte à 802.11 Cyclic Shift Diversity ( CSD ) ou Cyclic Delay Diversity ( CDD )
    61. Deve implementar Maximal Ratio Combining ( MRC ).
    62. O equipamento deve realizar a monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências WiFi e Interferências Não-WiFi e simultaneamente atender os usuários da rede WiFi.
    63. As funções de monitoração real-time em Rádio Frequência (análise espectral) devem ser realizadas via hardware, com chipset (ASIC) dedicado para esta função localizado dentro do ponto de acesso.
    64. Deve detectar interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar e classificar interferências não-WiFi, tais como Bluetooth, telefones sem fio, câmeras de video sem fio, Microondas e outros.
    65. Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente.
    66. Deve operar nos seguintes modos: “Modo Local”, “Modo Monitor” e “Modo Analisador de Espectro”.
    67. Operando em “Modo Local” o ponto de accesso deve fornecer informações ao Controlador WiFi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi. Deve fazer tanto a transmissão de dados WiFi quanto a análise de espectro simultaneamente, sem prejuizo ao fornecimento de wifi aos usuários.
    68. Operando em “Modo Monitor” deve fornecer informações ao Controlador WiFi referente à qualidade do espectro de RF para todos os canais monitorados em 2.4GHz e em 5GHz, simultâneamente, identificando equipamentos interferentes na rede WiFi e rogue APs.
    69. Deve ser fornecido com Power Injector do mesmo fabricante que permita, no minimo, que o equipamento ponto de acesso funcione com as carcacteristicas MIMO 3x3 solicitadas na descrição do equipamento, para ambos os rádios simultaneamente. O Power Injector deve possuir no minimos as seguintes caracteristicas:
    70. Deve ser instalado a uma distância máxima entre o dispositivo e equipamento ativo de rede de 100m com cabos de rede cat. 5e;
    71. O injetor de PoE deverá ser compatível a conexão em Switch, hub ou rede em 10/100/1000;
    72. Deve possuir conector do tipo RJ-45, com portas 10/100/1000BASE-TX para conexão de rede;
    73. Deve possuir leds indicadores, no minimo, de status;
    74. O Power Injector deve ser aderente no minimo aos padroes EN60950, EN55022 e EN55024.
    75. O equipamento deverá obrigatoriamente vir acompanhado de antena externa do mesmo fabricante.
12. Appliance de Gerenciamento de rede e Controle WLAN
    1. 02 (dois) processadores de 8 núcleos (Octa core), arquitetura x64 (x86 com extensões de 64bits) sendo:
    2. Performance de referência Intel E5 2600 (Dois mil e seiscentos).
    3. O servidor deverá possuir capacidade de prover índice SPECint2006 Rate “base”, devidamente auditado pela Standard Performance Evaluation Corporation – SPEC.
    4. Outro fabricante compatível comprovadamente igual ou superior ao supracitado em funcionalidade e desempenho. Para a comprovação de desempenho, o equipamento ofertado deverá apresentar todos os índices de desempenho em valores iguais ou superiores aos índices exigidos no item anterior.
    5. 128 GB (cento e vinte e oito gigabytes) de memória ECC e com possibilidade de expansão para 512 GB (quinhentos e doze gigabytes).
    6. 04 (quatro) discos rígidos de 600GB (seiscentos gigabytes), 10k rpm (dez mil rotações por minuto), “hot pluggable/hot swap”, padrão SAS, configuráveis para RAID 0, 1, 5 e 10 em seu controlador.
    7. No mínimo 8 slots internos para discos rígidos.
    8. No mínimo 2 slots PCIe 3.0.
    9. No mínimo 2 portas USB.
    10. Possuir placa de vídeo integrada.
    11. Suporte a Leitor de mídia DVD (interno ou externo), compatível com o servidor.
    12. Deverá possuir BIOS desenvolvida pelo mesmo fabricante do equipamento.
    13. 02 (duas) portas de rede GigaBitEthernet elétricas compatíveis com IEEE 802.1q (multi-VLAN) e IEEE 802.3ad (link aggregation), configuráveis para boot PXE. Podem ser fornecidas em adaptadores ou conjunto no sistema on-board.
    14. 01 (uma) placa com duas portas fiber-channel full-fabric, 08Gb/s (oito gigabits por segundo), com as seguintes características:
    15. Padrão de referência: EMULEX, QLOGIC ou similar com especificações técnicas equivalentes.
    16. Permita ligações de velocidades 2 Gb/s, 4Gb/s e 8Gb/s.
    17. Suporte a balanceamento de carga, suporte à implementação de tolerância a falhas (Failover) de forma automática.
    18. 01 (uma) placa com duas portas 10GE SFP+ FCoE de acordo com o padrão T11 FCoE.
    19. As placas e o conjunto do equipamento deverão permitir a realização de “Boot pela HBA”.
    20. Ventiladores redundantes , suportando o servidor em completa operacionalidade em caso de falha de um deles.
    21. Solução por hardware e/ou software de gerenciamento remoto, independente do sistema operacional e do estado do computador, com as seguintes características:
    22. Controle remoto liga/desliga do servidor.
    23. Console remota.
    24. Servidor http e https.
    25. Servidor SSH ou Telnet+SSL.
    26. Criptografia SSL de 128 bits na comunicação.
    27. Suporte a SNMP para consulta e traps.
    28. Capacidade de inicializar-se (boot) por meio de CD, DVD, pela rede SAN (HBAs) ou imagem dos mesmos, localizados em estação remota.
    29. Capacidade de atualização da BIOS a partir de estação remota.
    30. Suporte à autenticação de 08 (oito) administradores.
    31. Capacidade para registrar eventos e emitir alertas, em caso de falha de ventiladores ou fontes, temperaturas e tensões fora de limites e erros de memória.
    32. 01 (uma) porta Ethernet para gerenciamento “out-of-band” independente das portas exigidas.
    33. Alimentação elétrica:
    34. Fontes redundantes, hot-pluggable e suporte a redundância 1+1.
    35. A alimentação será disponibilizada em dois circuitos, sendo que o equipamento deverá manter a operacionalidade, em caso de falha de qualquer um deles.
    36. Tensão de operação entre 200 a 240VCA, 60Hz circuito monofásico.
    37. O equipamento e demais componentes deverão ser compatíveis com os seguintes sistemas operacionais:
    38. Sistema Operacional “Red Hat Enterprise/Advanced Linux 5” ou superior para sistema “x86\_64” em nível “Certified”. A comprovação será realizada através do site oficial da Red Hat <http://hardware.redhat.com/>
    39. Sistema Operacional “Microsoft Windows Server versão 2008 R2 x64” ou superior em nível “Certified”. A comprovação será realizada através do site oficial da Microsoft <http://www.windowsservercatalog.com/>
    40. Sistema Operacional “Vmware ESX ou ESXi versão 4.1” ou superior. A comprovação será realizada através do site oficial da VMWare <http://www.vmware.com/resources/compatibility/>
    41. Fornecer todos os discos necessários para reinstalação do sistema, drivers e software de gerencia ou imagem através do site do fabricante.
    42. Garantia de 36 meses.
    43. A fornecedora deverá prover, durante o período de garantia do equipamento, a homologação nas versões posteriores dos sistemas operacionais, caso a fabricante da placa não a realize em tempo hábil. Os custos de homologação devem ser arcados pelo fornecedor, e o prazo para essa homologação não deve ultrapassar 30 dias corridos das atualizações.
    44. A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante, através de chamada gratuita a número 0800 no Brasil e por interface Web, sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software. Poderá ser solicitado ao fabricante acesso remoto aos equipamentos para ajuda na identificação de problemas dos diversos tipos inclusive configuração. Solução de problemas de funcionamento durante a operação dos equipamentos, incluindo substituição de peças
    45. **Da solução de Software de Gerencia de rede:**
        1. **Sistema de Gerenciamento de Rede Controle Administrativo**
        2. Esta plataforma poderá ser entregue em formato de appliance virtual ou appliance físico;
        3. Tanto o hardware quanto o software necessários para a implantação de qualquer funcionalidade exigida, deverão fazer parte do fornecimento, incluindo o computador/servidor e as licenças de sistema operacional além de outros dispositivos eventualmente necessários para o seu pleno funcionamento inclusive em alta-disponibilidade (ativo-standby);
        4. Plataforma de gerenciamento capaz de gerenciar todos os tipos de switches, controladores e pontos de acesso descritos neste documento e capaz de fornecer todas as funcionalidades descritas neste documento para todos os equipamentos descritos;
        5. Produto ofertado deve estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta;
        6. Caso seja fornecido em solução de virtualização, deverá ser compatível com a plataforma vmware, porém todo o hardware necessário deverá ser fornecido, inclusive para acontecer a redundância já descrita;
        7. Deve ser acompanhado de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;
        8. Possuir alta disponibilidade, ativo/standby, trabalhando com no mínimo dois servidores físicos ou virtuais. Os servidores podem estar em sites diferenciados ou subnets diferenciadas. As licenças necessárias e o hardware necessário para implementar esse recurso devem estar incluídas, inclusive de banco de dados se for o caso;
        9. A plataforma de gerência ofertada deve ser fornecida com capacidade mínima de hardware capaz de gerenciar simultaneamente no mínimo o total de equipamentos descritos nas especificações técnicas deste edital, com adição de 10% de equipamentos.
        10. Deverá licenciado com capacidade inicial para gerenciar, no mínimo e simultaneamente, o quantitativo total de equipamentos descritos na presente especificação;
        11. Ser fornecida em appliance ou acompanhada de servidores do mesmo fabricante da solução;
        12. Deve ser capaz de permitir a visualização de zonas de interfêrencias não wi-fi nos mapas de pelo menos os seguintes tipos: blue-tooth, cameras sem fio operando nas frequências de wi-fi, fornos micro-ondas e telefones sem fio operando nas frequências de wi-fi.
        13. Permitir a visualização e localização na planta de equipamentos de localização do tipo Bluetooth Low Energy ( BLE).
        14. Deve permitir a localização de tags rfid nas plantas;
        15. Deve permitir a localização de usuários conectados, rogue-clients e rogue-aps nas plantasse permitir o tracking destes usuários.
        16. Deve fornecer API pública para que seja possível a criação de aplicações que utilizem os dados de localização dos usuários como por exemplo bluedot.
        17. Caso a solução ofertada não possua os recursos acima de localização acima descritos, serão aceitas composições com outras plataformas de localização desde que homologadas pelo fabricante da plataforma de gerencia e infraestrutura. Esta homologação deve possuir documentação publicada em site do fabricante para localizar os itens acima.
        18. Deve permitir o monitoramento de Controladoras Wireless, Access Points e Switches e Roteadores;
        19. Deverá ser do mesmo fabricante da solução;
        20. Deve possibilitar a visualização rápida de alarmes e estatísticas de utilização para fácil e rápido monitoramento e troubleshooting;
        21. Deve possuir mecanismos para consolidar informações de rede, tais como: níveis de ruído, relação sinal ruído, interferência, potencia de sinal, permitindo ao administrador isolar e resolver problemas nos vários níveis da rede;
        22. Deve permitir a atualização de software dos Pontos de Acesso de modo centralizado;
        23. Deve descobrir automaticamente os dispositivos individuais na infraestrutura de rede wireless, eliminando a necessidade de configuração e manutenção e provendo inform ação para fins de planejamento da capacidade e troubleshooting;
        24. Possuir possibilidade de geração de relatórios que relacionam atividade da rede e informações de sistema, incluindo estatísticas dos usuários/clientes, utilização de rádio frequência, contadores IEEE 802.11 a/b/g/n;
        25. Deve possuir suporte para gerenciamento de falhas via Simple Network Management Protocol (SNMP) version 3 (além do SNMP versao 2 e 1) para gerenciamento seguro entre a plataforma de gerenciamento e os switch controllers;
