TERMO DE REFERÊNCIA – TR
REDE METROPOLITANA

1. DO OBJETIVO

1.1. A Prefeitura Municipal de Balneário Camboriú tem como objetivo a **contratação de empresa especializada para substituir os serviços atualmente prestados no âmbito do Contrato nº 233/2019**, referentes à operação da **Rede Metropolitana de Dados**, responsável por integrar e interligar todas as unidades administrativas do município em uma infraestrutura única de comunicação.

1.2. A empresa contratada será responsável por **implantar, operar, manter e evoluir uma nova infraestrutura de Rede Metropolitana**, com abrangência lógica e física, que atenda às necessidades atuais e futuras do Município, incluindo:

1.2.1. Transporte de dados entre unidades públicas, com alta disponibilidade e desempenho;

1.2.2. Instalação, configuração e manutenção de ativos de rede;

1.2.3. Suporte técnico especializado, com destaque para o **Suporte Nível 2 das redes internas legadas da Prefeitura**, promovendo interoperabilidade com a nova rede metropolitana;

1.2.4. Implementação, operação e manutenção da **rede Wi-Fi pública (WiFi-BC)**;

1.2.5. Monitoramento contínuo e proativo da infraestrutura e dos ativos;

1.2.6. Atuação integrada em uma **Central de Operações (NOC)**, com capacidade de resposta e controle compatível com funções de **Centro de Operações de Segurança (SOC)**, a partir do uso dos recursos avançados dos firewalls definidos no projeto;

1.2.7. Garantia de **interoperabilidade entre a rede interna e a Rede Metropolitana**, promovendo maior eficiência na prestação dos serviços públicos.

1.3. Todos os serviços deverão ser executados conforme os padrões de qualidade, disponibilidade e segurança previstos nas **boas práticas de governança de TI e segurança da informação**, conforme os frameworks ITIL, ISO/IEC 27001 e ISO/IEC 20000, e em conformidade com os requisitos técnicos estabelecidos neste Termo de Referência e seus anexos.

1.4. O contrato terá vigência de 60 (sessenta) meses, podendo ser prorrogado por igual período, mediante acordo entre as partes.

1.5. Requisitante:

1.5.1. Secretaria de Governo Inovação e Orçamento, através da Diretoria de Divisão de Tecnologia da Informação - DTI;

1.5.2. Demais unidades necessitantes deste certame.

2. DEFINIÇÃO DO OBJETO

2.1. A presente licitação tem por objeto a contratação de empresa especializada para substituir os serviços atualmente prestados no âmbito do Contrato nº 233/2019, por meio da implantação, operação, gestão e suporte técnico de uma nova Rede Metropolitana de Dados (MAN), que assegure a interligação de todas as unidades administrativas da Prefeitura de Balneário Camboriú, com infraestrutura moderna, segura e aderente às normas técnicas e de segurança da informação.

2.2. A empresa contratada será responsável por fornecer infraestrutura de fibra óptica, equipamentos de rede, serviços de transporte de dados (LAN/WAN), bem como pela instalação, configuração e manutenção de sistemas e ativos necessários à comunicação entre os pontos da rede.

2.3. O escopo inclui também a operação de uma rede pública de acesso à internet (WiFi-BC), a ser disponibilizada em áreas e pontos estratégicos definidos pela Administração, com controle de acesso, autenticação, rastreabilidade e segurança compatíveis com os padrões legais e normativos vigentes.

2.4. A CONTRATADA deverá prover ainda:

2.5. Suporte técnico especializado, incluindo Suporte Nível 2 para as redes internas legadas da Prefeitura, com foco em interoperabilidade com a nova Rede Metropolitana;

2.6. Monitoramento contínuo e proativo dos ativos e da performance da rede;

2.7. Implantação de uma Central de Operações (NOC) equipada com ferramentas de gestão de rede e com funções integradas de segurança;

2.8. Operação de recursos de firewall com atuação conjunta ao NOC, assumindo funções equivalentes às de um Centro de Operações de Segurança (SOC), com aplicação de políticas de segurança, análise de logs, resposta a incidentes e prevenção de ameaças;

2.9. Documentação técnica completa, versionada e auditável de todas as etapas da implantação e da operação;

2.9.1. A solução implantada deverá garantir **alta disponibilidade, baixa latência e segurança na transmissão de dados**, promovendo a **interoperabilidade entre a nova Rede Metropolitana e os sistemas já existentes na rede interna da Prefeitura**, de modo a **aumentar a eficiência operacional dos serviços públicos municipais**.

2.9.2. Todas as atividades deverão estar em conformidade com as **melhores práticas de governança de TI e segurança da informação**, com observância das normas e diretrizes dos frameworks **ITIL, ISO/IEC 27001, ISO/IEC 20000**, e demais legislações técnicas pertinentes.

2.10. LOCAL DE ENTREGA:

2.10.1. A contratada deverá realizar a entrega dos serviços/produtos no local indicado pela PREFEITURA MUNICIPAL DE BALNEÁRIO CAMBORIÚ-SC de acordo com a Autorização de Fornecimento.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. Performance e Eficiência Operacional

3.1.1. A implantação de uma rede metropolitana (MAN) baseada em fibra óptica, com enlaces redundantes e capacidade de 10 Gbps nas rotas críticas, é imprescindível para atender às demandas atuais de tráfego de dados. Somente com alta largura de banda garantida será possível suportar simultaneamente:

3.1.2. Sistemas de gestão escolar, que atendem aproximadamente 16000 alunos distribuídos em 44 unidades educacionais;

3.1.3. Plataforma de telemedicina e prontuário eletrônico que sustenta o Hospital Municipal Ruth Cardoso, unidades básicas de saúde, responsáveis por atendimentos médicos diários em todo o município;

3.1.4. Aplicações de segurança pública: transmissão em tempo real de câmeras de videomonitoramento, centros de despacho da Guarda Municipal e autoridade de trânsito;

3.1.5. Serviços online de arrecadação tributária e financeira e portal de atendimento ao cidadão.

3.2. Confiabilidade e Alta Disponibilidade

3.2.1. Diferentemente de soluções que dependem de links sobre a Internet pública, a MAN dedicada utiliza infraestrutura própria e topologia em anel com proteção automática (self-healing). Isso reduz drasticamente o risco de interrupções e garante SLA de disponibilidade acima de 99,9 %, minimizando o tempo de inatividade e assegurando continuidade ininterrupta dos serviços críticos à população.

3.3. Integração de Serviços e Telefonia Corporativa

3.3.1. A nova rede permitirá convergir voz e dados numa única plataforma IP (VoIP), substituindo centrais telefônicas legadas e reduzindo custos de chamadas. Além disso, viabiliza:

3.3.2. Integração de centrais de alarme e controle de acesso físico;

3.3.3. Conexão segura entre diferentes módulos de sistemas (educação, saúde, finanças, segurança), promovendo troca de informações em tempo real;

3.3.4. Adoção de serviços unificados de colaboração (videoconferência, chat interno, VPN para trabalho remoto).

3.4. Segurança da Informação e Conformidade

3.4.1. Com uma rede própria, será possível implementar em borda e núcleo:

3.4.2. Criptografia de ponta a ponta (IPsec/MPLS) em todos os túneis de transmissão;

3.4.3. Firewalls de próxima geração e sistemas de prevenção/detecção de intrusão (IDS/IPS);

3.4.4. Segmentação lógica por VLANs para isolar ambientes, garantindo integridade e confidencialidade de dados pessoais e administrativos, em conformidade com a LGPD e normas de segurança da informação.

3.5. Escalabilidade e Flexibilidade

3.5.1. A infraestrutura projetada admite expansão modular, sem necessidade de intervenções disruptivas. Novas unidades administrativas, escolas ou postos de saúde podem ser agregados ao backbone com simples ativação de portas ópticas, permitindo adequar-se rapidamente ao crescimento populacional e às futuras demandas por serviços digitais.

3.6. Otimização de Custos e Sustentabilidade

3.6.1. Embora o investimento inicial em fibra óptica e equipamentos de última geração seja relevante, a centralização da gestão em um único provedor especializado garante:

3.6.2. Redução de gastos com múltiplos contratos de link de internet e telefonia;

3.6.3. Economia de escala na manutenção (contrato único de SLA, suporte 24×7);

3.6.4. Vida útil estendida dos ativos, diminuindo trocas prematuras e o consumo de materiais, o que reforça o compromisso com práticas sustentáveis.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

4.1. A REDE METROPOLITANA visa fornecer serviços de comunicação de dados de forma convergente e redundante, utilizando o protocolo TCP/IP como base. Ela integrará, em um ambiente homogêneo de comunicação, as unidades que compõem a estrutura organizacional do Município de Balneário Camboriú, conforme listado no TERMO DE REFERÊNCIA. Além disso, a rede permitirá o gerenciamento centralizado dos recursos utilizados em sua configuração, incluindo os serviços de Centro de Operações de Rede (NOC), conforme destacado nos itens anteriores.

4.2. CONEXÃO REDUNDANTE

4.2.1. A REDE METROPOLITANA será responsável por estabelecer uma conexão redundante entre a Secretaria de Segurança, localizada na Marginal Oeste, Bairro dos Municípios, e a Divisão de Tecnologia da Informação, atuando como concentradores da rede. O anel óptico também incluirá as Secretarias da Saúde, Hospital Ruth Cardoso e Secretaria de Educação e a Central de Operações da Operadora.

4.3. TOPOLOGIA DE REDE

4.3.1. Essa conexão será implementada utilizando uma topologia em anel, que incluirá um ponto de presença da operadora estrategicamente localizado. A rede interconectará todas as unidades administrativas públicas municipais, hotspots, câmeras de segurança, dispositivos OCR, sensores, semáforos e outros dispositivos que demandem transporte de dados.

4.4. ARQUITETURA

4.4.1. A topologia em anel proporcionará uma arquitetura robusta e altamente confiável, garantindo redundância e continuidade operacional em caso de falha em qualquer ponto da rede. A utilização de tecnologias modernas de comutação e roteamento, juntamente com equipamentos de rede de alta qualidade, permitirá uma conectividade eficiente e estável entre todas as unidades administrativas e dispositivos distribuídos pelo município.

4.5. CONEXÃO REDUNDANTE

4.5.1. A implementação de uma conexão redundante entre o Ponto de Operação do Fornecedor e a Secretaria Municipal de Segurança reforçará a importância da disponibilidade e continuidade dos serviços essenciais, especialmente em áreas críticas como segurança pública e sistemas de saúde pública. A configuração proposta é tecnicamente viável e adequada para atender às necessidades de conectividade e redundância do Município de Balneário Camboriú.

4.6. DESIGNAÇÃO DA OPERADORA

4.6.1. Neste contexto, a empresa contratada para a prestação dos serviços mencionados será designada como OPERADORA.

4.7. OBJETIVOS DA REDE METROPOLITANA

4.7.1. A REDE METROPOLITANA visa fornecer serviços de comunicação de dados de forma convergente e redundante, utilizando o protocolo TCP/IP como base. Ela integrará, em um ambiente homogêneo de comunicação, as unidades que compõem a estrutura organizacional do Município de Balneário Camboriú, conforme listado no TERMO DE REFERÊNCIA. Além disso, a rede permitirá o gerenciamento centralizado dos recursos

utilizados em sua configuração, incluindo os serviços de Centro de Operações de Rede NOC), conforme destacado nos itens anteriores.

4.8. **NÓ (NODE) DA REDE METROPOLITANA**

4.8.1. Os NÓS (NODES) referem-se a unidades como Sedes de Secretarias, Postos de Saúde, Escolas, Núcleos de Educação, entre outros, ou a Pontos de Presença, como Câmeras, Sensores, Dispositivos de OCR, Hotspots, Semáforos, Radares, interconectados à REDE METROPOLITANA, conforme detalhado neste TERMO DE REFERÊNCIA. Em cada NÓ (NODE) da rede, sito os NÓS da DISTRIBUIÇÃO, é obrigatória a implementação de um Ponto de Acesso Público à Internet para uso dos cidadãos, com capacidade para pelo menos 1024 pessoas conectadas simultaneamente em ambientes internos, conforme especificações.

4.9. **CLASSIFICAÇÃO DO NÓ (NODE)**

4.9.1. Os NÓS (NODES) da REDE METROPOLITANA serão classificados de acordo com sua importância e criticidade no caso de interrupção do fornecimento de serviços de interconexão para o MUNICÍPIO, além da quantidade de equipamentos e dispositivos mantidos.

4.10. **QUANTIDADE E LOCALIZAÇÃO DOS NÓS (NODES):** A REDE METROPOLITANA será inicialmente composta por um total de 313 Nodes, conforme especificados no TERMO DE REFERÊNCIA, divididos, tipificados e classificados da seguinte forma:

Item	Descrição	Class	Conexão	SLA	Qtd
1	NÓS: NODES CORE (gateways) da rede serão equipados com conexões de fibra óptica redundantes, provenientes de rotas físicas distintas, formando um anel óptico bidirecional. Esses NÓS (NODE) deverão possuir sistemas de firewall em alta disponibilidade, configurados em um cluster ativo/passivo, e devem ser interconectados para garantir a máxima segurança e continuidade do serviço.	Criticidade 0	LAN-to-LAN	≥ 99, 5 %	2
2	NÓS: NODES ANEL que devem possuir redundância através de rotas físicas distintas e fazer parte do anel óptico bidirecional da rede, garantindo a continuidade e disponibilidade do serviço. Esses NÓS (NODES), que geralmente fornecem serviços aos munícipes e têm alta demanda de acesso a dados.	Criticidade 1	LAN-to-LAN	≥ 98, 5 %	4
3	NÓS: NODES DISTRIBUIÇÃO que interconectarão as demais unidades da Rede Metropolitana. Estes NÓS (NODES) são essenciais para a comunicação eficiente entre todas as unidades da Rede Metropolitana, assegurando a continuidade e a qualidade dos serviços prestados.	Criticidade 2	GPON	≥ 98 %	160

4	NÓS: NODES HOTSPOT EXTERNOS similares aos do DISTRIBUIÇÃO, mas que incluem a instalação e fornecimento de pontos de acesso para WiFi público à internet, possuirão gerenciamento especializado por software para garantir conformidade com a legislação. Esses NÓS (NODES) são equipados com dispositivos dimensionados e apropriados para atendimento externo (outdoor). Eles deverão possuir uma rota específica da rede com acesso à internet em link dedicado para o serviço.	Criticidade 3	GPON	≥ 98 %	37
5	NÓS: NODES DISPOSITIVOS IOT que interconectarão dispositivos diversos como câmeras de segurança, sensores, dispositivos de ocr, dispositivos de IoT e outros, que não possuam necessidade de conexões criptografada.	Criticidade 4	GPON	≥ 97 %	110
NODES SOBRE DEMANDA (Curta duração)					
Item	**Descrição**	**Class**	**Conexão**	**Implantação**	**Qtd**
6	NÓS: NODES EVENTOS que possuem as mesmas características dos **NÓS (NODES) Item 3**, mas que não têm um local definido para instalação, servem como reserva técnica para possíveis expansões. Esses NÓS (NODES) são mantidos em prontidão para garantir flexibilidade e suporte a futuras necessidades de crescimento da Rede Metropolitana.	Demanda	GPON	Até 5 dias uteis	50
7	NÓS: NODES HOTSPOT que possuem as mesmas características dos **NÓS (NODES) Item 4**, mas que não têm um local definido para instalação, servem como reserva técnica para possíveis expansões. Esses NÓS (NODES) são mantidos em prontidão para garantir flexibilidade e suporte a futuras necessidades de crescimento da Rede Metropolitana.	Demanda	GPON	Até 10 dias uteis	50
8	NÓS: NODES DISPOSITIVOS IOT que possuem as mesmas características dos **NÓS (NODES) Item 5**, mas que não têm um local definido para instalação, servem como reserva técnica para possíveis expansões. Esses NÓS (NODES) são mantidos em prontidão para garantir flexibilidade e suporte a futuras necessidades de crescimento da Rede Metropolitana.	Demanda	GPON	Até 15 dias úteis	100

4.10.1. A instalação dos NÓS (NODES) será realizada conforme a necessidade do **MUNICÍPIO**, não havendo garantia da instalação de todos os NÓS (NODE) descritos no projeto.

4.11. **ACESSO À INTERNET**

4.11.1. Os NÓS (NODES) participantes da REDE METROPOLITANA acessam a internet por meio da infraestrutura contratada pela prefeitura municipal, já instalada nos pontos concentradores.

4.12. **CONSIDERAÇÕES DA TOPOLOGIA E OPERAÇÃO DOS NÓ (NODE)**

4.12.1. Instalação de novos NÓS (NODES): Qualquer adição de novos pontos de conexão na rede NÓS (NODES) deverá ser formalizada mediante abertura de chamado técnico (ticket), contendo no mínimo as seguintes informações, endereço completo, telefone/ mensageiro instantâneo ex.: whatsapp de agente público designado e responsável pelo local, através de sistema de Helpdesk;

4.12.2. Mudanças de endereço: Se os pontos de conexão necessitarem ser realocados durante o contrato, a OPERADORA será responsável pela operação, cobrando o valor de instalação conforme a classificação do NÓ (NODE), neste caso também deverá ocorrer formalização via chamado técnico, indicando o novo endereço, telefone / mensageiro instantâneo ex.: whatsapp do responsável pelo novo local;

4.12.3. Procedimentos formais para solicitações: A entidade operadora deverá estabelecer procedimentos formais para tratar solicitações relacionadas à instalação, realocação ou remoção de pontos de conexão na rede;

4.12.4. **Descrição do Fluxo de Dados para o NÓ (NODE) do CORE Primário (Secretaria de Segurança):** A conexão à Internet deverá ser realizada por um roteador de borda que será diretamente conectado à Internet. Este roteador será responsável pelo roteamento externo e pela troca de rotas através do BGP. Em seguida, visando garantir a segurança da rede, deve ser interconectado um firewall que inspecionará todo o tráfego que entra e sai da Rede Metropolitana, aplicando políticas de segurança e estabelecendo conexões criptografadas. Após o firewall, um switch core deve ser interconectado para realizar a distribuição interna. Este switch core servirá como o backbone da rede interna, interligando todos os outros switches e formando uma topologia de anel para garantir redundância e resiliência. Posteriormente, uma OLT (Optical Line Terminal) deve ser interconectada ao switch core para permitir a comunicação com toda a estrutura da rede GPON;

4.12.5. **Implementação de um Segundo NÓ (NODE) CORE Secundário (Divisão de Tecnologia da Informação):** Um segundo NÓ (NODE) do CORE, denominado Secundário, deverá ser implementado junto a Divisão de Tecnologia da Informação. A principal função deste NÓ (NODE) será proporcionar redundância e resiliência à rede, além de oferecer uma segunda conexão de saída para a Internet. Este NÓ (NODE) secundário também deve seguir a mesma estrutura básica de interconexão de dispositivos para garantir a continuidade do serviço em caso de falhas no NÓ (NODE) primário;

4.12.6. **Topologia, Tecnologia e Velocidade dos Nós (Nodes) CORE**: Os nós da categoria CORE deverão operar com uma velocidade mínima de 10 Gbps e ser implementados em uma topologia de anel bidirecional, que garante resiliência e continuidade de serviço em caso de falhas de enlace. Os nós devem estar interconectados a essa velocidade, proporcionando alta disponibilidade, desempenho elevado e redundância. Além disso, os pontos concentradores destinados à Divisão de Tecnologia da Informação e à Secretaria de Segurança deverão ser integrados, assegurando que a rede suporte de forma eficiente o volume de tráfego de dados e mantenha a integridade e continuidade dos serviços essenciais para ambas as áreas;

4.12.7. **Topologia, Tecnologia e Velocidade dos Nós (Nodes) para Distribuição, Hotspot e Dispositivos IoT:** A infraestrutura de rede deverá garantir uma velocidade mínima de 1 Gbps para cada nó de distribuição, pontos de acesso (hotspots) e dispositivos IoT. Para isso, a tecnologia GPON (Gigabit Passive Optical Network) será utilizada com uma topologia ponto-multiponto, que permite a distribuição eficiente do sinal de uma única fibra óptica para múltiplos terminais. Os nós da rede deverão estar interconectados em uma estrutura que assegure alta disponibilidade, baixa latência e desempenho estável. A topologia ponto-multiponto será configurada para otimizar o uso de divisores ópticos passivos, distribuindo o tráfego de dados de maneira uniforme e suportando a conectividade dos dispositivos finais com redundância e resiliência a falhas. As instalações ocorrerão conforme cronogramas acordados entre o município e entidade operadora.

4.13. **TECNOLOGIAS**

4.13.1. MEIOS DE COMUNICAÇÃO

4.13.1.1. O acesso dos NÓS (NODE) à REDE METROPOLITANA deverá ser feito exclusivamente por meio de Fibra óptica, respeitando às bandas mínimas garantidas para cada NÓ (NODE), sendo o OPERADOR responsável por sua completa operação, gerenciamento e manutenção.

4.14. **ENDEREÇAMENTO IP**

4.14.1. PRIORIDADE DE TRÁFEGO

4.14.1.1. Seguir o padrão IEEE 802.1Q e o conceito de Quality of Service (QoS), a priorização de tráfego na rede deverá ser configurada da seguinte forma:

4.14.1.1.1. Prioridade 0: ZONA DE ISOLAMENTO;

4.14.1.1.2. Prioridade 1: HOTSPOT;

4.14.1.1.3. Prioridade 2: DISPOSITIVOS DE USUÁRIO FINAL;

4.14.1.1.4. Prioridade 3: SERVIDORES PREFEITURA;

4.14.1.1.5. Prioridade 4: VÍDEO;

4.14.1.1.6. Prioridade 5: VOIP;

4.14.1.1.7. Prioridade 6: DISPOSITIVOS DE REDE;

4.14.1.1.8. Prioridade 7: GERENCIAMENTO;

4.15. **SUBDIVISÃO DE ENDEREÇAMENTO IP SUGERIDA**

4.15.1. Zona de Isolamento (192.168.128.0/20): Destinada a dispositivos que entram na rede pela primeira vez e obtêm um IP via DHCP. Esses dispositivos permanecem isolados e recebem acesso restrito até serem registrados e movidos para a rede apropriada;

4.15.2. Dispositivos de Usuário Final (192.168.144.0/18): Bloco grande para desktops, laptops e outros dispositivos de usuário final, garantindo ampla capacidade de endereçamento;

4.15.3. Servidores Prefeitura (192.168.192.0/20): Bloco para servidores da prefeitura, incluindo servidores de aplicação, banco de dados e outros serviços críticos;

4.15.4. Vídeo (192.168.208.0/20): Bloco para sistemas de videoconferência e câmeras de segurança, assegurando largura de banda suficiente e gerenciamento de tráfego;

4.15.5. VOIP (192.168.224.0/20): Bloco para dispositivos e servidores de telefonia IP, garantindo qualidade de serviço e comunicação eficiente;

4.15.6. Dispositivos de Rede da Prefeitura (192.168.240.0/20): Bloco destinado a switches e roteadores de borda, pontos de acesso Wi-Fi e outros dispositivos de rede interna da prefeitura;

4.15.7. Dispositivos de Rede da Operadora (10.168.0.0/20): Bloco destinado a dispositivos como switches e roteadores de núcleo e distribuição, equipamentos de redes ópticas passivas, firewalls e serviços de rede;

4.15.8. Gerenciamento (10.168.16.0/20): Bloco destinado a sistemas de gerenciamento e monitoramento de rede, garantindo acesso seguro e administração centralizada;

4.15.9. Hotspot (10.128.0.0/14): O serviço de Wi-Fi gratuito para os cidadãos ficará fisicamente separado, utilizando um roteador dedicado exclusivamente para essa finalidade.

4.16. **DHCP E VLAN DINÂMICA**

4.16.1. Para reforçar a segurança, todos os dispositivos que se conectarem à rede devem ser inicialmente direcionados para a Zona de Isolamento, sem quaisquer acessos a rede ou a internet, onde ocorre a distribuição automática de IPs via DHCP. Se um dispositivo não for compatível com DHCP cliente, seu registro deve ser feito antecipadamente no servidor DHCP, permitindo o uso desse IP como estático. Este procedimento garante que apenas dispositivos autorizados acessem a rede, bloqueando aqueles que não estejam cadastrados no servidor DHCP ou que usem um IP fixo não registrado, prevenindo acessos não autorizados;

4.16.2. O servidor DHCP deve contar com uma função de autolimpeza, excluindo automaticamente o endereçamento de dispositivos que fiquem 30 dias sem contato. Após 90 dias de inatividade, o equipamento que voltar à rede receberá um IP da Zona de Isolamento e precisará ser cadastrado novamente.

4.16.3. A rede destinada a VÍDEO, VOIP e dispositivos da prefeitura deve utilizar a funcionalidade de VLAN dinâmica. Essa funcionalidade permite atribuir VLANs específicas aos hosts com base nos seis primeiros dígitos do endereço MAC (Organizationally Unique Identifier, OUI).

4.17. **EQUIPAMENTOS**

4.17.1. O OPERADOR deverá fornecer e instalar todos os equipamentos e materiais necessários à interligação de cada NÓ (NODE) à REDE METROPOLITANA, e todos os equipamentos necessários na REDE METROPOLITANA (pontos concentradores) para garantir o funcionamento, em conformidade com a sua classificação e que possibilite a utilização dos serviços contratados para cada NÓ (NODE);

4.17.2. Todos os equipamentos deverão ser novos, sem uso, reforma ou recondicionamento e que estejam em produção do fabricante na data da abertura edital;

4.17.3. Colocar à disposição do CONTRATANTE todos os meios necessários à comprovação da qualidade e operacionalidade dos equipamentos fornecidos, permitindo a verificação de sua conformidade com as especificações do TERMO DE REFERÊNCIA e seus anexos;

4.17.4. Nos pontos concentradores denominados PREFEITURA DE BALNEÁRIO CAMBORIÚ NÓ (NODE) CORE e SECRETEARIA MUNICIPAL DE SEGURANÇA NÓ (NODE) CORE, será necessário a instalação de rack de piso padrão 19”, tamanho 44U, dimensões externas (L x A x P) 600 x 2045 x 1070 mm, aderente a norma IEC 60297, contendo porta perfurada com fecho e chave, com abertura direita ou esquerda, em aço SAE 1008, espessura

estrutural de no mínimo 1, 9 mm e 1, 2 mm e fechamentos de 0,9 mm, parafusos Philips cabeça panela, suportar uma carga de no mínimo 1000 kg, pintura eletrostática epóxi pó micro texturizado em preto fosco, para ambiente indoor, com 4 aberturas superiores e abertura total inferior, abertura para sistema de ventilação no teto, estrutura com ponto para aterramento, moldura para passagem e fixação de cabos, fechamento lateral com venezianas e fecho para abertura, possuir kit de 4 rodízios em aço carbono na cor preto, 2 com freio e 2 sem freio, compatível ou da mesma fábrica do rack, possuir conjunto de 4 ventiladores compatíveis ou da mesma fábrica do rack com padrão 19", tamanho de 1U, tensão nominal entre 100 ~ 240 Vac, corrente máxima 10 A, com rotação entre 2600 e 3000 rpm, cabo de força com 3 metros de comprimento, possuir chave tipo disjuntor inteligente rearmável, sendo o material das hélices em plástico de engenharia PBT, e a estrutura em aço SAE 1008, com pintura eletrostática epóxi pó micro texturizado, ainda, deverá acompanhar dois protetores eletrônico PDU, padrão 19", tamanho de 1U, com corrente máxima de 10 A, com potência máxima de operação de 1270 W (127Vac) e 2200 W (220Vac), com frequência de 50 ou 60 Hz, plugue de entrada 2P + T (NBR 14136) 10 A e saída de 8 tomadas 2P + T (NBR 14136) 10 A, comprimento do cabo de 3 metros, grau de proteção IP 20, com chave tipo disjuntor rearmável com indicador luminoso de funcionamento, possuir proteção contra surtos de tensão como curto circuito e sobrecarga;

4.17.5. Em cada NÓ (NODE) ANEL será necessário a instalação de rack de piso desmontável padrão 19", tamanho 24U, dimensões externas (L x A x P) 600 x 1147 x 670 mm, aderente a norma IEC 60297, contendo porta de acrílico com fecho e chave, com abertura direita ou esquerda, em aço SAE 1008, espessura estrutural de no mínimo 1, 2 mm e fechamentos de 0, 9 mm, parafusos Philips cabeça panela, suportar uma carga de no mínimo 1000 kg, pintura eletrostática epóxi pó micro texturizado em preto fosco, para ambiente indoor com 3 aberturas superiores e 5 aberturas inferiores para cabos, abertura para sistema de ventilação no teto, estrutura com ponto para aterramento, moldura para passagem e fixação de cabos, fechamento lateral com venezianas e fecho para abertura, possuir kit de 4 rodízios em aço carbono na cor preto, 2 com freio e 2 sem freio, compatível ou da mesma fábrica do rack, possuir conjunto de 4 ventiladores compatíveis ou da mesma fábrica do rack com padrão 19", tamanho de 1U, tensão nominal entre 100 ~ 240 Vac, corrente máxima 10 A, com rotação entre 2600 e 3000 rpm, cabo de força com 3 metros de comprimento, possuir chave tipo disjuntor inteligente rearmável, sendo o material das hélices em plástico de engenharia PBT, e a estrutura em aço SAE 1008, com pintura eletrostática epóxi pó micro texturizado, ainda, deverá acompanhar um protetor eletrônico PDU, padrão 19", tamanho de 1U, com corrente máxima de 10 A, com potência máxima de operação de 1270 W (127Vac) e 2200 W (220Vac), com frequência de 50 ou 60 Hz, plugue de entrada 2P + T (NBR 14136) 10 A e saída de 8 tomadas 2P + T (NBR 14136) 10 A, comprimento do cabo de 3 metros, grau de proteção IP 20, com chave tipo disjuntor rearmável com indicador luminoso de funcionamento, possuir proteção contra surtos de tensão como curto circuito e sobrecarga;

4.17.6. Em cada NÓ (NODE) DISTRIBUIÇÃO será necessário a instalação de mini rack montado padrão 19", tamanho 5U, dimensões externas (L x A x P) 520 x 271, 4 x 370 mm, para

montagem em parede, aderente a norma IEC 60297, contendo porta com fecho e chave, com abertura frontal removível, em aço SAE 1008, espessura estrutural 0.75 mm, lateral com venezianas, suportar uma carga de no mínimo 50 kg, pintura eletrostática epóxi pó micro texturizado em preto fosco, para ambiente indoor, deverá acompanhar um protetor eletrônico PDU, padrão 19", tamanho de 1U, com corrente máxima de 10 A, com potência máxima de operação de 1270 W (127Vac) e 2200 W (220Vac), com frequência de 50 ou 60 Hz, plugue de entrada 2P + T (NBR 14136) 10 A e saída de 8 tomadas 2P + T (NBR 14136) 10 A, comprimento do cabo de 3 metros, grau de proteção IP 20, com chave tipo disjuntor rearmável com indicador luminoso de funcionamento, possuir proteção contra surtos de tensão como curto circuito e sobrecarga;

4.17.7. Os Equipamentos que farão parte dos pontos concentradores em topologia anel, sito, NÓS (NODE) CORE e NÓS (NODE) ANEL deverão ter em caso de falha no fornecimento de energia elétrica, autonomia mínima de 40 minutos;

4.17.8. Os Equipamentos que farão parte dos NÓS (NODE) DISTRIBUIÇÃO, 4, 5 deverão ter em caso de falha no fornecimento de energia elétrica, autonomia mínima de 25 minutos;

4.17.9. Portanto, abaixo está a descrição dos equipamentos com as características mínimas necessárias para assegurar autonomia e proteção contra surtos e oscilações na rede elétrica:

4.17.9.1. ESPECIFICAÇÃO NOBREAK DE NÓ (NODE) CORE:

4.17.9.1.1. Online rack/torre;

4.17.9.1.2. Deve possuir fator de potência de saída igual a 0, 9, com potência de pico de saída de no mínimo, 3.000 VA e 2.700 W, do tipo monofásico/monofásico;

4.17.9.1.3. Deve ter topologia dupla-conversão, possuindo estágios de retificação e conversor CCCA para o funcionamento principal, também chamado de funcionamento online, dupla conversão ou modo rede;

4.17.9.1.4. Para que haja compatibilidade com a tensão fornecida pela distribuidora da região, deve possuir tensão nominal na entrada de 220V, alterável para 230V ou 240V, e deve operar com frequência nominal de entrada de 60 Hz (definido como padrão pela ANEEL), suportando oscilações na faixa de frequência de entrada de 40/70 Hz, decorrentes do fornecimento de energia, sem que passe a operar no modo bateria.