        26. Possuir recursos instalados e licenciados para visualização e configuração das políticas de qualidade de serviço ( QOS ) do ambiente de redes e permitir a criação de relatórios.
        27. Possuir recursos instalados e licenciados de forma que seja possível visualizar as aplicações mais utilizadas no ambiente, tipo bittorrent, whatsapp, browsing entre outros e também os usuários que estão utilizando estas aplicações.
        28. Sistema de gerencia deve ser acessado através de qualquer browser via HTTP ou Secure HTTP (HTTPS), permitindo o acesso à plataforma de gerência a qualquer momento de qualquer local;
        29. Permitir a criação de Domínios de Gerencia Virtuais, ou seja permitir a criação de perfis de administração que possibilite limitar a administração de seguimentos da rede wireless e a toda rede;
        30. Deve possuir ferramentas integradas para prever os requerimentos de RF para projeto da rede wireless LAN, incluindo qual o melhor local para os pontos de acesso na planta do prédio/andar, configuração, estimar performance e cobertura;
        31. Permitir importação de plantas baixas nos formatos jpg;
        32. Deve possuir ferramenta de projeto e planejamento da rede sem fio, permitindo que sejam carregadas as plantas baixas dos locais de instalação e sejam simulados a cobertura e o desempenho da rede sem fio:
        33. Deve ser compatível com arquivos de CAD no formato DWG e arquivos nos formatos PNG ou GIF ou JPG;
        34. Deve permitir o posicionamento automático e manual dos Pontos de Acesso, e os ajustes das características dos rádios destes APs;
        35. Deve gerar relatório com os mapas de cobertura e desempenho projetados e lista dos dispositivos utilizados na simulação;
        36. Permitir a visualização de alertas da rede em tempo real;
        37. Deve permitir ao administrador importar a planta dos andares e assinalar as características de RF dos Pontos de Acesso aumentando a precisão do projeto;
        38. Possuir ferramentas para permitir ao administrador visualizar o layout da rede wireless LAN e monitorar a performance da mesma - incluindo mapa detalhado (heat map) que exibe a cobertura de RF sobre os mapas com layout real dos andares;
        39. Possuir capacidade de listagem on-line da localização de usuários, endereço IP, endereço MAC, nível de potencia de recepção e dados de associação e de autenticação 802.1x;
        40. Deve possibilitar a visualização rápida de eventuais buracos de cobertura de RF, alarmes e estatísticas de utilização para fácil e rápido monitoramento e troubleshooting;
        41. Deve permitir a atualização de software dos Pontos de Acesso de modo centralizado via interface browser - web based;
        42. Deve descobrir automaticamente os pontos de acesso (AP) individuais na infraestrutura de rede wireless, eliminando a necessidade de configuração e manutenção e provendo informação para fins de planejamento da capacidade e troubleshooting;
        43. Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada AP;
        44. Possuir possibilidade de geração de relatórios que relacionam atividade da rede e informações de sistema, incluindo estatísticas dos usuários/clientes, utilização de rádio frequência, contadores 802.11, histórico da configuração de gerenciamento de RF;
        45. Deve ser possuir relatórios contendo ameaças de segurança recorrentes antes que estes causem danos a infraestrutura Wireless LAN e LAN;
        46. Suporte a criação e aplicação de políticas que permitam ao administrador gerir/criar: VLAN, RF, qualidade de serviço (QoS) e política de segurança, SSIDs múltiplos e únicos com parâmetros individuais de segurança.
        47. Implementando alta disponibilidade, trabalhando com no mínimo, dois sistemas completos., garantindo replicação automática da toda base de dados. As licenças necessárias para implementar este recurso deverão incluídas;
        48. Permitir throubleshooting de clientes com dificuldade de se conectarem a rede wireless;
        49. Permitir integração com Chokepoints para aplicações de localização mais precisas;
        50. Permitir a criação de templates de configuração, permitindo “scheduling” de horário para aplicação do mesmo;
        51. Deve implementar protocolo de autenticação para controle do acesso administrativo a qualquer componente da gerência da solução utilizando servidor Radius e auditoria de comandos com mecanismos de AAA;
        52. Deve possuir interface web que permita o acesso integral à ferramenta através de um navegador padrão(Firefox e Internet Explorer);
        53. Deve permitir o acesso de, no mínimo, 25 (vinte e cinco) operadores do sistema de forma simultânea;
        54. Deve implementar controle de acesso baseado em privilégios, permitindo a criação de grupos de operadores com limitação de quais equipamentos e quais serviços da plataforma poderão ser usados;
        55. Deve permitir a autenticação dos operadores através de base local e através de RADIUS;
        56. Deve executar o registro das ações executadas pelos operadores nos equipamentos gerenciados, para efeito de auditoria;
        57. Deve permitir a descoberta de elementos de rede através da faixa de endereços IP, e tabela de roteamento;
        58. Deve permitir a configuração, monitoramento, adição e gerência de um dispositivo e também de um grupo de dispositivos;
        59. Deve possuir recursos instalados e licenciados para o gerenciamento de redes sem fio, contemplando a configuração, monitoramento dos dispositivos WLAN, permitindo o gerenciamento integrado de redes sem fio e cabeada na mesma plataforma;
        60. Deve permitir a customização página principal do sistema, permitindo a inclusão alarmes, estatísticas de desempenho;
        61. Deve permitir importar uma lista de dispositivos através de um arquivo;
        62. Deve permitir visualização de estatísticas de utilização do equipamento contemplando no mínimo utilização de memória e de CPU;
        63. Deve permitir a visualização de informações dos dispositivos e componentes instalados, trazendo no mínimo, informações como fabricante, modelo, número de série, versão de hardware e software e outras informações que sejam disponibilizadas pelo equipamento gerenciado.
        64. Deve permitir a localização de endereço IP e de endereço MAC na infraestrutura de rede.
        65. Deve ser capaz de distinguir uma porta de usuário de um dispositivo de rede e exibir apenas resultados referentes a estações de trabalho ou terminais.
        66. Deve permitir a visualização do histórico dos arquivos de configuração dos dispositivos;
        67. Deve permitir visualizar, comparar, aplicar e fazer o backup da configuração dos dispositivos gerenciados;
        68. Deve permitir atualizar o software do dispositivo gerenciado;
        69. Deve permitir a criação de modelos de configuração para serem aplicados aos dispositivos gerenciados. Deve permitir criar modelos de parte da configuração e da configuração inteira do dispositivo;
        70. Deve permitir o agendamento de backups da configuração dos dispositivos gerenciados;
        71. Deve possuir recursos instalados e licenças para a criação de relatórios de histórico de backups e atualizações de software;
        72. Deve permitir a criação de regras de verificação de configuração e comparar com a configuração dos dispositivos gerenciados;
        73. Deve gerar relatório da verificação;
        74. Deve possuir recursos instalados para executar operação como servidor syslog, permitindo a recepção de mensagens Syslog dos dispositivos;
        75. Deve possuir capacidade de gerar alarmes a partir de traps SNMP e mensagens Syslog;
        76. Deve possuir mecanismo de análise de causa do problema para a supressão de eventos que são apenas sintoma da falha;
        77. Deve possuir painel único de visualização dos alarmes e a partir desta tela verificar detalhes específicos de um alarme;
        78. Deve possuir a capacidade de enviar emails para um administrador em caso de algum evento especificado de acordo com o nível de criticidade.
        79. Deve possuir capacidade de monitorar o desempenho dos equipamentos gerenciados;
        80. Deve possuir capacidade de monitorar a utilização de CPU, utilização de Memória, tempo de resposta e Disponibilidade;
        81. Deve permitir ao administrador escolher quais monitores de desempenho devem ser configurados para ativar um alarme;
        82. Deve permitir a visualização em tempo real de itens monitorados;
        83. Deve permitir a visualização e configuração de listas de controle de acesso (ACL) nos equipamentos gerenciados e compatíveis;
        84. Deve permitir a criação de templates ACLs para a distribuição em diversos equipamentos;
        85. Deve possuir capacidade de configurar interface vlan ou interfaces virtuais, adicionar portas de acesso e do tipo trunk;
        86. Deve permitir o gerenciamento centralizado de dispositivos de rede sem fio:
        87. Controladores de Acesso (AC's);
        88. Pontos de Acesso Gerenciados (FIT AP's);
        89. Pontos de Acesso Autonomos (FAT AP's).
        90. Deve permitir a visualização dos Controladores e Pontos de Acesso;
        91. Deve fornecer informações dos clientes online associados aos Pontos de Acesso.
        92. Deve oferecer serviço de alarmes para os Controladores, Pontos de Acesso e Clientes associados a redes sem fio baseadas no padrão IEEE 802.11;
        93. Deve possibilitar o gerenciamento dos Rádios e SSID's dos Pontos de Acesso;
        94. A plataforma de gerencia da solução deve permitir a coleta de informações dos clientes conectados, incluindo informações de endereçamento de camada 3 do modelo OSI. Deverá ser possível monitorar os endereçamentos IPv4 e IPv6 dos clientes wifi na página de administração da plataforma de gerencia;
        95. Deve fornecer informações estatísticas de performance baseadas no histórico dos Controladores (AC's) e Pontos de Acesso Gerenciados;
        96. Deve possuir capacidade de gerar relatórios customizados:
        97. Ativos de Rede;
        98. Estado dos dispositivos e Links;
        99. Lista total de portas e lista de portas disponíveis;
        100. Inventário dos equipamentos;
        101. Informações sobre os dispositivos ativos;
        102. Erros durante o processo de descoberta;
        103. Os serviços de suporte e manutenção e substituição de hardware deste item deverão ser realizados em regime 8x5xnbd (8 horas x 5 dias da semana com prazo para resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 01 (hum) ano;
        104. A contratante poderá abrir chamados de manutenção diretamente no fabricante do ítem, através de chamada gratuita a número 0800 e por interface web, sem necessidade de prévia consulta e/ou qualquer liberação por parte da contratada. não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software. poderá ser solicitado ao fabricante acesso remoto aos equipamentos para ajuda na correção de problemas dos diversos tipos inclusive configuração sem custos adicionais ou necessidade de autorização da contratada no momento desta abertura;
        105. Deverá ser garantido à contratante o pleno acesso ao site do fabricante dos equipamentos e softwares. esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto;
        106. Os valores bem como partnumber dos serviços acima devem estar contidos na oferta apresentada.
    46. **Da solução de Controler de rede Wireless WLAN:**
        1. **Sistema de Controle e Gerenciamento dos Pontos de Acesso.**
        2. Sistema de Controladora Centralizada para até 200 pontos de acesso;
        3. O equipamento deve ter capacidade mínima de gerenciar simultaneamente pelo menos 200 (duzentos) Pontos de Acesso WiFi Externo ou Internos. Não serão considerados nestes totais Pontos de Acesso em Gerenciamento de Alta-Disponibilidade.
        4. Deve ter capacidade máxima de suportar no mínimo 6000 (seis mil) clientes conectados à rede WiFi.