4.17.9.1.5. Para atender a demanda dos equipamentos alimentados pela UPS, a tensão nominal de saída no modo dupla conversão deverá ser de 220 V padrão, ajustável para 230V e 240V, e deverá apresentar frequência nominal de saída de 60 Hz, com regulação de ±2%, e com faixa de frequência de saída em modo dupla conversão de ±0, 2 Hz;

4.17.9.1.6. A alimentação do nobreak deve ser via cabo com plugue conforme ABNT 14136, e para a saída de alimentação deve apresentar no mínimo 2 tomadas de 10A e 2 tomadas de 20ª conforme ABNT 14136;

4.17.9.1.7. Deve operar em modo dupla conversão em faixas de tensão de 110-290V quando com carga menor que 50%, e em faixas de tensão de 120-290V com cargas maiores que 50%;

4.17.9.1.8. Para um melhor aproveitamento da capacidade do equipamento, este deverá possuir correção de fator de potência de cargas;

4.17.9.1.9. Para a garantia de integridade dos equipamentos instalados na UPS, a distorção harmônica de corrente de entrada máxima permitida em carga máxima, THDi, deve ser de no máximo 4% em carga linear;

4.17.9.1.10. Deverá apresentar compatibilidade de operação com geradores;

4.17.9.1.11. A faixa de frequência do modo Bypass deve ser menor ou igual a ±10%;

4.17.9.1.12. Para garantir a segurança do sistema, deverá apresentar protetor contra surto na entrada (Disjuntor bipolar);

4.17.9.1.13. Deve possuir fator de crista para corrente de saída de 3:1;

4.17.9.1.14. A forma de onda na saída deve ser senoidal pura, não será aceito outro tipo de onda, como exemplo senoidal por aproximação, devido a compatibilidade dos dispositivos que serão alimentados pela UPS;

4.17.9.1.15. A distorção harmônica de tensão de saída deve ser ≤1 com carga linear, e ≤2 com carga não linear;

4.17.9.1.16. A UPS deverá apresentar as seguintes eficiências de saída: 94% em modo dupla conversão; 97% em modo Eco; 97% em modo Bypass;

4.17.9.1.17. Caso o equipamento não possua bateria interna, este deve ser fornecido juntamente com módulo de bateria externa, composto por baterias do tipo VRLA 12V/7Ah, com tensão de barramento de 192V. O equipamento deve também conter capacidade para expansão de no mínimo 4 módulos de bateria extra com engate rápido tipo SB-50;

4.17.9.1.18. Para garantir a integridade do equipamento, este deve possuir proteção nas baterias externas via disjuntor;

4.17.9.1.19. Deve possuir tensão de flutuação e tensão de profundidade de descarga (DOD) configurável;

4.17.9.1.20. Para possibilidade de manutenção e manuseio sem a interrupção de alimentação, a UPS deve possuir chave manual de Bypass, protegido por disjuntor, e tempo de transferência de 0ms;

4.17.9.1.21. Para não haver oscilação na alimentação dos equipamentos conectados a UPS, o tempo de transferência do modo dupla conversão para o modo bateria deve ser de 0ms, e do modo dupla conversão para o modo Bypass automático deve ser de 0ms;

4.17.9.1.22. Deve suportar proteção contra sobrecarga nas seguintes proporções: 100% a 105% tempo indefinido; 106% a 110% - 10 minutos; 111% a 125% - 1 minuto; 126% a 150% - 30 segundos;

4.17.9.1.23. Deverá possuir função Bypass interno automático, proporcionando energia contínua aos equipamentos conectados, mesmo se o nobreak sofrer falhas ou sobrecargas;

4.17.9.1.24. Deve possuir no mínimo 8 níveis de proteção, tais quais, contra sobrecarga nas tomadas de saída, contra curto-circuito nas tomadas de saída, contra variação da frequência da rede de entrada, contra surtos de tensão de entrada, contra sub e sobre tensão da rede elétrica, contra sobreaquecimento no inversor, bem como contra descarga total e sobrecarga da bateria;

4.17.9.1.25. Deve possuir gerenciamento local via cabo USB, RS232 e remoto via placa SNMP;

4.17.9.1.26. Deverá possuir display LCD luminoso que exibe informações do sistema e estado dos alarmes, e permite configuração do nobreak;

4.17.9.1.27. Deverá possuir função Modo Eco, permitindo que se configure o nobreak para trabalhar em modo economia de energia. A tensão da rede elétrica passará pelos filtros de linha e será disponibilizada na saída enquanto estiver dentro da faixa configurada;

4.17.9.1.28. O equipamento deve suportar paralelismo com outros nobreaks, suporte a até 4 equipamentos em paralelo, possibilitando redundância de alimentação ou também aumento da capacidade de carga;

4.17.9.1.29. A 1 metro do equipamento o ruído audível deve ser de <60 dB;

4.17.9.1.30. O equipamento deve ocupar no rack uma altura não superior a 2U, não considerando módulos de baterias externas e outros acessórios;

4.17.9.1.31. Possuir 2 módulos de baterias para uso em nobreaks, que deverá apresentar no mínimo as seguintes especificações técnicas cada:

4.17.9.1.32. Deve possuir no mínimo 12 baterias tipo estacionária, com tensão de 12 V cada e capacidade de 09 Ah, com tensão de barramento de no mínimo 72 V;

4.17.9.1.33. Deverá possuir, no mínimo dois conectores de engate rápido SB 50 (Anderson Power) para conectar o módulo de bateria ao nobreak, permitindo a expansão de autonomia deste;

4.17.9.1.34. Deve possuir fusível interno para garantir a segurança e integridade do equipamento;

4.17.9.1.35. Para melhor manutenção e armazenamento deve ser fabricado em material metálico com pintura epóxi pó micro texturizado;

4.17.9.1.36. Deve possuir altura não superior a 2U para instalação em rack;

4.17.9.1.37. Deve possuir placa SNMP para gerenciamento remoto de nobreaks, que deverá apresentar as seguintes especificações técnicas:

4.17.9.1.38. Deverá suportar o protocolo SNMP;

4.17.9.1.39. Deverá possuir Leds de sinalização;

4.17.9.1.40. Deve possuir conector de Slot tipo mini;

4.17.9.1.41. Deve permitir no mínimo, o monitoramento de eventos e da qualidade de energia da rede, desligamento programado e envio de notificações ao usuário;

4.17.9.1.42. Deve ser compatível com softwares de gerenciamento de placas SNMP.

4.17.9.2. ESPECIFICAÇÃO NOBREAK DE NÓ (NODE) ANEL:

4.17.9.2.1. Online rack/torre;

4.17.9.2.2. Deve possuir fator de potência de saída igual a 0, 9, com potência de pico de saída de no mínimo, 1.500 VA e 1.350 W, do tipo monofásico/monofásico;

4.17.9.2.3. Deve ter topologia dupla-conversão, possuindo estágios de retificação e conversor CCCA para o funcionamento principal, também chamado de funcionamento online, dupla conversão ou modo rede;

4.17.9.2.4. Para que haja compatibilidade com a tensão fornecida pela distribuidora da região, deve possuir tensão nominal na entrada de 220V, alterável para 230V ou 240V, e deve operar com frequência nominal de entrada de 60 Hz (definido como padrão pela

ANEEL), suportando oscilações na faixa de frequência de entrada de 40/70 Hz, decorrentes do fornecimento de energia, sem que passe a operar no modo bateria.

4.17.9.2.5. Para atender a demanda dos equipamentos alimentados pela UPS, a tensão nominal de saída no modo dupla conversão deverá ser de 220 V padrão, ajustável para 230V e 240V, e deverá apresentar frequência nominal de saída de 60 Hz, com regulação de ±2%, e com faixa de frequência de saída em modo dupla conversão de ±0, 2 Hz;

4.17.9.2.6. A alimentação do nobreak deve ser via cabo com plugue conforme ABNT 14136, e para a saída de alimentação deve apresentar no mínimo 6 tomadas de 10A conforme ABNT 14136;

4.17.9.2.7. Deve operar em modo dupla conversão em faixas de tensão de 110-290V quando com carga menor que 50%, e em faixas de tensão de 120-290V com cargas maiores que 50%;

4.17.9.2.8. Para um melhor aproveitamento da capacidade do equipamento, este deverá possuir correção de fator de potência de cargas;

4.17.9.2.9. Para a garantia de integridade dos equipamentos instalados na UPS, a distorção harmônica de corrente de entrada máxima permitida em carga máxima, THDi, deve ser de no máximo 4% em carga linear;

4.17.9.2.10. Deverá apresentar compatibilidade de operação com geradores;

4.17.9.2.11. A faixa de frequência do modo Bypass deve ser menor ou igual a ±10%;

4.17.9.2.12. Para garantir a segurança do sistema, deverá apresentar protetor contra surto na entrada (Disjuntor bipolar);

4.17.9.2.13. Deve possuir fator de crista para corrente de saída de 3:1;

4.17.9.2.14. A forma de onda na saída deve ser senoidal pura, não será aceito outro tipo de onda, como exemplo senoidal por aproximação, devido a compatibilidade dos dispositivos que serão alimentados pela UPS;

4.17.9.2.15. A distorção harmônica de tensão de saída deve ser ≤1 com carga linear, e ≤2 com carga não linear;

4.17.9.2.16. A UPS deverá apresentar as seguintes eficiências de saída: 94% em modo dupla conversão; 97% em modo Eco; 97% em modo Bypass;

4.17.9.2.17. Caso o equipamento não possua bateria interna, este deve ser fornecido juntamente com módulo de bateria externa, composto por baterias do tipo VRLA 12V/7Ah, com tensão de barramento de 192V. O equipamento deve também conter capacidade para expansão de no mínimo 4 módulos de bateria extra com engate rápido tipo SB-50;

4.17.9.2.18. Para garantir a integridade do equipamento, este deve possuir proteção nas baterias externas via disjuntor;

4.17.9.2.19. Deve possuir tensão de flutuação e tensão de profundidade de descarga (DOD) configurável;

4.17.9.2.20. Para possibilidade de manutenção e manuseio sem a interrupção de alimentação, a UPS deve possuir chave manual de Bypass, protegido por disjuntor, e tempo de transferência de 0ms;

4.17.9.2.21. Para não haver oscilação na alimentação dos equipamentos conectados a UPS, o tempo de transferência do modo dupla conversão para o modo bateria deve ser de 0ms, e do modo dupla conversão para o modo Bypass automático deve ser de 0ms;

4.17.9.2.22. Deve suportar proteção contra sobrecarga nas seguintes proporções: 100% a 105% tempo indefinido; 106% a 110% - 10 minutos; 111% a 125% - 1 minuto; 126% a 150% - 30 segundos;

4.17.9.2.23. Deverá possuir função Bypass interno automático, proporcionando energia contínua aos equipamentos conectados, mesmo se o nobreak sofrer falhas ou sobrecargas;

4.17.9.2.24. Deve possuir no mínimo 8 níveis de proteção, tais quais, contra sobrecarga nas tomadas de saída, contra curto-circuito nas tomadas de saída, contra variação da frequência da rede de entrada, contra surtos de tensão de entrada, contra sub e sobre tensão da rede elétrica, contra sobreaquecimento no inversor, bem como contra descarga total e sobrecarga da bateria;

4.17.9.2.25. Deve possuir gerenciamento local via cabo USB, RS232 e remoto via placa SNMP;

4.17.9.2.26. Deverá possuir display LCD luminoso que exibe informações do sistema e estado dos alarmes, e permite configuração do nobreak;

4.17.9.2.27. Deverá possuir função Modo Eco, permitindo que se configure o nobreak para trabalhar em modo economia de energia. A tensão da rede elétrica passará pelos filtros de linha e será disponibilizada na saída enquanto estiver dentro da faixa configurada;

4.17.9.2.28. O equipamento deve suportar paralelismo com outros nobreaks, suporte a até 4 equipamentos em paralelo, possibilitando redundância de alimentação ou também aumento da capacidade de carga;

4.17.9.2.29. A 1 metro do equipamento o ruído audível deve ser de <60 dB;

4.17.9.2.30. O equipamento deve ocupar no rack uma altura não superior a 2U, não considerando módulos de baterias externas e outros acessórios;

4.17.9.2.31. Deve possuir placa SNMP para gerenciamento remoto de nobreaks, que deverá apresentar as seguintes especificações técnicas:

4.17.9.2.32. Deverá suportar o protocolo SNMP;

4.17.9.2.33. Deverá possuir Leds de sinalização;

4.17.9.2.34. Deve possuir conector de Slot tipo mini;

4.17.9.2.35. Deve permitir no mínimo, o monitoramento de eventos e da qualidade de energia da rede, desligamento programado e envio de notificações ao usuário;

4.17.9.2.36. Deve ser compatível com softwares de gerenciamento de placas SNMP.

4.17.9.3. ESPECIFICAÇÃO NOBREAK DE NÓ (NODE) DISTRIBUIÇÃO, 4, 5:

4.17.9.3.1. Os Equipamentos que farão parte dos pontos concentradores NÓ (NODE) DISTRIBUIÇÃO, 4, 5 da REDE METROPOLITANA deverão ter autonomia mínima de 25 minutos em caso de falha no fornecimento de energia elétrica como segue:

4.17.9.3.2. Nobreak que deve oferecer proteção para equipamentos eletrônicos das oscilações da rede elétrica;

4.17.9.3.3. Deve possuir potência de pico de saída de, no mínimo, 600 VA e 300 W, com fator de potência de saída de, no mínimo, 0, 5, topologia do tipo interativo;

4.17.9.3.4. Deve possuir tensão nominal na entrada de 220V, com faixa de tensão de entrada no mínimo entre 176 a 264 V;

4.17.9.3.5. Deve operar com frequência de entrada de 60 Hz com variação de +/-3Hz;

4.17.9.3.6. Para proteção de entrada do equipamento, deve possuir fusível rearmável;

4.17.9.3.7. Para alimentação do equipamento deve possuir cabo de força de no mínimo 1m com plugue tripolar conforme NBR 14136;

4.17.9.3.8. Em modo bateria, deve apresentar forma de onda do tipo senoidal por aproximação (retangular PWM – controle de largura de pulso);

4.17.9.3.9. Deve possuir tensão nominal de saída, em modo rede, de 220V, com variação máxima de +/-10%;

4.17.9.3.10. Deve possuir tensão nominal na saída, em modo bateria, de 220 V, com variação máxima de 5% Em modo bateria deve apresentar frequência de 60 HZ e variação de +/-1Hz;

4.17.9.3.11. Deve possuir, no mínimo, uma bateria interna do tipo VRLA - chumbo-ácido selada regulada por válvulas, com tensão de 12 V e capacidade de 7 Ah, para prolongar a utilização dos equipamentos em caso de queda no fornecimento de energia elétrica;

4.17.9.3.12. Deve possuir no mínimo 9 níveis de proteção, como contra sobrecarga nas tomadas de saída, contra curto-circuito nas tomadas de saída, contra surto de tensão, contra blecaute, contra variação de frequência, contra sobreaquecimento no inversor, contra sub e sobre tensão da rede elétrica, bem como contra descarga total das baterias;

4.17.9.3.13. Deverá possuir no mínimo 4 tomadas de no mínimo 10 A, de acordo com norma NBR 14136;

4.17.9.3.14. Deve possuir no mínimo sinalização luminosa que indique status como curto-circuito ou sobrecarga na saída, modo bateria, carga de bateria e modo de rede;

4.17.9.3.15. Deve possuir no mínimo sinalização sonora indicando que entrou no modo de bateria, indicação de carga baixa, indicação de sobrecarga e curto-circuito.