        5. O equipamento ou soma de equipamentos deve ser entregue com capacidade inicial para gerenciar e controlar, no mínimo e simultaneamente, 11 (onze) Pontos de Acesso WiFi Indoor e Outdoor descritos nesta Especificação Técnica com todas as funcionalidades abaixo descritas licenciadas para uso imediato, caso sejam necessárias licenças por funcionalidades.
        6. Cada expansão deverá ocorrer apenas por número de pontos de acesso e caso a controladora tenha licenças para alguma das funcionalidades descritas, esta licença deverá constar também para o número de pontos de acesso da expansão.
        7. No caso de falha de um equipamento controlador WiFi “ativo”, todos os pontos de acesso WiFi associados e controlados pelo mesmo deverão se associar de forma automática ao equipamento controlador WiFi “redundante” e passar a ser controlados por este.
        8. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação elétrica, voltar à operação normalmente na mesma configuração anterior à queda da alimentação elétrica;
        9. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
        10. Permitir que os eventos sejam gravados remotamente utilizando syslog;
        11. Possui suporte a MIB II, conforme RFC 1213;
        12. Possibilitar a obtenção da configuração lógica e física do equipamento através do protocolo SNMP;
        13. O controlador WiFi deve ser capaz de controlar pontos de acesso WiFi do tipo indoor e outdoor, simultaneamente, nos padrões 802.11a, 802.11b/g, 802.11n e 802.11ac;
        14. O controlador WiFi deve ser capaz de controlar pontos de acesso WiFi operando em modo mesh e ponto local (não-mesh), simultaneamente, nos padrões 802.11a, 802.11b/g, 802.11n e 802.11ac;
        15. Deve atender aos padrões IEEE 802.11d e 802.11h;
        16. Implemetar DHCP Relay;
        17. Permitir o uso de múltiplos SSIDs simultaneamente
        18. Permitir definir o numero máximo de clientes por SSIDs.
        19. O controlador WiFi deve ser capaz de operar em modo de “tráfego centralizado” e de “chaveamento de tráfego local”, simultaneamente, nos padrões 802.11a, 802.11b/g, 802.11n e 802.11ac;
        20. No modo de operação de “tráfego centralizado”, o tráfego de dados gerado pelos usuários associados aos pontos de acesso WiFi deve passar através do controlador WiFi (“ativo” ou “redundante”). O tráfego de controle dos pontos de acesso WiFi deve ser enviado para o controlador WiFi;
        21. Deve ser possível, em conjunto com os pontos de acesso, analisar, exibir relatórios, bloquear, fazer marcação de DSCP e até definir o uso de banda, no mínimo, das seguintes aplicações através de análise profunda de pacotes ( DPI ) :
        22. Bittorrent, Emule e outras aplicações peer-to-peer;
        23. Skype, Google Talk, Whatsapp e outras aplicações realtime;
        24. Gmail, Youtube, Netflix, Dropbox e outras aplicações web;
        25. Citrix, Exchange, Oracle e outras aplicações empresariais;
        26. Caso o usuário venha à trocar as portas de aplicações referenciadas acima, o controlador deve continuar identificando e nomeando as aplicações acima corretamente.
        27. Deve ser capaz de controlar pontos de acesso do mesmo fabricante operando em “chaveamento de tráfego local” ;
        28. No modo de operação de “chaveamento de tráfego local”, deve permitir a configuração de pontos de acesso WiFi de forma que os mesmos realizem o chaveamento (switching) local do tráfego de dados gerado pelos usuários a eles associados, evitando que o tráfego de dados destes usuários passem através do controlador WiFi (“ativo” ou “redundante”). O tráfego de controle dos pontos de acesso WiFi deve ser enviado para o controlador WiFi;
        29. Operando no modo de “chaveamento de tráfego local”, o controlador WiFi deve:
        30. No caso de falha na comunicação lógica entre os pontos de acesso da localidade com o controlador centralizado WiFi, ou com o Sistema de Autenticação Centralizado dos usuários, ou mesmo em caso de falha no link WAN (ou LAN) que realize a conexão lógica dos pontos de acesso com o controlador WiFi, os usuários já associados aos pontos de acesso da localidade devem continuar a ter acesso à rede local. Também deve ser possível que novos usuários se autentiquem através de 802.1X e se associem de forma alternativa à rede local sem qualquer prejuízo de acesso local. Os usuários também devem continuar realizando o fast-roaming entre os pontos de acesso WiFi locais;
        31. A rede WiFi local não pode se tornar inoperante devido a ocorrência de qualquer uma das 03 (três) falhas isoladas ou simultâneas apresentadas anteriormente: falha no controlador WiFi, falha no Sistema de Autenticação Centralizado ou falha no link de comunicação entre os pontos de acesso e o controlador (WAN ou LAN);
        32. Caso a solução proposta não atenda os itens anteriores, necessário para a sobrevivência dos serviços dos sites remotos, a CONTRATADA deverá deverá fornecer uma solução alternativa de redundância e autenticação para pontos de acesso operando com “chaveamento de tráfego local” para, pelo menos, cada uma das localidades que serão atendidas. A solução alternativa deverá ter capacidade de controlar, no mínimo e simultaneamente, 25 (vinte e cinco) pontos de acesso do mesmo fabricante operando com “chaveamento de tráfego local” e seus custos deverão ser inseridos no item “Controlador WiFi”.
        33. O controlador WiFi deve ajustar automaticamente os canais 802.11 para a otimizar a cobertura de rede e mudar as condições de RF baseado em performance mantendo uma distribuição lógica de canais evitando interferências do tipo co-channel;
        34. Possibilitar a implementação de criptografia do tráfego de dados dos usuários e também do trafego de controle, na comunicação entre Pontos de acesso e Controlador WiFi. Deve permitir que todos os dados de usuários e controle sejam criptografados com no mínimo 500Mbps de troughput.
        35. Deve possuir funcionalidade que permita a utilização dos Aps em sites remotos, onde através de conexão pela internet este automaticamente estabeleça um túnel seguro até o controlador permitindo que os SSIDs corporativos sejam disponibilizados aos usuários. Devera também permitir a criação de um SSID local, que efetue a conexão direta via internet, sem a utilização do túnel seguro. Caso esta funcionalidade necessite de licenças adicionais, estas deverão estar contempladas para totalidade da capacidade do controlador, ou seja 200Aps.
        36. Deve implementar o protocólo IEEE 802.1x, para suportar autenticação dos diversos tipos de clientes, com pelo menos os seguintes métodos EAP:
        37. EAP-Transport Layer Security (EAP-TLS);
        38. EAP-TTLS/MSCHAPv2;
        39. PEAPv0/EAP-MSCHAPv2;
        40. PEAPv1/EAP-GTC;
        41. EAP-FAST,
        42. EAP Subscriber Identity Module (EAP-SIM).
        43. Deve possuir recursos instalados e licenciados para requisições radius em servidores externos de mesmo fabricante e também de terceiros, de maneira que possa ser usado o radius existente.
        44. Permitir a selação/uso de servidor Radius ou LDAP por SSID;
        45. Implementar associação dinâmica de usuários a VLANs, com base nos parâmetros da etapa de autenticação;
        46. Deve possuir base de dados de usuários interno para autenticação de usuários convidados/temporários (acesso guest);
        47. Estes usuários autenticados através do portal Web devem se autenticar e ser desviados para segmentos específicos da rede LAN(VLANs);
        48. O controlador WiFi deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes, temporários ou clientes corporativos;
        49. Permitir a utilização de portal Web (Capitive) externo a controladora;
        50. Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
        51. Deve implementar WEP (Wired Equivalent Privacy), chaves estáticas e dinâmicas (40 bits e 128 bits);
        52. Dever suportar WPA com algoritmo de criptografia TKIP;
        53. Deve implementar WPA-2 (Wi-Fi Protected Access) com algoritmo de criptografia AES;
        54. Deve implementar o padrão IEEE 802.11i;
        55. Permitir e priorizar adequadamente o uso de voz e dados sobre um mesmo SSID;
        56. Implementar CAC ( Call Admission Control ) para Voz;
        57. Deve suportar 802.11e com WMM, U-APSD e T-SPEC;
        58. Implementar padrão Wireless Multi-media QoS (WMM) da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
        59. Implementar qualidade de serviço com a marcação de pacotes utilizando Diffeservice e suporte a 802.1p, para QoS.
        60. Deve implementar o bloqueio da comunicação entre usuários em um mesmo SSID permitindo o isolamento dos usuários;
        61. Deve ser fornecido com recursos e licenças instaladas para implementar mecanismo de detecção e contenção de pontos de acesso invasor do tipo “Rogue AP”;
        62. Deve ser fornecido com recursos e licenças instaladas para implementar mecanismo de detecção e contenção de clientes invasores do tipo “Clientes Rogue”;
        63. Deve ser fornecido com recursos e licenças instaladas para implementar mecanismo de detecção e contenção de “Redes Ad-Hoc”;
        64. Deve ser fornecido com recursos e licenças instaladas para implementar detecção de ataques “Denial of Service (DoS)” no mínimo dos seguintes tipos:
13. “Association flood or storm”;
14. “Authentication flood or storm”;
15. “EAPOL Start”;
16. “EAPOL Logoff”;
17. “Deauthentication flood or storm”;
18. “Disassociation flood or storm”.
    * 1. Deve ser fornecido com recursos e licenças instaladas para implementar detecção de ataques “Security Penetration Attacks” no mínimo dos seguintes tipos:
19. Detecção de “NetStumbler”;
20. Detecção de “Wellenreiter”;
21. Detecção de “Fake APs”.
    * 1. Deve ser fornecido com recursos instalados para implementar listas de controle de acesso (ACL) com suporte a contadores (ACL Counters), ou seja, para um determinado pacote deve ser possível verificar qual entrada da lista de controle de acesso foi utilizada;
      2. Implementar listas de controle de acesso (ACL) baseadas em protocolos e endereços MAC;
      3. Deve implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar a performance durante elevada utilização da rede;
      4. Deve possuir recursos instalados para implementar mecanismos automáticos de gerenciamento de recursos de rádio, detectando áreas sem cobertura, indisponibilidades de pontos de acesso, e executando auto-configuração, auto-correção e otimização, trocando os canais atribuídos automaticamente e ajustando a potência dos pontos de acesso quando necessário de forma a criar uma distribuição lógica entre potência e canais nos pontos de acesso da planta;
      5. Deve possuir recursos instalados para implementar mecanismo que no evento de falha de um ponto de acesso WiFi, o controlador WiFi ajuste automaticamente a potência dos pontos de acesso adjacentes para realizar a cobertura da área onde o ponto de acesso WiFi que falhou estava provendo o sinal;
      6. Deve possuir recursos instalados para implementar mecanismo que ajuste dinamicamente a potência de saída dos pontos de acesso, individualmente, para acomodar possíveis variações nas condições de radio frequência (RF) da rede, garantindo a performance e escalabilidade;
      7. Implementar varredura de RF continua, programada ou sob demanda;
      8. Ajustar, dinamicamente, o nível de potência e canal dos rádios dos pontos de acesso WiFi de modo a otimizar o tamanho da célula de RF, garantido a performance e escalabilidade;
      9. Deve implementar detecção de interferências wi-fi e não wi-fi e reajuste dos parâmetros de RF evitando problemas de cobertura e performance;
      10. Deve detectar e gerar alarmes de interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar, classificar e gerar alarmes de interferências não-WiFi, no mínimo de Bluetooth, telefones sem fio, câmeras de video sem fio, Microondas e outros. Deverá ser capaz de identificar no mínimo 20 tipos diferentes de interferências;
      11. Deve ser capaz de identificar a quantidade de interferências citadas no item anterior, mesmo quando de mesmo tipo. Exemplo: 3 interferências bluetooth;