4.17.9.3.16. Os equipamentos, ativos / passivos de rede, além dos materiais fornecidos para estabelecer a conectividade em cada NÓ (NODE), estarão sob a responsabilidade do OPERADOR até o final do contrato quando deverão ser transferidos como propriedade da Prefeitura Municipal;

4.17.9.3.17. Os equipamentos deverão ser rotulados, identificados e patrimoniados. O OPERADOR deverá manter um cadastro em seu sistema de gestão de chamados e inventário de todos os equipamentos ativos e passivos de rede em seus locais de instalação, proporcionando ao MUNICÍPIO total transparência, tendo acesso a qualquer tempo do parque de equipamentos instalados no projeto podendo realizar consultas, emitir relatórios e extrair histórico de suporte e manutenção de cada node;

4.17.9.3.18. O OPERADOR deverá fazer seguro contra roubo e acidentes provocados por qualquer natureza que permitam a rápida reposição de equipamentos sinistrados, respeitando a disponibilidade exigida de cada NÓ (NODE). A Contratada deverá fazer a reposição no prazo de 24 horas.

4.18. **ATIVOS DA REDE DE DADOS**

4.18.1. Os equipamentos da rede de dados devem obedecer às legislações e normas vigentes na ANATEL que disciplinam sua instalação e operação. Devem possuir certificações técnicas e, no caso de equipamentos de comunicação e transmissão/recepção de dados, devem ser homologados pela ANATEL e/ou outros órgãos competentes;

4.18.2. A prefeitura de Balneário Camboriú se transformou em um sistema autônomo, com sua própria numeração de IP, onde as empresas operadoras de internet irão somente propagar tais endereços, tanto a numeração (endereçamento) IPV4 como IPV6, e visando garantir a disponibilidade dos serviços e possuir contingência e redundância gerencial com o menor tempo de SLA possível, deverá ser utilizado os seguintes equipamentos:

4.18.3. SOLUÇÃO DE NGFW, RELATORIA E CENTRALIZAÇÃO DE LOGS, PROTEÇÃO APLICAÇÕES WEB

4.18.3.1. Throughput de Firewall de no mínimo 160Gbps, considerando pacotes UDP de 512 bytes;

4.18.3.2. Throughput de, no mínimo, 21 (vinte e um) Gbps com funcionalidades de firewall, IPS e controle de aplicação habilitadas;

4.18.3.3. Throughput de, no mínimo, 20 (vinte) Gbps com funcionalidades de firewall, IPS, controle de aplicação e antivírus habilitadas;

4.18.3.4. Throughput de, no mínimo, 54 (cinquenta e quatro) Gbps de VPN IPSec;

4.18.3.5. Estar licenciado para, ou suportar sem o uso de licença, 1.800 (mil e oitocentos) túneis de VPN IPSEC Site-to-Site simultâneos;

4.18.3.6. Estar licenciado para, ou suportar sem o uso de licença, 45.000 (quarenta e cinco mil) túneis de VPN IPSEC Client-to-Site simultâneos;

4.18.3.7. Suporte a, no mínimo, 700.000 novas sessões por segundo (TCP);

4.18.3.8. Suporte a, no mínimo, 15 milhões de sessões totais (TCP);

4.18.3.9. Suportar 9.000 (9 mil) políticas de firewall;

4.18.3.10. O fabricante ofertado deve estar posicionado no quadrante “Leader” do quadrante mágico do Gartner de 2022, na categoria Network Firewalls. Este item deverá ser comprovado através de documentação anexada juntamente à habilitação da proponente;

4.18.3.11. Suportar encaminhamento no mínimo 225 (duzentos e vinte e cinco) milhões de pacotes por segundo;

4.18.3.12. Suportar no mínimo 16 (dezesseis) Gbps de throughput de Inspeção SSL;

4.18.3.13. Possuir ao menos 1 interfaces de gerenciamento operando em Gigabit RJ45;

4.18.3.14. Deverá possuir no mínimo 16 interfaces RJ45 com suporte a operação em 1 Gigabit;

4.18.3.15. Deverá possuir no mínimo 6 interfaces 1 Gigabit SFP para uso com transceivers de fibra óptica;

4.18.3.16. Deverá possuir no mínimo 4 interfaces 10 Gigabit SFP+ para uso com transceivers de fibra óptica;

4.18.3.17. Deverá possuir no mínimo 4 interfaces 25 Gigabit SFP28 para uso com transceivers de fibra óptica;

4.18.3.18. Possuir porta console;

4.18.3.19. Deverá possuir controladora Wi-Fi integrada, permitindo gerenciar até 2048 Access Points do mesmo fabricante;

4.18.3.20. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

4.18.3.21. Os hardwares e os softwares que compõem a solução devem ser do mesmo fabricante;

4.18.3.22. As funcionalidades de NGFW devem ser ofertadas no mesmo appliance, não sendo permitido a composição de equipamentos separados para cada uma das funções;

4.18.3.23. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

4.18.3.24. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.18.3.25. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

4.18.3.26. Deverá suportar tags de VLAN (802.1Q);

4.18.3.27. Deverá possuir suporte a agregação de links via 802.3ad LACP;

4.18.3.28. Deverá possuir ferramenta de diagnóstico do tipo tcpdump e ainda dispor de ferramenta integrada à interface web para capturar informações dos pacotes em tempo real, podendo aplicar filtros, tais como IPs e portas, e ainda ter disponível a possibilidade de exportar a captura para um arquivo do tipo PCAP visando estender a análise para um software terceiro, tal como Wireshark;

4.18.3.29. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

4.18.3.30. Deverá possuir integração com tokens para autenticação de duplo fator;

4.18.3.31. Deverá suportar single-sign-on;

4.18.3.32. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;

4.18.3.33. Deverá suportar roteamento estático para IPv4 e IPv6;

4.18.3.34. Deverá suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP, RIP);

4.18.3.35. Deverá suportar sua implementação em formato de AS (Autonomous System) utilizando o protocolo BGP, em formato Full Route. Este será o formato implementado para atender às necessidades da Prefeitura;

4.18.3.36. Deverá suportar ECMP;

4.18.3.37. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

4.18.3.38. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.18.3.39. Deverá suportar aplicações multimídia, tais como: H.323 e SIP;

4.18.3.40. Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo;

4.18.3.41. Deverá permitir o funcionamento em modo transparente tipo “bridge”;

4.18.3.42. Deverá suportar PBR – Policy Based Routing;

4.18.3.43. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

4.18.3.44. Deverá possuir mecanismo de anti-spoofing;

4.18.3.45. Deverá permitir criação de regras definidas pelo usuário;

4.18.3.46. Deverá suportar sFlow ou Netflow;

4.18.3.47. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

4.18.3.48. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

4.18.3.49. Deverá permitir funcionamento em modo bridge em camada 2, roteador em camada 3, proxy explícito e sniffer via espelhamento;

4.18.3.50. Deverá possuir mecanismo de tratamento de sessão (session-helpers ou ALGs);

4.18.3.51. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

4.18.3.52. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

4.18.3.53. Deve suportar o protocolo padrão da indústria VXLAN;

4.18.3.54. Permitir, para o gerenciamento da solução, interface de administração via web no próprio dispositivo;

4.18.3.55. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster, eventos de segurança e estatísticas das verificações de saúde da camada SDWAN;

4.18.3.56. Deve disponibilizar controle, inspeção e de-criptografia de SSL para tráfego de entrada e saída, sendo que deve suportar ainda o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais;

4.18.3.57. Em caso de ser gerenciado de forma centralizada, o equipamento ofertado deverá continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos com a solução de gerência centralizada;

4.18.3.58. Deverá possuir conectores de SDN e dessa forma ser capaz de sincronizar de forma automática objetos;

4.18.3.59. Deverá suportar ambientes multi-cloud;

4.18.3.60. Deverá possuir a capacidade de criar automações através de gatilhos e ações, possibilitando uma atuação mais proativa;

4.18.3.61. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.18.3.62. A configuração em alta disponibilidade deve sincronizar:

4.18.3.63. Sessões;

4.18.3.64. Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;

4.18.3.65. Associações de Segurança das VPNs;

4.18.3.66. Tabelas FIB;

4.18.3.67. Assinaturas de IPS, Antivírus e AntiSpyware;

4.18.3.68. A configuração de alta disponibilidade deve possibilitar monitoração de falha de link;

4.18.3.69. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

4.18.3.70. Deverá possuir controle de acesso à Internet por endereço IP de origem e destino;

4.18.3.71. Deverá possuir controle de acesso à Internet por subrede;

4.18.3.72. Deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;

4.18.3.73. Deverá suportar controles por zonas de segurança;

4.18.3.74. Deverá suportar controles de políticas por porta e protocolo;

4.18.3.75. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

4.18.3.76. Controle de políticas por usuários, grupos de usuários, IPs, range de IPs, subrede, FQDN e zonas de segurança;

4.18.3.77. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;

4.18.3.78. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.18.3.79. Deve ser viável criar políticas com exceções, onde seja possível especificar que uma política será aplicada somente caso a origem ou destino do tráfego não seja um determinado objeto, tal como uma subrede, por exemplo, ou seja, se a subrede não for 192.168.0.0/24, o tráfego deverá ser tratado;

4.18.3.80. Controle, inspeção e de-criptografia de SSL por política para tráfego de saída;

4.18.3.81. Deve ser possível realizar um espelhamento do tráfego decriptografado;

4.18.3.82. Deve decriptografar tráfego de saída em conexões negociadas com TLS 1.2 e TLS 1.3;

4.18.3.83. A inspeção SSL deve ser compatível com HTTP3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos;

4.18.3.84. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

4.18.3.85. Deve suportar objetos de endereço IPv4 e IPv6 consolidados na mesma política de firewall;

4.18.3.86. Suporte a objetos e regras multicast;

4.18.3.87. Deve ser possível criar políticas de firewall utilizando serviços de ameaças de terceiros, onde o firewall receberá uma lista de endereços IPs maliciosos, por exemplo, a qual poderá ser utilizada para bloqueio do tráfego;

4.18.3.88. Deve ser possível criar política de firewall em modo de aprendizado, onde o equipamento deverá monitorar o tráfego que transita nas interfaces de origem e destino e registrar logs de eventos;

4.18.3.89. Deve possuir base com objetos contendo endereços IPs de serviços da Internet como, a citar, mas não se limitando a AWS S3, Microsoft Azure, Oracle, SAP, Google e Microsoft Office 365, atualizados dinamicamente pela solução;

4.18.3.90. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

4.18.3.91. Deve dispor de ferramenta para auxiliar a descobrir quais políticas correspondem a um determinado perfil de tráfego, facilitando assim a administração diária da solução e facilmente encontrando quais políticas estão sendo atribuídas a um determinado IP, por exemplo;

4.18.3.92. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

4.18.3.93. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.18.3.94. Reconhecer pelo menos 2000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.18.3.95. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

4.18.3.96. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.18.3.97. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

4.18.3.98. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.18.3.99. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

4.18.3.100. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.18.3.101. Atualizar a base de assinaturas de aplicações automaticamente;

4.18.3.102. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

4.18.3.103. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.18.3.104. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

4.18.3.105. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

4.18.3.106. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

4.18.3.107. Deve alertar o usuário quando uma aplicação for bloqueada;

4.18.3.108. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

4.18.3.109. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

4.18.3.110. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;

4.18.3.111. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

4.18.3.112. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse

4.18.3.113. Based, Network Protocol, etc);

4.18.3.114. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

4.18.3.115. Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet;

4.18.3.116. Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP;

4.18.3.117. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

4.18.3.118. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.18.3.119. Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP; 4.17.3.119 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

4.18.3.120. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

4.18.3.121. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.18.3.122. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

4.18.3.123. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

4.18.3.124. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

4.18.3.125. Deve permitir o bloqueio de vulnerabilidades;

4.18.3.126. Deve permitir o bloqueio de exploits conhecidos;

4.18.3.127. Deve incluir proteção contra-ataques de negação de serviços;

4.18.3.128. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

4.18.3.129. Detectar e bloquear a origem de portscans;

4.18.3.130. Bloquear ataques efetuados por worms conhecidos;

4.18.3.131. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.18.3.132. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.18.3.133. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.18.3.134. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

4.18.3.135. Identificar e bloquear comunicação com botnets;

4.18.3.136. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.18.3.137. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

4.18.3.138. Os eventos devem identificar o país de onde partiu a ameaça;

4.18.3.139. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

4.18.3.140. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

4.18.3.141. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

4.18.3.142. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

4.18.3.143. Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de call-back;

4.18.3.144. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento;

4.18.3.145. Deve ser possível filtrar assinaturas com base no identificador CVE;

4.18.3.146. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um “wildcard” do CVE para abranger mais de um identificador;

4.18.3.147. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável;

4.18.3.148. Deve incluir proteção contra ataques de negação de serviços;

4.18.3.149. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.18.3.150. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.18.3.151. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

4.18.3.152. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

4.18.3.153. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

4.18.3.154. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

4.18.3.155. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

4.18.3.156. Possuir pelo menos 70 categorias de URLs;

4.18.3.157. Deve possuir a função de exclusão de URLs do bloqueio;

4.18.3.158. Permitir a customização de página de bloqueio;

4.18.3.159. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

4.18.3.160. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

4.18.3.161. Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário;

4.18.3.162. Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego;

4.18.3.163. Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website;

4.18.3.164. Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado;

4.18.3.165. Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos;

4.18.3.166. Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo;

4.18.3.167. Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente;

4.18.3.168. A solução deverá permitir a implementação futura de ZTNA através da aquisição de licenciamento de Endpoints, permitindo a ativação das seguintes funcionalidades:

4.18.3.169. Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação deidentidade através de no mínimo:

4.18.3.169.1. Informação pessoal do sistema operacional;

4.18.3.169.2. LinkedIn;

4.18.3.169.3. Google;

4.18.3.169.4. SalesForce;

4.18.3.170. Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para osendpoints baseado em no mínimo:

4.18.3.170.1. DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DCHP específico;

4.18.3.170.2. DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DNS específico;

4.18.3.170.3. Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento;

4.18.3.170.4. Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em um range de IPs específico

4.18.3.170.5. Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway;

4.18.3.170.6. Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede;

4.18.3.170.7. VPN Tunnel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Tunel de VPN, deve ser permitida a escolha de túnel de VPN para cada perfil;

4.18.3.171. Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso;

4.18.3.172. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

4.18.3.173. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.18.3.174. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.18.3.175. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

4.18.3.176. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

4.18.3.177. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

4.18.3.178. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.18.3.179. Deve possuir integração e suporte a Microsoft Active Directory;

4.18.3.180. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

4.18.3.181. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.18.3.182. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

4.18.3.183. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

4.18.3.184. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.18.3.185. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

4.18.3.186. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento

de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider SP).

4.18.3.187. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

4.18.3.188. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.18.3.189. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.18.3.190. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

4.18.3.191. Deverá administrar e controlar de maneira centralizada pontos de acesso wireless do mesmo fabricante da solução ofertada, permitindo que futuramente a Prefeitura faça a aquisição de pontos de acesso, sem a necessidade de adquirir uma controladora Wi-Fi;

4.18.3.192. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;

4.18.3.193. 4Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;

4.18.3.194. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;

4.18.3.195. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

4.18.3.196. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

4.18.3.197. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

4.18.3.198. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;

4.18.3.199. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados localmente na interface do ponto de acesso;

4.18.3.200. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

4.18.3.201. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;

4.18.3.202. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os

pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

4.18.3.203. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

4.18.3.204. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

4.18.3.205. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

4.18.3.206. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;

4.18.3.207. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

4.18.3.208. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

4.18.3.209. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

4.18.3.210. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

4.18.3.211. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

4.18.3.212. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

4.18.3.213. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

4.18.3.214. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de

informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

4.18.3.215. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

4.18.3.216. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

4.18.3.217. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

4.18.3.218. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

4.18.3.219. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

4.18.3.220. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

4.18.3.221. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

4.18.3.222. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

4.18.3.223. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

4.18.3.224. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;

4.18.3.225. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

4.18.3.226. A solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitidos e bloqueados para cada perfil de usuário e SSID;

4.18.3.227. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;

4.18.3.228. A base de reconhecimento de aplicações através de DPI deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;

4.18.3.229. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;

4.18.3.230. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;

4.18.3.231. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

4.18.3.231.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);

4.18.3.231.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;

4.18.3.231.3. ASLEAP;

4.18.3.231.4. Null Probe Response / Null SSID Probe Response;

4.18.3.231.5. Long Duration;

4.18.3.231.6. Ataques contra Wireless Bridges;

4.18.3.231.7. Weak WEP;

4.18.3.231.8. Invalid MAC OUI.

4.18.3.232. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;

4.18.3.233. A solução deve implementar mecanismos de proteção contra ataques do tipo ARPPoisoning na rede wireless;

4.18.3.234. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;

4.18.3.235. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;

4.18.3.236. Deve implementar autenticação administrativa através do protocolo RADIUS;

4.18.3.237. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

4.18.3.238. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

4.18.3.239. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

4.18.3.240. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

4.18.3.241. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

4.18.3.242. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

4.18.3.243. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAPSIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

4.18.3.244. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;

4.18.3.245. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

4.18.3.246. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

4.18.3.247. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

4.18.3.248. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

4.18.3.249. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

4.18.3.250. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;

4.18.3.251. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

4.18.3.252. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

4.18.3.253. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;

4.18.3.254. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispostivo conectado à rede wireless;

4.18.3.255. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;

4.18.3.256. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

4.18.3.257. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

4.18.3.258. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

4.18.3.259. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

4.18.3.260. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;

4.18.3.261. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

4.18.3.262. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

4.18.3.263. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato .pcap;

4.18.3.264. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

4.18.3.265. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

4.18.3.266. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

4.18.3.267. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

4.18.3.268. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;

4.18.3.269. A solução deve possuir ferramentas de diagnósticos e debug;

4.18.3.270. A solução deve suportar comunicação com elementos externos através de APIs.

4.18.3.271. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

4.18.3.272. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.18.3.273. Suportar VPN IPSec Site-to-Site;

4.18.3.274. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

4.18.3.275. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

4.18.3.276. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

4.18.3.277. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

4.18.3.278. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.

4.18.4. SWITCH CORE:

4.18.4.1. Deve possuir 48 (quarenta e oito) portas Gigabit Ethernet 10/100/1000Base-T Conforme Padrões IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z e IEEE 802.3ae;

4.18.4.2. As interfaces deverão ser Full-Duplex, auto sensing com conectores RJ45 fêmea e implementar mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X;

4.18.4.3. Deve possuir adicionalmente no mínimo 8 (Oito) portas 10GE (SFP+) e 2(Duas) portas 100GE (QSFP28);

4.18.4.4. Deve possuir no mínimo 1 (uma) porta console exclusiva para fins de gerenciamento e configuração. Esta porta deverá ser do tipo: RJ45, USB ou micro USB;

4.18.4.5. Deve possuir fonte de alimentação redundante Hot-Swappable, que opere com tensões de entrada entre 100 e 240 VAC e frequência de 50/60Hz;

4.18.5. DESEMPENHO E CAPACIDADES

4.18.5.1. Deve possuir capacidade de processamento de no mínimo 656 Gbps;

4.18.5.2. Deve possuir taxa de encaminhamento de pacotes igual ou superior a 488 Mpps;

4.18.5.3. Sua tabela de MAC Address deve suportar no mínimo 64.000 MAC address;

4.18.5.4. Deve possuir Buffer de pacotes de no mínimo 4MB;

4.18.5.5. Deve suportar jumbo frame de no mínimo 9 KB;

4.18.5.6. O equipamento deve possuir no mínimo 3 (duas) ventoinhas internas para resfriamento;

4.18.5.7. Deve suportar temperatura de operação entre 0° e 45°;

4.18.5.8. Deve suportar operação sob umidade entre 10% e 90% RH sem condensamento.

4.18.6. FUNCIONALIDADES DE CAMADA 2

4.18.6.1. Deve implementar agregação de links de modo estático, bem como LACP (Link Aggregation Control Protocol) conforme IEEE 802.3ad;

4.18.6.2. Deve implementar o protocolo Spanning tree e suas variações:

4.18.6.3. IEEE 802.1d STP (Spanning tree protocol);

4.18.6.4. IEEE 802.1w RSTP (Rapid Spanning Tree Protocol);

4.18.6.5. IEEE 802.1s MSTP (Multiple Spanning Tree Protocol);

4.18.6.6. Deve possuir mecanismo de detecção e proteção contra loops;

4.18.6.7. Deve implementar Túneis de BPDU (Bridge Protocol Data Unit);

4.18.6.8. Deve possuir recurso de proteção da porta root como root guard, root protect ou similar;

4.18.6.9. Deve implementar controle de fluxo conforme IEEE 802.3X;

4.18.6.10. Deve implementar espelhamento de porta possibilitando o monitoramento de uma porta ou de um grupo de portas. Também deve possibilitar a escolha da direção do tráfego a ser espelhado, sendo TX, RX ou ambos;

4.18.6.11. Deve implementar no mínimo 4000 Vlans;

4.18.6.12. Deve possibilitar a configuração do ID da Vlan entre 2 e 4094;

4.18.6.13. Deve implementar Tagged Vlan conforme IEEE 802.1Q;

4.18.6.14. Deve implementar MAC Vlan;

4.18.6.15. Deve Implementar GVRP (Generic Vlan Registration Protocol);

4.18.6.16. Deve implementar Vlan de voz. O Switch deverá ser capaz de reconhecer um telefone IP automaticamente e atribuí-lo à uma VLAN de voz.
4.18.6.17. MULTICAST
4.18.6.18. Deve implementar IGMP Snooping v1, v2 e v3;
4.18.6.19. Deve suportar IGMP Fast Leave;
4.18.6.20. Deve suportar configuração de grupo de multicast estático;
4.18.6.21. Deve suportar MLD Snooping v1 e v2;
4.18.6.22. FUNCIONALIDADES L3
4.18.6.23. Deve suportar no mínimo 24.000 rotas estáticas IPv4;
4.18.6.24. Deve suportar no mínimo 14.000 rotas estáticas IPv6;
4.18.6.25. Deve implementar protocolo de roteamento RIP e RIPng;
4.18.6.26. Deve implementar protocolo de roteamento OSPF v2/v3;
4.18.6.27. Deve suportar empilhamento de no mínimo 4 unidades;
4.18.6.28. Deve suportar o protocolo VRRP v2/v3;
4.18.6.29. QUALIDADE DE SERVIÇO
4.18.6.30. Deve implementar classificação e marcação de pacotes em DSCP conforme IEEE 802.1p;
4.18.6.31. Deve implementar os seguintes algoritmos de gerenciamento de filas:
4.18.6.32. WRR (Weighted Round Robin);
4.18.6.33. SP (Strict Priority);
4.18.6.34. SP+WRR (Strict Priority + Weighted Round Robin);
4.18.6.35. Deve Implementar controle de banda por porta;
4.18.6.36. Deve possibilitar a implementação de no mínimo 8 filas;
4.18.6.37. SEGURANÇA:
4.18.6.38. Deve implementar Access Control List (ACL);
4.18.6.39. Deve suportar ACL baseada em tempo;
4.18.6.40. Deve suportar ACL Baseada em MAC Address:
4.18.6.41. Deve implementar ACL baseada em IP;
4.18.6.42. DSCP/IP TOS.
4.18.6.43. Deve implementar ACL sobre IPv6;
4.18.6.44. Deve implementar Global IP-MAC binding;
4.18.6.45. Deve implementar IP Source Guard;
4.18.6.46. Deve implementar proteção contra ataques DDoS;
4.18.6.47. Deve implementar port security;
4.18.6.48. Deve implementar Broadcast, Multicast e Unicast Storm Control;
4.18.6.49. Deve implementar IEEE 802.1X com autenticação baseada em porta e MAC;
4.18.6.50. Deve suportar IEEE 802.1X com associação automática de Vlan;
4.18.6.51. Deve ter suporte à servidor RADIUS para autenticação;
4.18.6.52. Deve implementar DHCP Snooping para IPv4 e para IPv6;
4.18.6.53. Deve suportar gerenciamento através de HTTPS;
4.18.6.54. Deve suportar gerenciamento através de interface de comandos segura com SSH V1 e v2;

4.18.6.55. GERENCIAMENTO

4.18.6.56. Deve implementar gerenciamento via WEB com HTTPS;

4.18.6.57. Deve permitir o gerenciamento através de linha de comandos (CLI) para interface console bem como para comunicação TCP com Telnet e SSH;

4.18.6.58. Deve ter suporte para AAA incluindo TACACS+;

4.18.6.59. Deve ter suporte para EEE (Energy Efficient Ethernet);

4.18.6.60. Deve suportar SNMP V1, V2c e V3;

4.18.6.61. Deve implementar RMON (1,2,3,9);

4.18.6.62. Deve implementar NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);

4.18.6.63. Deve implementar FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol);

4.18.6.64. Deve Implementar LLDP e LLDP MED conforme IEEE 802.1ab;

4.18.6.65. Deve implementar Syslog;

4.18.6.66. Deve implementar servidor DHCP;

4.18.6.67. Deve implementar DHCP/BOOT Cliente;

4.18.6.68. Deve Implementar DHCP Relay;

4.18.6.69. Deve possibilitar o monitoramento da CPU do Switch;

4.18.6.70. Deve possibilitar o armazenamento de dois arquivos de configuração simultaneamente (Dual Image);

4.18.6.71. Deve implementar diagnóstico de cabos;

4.18.6.72. Deve implementar Ethernet Link EFM baseado conforme IEEE 802.3ah;

4.18.6.73. Deve implementar DLDP (Device Link Detect Protocol);

4.18.6.74. Deve ser possível o gerenciamento do Switch através de solução de gerenciamento centralizado do próprio fabricante podendo ser este software ou apliance;

4.18.6.75. IPv6;

4.18.6.76. Deve implementar Pilha dupla (Dual IPv4/IPv6);

4.18.6.77. Deve implementar MLDv2 (Multicast Listener Discovery);

4.18.6.78. Deve implementar ACL sobre IPv6;

4.18.6.79. Deve implementar rotas estáticas em IPv6 e interfaces VLAN sobre IPv6;

4.18.6.80. Deve implementar IPv6 Neighbor Discover (ND);

4.18.6.81. Deve implementar ICMP v6;

4.18.6.82. Deve implementar DHCPv6 Snooping;

4.18.6.83. Deve implementar Path maximum transmission unit (MTU) Discovery;

4.18.6.84. Deve suportar as seguintes aplicações sobre IPv6:

4.18.6.85. DHCPv6 Cliente;

4.18.6.86. IPv6 SSH.

4.19. OLT (OPTICAL LINE TERMINATION)

4.19.1. A OLT deve seguir o padrão GPON ITU-T G.984, no tamanho de 1U do tipo cassete comcapacidade de transmissão mínima de 88 gbit/s;

4.19.2. Suportar downstream de 2,488 Gbps e upstream de 1,244 Gbps;

4.19.3. Permitir uma distância de comunicação de até 60 km utilizando módulos GPON Classe C+ ou C++;
4.19.4. Possuir 1 interface console RJ-45 (RS232) para gerência local;
4.19.5. Possuir 1 interface de gerenciamento fora de banda RJ-45 (Ethernet);
4.19.6. Possuir 1 interface de alarme (RS485);
4.19.7. Possuir 2 interfaces SFP+ de 10 Gbps para uplinks ópticos;
4.19.8. A OLT deve ser capaz de operar em redundância ativa-passiva (standby) ou ativa-ativa em configuração de alta disponibilidade, utilizando um segundo equipamento em nó distinto;
4.19.9. A OLT deve permitir interligação através de rede óptica bidirecional em anel, garantindo failover automático no caso de falha de um dos nós;
4.19.10. A OLT deve compartilhar o mesmo plano de controle e de dados, mantendo a sincronização constante das tabelas de rotas, perfis de serviço e configurações de ONU;
4.19.11. Deve permitir comunicação entre as OLTs por meio de interface 10 Gbps (uplinks SFP+), garantindo largura de banda suficiente para replicação de estados em tempo real;
4.19.12. A OLT deve ser compatível com racks de 19" e 21";
4.19.13. Deve ocupar no máximo 1U de altura do rack;
4.19.14. A OLT deve possuir no mínimo 16 interfaces GPON;
4.19.15. Suportar a até 128 ONUs por porta, com comunicação óptica nas seguintes faixas de comprimento de onda:
4.19.16. Downstream: 1490 nm;
4.19.17. Upstream: 1310 nm.
4.19.18. Possuir interface CLI para configuração via linha de comando;
4.19.19. Suportar protocolo SNMP (v1/v2c/v3);
4.19.20. Deverá possuir software de gerenciamento centralizado para múltiplos dispositivos em configuração de alta disponibilidade com as seguintes especificações:
4.19.21. Configurar e monitorar remotamente, centralizando a configuração da OLT e de todas as ONUs conectadas, incluindo gerenciamento de parâmetros de rede, perfis de serviço, controle de largura de banda (DBA), e QoS;
4.19.22. Monitoramento de status em tempo real: Monitora o desempenho das OLTs e ONUs, oferecendo uma visão geral da rede em tempo real, incluindo tráfego, consumo de largura de banda e alertas sobre falhas ou anomalias;
4.19.23. Suportar o provisionamento automático de serviços e ativações de ONUs, facilitando a instalação rápida de novos dispositivos e serviços com mínima intervenção humana;
4.19.24. Oferecer recursos de autenticação de ONUs e segurança por meio de ACLs (Listas de Controle de Acesso), garantindo que somente dispositivos autorizados possam ser conectados à rede, prevenindo ONUs "Rogue" e acessos não autorizados;
4.19.25. Gerenciar serviços de múltiplos tipos (dados, voz e vídeo) simultaneamente, suportando ambientes multisserviços com qualidade e eficiência, além de controle de multicast para otimizar a entrega de conteúdo em broadcast;
4.19.26. Enviar notificações e alarmes em tempo real sobre eventos críticos e falhas na rede. Isso permite que os administradores resolvam problemas rapidamente, minimizando o tempo de inatividade;

4.19.27. Permitir realizar atualizações de firmware das OLTs e ONUs de forma centralizada, garantindo que os dispositivos estejam sempre utilizando as versões mais recentes do software, melhorando a segurança e a funcionalidade;

4.19.28. O software deve ser compatível com SNMP (v1/v2c/v3), o que permite sua integração com sistemas de gerenciamento de rede de terceiros, oferecendo flexibilidade para grandes operações;

4.19.29. Gerar relatórios detalhados sobre o desempenho da rede, tráfego, e uso de recursos. Isso permite uma visão analítica para otimizar a operação e planejar expansões futuras de maneira eficiente;

4.19.30. É de responsabilidade da contratada o licenciamento e instalação stand alone do software de gerenciamento em sua própria instrutura durante a vigência do contrato;

4.19.31. Deverá suportar OMCI (Optical Network Unit Management and Control Interface);

4.19.32. Deverá suportar a multi-serviços (voz, vídeo e dados);

4.19.33. Deverá suportar roteamento L3;

4.19.34. Deverá suportar Multicast;

4.19.35. Servidor e Relay DHCP;

4.19.36. Deverá suportar funções MPLS incluindo static LSP, MPLS LDP e MPLS RSVP para atender a tecnologias recentes;

4.19.37. Deverá suportar segurança via listas de controle de acesso (ACL);

4.19.38. Deverá possuir detecção de ONU Rogue;

4.19.39. A OLT deve possuir redundância de fonte de alimentação VDC com fontes hot-swappable;

4.19.40. Deve possuir consumo máximo de energia de 430W.

4.20. ONU (OPTICAL NETWORK UNIT)

4.20.1. Deverá possuir 4 portas Gigabit Ethernet (10/100/1000BASE-T) com conectores RJ45;

4.20.2. Deverá possuir 1 porta FXS;

4.20.3. Deverá possuir 1 porta óptica hibrida (EPON/GPON),

4.20.4. Deverá possuir memória mínima SDRAM: 512 MB;

4.20.5. Deverá possuir memória flash mínima de 256 MB;

4.20.6. Deverá suportar no mínimo 64 clientes simultâneos;

4.20.7. Deverá suportar cabo UTP categoria 5e ou 6;

4.20.8. Deverá suportar fibra ótica monomodo (SMF) com distância de até 20 km (1000 BASE-FX);

4.20.9. Deverá possuir 1 (uma) interface óptica SC/APC;

4.20.10. Deverá possuir comprimento de onda de Tx 1310 nm e Rx 1490 nm;

4.20.11. Deverá possuir sensibilidade de recepção máxima -8 dBm;

4.20.12. Deverá possuir sensibilidade de recepção mínima -28 dBm;

4.20.13. Deverá possuir padrão GPON ITU-T G.984 (com suporte a 1.244 Gbps upstream e 2.488 Gbps downstream, classe óptica B+);