      12. Possuir mecanismo de classificação e detecção da intensidade de sinal das interferências. Estas interferências devem ser classificadas com uma severidade. Baseado em um nível de severidade programável, deve ser capaz de mudar os canais de transmissão dos pontos de acesso Externos ou Internos para evitar que a interferência prejudique o fornecimento do serviço de acesso WiFi aos clientes;
      13. Permitir a realização de “fast-roaming” dos usuários entre pontos de acesso WiFi distintos que atendam a uma mesma localidade.
      14. Implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso;
      15. Deve implementar um mecanismo de controle de associação de banda, de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN, para desocupar o máximo possível a frequência de 2.4GHz e utilizar a frequência de 5GHz que tem mais canais disponíveis;
      16. Possibilitar roaming com integridade de sessão, dando suporte à aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
      17. Deve implementar roaming rápido para os usuários autenticados por 802.1x (Fast Secure Roaming). O roaming de um cliente autenticado entre dois Pontos de Acesso deve ser inferior à 150ms (milissegundos);
      18. Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados  usuários da rede WLAN padrão 802.11abgn.
      19. Deve permitir comutação (bridging) de pacotes IPv6 com os controles mínimos necessários como RA Guard, IPv6 Neighbor Discovery Caching.
      20. Deve permitir mobilidade (roaming) de clientes IPv6 em camada 2, sem impacto na aplicação dos usuários.
      21. Deve permitir a visualização dos endereços IPv6 dos usuários conectados sejam estes IPv4 e IPv6 ou só IPv6.
      22. Suportar, no mínimo, 512 VLANs;
      23. Suportar, no mínimo, 512 SSIDs;
      24. SUPORTE E GARANTIA:
      25. Os serviços de suporte e manutenção e substituição de hardware deste item deverão ser realizados em regime 8x5xnbd (8 horas x 5 dias da semana com prazo para resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 01 (hum) ano;
      26. A contratante poderá abrir chamados de manutenção diretamente no fabricante do ítem, através de chamada gratuita a número 0800 e por interface web, sem necessidade de prévia consulta e/ou qualquer liberação por parte da contratada. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software. poderá ser solicitado ao fabricante acesso remoto aos equipamentos para ajuda na correção de problemas dos diversos tipos inclusive configuração sem custos adicionais ou necessidade de autorizaçao da contratada no momento desta abertura.
      27. Deverá ser garantido à contratante o pleno acesso ao site do fabricante dos equipamentos e softwares. esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto;
      28. Deve ser fornecido Rack de 44U completo para instalação do equipamento de aplliance.
      29. Os valores bem como partnumber dos serviços acima devem estar contidos na oferta apresentada.
22. Ativos de Rede
    1. Esse anexo relaciona os equipamentos ativos a serem implementados na rede da Prefeitura e que irá compor a Infovia e que deverão ser instalados e configurados pela empresa a ser CONTRATADA. Cada um dos diferentes equipamentos é relacionado com sua descrição e principais características e sua função na Infovia.
    2. Switch SFP Data Core – Tipo I: Este equipamento deverá ser configurado e instalado conforme descrito na Especificação Técnica nos itens 5.1, 5.1.1 e 51.4.
    3. Switch Distribuição – Tipo I: Este equipamento deverá ser configurado e instalado conforme descrita na Especificação Técnica no item 5.1.6.
    4. Switch de Acesso – Tipo I: Este equipamento deverá ser configurado e instalado nas localidades referenciadas e indicadas no plano de instalação Edital.
    5. Switch de Acesso – Tipo II: Este equipamento deverá ser configurado e instalado nas demais localidades, conforme for disposto entre a SMTI e a contratada durante a elaboração do plano de instalação Edital.
23. SWITCH SFP DATA CORE - TIPO I
    1. Switch de 48 portas 10/100/1000 UTP, 4 portas 1000BaseSX (fibra ótica), PoE.
    2. Possuir, no mínimo, 4 portas 1000Base-SX switching gigabit ethernet, full-duplex, para fibras óticas multimodo. Deverão ser fornecidos os GBIC ou SFP necessários.
    3. Possuir, no mínimo, 48 portas Ethernet 10/100/1000 com autosensing de velocidade e com conectores RJ-45.
    4. As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control).
    5. Implementar Power Over Ethernet (PoE) de acordo com os padrões IEEE 802.3af e 802.3at em todas as portas ethernet 10/100/1000.
    6. Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática.
    7. Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX)
    8. Possuir capacidade de associação das portas 10/100/1000 e 1000Base-SX, no mínimo, em grupo de oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
    9. Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
    10. Implementar VLANs por porta.
    11. Implementar VLANs compatíveis com o padrão IEEE 802.1q.
    12. Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.
    13. Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
    14. Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.
    15. FONTE DE ALIMENTAÇÃO: Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e freqüência (de 50/60 Hz);
    16. Suportar alimentação elétrica redundante capaz de suportar o equipamento com todas as funcionalidades;
    17. A fonte de alimentação deverá possuir no minimo 370W para alimentação PoE, além da energia necessária para funcionamento do switch.
    18. Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento;
    19. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
    20. Possuir LEDs para a indicação do status das portas e atividade, além de duplex e PoE.
    21. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
    22. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    23. Sem autenticação e sem privacidade (noAuthNoPriv);
    24. Com autenticação e sem privacidade (authNoPriv);
    25. Com autenticação e com privacidade (authPriv).
    26. Possuir suporte a MIB II, conforme RFC 1213.
    27. Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
    28. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
    29. Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE.
    30. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
    31. Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
    32. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
    33. Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
    34. Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757
    35. Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE.
    36. Implementar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 4 unidades, com velocidade de empilhamento de 40Gbps full-duplex.
    37. A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.
    38. FACILIDADES: Implementar Telnet para acesso à interface de linha de comando.
    39. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.
    40. Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface ), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
    41. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
    42. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
    43. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
    44. Permitir que a sua configuração seja feita através de terminal assíncrono.
    45. Permitir a gravação de log externo (syslog).
    46. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
    47. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
    48. Permitir o espelhamento do tráfego de portas que residem em um dado switch para uma porta que reside em switch diferente da pilha.
    49. Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
    50. Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
    51. Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
    52. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
    53. Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
    54. Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
    55. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
    56. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
    57. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA).
    58. Devem ser suportadas no mínimo as seguintes operações de teste:
    59. ICMP echo;
    60. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
    61. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
    62. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
    63. Protocolos: Implementar o protocolo NTPv3 (Network Time Protocol, versão 3. Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 1305.
    64. Implementar DHCP Relay e DHCP Server em múltiplas VLANS.
    65. Desempenho: Possuir capacidade para pelo menos 8.000 endereços MAC na tabela de comutação.
    66. Implementar , no mínimo, 255 vlans simultaneamente.
    67. Deve possuir switch-capacity de no mínimo 144Gbps e taxa de encaminhamento de no mínimo 77 Mpps.
    68. Suportar Jumbo frames de no mínimo 9216 Bytes.
    69. Segurança: Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;
    70. Implementar filtragem de pacotes (ACL - Access Control List);
    71. Proteger a interface de comando do equipamento através de senha.
    72. Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
    73. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
    74. Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
    75. Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
    76. Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
    77. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
    78. Possuir controle de broadcast, multicast e unicast por porta.
    79. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
    80. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.
    81. Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
    82. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units ) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
    83. Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
    84. Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.
    85. Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.
    86. Padrões: Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
    87. Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
    88. Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
    89. Implementar padrão IEEE 802.3ad.
    90. Implementar padrão IEEE 802.3af.
    91. Implementar padrão IEEE 802.3at.
    92. Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
    93. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x.
    94. Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
    95. Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
    96. A estação não tem cliente 802.1x (suplicante);
    97. As credenciais do usuário não estão corretas (falha de autenticação).
    98. Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).
    99. Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
    100. Nome do usuário;
    101. Switch em que o computador do usuário está conectado;
    102. Porta do switch utilizada par acesso;
    103. Endereço MAC da máquina utilizada pelo usuário;
    104. Endereço IP do usuário;
    105. Horários de início e término da conexão;
    106. Bytes transmitidos e recebidos durante a conexão.
    107. Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
    108. Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.
    109. Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
    110. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS.
    111. Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
    112. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
    113. Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
    114. Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.
    115. Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
    116. Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.
    117. Multicast: Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
    118. Implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego multicast IPv6 seja tratado como broadcast no switch.
    119. Qualidade de Serviço (QoS): Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
    120. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
    121. Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
    122. Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force);
    123. Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
    124. Deve ser possível a especificação de banda por classe de serviço;
    125. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
    126. Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
    127. Suportar diferenciação de QoS por VLAN.
    128. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection);
    129. Implementar pelo menos quatro filas de prioridade por porta de saída (egress port).
    130. Internet Protocol versão 6 (IPv6): Implementar IPv6;
    131. Permitir a configuração de endereços IPv6 para gerenciamento;
    132. Permitir consultas de DNS com resolução de nomes em endereços IPv6;
    133. Implementar ICMPv6 com as seguintes funcionalidades:
    134. ICMP request
    135. ICMP Reply
    136. ICMP Neighbor Discovery Protocol (NDP)
    137. ICMP MTU Discovery
    138. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
    139. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
24. SWITCH DISTRIBUIÇÃO – TIPO I
    1. Switch de 48 portas 10/100/1000 UTP, 4 portas 1000BaseSX (fibra ótica), PoE.
    2. Possuir, no mínimo, 4 portas 1000Base-SX switching gigabit ethernet, full-duplex, para fibras óticas multimodo. Deverão ser fornecidos os GBIC ou SFP necessários.
    3. Possuir, no mínimo, 48 portas Ethernet 10/100/1000 com autosensing de velocidade e com conectores RJ-45.
    4. As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control).
    5. Implementar Power Over Ethernet (PoE) de acordo com os padrões IEEE 802.3af e 802.3at em todas as portas ethernet 10/100/1000.
    6. Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática.
    7. Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);
    8. Possuir capacidade de associação das portas 10/100/1000 e 1000Base-SX, no mínimo, em grupo de oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.
    9. Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
    10. Implementar VLANs por porta.
    11. Implementar VLANs compatíveis com o padrão IEEE 802.1q.
    12. Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.
    13. Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
    14. Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.
    15. FONTE DE ALIMENTAÇÃO: Possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e freqüência (de 50/60 Hz);
    16. Suportar alimentação elétrica redundante capaz de suportar o equipamento com todas as funcionalidades;
    17. A fonte de alimentação deverá possuir no minimo 370W para alimentação PoE, além da energia necessária para funcionamento do switch.
    18. Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento;
    19. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
    20. Possuir LEDs para a indicação do status das portas e atividade, além de duplex e PoE.
    21. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
    22. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    23. Sem autenticação e sem privacidade (noAuthNoPriv);
    24. Com autenticação e sem privacidade (authNoPriv);
    25. Com autenticação e com privacidade (authPriv).
    26. Possuir suporte a MIB II, conforme RFC 1213.
    27. Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
    28. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
    29. Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE.
    30. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
    31. Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
    32. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
    33. Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
    34. Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757
    35. Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED, com auto negociação de energia para PoE.
    36. Implementar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 4 unidades, com velocidade de empilhamento de 40Gbps full-duplex.
    37. A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.
    38. FACILIDADES: Implementar Telnet para acesso à interface de linha de comando.
    39. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.
    40. Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface ), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
    41. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
    42. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
    43. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
    44. Permitir que a sua configuração seja feita através de terminal assíncrono.
    45. Permitir a gravação de log externo (syslog).
    46. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
    47. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
    48. Permitir o espelhamento do tráfego de portas que residem em um dado switch para uma porta que reside em switch diferente da pilha.
    49. Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
    50. Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
    51. Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
    52. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
    53. Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
    54. Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
    55. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
    56. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
    57. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA).
    58. Devem ser suportadas no mínimo as seguintes operações de teste:
    59. ICMP echo;
    60. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
    61. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
    62. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
    63. Protocolos: Implementar o protocolo NTPv3 (Network Time Protocol, versão 3. Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 1305.
    64. Implementar DHCP Relay e DHCP Server em múltiplas VLANS.
    65. Desempenho: Possuir capacidade para pelo menos 8.000 endereços MAC na tabela de comutação.
    66. Implementar , no mínimo, 255 vlans simultaneamente.
    67. Deve possuir switch-capacity de no mínimo 144Gbps e taxa de encaminhamento de no mínimo 77 Mpps.
    68. Suportar Jumbo frames de no mínimo 9216 Bytes.
    69. Segurança: Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;
    70. Implementar filtragem de pacotes (ACL - Access Control List);
    71. Proteger a interface de comando do equipamento através de senha.
    72. Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
    73. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
    74. Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
    75. Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.
    76. Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
    77. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
    78. Possuir controle de broadcast, multicast e unicast por porta.
    79. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
    80. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.
    81. Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
    82. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units ) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
    83. Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
    84. Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.
    85. Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.
    86. Padrões: Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
    87. Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
    88. Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
    89. Implementar padrão IEEE 802.3ad.
    90. Implementar padrão IEEE 802.3af.
    91. Implementar padrão IEEE 802.3at.
    92. Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
    93. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x.
    94. Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:
    95. Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
    96. A estação não tem cliente 802.1x (suplicante);
    97. As credenciais do usuário não estão corretas (falha de autenticação).
    98. Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).
    99. Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
    100. Nome do usuário;
    101. Switch em que o computador do usuário está conectado;
    102. Porta do switch utilizada par acesso;
    103. Endereço MAC da máquina utilizada pelo usuário;
    104. Endereço IP do usuário;
    105. Horários de início e término da conexão;
    106. Bytes transmitidos e recebidos durante a conexão.
    107. Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
    108. Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.
    109. Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
    110. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS.
    111. Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
    112. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
    113. Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
    114. Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.
    115. Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
    116. Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.
    117. Multicast: Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;
    118. Implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego multicast IPv6 seja tratado como broadcast no switch.
    119. Qualidade de Serviço (QoS): Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
    120. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
    121. Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
    122. Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force);
    123. Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
    124. Deve ser possível a especificação de banda por classe de serviço;
    125. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
    126. Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
    127. Suportar diferenciação de QoS por VLAN.
    128. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection);
    129. Implementar pelo menos quatro filas de prioridade por porta de saída (egress port).
    130. Internet Protocol versão 6 (IPv6): Implementar IPv6;
    131. Permitir a configuração de endereços IPv6 para gerenciamento;
    132. Permitir consultas de DNS com resolução de nomes em endereços IPv6;
    133. Implementar ICMPv6 com as seguintes funcionalidades:
    134. ICMP request
    135. ICMP Reply
    136. ICMP Neighbor Discovery Protocol (NDP)
    137. ICMP MTU Discovery
    138. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
    139. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
    140. Deve ser fornecido transceiver ethernet para conexão com OLT a ser instalado nos POP – Ponto de Presença, informar na proposta comercial marca e modelo do transcrever a ser utilizado.
    141. Há não indicação de marca e modelo do transceiver que compõe esse item é passível de desclassificação.
25. SWITCH DE ACESSO – TIPO I
    * + 1. Switch de acesso com 24 portas 10/100 Mbps UTP e 2 Interfaces com duplo proposito ou 10/100/1000 Mbps ou SFP.
    1. Arquitetura de Hardware: Montável em rack 19’’ incluindo todos os acessórios necessários.
    2. Fonte de alimentação
    3. Deve possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
    4. Deve possuir cabo de alimentação para a fonte com, no mínimo, 1,00m (um metro) de comprimento.
    5. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
    6. Deve ser do mesmo fabricante dos outros switches e módulos contantes neste decritivo.
    7. Desempenho de Hardware:
    8. Deve possuir capacidade para pelo menos 8.000 endereços MAC na tabela de comutação.
    9. Deve implementar, no mínimo, 255 vlans simultaneamente.
    10. Deve possuir Switching bandwidth full-duplex de no mínimo 16 Gbps e taxa de encaminhamento de no mínimo 6,5 Mpps.
    11. Deve suportar Jumbo frames de no mínimo 9016 Bytes.
    12. Interfaces / Slots:
    13. Deve possuir, no mínimo, 2 slots 1000 Mbps do tipo SFP (módulos/transceiver) não inclusos, full-duplex, para fibras óticas ou UTP.
    14. Deve possuir, no mínimo, 24 portas Ethernet 10/100 com autosensing de velocidade e com conectores RJ-45.
    15. As interfaces 10/100 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX) e IEEE802.3x (Flow Control).
    16. Todas as portas Ethernet 10/100 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática.
    17. Todas as portas Ethernet 10/100 devem suportar auto configuração de crossover (Auto MDIX)
    18. Deve possuir LEDs para a indicação do status das portas e atividade, além de duplex.
    19. O switch ofertado deve possuir no mínimo 26 portas ativas divididas de acordo com items acima deste descritivo.
    20. Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
    21. Deve possuir capacidade de associação das portas 10/100 ou das portas 1G, no mínimo, em grupo de até oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad. Deve poder formar no mínimo 6 grupos de portas.
    22. Deve possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
    23. Gerenciamento: Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
    24. Deve implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    25. Sem autenticação e sem privacidade (noAuthNoPriv);
    26. Com autenticação e sem privacidade (authNoPriv);
    27. Com autenticação e com privacidade (authPriv).
    28. Possuir criptografia 3DES e AES para proteção dos dados de gerência SNMPv3.
    29. Deve possuir suporte a MIB II, conforme RFC 1213.
    30. Deve implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
    31. Deve possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
    32. Deve possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
    33. Deve possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
    34. Deve possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
    35. Deve permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
    36. Deve implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757;
    37. Deve implementar os protocolos LLDP (IEEE 802.1AB);
    38. Deve implementar Telnet para acesso à interface de linha de comando.
    39. Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial;
    40. Deve ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface ), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
    41. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;
    42. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);
    43. Deve suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
    44. Deve permitir que a sua configuração seja feita através de terminal assíncrono;
    45. Deve permitir a gravação de log externo (syslog) e deve permitir a visualização também internamente;
    46. Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
    47. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;
    48. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA);
    49. Devem ser suportadas no mínimo as seguintes operações de teste:
        1. ICMP echo;
        2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);
        3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
        4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
    50. Facilidades: Deve implementar VLANs por porta.
    51. Deve implementar VLANs compatíveis com o padrão IEEE 802.1q;
    52. Deve implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
    53. Deve permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch;
    54. Deve ser possível definir o sentido do tráfego a ser espelhado:
        1. Somente tráfego de entrada.
        2. Somente tráfego de saída
        3. Ambos simultaneamente.
    55. Deve permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
    56. Deve implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
    57. Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
    58. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
    59. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
    60. Protocolos: Deve implementar o protocolo NTPv4 (Network Time Protocol, versão 4). Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 5905.
    61. Deve implementar DHCP Server em múltiplas VLANS.
    62. Deve implementar DHCP Option 82.
    63. Segurança: Deve implementar filtragem de pacotes (ACL - Access Control List);
    64. Deve permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
    65. Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, baseadas em tempo.
    66. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;
    67. Deve proteger a interface de comando do equipamento através de senha;
    68. Deve implementar o protocolo SSH V2 para acesso à interface de linha de comando;
    69. Deve possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido;
    70. Deve permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;
    71. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
    72. Deve possuir controle de broadcast, multicast e unicast por porta;
    73. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
    74. Deve permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede;
    75. Deve possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;
    76. Deve possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units ) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w);
    77. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;
    78. Deve possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP, essa filtragem deve ser por porta.
    79. Padrões: Deve implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
    80. Deve implementar padrão IEEE 802.1q (Vlan Frame Tagging);
    81. Deve implementar padrão IEEE 802.1p (Class of Service) para cada porta;
    82. Deve implementar padrão IEEE 802.3ad;
    83. Deve obrigatoriamente implementar padrão IEEE 802.3af.
    84. Deve implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);
    85. Deve implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree;
    86. Deve implementar PVST ou PVST+;
    87. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
    88. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;
    89. Deve implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Deve ser atendido, no mínimo, o seguinte requisito: Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
        1. A estação não tem cliente 802.1x (suplicante);
        2. As credenciais do usuário não estão corretas (falha de autenticação).
    90. Deve implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).
    91. Deve implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
        1. Nome do usuário;
        2. Switch em que o computador do usuário está conectado;
        3. Porta do switch utilizada por acesso;
        4. Endereço MAC da máquina utilizada pelo usuário;
        5. Endereço IP do usuário;
        6. Horários de início e término da conexão;
        7. Bytes transmitidos e recebidos durante a conexão.
    92. Deve suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
    93. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS.
    94. Deve implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
    95. Multicast: Deve implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego MULTICAST seja tratado como broadcast no switch.
    96. Deve implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego MULTICAST IPv6 seja tratado como broadcast no switch.
    97. Qualidade de serviço (QoS);
    98. Deve possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
    99. Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
    100. Deve permitir Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
    101. Deve permitir Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
    102. Deve suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
    103. Deve ser possível a especificação de banda por classe de serviço.
    104. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
    105. Deve suportar diferenciação de QoS por VLAN.
    106. Deve oferecer suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection).
    107. Deve implementar pelo menos quatro filas de prioridade por porta de saída (egress port).
    108. Deve implementar pelo menos duas filas de prioridade de entrada.
    109. Internet Protocol versão 6 (IPv6);
    110. Deve implementar IPv6.
    111. Deve permitir a configuração de endereços IPv6 para gerenciamento.
    112. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6.
    113. Deve implementar ICMPv6 com as seguintes funcionalidades:
         1. ICMP request;
         2. ICMP Reply;
         3. ICMP Neighbor Discovery Protocol (NDP);
         4. ICMP MTU Discovery.
    114. Deve implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SCP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
    115. Deve implementar NTPv4 com suporte a IPv6;
    116. Deve implementar IPv6 MLD snooping v1 e v2 ;
    117. Deve implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
    118. Especificações Técnicas do Nível Switch de Acesso – Funcionalidades para Gerenciamento Complementar;
    119. Deverá ter suporte a instalações do tipo "plug-and-play" para facilitar a troca de switches.
    120. Deverá ter suporte a configurações rápidas e trocas de switches sem necessidade de configuração local. Configurações deverão ser através de um único ponto de gerenciamento;
    121. Deverá ter suporte a funcionalidade de resolução de problemas que efetua testes em buscas de problemas apresentando diagnósticos para o administrador;
    122. O switch deve ter a capacidade de identificar, ao menos, pelos seguintes mecanismos MAC, OUI, LLDP, MAB e 8021.X os equipamentos diretamente conectados à qualquer interface. Ao identificar este equipamento deve ser capaz de configurar automaticamente a interface a que este equipamento estiver conectada, aplicando desde descrição da porta até as políticas de segurança e qualidade de serviço da mesma;
    123. Deverá ser capaz de identificar o equipamento, rede a que pertence ou que está autenticado e ser capaz de aplicar o QoS definido para ele de forma automatica. Sendo desta forma capaz de associar automaticamente a interface níveis de QoS de voz e video pré-definidos;
    124. O Switch deve possuir facilidade auto-configuração das políticas de qualidade de serviço através de todas as interfaces e chassis, permitindo a criação de políticas consistentes na rede com apenas comando.
    125. Deve possuir processo de auto-configuração de todos os parâmetros do switch sem necessidade de acesso à interface de gerênciamento. Uma vez conectado à rede o switch deve reconhecer seu arquivo de configuração e se auto-configurar, bem como a imagem ou firmware deste modelo de switch que seja homologado para esta rede e efetuar o upgrade sem necessidade de intervencão. Para tanto o switch não deve conter configuração nenhuma previamente aplicada.
    126. O Switch deve ser capaz de implementar funcionalidades para  visualização de consumo, gerenciamento remoto e local e como resultado economia de energia, desabilitando interfaces em horários pré-determinados que estejam alimentando equipamentos
    127. Deve suportar “Unidirectional Link Detection Protocol” (UDLD) para detectar problemas de conexão ou problemas em um cabo de fibra óptica, desativando as portas do switch.
    128. Deve implementar TDR ( Time Domain Reflectomenter ) para detectar, caracterizar e localizar falhas nos cabos metálicos tanto nas interfaces 10/100 como nas interfaces de proposito duplo.
    129. Deve obrigatoriamente implementar PoE (Power Over Ethernet).
26. SWITCH DE ACESSO – TIPO II
    1. Switch de acesso com 24 portas 10/100 Mbps UTP, e 2 Interfaces com duplo proposito ou 10/100/1000 Mbps ou SFP.
    2. Arquitetura de Hardware: Montável em rack 19’’ incluindo todos os acessórios necessários.
    3. Fonte de alimentação
    4. Deve possuir fonte de alimentação AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz).
    5. Deve possuir cabo de alimentação para a fonte com, no mínimo, 1,00m (um metro) de comprimento.
    6. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