4.20.14. Deverá possuir padrão EPON 1.25 Gbps upstream e downstream;

4.20.15. Deverá suportar o padrão IEEE 802.3, com suporte a autonegociação e controle de fluxo (802.3x);

4.20.16. Deverá suportar tecnologia Mu-MIMO com suporte a até 64 clientes simultâneos;

4.20.17. Deverá possuir 2 antenas de 5 dBi;

4.20.18. Deverá suportar as frequências 2.4 GHz e 5 GHz (com suporte a múltiplos SSIDs, 4 para cada frequência);
4.20.19. Deverá suportar taxa de transmissão em 2.4 GHz: até 573 Mbps e 5 GHz até 2400 Mbps;
4.20.20. Deverá suportar os protocolos GPON ITU-T G.984 com suporte a 8 T-CONTS por dispositivo, decodificação de criptografia AES-128 e FEC (Forward Error Correction), EPON, compatível com IEEE 802.3ah;
4.20.21. Deverá permitir ativação de descobrimento automático de SN e senha em conformidade com ITU-T G.984.3;
4.20.22. Deverá possuir suporte a multicast GEM port Ethernet / IP;
4.20.23. Deverá possuir bridging and switching (802.1D/802.1Q) com quatro classes de tráfego com 802.1p 802.3x Flow Control;
4.20.24. Suportar VLAN tagging /untagging VLAN stacking (Quin-Q);
4.20.25. Suportar até 4095 VLANS EPON;
4.20.26. Suportar criptografia: WPA2-PSK, WPA3-SAE;
4.20.27. Suportar firewall com ACL com filtragem baseada em MAC/IP/URL e proteção contra ataques DoS;
4.20.28. Suporte para até 1024 endereços MAC.
4.20.29. Suportar até operação como bridge ou router (IPv4 e IPv6);
4.20.30. Suportar gerenciamento via OMCI, Web UI e TR-06;
4.20.31. Deve atender às seguintes características construtivas:
4.20.31.1. Temperatura de operação: -5 a 45°C;
4.20.31.2. Umidade relativa de Operação: 10 a 95% (sem condensação);
4.20.31.3. Alimentação DC 12V com adaptador AC/DC incluso 100-240V, 50/60Hz;
4.20.31.4. LEDs indicativos de status;
4.20.32. A fim de garantir total compatibilidade a ONU e OLT devem ser do mesmo fabricante.
4.21. ESTRUTURA ORGANIZACIONAL DOS NODES E SEUS ATIVOS
4.21.1. COMPOSIÇÃO DE NODE CORE - LOCALIZADOS NA SECRETARIA DE SEGURANÇA (SITE A)
4.21.2. 1 (um) Link Dedicado através de fibra ótica, fornecido pela contratante, com 2 Gbps realizando o Peering BGP com o ASN da Prefeitura Municipal;
4.21.3. 1 (um) ROTEADOR BGP fornecido pela operadora, realizando as funções de estabelecimento de sessões, anúncio de rotas e sub-redes, recebimento de rotas, filtragem e políticas de roteamento, redundância e resiliência para segunda conexão BGP e monitoramento e diagnóstico do estado das sessões BGP.
4.21.4. 1 (um) FIREWALL NGFW fornecido pela operadora, realizando funções de IDS, IPS, tunelamento VPN com ONUs, Criptografia e autenticação de VPN, controle de acesso QoS, monitoramento de logs de segurança e segmentação de rede;
4.21.5. 1 (um) SWITCH CORE fornecido pela operadora, interconectado por fibra ótica aos outros switches que comporão o anel bidirecional através de conexão duplex, realizando a gestão e controle de tráfego além de mais uma camada de segurança e monitoramento;
4.21.6. 1 (uma) OLT fornecida pela operadora devem atuar como pontos centrais de conexão entre a rede de backbone (switches core) e os dispositivos finais (ONUs - Optical Network Units);

4.21.7. Cada node deve possuir sistema de monitoramento e sistema de detecção de acesso não autorizado sendo monitorado de forma ativa e online, registrando acessos indevidos através de logs e integrada em tempo real a central de monitoramento.

4.22. COMPOSIÇÃO DE NODE CORE - LOCALIZADO NA DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO (SITE B)

4.22.1. 1 (um) Link Dedicado através de fibra ótica, fornecido pela contratante, com 2 Gbps realizando o Peering BGP com o ASN da Prefeitura Municipal;

4.22.2. 1 (um) ROTEADOR BGP fornecido pela operadora, realizando as funções de estabelecimento de sessões, anúncio de rotas e sub-redes, recebimento de rotas, filtragem e políticas de roteamento, redundância e resiliência para segunda conexão BGP e monitoramento e diagnóstico do estado das sessões BGP.

4.22.3. 1 (um) FIREWALL NGFW fornecido pela operadora, realizando funções de IDS, IPS, tunelamento VPN com ONUs, Criptografia e autenticação de VPN, controle de acesso QoS, monitoramento de logs de segurança e segmentação de rede;

4.22.4. 1 (um) SWITCH CORE fornecido pela operadora, interconectado por fibra ótica aos outros switches que comporão o anel bidirecional através de conexão duplex, realizando a gestão e controle de tráfego além de mais uma camada de segurança e monitoramento;

4.22.5. Cada node deve possuir sistema de monitoramento e sistema de detecção de acesso não autorizado sendo monitorado de forma ativa e online, registrando acessos indevidos através de logs e integrada em tempo real a central de monitoramento.

4.23. COMPOSIÇÃO DE NODE ANEL - LOCALIZADOS NO HOSPITAL RUTH CARDOSO, SECRETARIA DE EDUCAÇÃO, SECRETARIA DA SAUDE, PREFEITURA MUNICIPAL E CENTRAL DE OPERAÇÕES

4.23.1. 1 (um) SWITCH CORE fornecido pela operadora, interconectado por fibra ótica aos outros switches que comporão o anel bidirecional através de conexão duplex, realizando a gestão e controle de tráfego além de mais uma camada de segurança e monitoramento;

4.24. COMPOSIÇÃO DE NODE DISTRIBUIÇÃO – LOCALIZADOS EM EDIFÍCIOS PUBLICOS E UNIDADES ADMINISTRATIVAS DA PREFEITURA DE BALNEÁRIO CAMBORIU

4.24.1. 1 (uma) ONU fornecido pela operadora, deverá realizar a interconexão entre NÓ da borda da rede e a OLT localizada nos NÓS CONCETRADORES CORE (SITE A) através de tecnologia GPON realizando a conexão de dados aos dispositivos e funções de controle de banda como QoS;

4.24.2. 1 (um) WIFI INDOOR fornecido pela operadora, será conectado a 1 ONU e realizará o fornecimento de conectividade e internet através de rede sem fio para os munícipes e colaboradores da Prefeitura realizando a função de HOTSPOT de no mínimo 1024 clientes simultâneos;

4.24.3. Cada node deve possuir sistema de monitoramento e sistema de detecção de acesso físico ao rack de forma não autorizada sendo monitorado de forma ativa e online, registrando acessos indevidos através de logs e integrada em tempo real ao monitoramento da central de operações.

4.25. COMPOSIÇÃO DE NODE HOTSPOT – LOCALIZADOS EM AMBIENTES E PÚBLICOS E PRAÇAS EM AMBIENTE ABERTO (OUTDOOR)

4.25.1. 1 (uma) ONU fornecido pela operadora, deverá realizar a interconexão entre NÓ da borda da rede e a OLT localizada nos NÓS CONCETRADORES CORE (SITE A) através de tecnologia GPON realizando a conexão de dados aos dispositivos e funções de controle de banda como QoS;

4.25.2. 1 (um) WIFI OUTDOOR fornecido pela operadora, será conectado a ONU e realizará o fornecimento de conectividade e internet através de rede sem fio para os munícipes e colaboradores da Prefeitura realizando a função de HOTSPOT até um no mínimo 1024 clientes simultâneos;

4.26. COMPOSIÇÃO DE NODE DISPOSITIVOS IOT – LOCALIZADOS EM LOCAIS ONDE SERÃO UTILIZADOS DISPOSITIVOS COMO SEMAFOROS, CAMERAS DE SEGURANÇA, OCRs, DISPOSITIVOS DE IOT DENTRE OUTRAS CONEXÕES QUE NÃO PRECISEM DE CRIPTOGRAFIA PONTO A PONTO COM TUNELAMENTO ATRAVÉS DE VPN

4.26.1. 1 (uma) ONU fornecido pela operadora, deverá realizar a interconexão entre NÓ da borda da rede e a OLT localizada nos NÓS CONCETRADORES CORE (SITE A E SITE B) através de tecnologia GPON realizando a conexão de dados aos dispositivos e funções de controle de banda como QoS.

4.27. REFENTE AOS NODES SOB DEMANDA

4.27.1. São nodes utilizados sob demanda para expansões futuras na rede.

4.27.2. Os mesmos serão “kits” compostos com a tecnologia para a chegada da fibra óptica e disponibilidade do WiFi para transmissões dos eventos, Wifi-BC e para acesso à internet para o realizador do evento através de SSID específico;

4.27.3. Os pontos de eventos não deverão ter acesso a rede da prefeitura;

4.27.4. A Contratada deverá deixar funcionando os serviços de internet no equipamento concentrador, quando houver, da realizadora do evento, realizando contato direto com a mesma.

4.28. **SEGURANÇA**

4.28.1. SEGURANÇA DA REDE METROPOLITANA

4.28.1.1. Para garantir uma abordagem robusta, serão empregadas tecnologias avançadas, incluindo NETFLOW, IDS (Sistema de Detecção de Intrusão), IPS (Sistema de Prevenção de Intrusão), SOAR (Resposta Automatizada e Orquestração de Segurança). Essas tecnologias serão responsáveis por inspecionar e prevenir uma ampla gama de ameaças potenciais, catalogando anomalias e atividades suspeitas. Entre os alvos estão a propagação de malwares, tentativas de pishing, ataques de ransomware, exfiltração de dados e ataques de DDoS, bem como tentativas de acesso não autorizado aos servidores. Essa abordagem proativa será crucial para manter a segurança da Rede Metropolitana e garantir a proteção adequada dos sistemas e dados sensíveis;

4.28.1.2. Para garantir uma abordagem robusta, serão empregadas tecnologias avançadas, incluindo NETFLOW, IDS (Sistema de Detecção de Intrusão), IPS (Sistema de Prevenção de Intrusão), SOAR (Resposta Automatizada e Orquestração de Segurança). Essas tecnologias serão responsáveis por inspecionar e prevenir uma

ampla gama de ameaças potenciais, catalogando anomalias e atividades suspeitas. Entre os alvos estão a propagação de malwares, tentativas de pishing, ataques de ransomware, exfiltração de dados e ataques de DDoS, bem como tentativas de acesso não autorizado aos servidores. Essa abordagem proativa será crucial para manter a segurança da Rede Metropolitana e garantir a proteção adequada dos sistemas e dados sensíveis;

4.28.1.3. Segmentação: A segmentação de rede deverá ser implementada por meio de uma combinação de configurações aplicadas nos comutadores de informação (switch / roteador / firewall) através de recursos abrangentes nas camadas L2, L3, L4, em combinação com políticas de segurança, isolando de forma granular cada dispositivo da rede sendo permitido somente as comunicações necessárias para operacionalização e viabilização de serviços, desde que não venham a criar gaps na segurança da rede isolamento de cada dispositivo.

4.28.1.4. O OPERADOR será responsável por gerenciar esses mecanismos identificando e filtrando os “falsos positivos” gerados, e atuando de maneira preventiva e proativa com maior eficácia possível na resolução dos possíveis incidentes. Estes mecanismos deverão funcionar continuamente na REDE METROPOLITANA sem que isto incorra em diminuição das performances determinadas para cada NÓ (NODE);

4.28.1.5. O OPERADOR é responsável por replicar e disponibilizar ferramentas que permitam consultas à DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO, abrangendo todos os eventos e alarmes gerados pelos equipamentos e ferramentas de monitoramento e segurança utilizados na operação e gerenciamento da REDE METROPOLITANA. Essas ferramentas devem fornecer acesso transparente e abrangente aos registros de eventos, permitindo uma análise detalhada do desempenho e da segurança da infraestrutura de rede.

4.28.2. CRIPTOGRAFIA

4.28.2.1. Para garantir a integridade e confidencialidade dos dados transmitidos pela REDE METROPOLITANA em suas unidades administrativas, é exigido que qualquer meio de comunicação utilizado para trafegar informações do MUNICÍPIO implemente um túnel cifrado. Essa medida é uma exigência em conformidade com as recomendações, práticas e procedimentos estabelecidos pela Infraestrutura de Chaves Públicas Brasileira (ICP - Brasil), seguindo rigorosamente os critérios estabelecidos na lei nº 13.709/2018 (Lei Geral de Proteção de Dados);

4.28.2.2. A tecnologia de criptografia adotada deve aderir a padrões reconhecidos que garantam a segurança necessária para proteger os dados em trânsito. Para isso, será implementada uma chave de criptografia com no mínimo AES-128. Esta escolha visa assegurar um alto nível de segurança, utilizando um algoritmo robusto e amplamente reconhecido pela sua eficácia na proteção de dados sensíveis;

4.28.2.3. Além de atender aos requisitos legais e regulamentares, a adoção dessas medidas de criptografia contribuirá significativamente para a proteção dos dados do MUNICÍPIO contra acessos não autorizados e possíveis violações de privacidade.

4.28.3. SERVIÇOS PRESTADOS PELO OPERADOR

4.28.3.1. O OPERADOR será encarregado de prestar serviços essenciais para a infraestrutura da REDE METROPOLITANA, incluindo transporte de dados, gerenciamento de rede, análise de desempenho, segurança cibernética e monitoramento contínuo. Isso envolve a utilização de ferramentas avançadas de monitoramento e análise de dados, como sistemas de monitoramento de rede (NMS) e plataformas de análise de segurança (SIEM). O OPERADOR também será responsável por implementar e manter medidas de segurança proativas, como firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), e realizar análises de vulnerabilidades periodicamente como também implementações de regras solicitadas pela contratante;

4.28.3.2. Além disso, é crucial que o OPERADOR adote uma abordagem proativa para garantir o funcionamento contínuo da REDE METROPOLITANA. Isso inclui a implementação de práticas de gerenciamento de capacidade para evitar congestionamentos de rede, a otimização de rotas de dados para garantir a eficiência na transmissão de informações e a realização de atualizações de software e firmware de forma regular para mitigar vulnerabilidades de segurança conhecidas. O monitoramento ativo da rede permite identificar rapidamente quaisquer problemas ou anomalias e tomar medidas corretivas imediatas, garantindo assim a disponibilidade e integridade dos serviços prestados pela REDE METROPOLITANA.

4.28.4. REDE DE DADOS

4.28.4.1. É responsabilidade do OPERADOR administrar a REDE METROPOLITANA de forma a garantir o desempenho excepcional do tráfego de dados em cada enlace. Isso inclui o cumprimento rigoroso de todos os padrões de velocidade (taxa de bits), qualidade de serviço, conformidade com a legislação aplicável e os requisitos de segurança estabelecidos neste documento. Para alcançar esse objetivo, o OPERADOR utilizará tecnologias avançadas, como QoS (Quality of Service), para priorizar e gerenciar o tráfego de acordo com as necessidades específicas de cada serviço e aplicação;

4.28.4.2. A integração completa dos enlaces à infraestrutura de ativos e passivos de rede instalados nas Unidades do MUNICÍPIO é crucial para garantir a operacionalidade total do sistema. Isso envolve não apenas a conexão física dos enlaces aos equipamentos de rede, mas também a configuração adequada de protocolos de roteamento, como OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol), para garantir a comunicação eficiente entre os diversos pontos da rede. Além disso, o OPERADOR implementará redundância e tolerância a falhas em todos os níveis da infraestrutura, garantindo assim a alta disponibilidade e confiabilidade do serviço prestado pela REDE METROPOLITANA.