    7. Deve ser do mesmo fabricante dos outros switches e módulos contantes neste decritivo.
    8. Desempenho de Hardware:
    9. Deve possuir capacidade para pelo menos 8.000 endereços MAC na tabela de comutação.
    10. Deve implementar , no mínimo, 255 vlans simultaneamente.
    11. Deve possuir Switching bandwidth full-duplex de no mínimo 16 Gbps e taxa de encaminhamento de no mínimo 6,5 Mpps.
    12. Deve suportar Jumbo frames de no mínimo 9016 Bytes.
    13. Interfaces / Slots:
    14. Deve possuir, no mínimo, 2 slots 1000 Mbps do tipo SFP (módulos/transceiver) não inclusos, full-duplex, para fibras óticas ou UTP.
    15. Deve possuir, no mínimo, 24 portas Ethernet 10/100 com autosensing de velocidade e com conectores RJ-45.
    16. As interfaces 10/100 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX) e IEEE802.3x (Flow Control).
    17. Todas as portas Ethernet 10/100 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática.
    18. Todas as portas Ethernet 10/100 devem suportar auto configuração de crossover (Auto MDIX)
    19. Deve possuir LEDs para a indicação do status das portas e atividade, além de duplex.
    20. O switch ofertado deve possuir no mínimo 26 portas ativas divididas de acordo com items acima deste descritivo.
    21. Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.
    22. Deve possuir capacidade de associação das portas 10/100 ou das portas 1G, no mínimo, em grupo de até oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad. Deve poder formar no mínimo 6 grupos de portas.
    23. Deve possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.
    24. Gerenciamento: Deve implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.
    25. Deve implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    26. Sem autenticação e sem privacidade (noAuthNoPriv);
    27. Com autenticação e sem privacidade (authNoPriv);
    28. Com autenticação e com privacidade (authPriv).
    29. Possuir criptografia 3DES e AES para proteção dos dados de gerência SNMPv3.
    30. Deve possuir suporte a MIB II, conforme RFC 1213.
    31. Deve implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.
    32. Deve possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.
    33. Deve possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.
    34. Deve possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.
    35. Deve possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.
    36. Deve permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.
    37. Deve implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757;
    38. Deve implementar os protocolos LLDP (IEEE 802.1AB);
    39. Deve implementar Telnet para acesso à interface de linha de comando.
    40. Deve permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial;
    41. Deve ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface ), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;
    42. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;
    43. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP);
    44. Deve suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;
    45. Deve permitir que a sua configuração seja feita através de terminal assíncrono;
    46. Deve permitir a gravação de log externo (syslog) e deve permitir a visualização também internamente;
    47. Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
    48. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;
    49. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA);
    50. Devem ser suportadas no mínimo as seguintes operações de teste:
    51. ICMP echo;
    52. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique);
    53. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
    54. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
    55. Facilidades: Deve implementar VLANs por porta.
    56. Deve implementar VLANs compatíveis com o padrão IEEE 802.1q;
    57. Deve implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
    58. Deve permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch;
    59. Deve ser possível definir o sentido do tráfego a ser espelhado:
    60. Somente tráfego de entrada.
    61. Somente tráfego de saída
    62. Ambos simultaneamente.
    63. Deve permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
    64. Deve implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
    65. Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
    66. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.
    67. Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
    68. Protocolos: Deve implementar o protocolo NTPv4 (Network Time Protocol, versão 4). Deve ser suportada autenticação e criptografia entre os peers NTP, conforme definições da RFC 5905.
    69. Deve implementar DHCP Server em múltiplas VLANS.
    70. Deve implementar DHCP Option 82.
    71. Segurança: Deve implementar filtragem de pacotes (ACL - Access Control List);
    72. Deve permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
    73. Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, baseadas em tempo.
    74. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;
    75. Deve proteger a interface de comando do equipamento através de senha;
    76. Deve implementar o protocolo SSH V2 para acesso à interface de linha de comando;
    77. Deve possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido;
    78. Deve permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;
    79. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
    80. Deve possuir controle de broadcast, multicast e unicast por porta;
    81. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
    82. Deve permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede;
    83. Deve possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;
    84. Deve possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units ) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w);
    85. Deve possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;
    86. Deve possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP, essa filtragem deve ser por porta.
    87. Padrões: Deve implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
    88. Deve implementar padrão IEEE 802.1q (Vlan Frame Tagging);
    89. Deve implementar padrão IEEE 802.1p (Class of Service) para cada porta;
    90. Deve implementar padrão IEEE 802.3ad;
    91. Deve implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);
    92. Deve implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 64 instâncias simultâneas do protocolo Spanning-Tree;
    93. Deve implementar PVST ou PVST+;
    94. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);
    95. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto 802.1x;
    96. Deve implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Deve ser atendido, no mínimo, o seguinte requisito: Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:
    97. A estação não tem cliente 802.1x (suplicante);
    98. As credenciais do usuário não estão corretas (falha de autenticação).
    99. Deve implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).
    100. Deve implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:
    101. Nome do usuário;
    102. Switch em que o computador do usuário está conectado;
    103. Porta do switch utilizada por acesso;
    104. Endereço MAC da máquina utilizada pelo usuário;
    105. Endereço IP do usuário;
    106. Horários de início e término da conexão;
    107. Bytes transmitidos e recebidos durante a conexão.
    108. Deve suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
    109. Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS.
    110. Deve implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
    111. Multicast: Deve implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego MULTICAST seja tratado como broadcast no switch.
    112. Deve implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego MULTICAST IPv6 seja tratado como broadcast no switch.
    113. Qualidade de serviço (QoS);
    114. Deve possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
    115. Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
    116. Deve permitir Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
    117. Deve permitir Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
    118. Deve suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
    119. Deve ser possível a especificação de banda por classe de serviço.
    120. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
    121. Deve suportar diferenciação de QoS por VLAN.
    122. Deve oferecer suporte aos mecanismos de QoS WRR (Weighted Round Robin) e WRED (Weighted Random Early Detection).
    123. Deve implementar pelo menos quatro filas de prioridade por porta de saída (egress port).
    124. Deve implementar pelo menos duas filas de prioridade de entrada.
    125. Internet Protocol versão 6 (IPv6);
    126. Deve implementar IPv6.
    127. Deve permitir a configuração de endereços IPv6 para gerenciamento.
    128. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6.
    129. Deve implementar ICMPv6 com as seguintes funcionalidades:
    130. ICMP request;
    131. ICMP Reply;
    132. ICMP Neighbor Discovery Protocol (NDP);
    133. ICMP MTU Discovery.
    134. Deve implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SCP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
    135. Deve implementar NTPv4 com suporte a IPv6;
    136. Deve implementar IPv6 MLD snooping v1 e v2 ;
    137. Deve implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
    138. Especificações Técnicas do Nível Switch de Acesso – Funcionalidades para Gerenciamento Complementar;
    139. Deverá ter suporte a instalações do tipo "plug-and-play" para facilitar a troca de switches.
    140. Deverá ter suporte a configurações rápidas e trocas de switches sem necessidade de configuração local. Configurações deverão ser através de um único ponto de gerenciamento;
    141. Deverá ter suporte a funcionalidade de resolução de problemas que efetua testes em buscas de problemas apresentando diagnósticos para o administrador;
    142. O switch deve ter a capacidade de identificar, ao menos, pelos seguintes mecanismos MAC, OUI, LLDP, MAB e 8021.X os equipamentos diretamente conectados à qualquer interface. Ao identificar este equipamento deve ser capaz de configurar automaticamente a interface a que este equipamento estiver conectada, aplicando desde descrição da porta até as políticas de segurança e qualidade de serviço da mesma;
    143. Deverá ser capaz de identificar o equipamento, rede a que pertence ou que está autenticado e ser capaz de aplicar o QoS definido para ele de forma automatica. Sendo desta forma capaz de associar automaticamente a interface níveis de QoS de voz e video pré-definidos;
    144. O Switch deve possuir facilidade auto-configuração das políticas de qualidade de serviço através de todas as interfaces e chassis, permitindo a criação de políticas consistentes na rede com apenas comando.
    145. Deve possuir processo de auto-configuração de todos os parâmetros do switch sem necessidade de acesso à interface de gerênciamento. Uma vez conectado à rede o switch deve reconhecer seu arquivo de configuração e se auto-configurar, bem como a imagem ou firmware deste modelo de switch que seja homologado para esta rede e efetuar o upgrade sem necessidade de intervencão. Para tanto o switch não deve conter configuração nenhuma previamente aplicada.
    146. O Switch deve ser capaz de implementar funcionalidades para  visualização de consumo, gerenciamento remoto e local e como resultado economia de energia, desabilitando interfaces em horários pré-determinados que estejam alimentando equipamentos
    147. Deve suportar “Unidirectional Link Detection Protocol” (UDLD) para detectar problemas de conexão ou problemas em um cabo de fibra óptica, desativando as portas do switch.
    148. Deve implementar TDR ( Time Domain Reflectomenter ) para detectar, caracterizar e localizar falhas nos cabos metálicos tanto nas interfaces 10/100 como nas interfaces de proposito duplo.

**ANEXO III –PLANILHA DE QUANTITATIVOS MINIMOS / MODELO DE PROPOSTA**

Para todos os itens da planilha quantitativa abaixo, a ser apresentada na proposta comercial, deverão ser informados marca/modelo.

Planilha a seguir contém o quantitativo mínimo de fornecimento para o projeto, caberá a contratada fornecer inclusive eventuais materiais omissos para a completa solução.







Condições de pagamento:

Validade da proposta: 60 (sessenta) dias

Informar dados bancários:

Informar prazo de garantia dos Equipamentos:

Informar prazo de garantia dos serviços:

Informar código finame para os itens (23,24,37,,41,42,43,44,45,46)

**ANEXO IV**

**Cronograma Físico Financeiro**

Esse anexo descreve o percentual de desembolso máximo por período.

Objeto: Contratação de empresa técnica especializada para prestação de serviços de implantação de conectividade digital do Município de Bragança Paulista (rede de comunicação óptica), com fornecimento de materiais e equipamentos, necessários para implementação desta solução com suporte técnico remoto e on site pelo período de 12 meses

Cronograma e percentual de desembolso



**ANEXO V**

**Concepção Geral da Infovia**

Esse anexo descreve a concepção geral do projeto de conectividade digital (Infovia) da Prefeitura Municipal de Bragança Paulista.

1. Objeto: Contratação de empresa para prestação de serviços de implantação de conectividade digital do Município de Bragança Paulista (rede de comunicação óptica), com fornecimento de materiais e equipamentos, necessários para implementação desta solução com suporte técnico remoto e on site pelo período de 12 meses.
2. O projeto consiste na interligação por meio de backbone de fibra óptica de unidades públicas descentralizadas, à rede de dados da Prefeitura com tecnologia GPON e criação de 13 pontos de acesso wi-fi Hot Spot
3. Com o objetivo de cobertura e atendimento de cada vez mais serviços com maior velocidade e alta disponibilidade, se faz necessário a implantação de uma rede MAN para unidades da Prefeitura, formada por 1 (um) Anel Óptico redundante que prepara a rede para conexão de todos os próprios da Prefeitura com rotas e pontos de presença posicionados de forma estratégica para facilitar estas e futuras interligações.
4. A arquitetura do anel óptico com solução Gigabit Ethernet e fibra monomodo ponto-a-ponto para atendimento de diversas unidades possibilita a criação de uma rede multisserviços que pode suprir as necessidades de conexão de forma integrada e possibilitar a rápida oferta de serviços de Dados, Voz, Imagem, Segurança Eletrônica, Controle de Trânsito, Controles Ambientais entre outros serviços típicos.
5. Lista e **endereços** das unidades que serão interligadas:

A ser fornecida pela Prefeitura no momento da publicação do edital.

* 1. A contratada deverá prover a interligação via fibra óptica dos pontos de acesso a rede municipal da Prefeitura, sendo de responsabilidade do município prover o link de acesso saída a internet.
  2. A contratada será responsável pela instalação dos pontos de acesso, que serão fixados nos poste metálicos descritos no Anexo II Requisitos Minimos.
  3. A contratada será responsável pela configuração dos pontos de acesso com intuito de prover a conectividade aos munícipes e turistas.

1. **Descrição** Anel Óptico:
   1. Os serviços compreenderão a implantação do Anel óptico principal com velocidade de transmissão de 10 Gigabit Ethernet, estando preparado para futuras ampliações na rede, assim como implantação das derivações para todas as unidades, criação dos POP`s (Ponto de Presença e Interconexão da Rede), criação de caixas de emenda óptica e toda a infraestrutura necessária para a completa instalação do sistema.
   2. Anel óptico: O backbone principal da interligação óptica da Prefeitura será composto por 01 anel óptico resiliente com performance 10 Gbps, sendo denominado “Principal” em cabos ópticos autossustentáveis de 12FO monomodo (9/125µm).
   3. O anel principal contemplará uma rota mais abrangente facilitando as futuras interligações com as unidades da Prefeitura. Nestas interligações serão alocados em pontos estratégicos os POPs conforme Anexo I, que possuíram switches na camada de distribuição e conexão com o Anel (Camada de Núcleo).
   4. Para conexão entre as camadas de distribuição e de acesso, serão instalados switches Gigabit Ethernet, conforme Anexo II.
   5. A conexão das unidades ao anel óptico será através da rede GPON, com enlaces de até 1Gbps interligando os switches de acesso aos POPs.
   6. Os switches a serem fornecidos e instalados para compor o anel (Data Center e POPs) serão gerenciáveis com 48 portas Gigabit Ethernet 10/100/1000Base-T para conexão dos segmentos do anel. Serão realizadas todas as configurações de otimização de trafego, VLAN, gerenciamento e segurança de rede.
   7. Todos os cabos ópticos serão lançados de modo aéreo através dos postes existentes da Concessionária de Energia. Será efetuada a instalação de todos os acessórios de fixação (alças, suportes, isoladores) na faixa de comunicação dos postes para ancoragens das novas fibras.
   8. A negociação quanto à aprovação por parte da Concessionária de Energia Elétrica para utilização desta infraestrutura será de responsabilidade da Prefeitura Municipal de Ubatuba. Deverá estar previsto no presente escopo, a elaboração do projeto de ocupação a ser apresentado para a concessionária, conforme detalhado na Especificação Técnica - plano de instalação.
   9. Os cabos ópticos serão terminados em DIO´s em ambas as extremidades, através de fusões em extensões conectorizadas e testadas em fábrica.
   10. Serão instaladas ainda em pontos estratégicos para derivações, caixas de emenda aéreas que suportarão as saídas dos cabos de acesso para as unidades.
2. Descrição rede de acesso:
   1. A rede de acesso que atenderá as derivações/ramais será instalada utilizando tecnologia Gigabit Ethernet 1000-LX.
   2. Este escopo contempla a interligação inicial de 45 unidades e 11 pontos de acesso Wi-Fi Hot Spot, através de cabos de fibra óptica 06FO monomodo. Os cabos partirão das caixas de derivação no anel de 12FO até os racks de cada unidade onde serão terminados em mini DIO`s por meio de fusão em extensões conectorizadas e testadas em fábrica.
   3. Nas unidades de borda será instalado um switch de acesso com 24 portas fast ethernet 10/100Base-TX.
   4. Infraestrutura: Todos os cabos ópticos serão lançados de modo aéreo dos postes existentes da concessionária de energia. Será efetuada a instalação de todos os acessórios de fixação (alças, suportes, isoladores) na faixa de comunicação dos postes para ancoragens das novas fibras.
   5. Será submetido à aprovação por parte da concessionária de energia o projeto executivo de instalação das novas fibras detalhando a ocupação dos postes, memoriais de cálculo de esforços, memoriais descritivo e diagrama de ligações das fibras, pontos de conexão e emendas.
   6. Estão contempladas ainda as instalações de infraestrutura de tubulações necessárias para entrada dos cabos nos POPs e unidades de borda.
   7. O cabo óptico será lançado em postes da Concessionária de Energia até a entrada de cada prédio onde será encaminhado até a fachada de modo aéreo e por infraestrutura a ser construída até o Mini-Dio no rack. Para os postes haverá o fornecimento de uma abraçadeira ajustável e uma armação press bow com 1 isolador.
   8. Na entrada do cabo na unidade o cabo ótico deverá ser lançado até o poste mais próximo de onde será encaminhado até a fachada de cada localidade que terá uma armação press bow com 1 isolador para a fixação do cabo de aço.
   9. O cabo óptico monomodo será lançado no percurso com fibras autossustentável de 3 pares (6 fibras) para as derivações e de 06 pares (12 fibras) para o anel óptico principal. Os cabos (cada lance) terão uma identificação única e através de plaquetas de identificação que serão fixadas em cada poste, caixas de passagem e rack`s em todo o seu percurso.
   10. Nas unidades de borda a fibra óptica será terminada em Mini-DIO`s a serem fornecidos e instalados nos Rack em cada unidade. Dentro dos Mini-DIO`s o cabo será desencapado e feita as fusões e conectorizações com os conectores SC.