4.28.5. ROTEAMENTO IP

4.28.5.1. É de responsabilidade do OPERADOR gerenciar as tabelas de roteamento IP para garantir a conectividade eficiente entre todos os dispositivos na REDE METROPOLITANA. Isso inclui a atualização contínua das tabelas de roteamento para refletir qualquer mudança na topologia da rede, como adição ou remoção de dispositivos ou alterações nas rotas disponíveis;

4.28.5.2. Um aspecto crítico do gerenciamento de roteamento é garantir que as atualizações de rotas não sejam divulgadas inadvertidamente para redes externas ou para a internet, o que poderia levar a problemas de segurança ou congestionamento de tráfego. Para isso, o OPERADOR deve implementar técnicas de controle de tráfego, como filtros de saída e políticas de distribuição de rota, para restringir a divulgação de informações de roteamento apenas para os dispositivos autorizados na rede;

4.28.5.3. Além disso, é essencial que o OPERADOR esteja ciente dos critérios de disponibilidade da REDE METROPOLITANA ao fazer alterações nas tabelas de roteamento. Mudanças repentinas ou mal planejadas nas rotas podem impactar negativamente a disponibilidade dos serviços e a qualidade da comunicação na rede.

4.28.6. DISPONIBILIDADE DA REDE METROPOLITANA

4.28.6.1. A garantia da disponibilidade da REDE METROPOLITANA é fundamental para assegurar a continuidade das operações e serviços essenciais oferecidos pela rede. A disponibilidade contínua, 24 horas por dia, 7 dias por semana e 365 dias por ano, é um objetivo crítico para garantir que os cidadãos, empresas e órgãos governamentais possam acessar os recursos e informações necessários a qualquer momento;

4.28.6.2. Para alcançar esse nível de disponibilidade, é necessário adotar práticas de implementação de rede que minimizem os pontos únicos de falha e maximizem a resiliência da infraestrutura. Isso inclui a implementação de redundância em vários níveis da rede, como links de conexão, topologia em anel, dispositivos de rede e fontes de energia, garantindo que haja sempre rotas alternativas disponíveis em caso de falha;

4.28.6.3. Além disso, a monitorização constante da rede é essencial para identificar e resolver rapidamente quaisquer problemas que possam surgir. O uso de sistemas de monitoramento de rede automatizados, através do protocolo SNMP (Simple Network Management Protocol) e ferramentas de monitoramento de desempenho, permite aos administradores e operadores da rede detectem anomalias, e analisem as tendências de tráfego para tomada de medidas corretivas antes que ocorram interrupções significativas;

4.28.6.4. Para garantir a confiabilidade e o desempenho da Rede Metropolitana, fica estabelecido que a rede deva manter uma disponibilidade e velocidade mínima obrigatória de acordo com a Criticidade conforme tabela a seguir:

Tabela de Criticidade

Descrição	Criticidade	SLA (MÊS)
Node Core	0	99, 5 %
Node Anel	1	99, 0 %
Node Distribuição	2	98, 5 %
Node Hotspot	3	98, 0 %
Node Dispositvo IoT	4	97, 5 %

4.28.6.5. Se ocorrerem interrupções que excedam esse limite de tempo, o tempo de inatividade, será contabilizado integralmente no total geral das horas acumuladas de indisponibilidade;

4.28.6.6. É importante ressaltar que a disponibilidade e a velocidade dos NÓ (NODE) da rede são aspectos críticos para garantir a conectividade e o bom funcionamento dos serviços municipais. Portanto, é fundamental que sejam tomadas medidas proativas para minimizar o tempo de inatividade e garantir que os padrões de disponibilidade sejam atendidos;

4.28.6.7. Devem ser implementadas estratégias de monitoramento contínuo da rede, juntamente com procedimentos eficazes de manutenção preventiva, para identificar e resolver potenciais problemas antes que afetem significativamente a operação da rede. Isso inclui a realização de atualizações regulares e programadas de software, verificações de integridade dos equipamentos de rede, e planos de contingência bem definidos para lidar com falhas imprevistas;

4.29. A disponibilidade mensal da rede de dados para os NÓ (NODE) Regulares será calculada como:

4.29.1. Quando o node estiver abaixo da SLA conforme Tabela de Criticidade, será descontado o valor do ponto integralmente pelo período de competência, conforme relatório de disponibilidade e quantidade a ser emitido pela contratante e fiscalização do contrato em sistema da contratada com emissão de relatório a qualquer tempo como também quando houver em sistema da contratante.

4.30. **CENTRAL DE OPERAÇÕES – SUPORTE MULTICAMADAS À INFRAESTRUTURA DE REDE METROPOLITANA E REDES INTERNAS**

4.30.1. Gestão Integrada da Infraestrutura Lógica e Física

4.29.1.1. Com o objetivo de assegurar a continuidade, segurança, eficiência e qualidade dos serviços prestados, a OPERADORA será responsável pela operação, manutenção, suporte técnico e evolução da infraestrutura de rede física e lógica da Rede Metropolitana (MAN), bem como da infraestrutura lógica da rede interna legada (LAN) da Prefeitura Municipal de Balneário Camboriú;

4.29.1.2. Essa atuação integrada entre a rede interna e a rede metropolitana deverá garantir a interoperabilidade entre os sistemas, serviços e unidades públicas, promovendo maior eficiência operacional, agilidade na comunicação entre setores e melhoria na prestação de serviços públicos à população;

4.29.1.3. Toda a gestão deverá estar em conformidade com os princípios da **segurança da informação** — disponibilidade, integridade e confidencialidade — com base nas boas práticas dos frameworks **ITIL, ISO/IEC 27001 e ISO/IEC 20000**, compatíveis com a criticidade e complexidade do ambiente tecnológico da Administração Pública.

4.30.2. **Central de Operações (NOC) – Monitoramento, Segurança e Suporte Técnico**

4.30.2.1. A CONTRATADA deverá implantar e manter uma Central de Operações (NOC) no município de Balneário Camboriú, em endereço físico e fixo, a no máximo 15 km dos pontos concentradores da rede, obrigatoriamente conectada ao anel óptico bidirecional da Rede Metropolitana.

4.30.2.2. Essa Central deverá operar com equipe técnica exclusiva e infraestrutura completa de hardware, software e recursos de monitoramento, permitindo:

4.30.2.2.1. Monitoramento contínuo e em tempo real de todos os ativos de rede (switches, roteadores, access points, firewalls, servidores DNS, equipamentos GPON, etc.);

4.30.2.2.2. Gerenciamento de incidentes, problemas e mudanças segundo práticas ITSM;

4.30.2.2.3. Classificação de eventos conforme criticidade dos NÓs (Nodes) e SLAs estabelecidos;

4.30.2.2.4. Registro e atendimento de chamados por múltiplos canais (telefone, e-mail, sistema web, WhatsApp e chat);

4.30.2.2.5. Backups automatizados e versionamento de configurações com repositório controlado;

4.30.2.2.6. Elaboração e manutenção de documentação técnica atualizada e base de conhecimento acessível à equipe da Prefeitura.

4.30.2.3. Os firewalls definidos no projeto deverão estar integrados à estrutura de monitoramento da Central de Operações, atuando como ponto estratégico de controle de segurança, com funções de inspeção de tráfego, aplicação de políticas de segurança, auditoria de acessos e resposta a incidentes. Esses recursos, devidamente operados pela CONTRATADA, conferem à Central atribuições equivalentes a um Centro de Operações de Segurança (SOC), reforçando a proteção das redes contraameaças internas e externas;

4.30.2.4. A CONTRATADA será responsável pela administração das regras de segurança, alarmes, logs e configurações críticas. A cooperação com a equipe técnica da Prefeitura deverá ocorrer por meio de fluxos operacionais previamente definidos, respeitando os critérios de controle de acesso, gestão de risco e níveis autorizativos, estabelecendo um relacionamento técnico estruturado que promova confiabilidade e segurança;

4.30.3. **Suporte Técnico Nível 2 – Abrangência e Responsabilidades**

4.30.3.1. A equipe de Suporte Técnico Nível 2 atuará em conjunto com o Nível 1 e com a equipe técnica da Prefeitura, sendo responsável por:

4.30.3.1.1. Configuração, reconfiguração e análise de desempenho dos seguintes dispositivos:

4.30.3.1.1.1. Switches de core e borda;

4.30.3.1.1.2. Roteadores com protocolos OSPF e BGP;

4.30.3.1.1.3. Servidores DNS autoritativos;

4.30.3.1.1.4. Pontos de acesso Wi-Fi (indoor/outdoor);

4.30.3.1.1.5. Equipamentos legados e novos da rede municipal.

4.30.3.1.1.6. Implantação e manutenção da infraestrutura lógica da rede interna e sua interoperabilidade com a rede metropolitana;

4.30.3.1.1.7. Monitoramento e análise de performance da LAN e WAN, com resposta a falhas e degradações;

4.30.3.1.1.8. Gestão de mudanças, sugestões de melhorias e adequações técnicas;

4.30.3.1.1.9. Suporte direto em incidentes de média e alta complexidade, com elaboração de RCA (Root Cause Analysis);

4.30.3.1.1.10. Registro detalhado de todas as alterações e configurações realizadas, com versionamento;

4.30.3.1.1.11. Apoio à Divisão de TI da Prefeitura na execução de configurações específicas e ajustes operacionais.

4.30.4. Composição Mínima da Equipe Técnica da Central de Operações

4.30.4.1. A equipe deverá ser alocada exclusivamente ao projeto e composta, no mínimo, por:

Qtd	Cargo	Requisitos Técnicos
3	Analistas de Suporte Nível 1	Curso técnico ou superior (em curso) na área de TI.
2	Analistas de Suporte Nível 2	Certificações IPv6 Sage, WiFi, TCP/IP, OSPF, BGP, VLANs e fabricante dos equipamentos ofertados.
1	Técnico de Rede Externa Nível 2	NR-10, NR-35, OTDR, Power Meter, fusão de fibras, 2 anos de experiência comprovada.
2	Técnicos de Rede Externa Nível 1	NR-10, NR-35, 2 anos de experiência.
1	Gerente de Projetos	Graduação em Gestão de TI, experiência mínima de 2 anos.
1	Gerente Técnico Operacional	Graduação em Engenharia com foco em Telecomunicações, 2 anos de experiência.

Obs.: É vedado o acúmulo de funções por um mesmo profissional.

4.30.5. **Exclusividade Operacional e Governança Técnica**

4.30.5.1. Todos os sistemas utilizados para monitoramento, gestão de rede, helpdesk, segurança e visualização de desempenho deverão ser dedicados exclusivamente à Prefeitura Municipal de Balneário Camboriú, sem compartilhamento com outras localidades ou contratos;

4.30.5.2. A infraestrutura deverá operar integralmente dentro do território municipal, conforme definido no projeto técnico e seus anexos;

4.30.5.3. A CONTRATADA será responsável por prover o conhecimento técnico, os recursos e o suporte necessários para a manutenção da continuidade operacional, interoperabilidade entre redes e evolução tecnológica da infraestrutura pública, em cooperação com a equipe da Prefeitura.

4.31. ESPECIFICAÇÕES DAS INSTALAÇÕES E DOS SERVIÇOS

4.31.1. A empresa contratada deverá possuir instalações adequadas e completas de laboratório na cidade de Balneário Camboriú, para comportar seus técnicos, equipamentos e mobiliário adequado;

4.31.2. Os técnicos do contratado deverão possuir identificação (crachá) e vestuário (uniforme) padrão que permita sua identificação quando estiverem em atendimento nas unidades públicas municipais;

4.31.3. Os técnicos do contratado deverão estar capacitados para realizarem instalações de quaisquer tipos de software.

4.32. HORÁRIOS DE EXPEDIENTE

4.32.1. A contratada deverá seguir o horário padrão das 8h às 18h de segunda a sexta e, excepcionalmente, poderá ser solicitado mediante aviso prévio por parte da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO o atendimento em dia e horário extraordinários, tais como finais de semana e feriados;

4.32.2. A contratada deverá manter pelo menos 2 (dois) técnicos em regime de sobreaviso com disponibilidade para atender eventuais demandas emergenciais ou situações críticas que possam ocorrer fora do horário regular de trabalho. Devendo disponibilizar um número de telefone para este contato imediato.

4.32.3. Durante o período de sobreaviso, o funcionário deverá permanecer em seu domicílio, de forma a garantir sua prontidão para o atendimento às solicitações.

4.33. MONITORAMENTO E GERÊNCIA DA REDE

4.33.1. O OPERADOR compromete-se a disponibilizar um ambiente de atendimento e monitoramento integrado, equipado com todas as ferramentas necessárias para uma abordagem preditiva e proativa no gerenciamento de incidentes, agindo de forma ágil e eficiente na resolução de problemas. Este ambiente busca encurtar a distância entre os suportes de Nível 1 e Nível 2, para melhor atender aos usuários, além de facilitar o despacho de demandas;

4.33.2. Possuir ilha de atendimento e suporte, onde grupos de profissionais do contratado, dedicados ao atendimento e suporte ao usuário de infraestrutura de TI dentro dos níveis acordados, além do gerenciamento e gestão de requisições e incidentes. Deverá haver disponibilidade presencial do contingente suficiente de profissionais do contrato, com as e comprovadas qualificações para a execução do serviço;

4.33.3. O monitoramento será realizado de maneira visual e inteligente, empregando ferramentas gráficas e analíticas tanto de hardware quanto de software. A detecção de anomalias será realizada de forma abrangente, abarcando qualquer deformidade na estrutura de pacotes de rede transportados, que se incompatibilizem dos padrões e normas de integridade. Isso inclui a análise de oscilações de temperatura e desempenho dos equipamentos comutadores de dados e suas vias em toda a rede metropolitana;

4.33.4. Todos os eventos serão meticulosamente examinados, desde o tráfego de entrada e saída em dispositivos ativos na rede, até a identificação de protocolos, requisições, flags de rede, larguras de banda, gargalos, logs, potência de transmissão e indisponibilidades. Esse monitoramento abrangente visa identificar quaisquer elementos que possam impactar negativamente a integridade e a disponibilidade da informação;

4.33.5. Além disso, serão observados todos os padrões que possam indicar a presença de pragas virtuais, invasões, ataques de negação de serviço distribuído (DDoS) ou infecções por malware, frequentemente causadas por vírus, ransomwares ou falhas de segurança devido à imperícia dos usuários;

4.33.6. Para garantir a credibilidade e eficácia do ambiente de monitoramento, o OPERADOR deve seguir as melhores práticas e padrões reconhecidos internacionalmente. Isso inclui a utilização de tecnologias avançadas de análise de dados, inteligência artificial e machine learning para identificar e responder rapidamente a possíveis ameaças e anomalias na rede;

4.33.7. Além disso, a equipe de operadores é composta por profissionais altamente qualificados e certificados, com experiência sólida em segurança da informação e monitoramento de redes. O ambiente de trabalho será projetado para promover a colaboração e eficiência, com estações de trabalho ergonômicas e salas de reunião equipadas com recursos audiovisuais para discussões técnicas e tomada de decisões;

4.33.8. Em suma, o ambiente de atendimento e monitoramento integrado oferecido pelo OPERADOR deverá possuir uma combinação de tecnologia de ponta, expertise técnica e práticas de mercado robustas, garantindo a segurança, integridade e disponibilidade da rede em todos os momentos;

4.33.9. Na Central de Operações, é essencial que o operador disponibilize um ambiente altamente equipado para visualização e monitoramento eficiente de eventos, tráfego de rede e anomalias, facilitando a detecção rápida de incidentes. Para isso, deverá manter 6 displays de no mínimo 50 polegadas, cada um com resolução 4K. Este arranjo permite uma visão clara e detalhada de todos os mapas de rede, eventos e chamados técnicos;

4.33.10. A configuração proposta está alinhada com as práticas recomendadas por entidades globais como a ISO/IEC 27001, que enfatiza a importância da monitoração contínua e análise de eventos de segurança para a gestão eficaz de incidentes. Este setup permite não apenas a visualização, mas também a análise integrada de dados, essencial para uma resposta rápida e informada a incidentes de segurança ou operacionais;

4.33.11. A utilização de múltiplos displays de alta resolução facilita o trabalho colaborativo e a tomada de decisão em tempo real por parte das equipes de operações e segurança. Isso é crucial para manter a integridade e a performance da rede, garantindo uma operação resiliente e eficiente.

4.34. MONITORAMENTO ATIVO

4.34.1. O sistema deverá realizar a supervisão conjunta e integrada de banco de dados, serviços de e-mail, internet, e todos os componentes da infraestrutura de rede de fibra óptica municipal, incluindo dispositivos e serviços críticos, como switches, roteadores, OLTs, e outros equipamentos relevantes. O sistema deve ser capaz de fornecer uma visão unificada e em tempo real do status de todos esses componentes, permitindo a detecção e resposta imediata a falhas ou degradação de desempenho;

4.34.2. O monitoramento deve ser realizado sem o uso de agentes para sistemas operacionais Windows, Linux e MacOS, e incluir a capacidade de monitoramento de dispositivos de rede específicos sem necessidade de software adicional nos dispositivos monitorados, proporcionando assim uma maior facilidade de implementação e redução de custos operacionais;

4.34.3. Deve suportar a descoberta automática e visualização imediata de dispositivos na rede, com capacidade de mapeamento automático da topologia de rede, incluindo links e dependências entre dispositivos, e suporte à visualização gráfica dessas topologias em tempo real;

4.34.4. O sistema deve permitir a configuração de alertas predefinidos e personalizados, baseados em múltiplos critérios, como limites de utilização de banda, latência, perda de pacotes, disponibilidade de dispositivos e outros KPIs críticos para a operação da rede de fibra

óptica. Esses alertas devem ser configurados para garantir a rápida notificação das equipes de operação em caso de incidentes;

4.34.5. A notificação deve ser realizada via múltiplos canais, incluindo e-mail, SMS, Slack, solicitação HTTP, Microsoft Teams, notificações push, execução de scripts ou aplicativos, e mensagens para syslog. Além disso, deve ser possível configurar alertas baseados em horários específicos (horários de pico, manutenção programada, etc.), garantindo que as notificações sejam enviadas ao pessoal apropriado em tempo hábil;

4.34.6. O sistema deve permitir o agendamento automático de relatórios detalhados sobre o desempenho da rede, incluindo análise de tendências, status de dispositivos, alertas críticos e uso de recursos. Os relatórios devem ser configuráveis e enviados automaticamente para os administradores responsáveis em horários predefinidos;

4.34.7. Deve permitir a personalização completa de relatórios, com suporte para inclusão de logotipos, cabeçalhos personalizados, e formatação específica em HTML e PDF, garantindo que os relatórios atendam às necessidades de comunicação interna e externa da organização;

4.34.8. O sistema deve manter um registro detalhado de todas as atividades, incluindo monitoramento de eventos, alterações de configuração, respostas a incidentes e outras operações críticas, armazenando esses registros em arquivos seguros e acessíveis para auditoria e conformidade regulatória;

4.34.9. Deve permitir a abertura automática de tickets em sistemas internos de gerenciamento de incidentes (ITSM), com integração nativa ou via API com as principais plataformas de mercado, garantindo que todos os incidentes sejam rastreados e gerenciados conforme as melhores práticas de ITIL;

4.34.10. O sistema deve ser compatível com os principais protocolos de monitoramento e gestão de rede, incluindo SNMP, ICMP, WMI, HTTP, SSH, REST, OPC UA, garantindo ampla cobertura e suporte para dispositivos de rede, sistemas operacionais e serviços utilizados na infraestrutura de fibra óptica;

4.34.11. Deve suportar os protocolos de fluxo de rede NETFLOW, IPFIX, sFlow, jFlow, além de capacidades de sniffing para análise profunda de pacotes, permitindo o monitoramento detalhado do tráfego de rede, identificação de gargalos e análise de segurança;

4.34.12. O sistema deve ser capaz de monitorar o hardware, software, ambientes virtuais e aplicativos, incluindo compatibilidade com hypervisors populares (como VMware, Hyper-V) e plataformas de virtualização de redes (SDN/NFV), garantindo a monitorização integral da infraestrutura de TI;

4.34.13. Deve ser compatível com tecnologias e marcas reconhecidas no mercado, como Cisco, VMware, AWS (Amazon Web Services), Microsoft, NetApp, Oracle, Nutanix, HPE, Dell, Juniper, APC, Fujitsu, entre outras, assegurando interoperabilidade com a infraestrutura existente e futura da Rede Metropolitana;

4.34.14. Deve permitir a importação e integração de dados relacionados à propriedade e características dos componentes de rede, incluindo inventário automatizado e atualização contínua das informações sobre dispositivos de rede e suas configurações.

4.34.15. O sistema deve oferecer suporte a sensores API RESTful e personalizados, permitindo o monitoramento de aplicativos em nuvem, serviços SaaS, e outras soluções personalizadas, garantindo flexibilidade para atender às necessidades específicas da operação da rede óptica;

4.34.16. Deve realizar o monitoramento contínuo do registro de eventos (event logs), incluindo eventos de segurança, operação e performance, com suporte para retenção de logs e compliance com normativas como a LGPD (Lei Geral de Proteção de Dados) e outras regulatórias aplicáveis;

4.34.17. A interface do usuário deve estar disponível em português (Brasil), assegurando que todas as funcionalidades do sistema sejam plenamente acessíveis às equipes locais, incluindo opções de suporte e documentação técnica no idioma;

4.34.18. Deve possuir um editor de mapas interativo, com recursos de arrastar e soltar, permitindo a criação de dashboards individualizados e customizados, que possam refletir a topologia da rede, status de dispositivos e outras métricas em tempo real, facilitando a gestão proativa da rede;

4.34.19. O sistema deve ser capaz de gerar relatórios integrados, com saídas em formatos HTML, PDF e CSV, permitindo a distribuição fácil e rápida das informações críticas aos stakeholders e partes interessadas;

4.34.20. Deve possuir aplicativos móveis para dispositivos Android e iOS, com suporte completo para o monitoramento remoto da rede, envio de alertas e visualização de dashboards, garantindo que a equipe de operação tenha acesso às informações críticas em qualquer lugar;

4.34.21. Deve incluir uma interface web interativa para acesso via internet, compatível com as versões atuais de navegadores como Chrome, Firefox e Edge, assegurando uma experiência de usuário segura e consistente, independentemente do dispositivo de acesso;

4.34.22. O sistema deve incluir um aplicativo desktop que suporte multivisualização de instalações distintas, permitindo a gestão centralizada de múltiplos sites ou sub-redes dentro da infraestrutura municipal;

4.34.23. Deve integrar um banco de dados próprio, sem a necessidade de um SGBD externo, com suporte para replicação, backup e failover, garantindo alta disponibilidade e confiabilidade dos dados monitorados;

4.34.24. O sistema deve suportar o monitoramento de histórico de dados armazenados em intervalos originais (dados brutos), sem consolidação, permitindo análises detalhadas e precisas do desempenho da rede ao longo do tempo;

4.34.25. Deve incluir recursos nativos de failover de cluster, com suporte para alta disponibilidade e continuidade de negócios, garantindo que o sistema continue operando mesmo em caso de falhas ou desastres;

4.34.26. O sistema deve ser compatível com todas as versões do Windows atualmente suportadas pela Microsoft, garantindo ampla cobertura e suporte para ambientes heterogêneos;

4.34.27. A interface web deve ser compatível com as versões mais recentes dos principais navegadores, como Chrome, Firefox, e Edge, garantindo uma experiência de usuário moderna e sem falhas;

4.34.28. O sistema deve ser fornecido com todas as licenças necessárias para a operação plena dentro do ambiente municipal, com suporte técnico especializado disponível em português (Brasil) e conforme as normas vigentes no país;

4.34.29. O fornecedor deve garantir que o sistema esteja em conformidade com todas as regulamentações locais e internacionais aplicáveis, incluindo, mas não se limitando a normas de segurança de TI, proteção de dados pessoais e regulamentos de redes de telecomunicações.

4.35. GESTÃO DE ATENDIMENTOS E INVENTÁRIO DE REDE

4.35.1. A operadora deverá fornecer aos usuários um sistema de Helpdesk baseado na web, que permita uma comunicação imediata, intuitiva e eficiente. Este sistema será responsável por registrar de forma estruturada e automatizada todas as solicitações relacionadas a incidentes, problemas, manutenções e novas instalações. Além disso, deverá facilitar a criação e a gestão de uma base de conhecimento abrangente, documentando o histórico de ocorrências e gerenciando o inventário de ativos e passivos da rede, com capacidade para rastrear e auditar mudanças de configuração, garantindo conformidade e segurança.

4.35.2. O Sistema deverá oferecer no mínimo as seguintes funcionalidades básicas:

4.35.2.1. Ser integrado por meio de API RESTful, utilizando scripts de integração que realizem chamadas à API para transferir informações de tickets, usuários, ativos, entre outros, sincronizando a criação, atualização e fechamento de tickets entre o sistema ofertado pela operadora e o sistema de Helpdesk da Prefeitura Municipal. Essa integração deve assegurar que ambos os sistemas possam acompanhar o ciclo de vida completo do chamado técnico, permitindo um fluxo de informações contínuo e consistente;

4.35.2.2. Suporte à abertura de chamados multicanais (web, chat, aplicativo móvel, e-mail, WhatsApp, telefone), permitindo que os usuários escolham o canal mais conveniente para suas necessidades. Essa funcionalidade deve ser complementada por notificações automáticas e atualizações de status em tempo real;

4.35.2.3. Integração com o sistema de monitoramento ativo da central de operações, automatizando a abertura de ocorrências baseadas em alertas de desempenho ou falhas detectadas na infraestrutura de rede, garantindo uma resposta rápida e eficiente a incidentes críticos;

4.35.2.4. Capacidade de criação de dashboards personalizados, permitindo a priorização de chamados e visualização de métricas relevantes de acordo com as necessidades operacionais e estratégicas do projeto;

4.35.2.5. Permitir a criação de indicadores de desempenho (KPIs) personalizáveis, alinhados às metas do projeto, garantindo que a gestão possa acompanhar e melhorar continuamente a eficiência operacional e a satisfação dos usuários;

4.35.2.6. Suporte ao agendamento de chamados, permitindo que os usuários programem atendimentos para horários específicos, conforme a disponibilidade e necessidades operacionais;

4.35.2.7. Funcionalidade para reabertura de chamados, assegurando que incidentes não resolvidos ou recorrentes possam ser tratados de maneira contínua sem a necessidade de iniciar um novo processo de registro;

4.35.2.8. Suporte à abertura de chamados diretamente da área de trabalho do usuário, por meio de um agente específico que permita essa ação com um único clique, simplificando o processo de solicitação de suporte;

4.35.2.9. Configuração, implementação e gerenciamento de Acordos de Nível de Serviço (SLAs) definidos no TERMO DE REFERÊNCIA, com monitoramento automático do cumprimento dos SLAs e geração de relatórios de conformidade;

4.35.2.10. Funcionalidade de base de conhecimento integrada, permitindo que soluções a problemas comuns sejam documentadas e acessadas rapidamente tanto por técnicos quanto por usuários finais, reduzindo o tempo de resolução de chamados e melhorando a autossuficiência dos usuários;

4.35.2.11. Ferramenta nativa de acesso remoto, permitindo que técnicos se conectem aos dispositivos dos usuários para resolução de problemas de forma eficiente e segura, com suporte para múltiplos sistemas operacionais;

4.35.2.12. Funcionalidade de interação por voz em chamados, facilitando a comunicação direta e imediata entre usuários e técnicos, melhorando o entendimento e a resolução de problemas;

4.35.2.13. Ferramenta de escaneamento de rede, capaz de detectar dispositivos conectados, verificar o status de ativos, monitorar links e gerar relatórios de desempenho e disponibilidade, contribuindo para a gestão proativa da infraestrutura de rede;

4.35.2.14. Recurso de geolocalização para dispositivos e locais de atendimento, possibilitando a visualização de onde os atendimentos estão sendo realizados em um mapa, facilitando a gestão de equipes de campo e priorização de atendimentos;

4.35.2.15. Possibilidade de personalização de alertas, permitindo que os administradores configurem notificações específicas para diferentes tipos de incidentes, conforme a criticidade e a necessidade operacional.

4.36. SUPORTE TÉCNICO

4.36.1. O Suporte Técnico compreende todas as ações realizadas por profissionais altamente qualificados e especializados no objeto do contrato, podendo ser executadas remotamente ou presencialmente nas Unidades do MUNICÍPIO. O objetivo dessas ações é identificar, solucionar e prevenir problemas, garantindo a continuidade dos serviços e minimizando impactos operacionais;

4.36.2. Para garantir a eficácia do Suporte Técnico, o processo de resposta a incidentes será gerenciado e medido de acordo com os Acordos de Nível de Serviço (SLAs). Cada incidente será classificado por sua criticidade, com parâmetros claros para tempo de resposta, tempo de resolução e tempo de inatividade tolerado, conforme a tabela a seguir:

Tipo de Node	Nível de Criticidade	SLA (%)	Tempo de Resposta	Tempo de Resolução	Tempo Inativo Tolerado (horas/mês)
CORE	0	>= 99, 5%	10 minutos	30 minutos	3, 6 horas

ANEL	1	>= 99, 0%	15 minutos	1 hora	7, 2 horas
DISTRIBUIÇÃO	2	>= 98, 5%	30 minutos	4 horas	10, 8 horas
HOTSPOT	3	>= 98, 0%	45 minutos	6 horas	14, 4 horas
DISPOSITIVOS IoT	4	>= 97, 5%	1 hora	8 horas	18, 0 horas

4.36.3. Para gerenciar e medir efetivamente o cumprimento dos SLAs, o processo de resposta a incidentes deve ser estruturado de acordo com as seguintes diretrizes, alinhadas às melhores práticas de mercado:

4.36.3.1. **Classificação de Incidentes:** Todos os incidentes devem ser rapidamente avaliados e classificados com base no seu impacto operacional e na criticidade do serviço afetado. A criticidade define a prioridade de atendimento, tempo de resposta e resolução necessários;

4.36.3.2. **Monitoramento Proativo:** Implementar um sistema de monitoramento contínuo que permita a identificação precoce de potenciais falhas e incidentes, antes mesmo que os usuários sejam impactados, permitindo uma intervenção rápida e eficiente;

4.36.3.3. **Escalonamento Automático:** Deve haver um processo automático de escalonamento que encaminhe incidentes não resolvidos dentro dos prazos estabelecidos para níveis superiores de suporte, garantindo que problemas críticos recebam a atenção adequada sem atrasos;

4.36.3.4. **Comunicação Efetiva:** Manter uma comunicação contínua e transparente com os usuários durante todo o ciclo de vida do incidente, informando sobre o status, ações tomadas e estimativas de tempo para resolução;

4.36.3.5. **Relatórios de SLA:** Relatórios detalhados devem ser gerados periodicamente para monitorar o desempenho do suporte técnico em relação aos SLAs acordados, identificando áreas para melhoria e garantindo a conformidade com os requisitos contratuais;

4.36.3.6. **Capacitação Contínua:** Os profissionais envolvidos no suporte devem participar regularmente de treinamentos e atualizações para garantir que estejam familiarizados com as tecnologias mais recentes e as melhores práticas de atendimento.

4.36.4. A adoção dessas práticas não apenas assegura o cumprimento dos SLAs, mas também promove a excelência no atendimento e a satisfação dos usuários, mantendo a operação da rede eficiente e minimizando interrupções que possam impactar os serviços essenciais fornecidos pelo MUNICÍPIO.

4.37. DESCRIÇÃO DOS NÍVEIS DE CRITICIDADE

4.37.1. **Criticidade 0:** Nodes de máxima importância, onde qualquer falha pode causar impacto crítico imediato nas operações. Esses nodes são essenciais para a continuidade do serviço e demandam tempos de resposta e resolução extremamente rápidos;

4.37.2. **Criticidade 1:** Nodes essenciais para operações críticas do negócio. A falha nesses nodes pode causar impacto significativo, mas não tão imediato quanto os de criticidade 0;

4.37.3. **Criticidade 2:** Nodes importantes, mas com menor impacto imediato. A falha pode ser tolerada por um período curto sem causar grandes interrupções;

4.37.4. **Criticidade 3:** Nodes de importância moderada. A falha pode ser tolerada por um período mais longo sem causar interrupções críticas;

4.37.5. **Criticidade 4:** Nodes de menor criticidade, com impacto mínimo nas operações. A falha pode ser tolerada por um período mais longo sem causar grandes interrupções.

4.38. DEFINIÇÕES

4.38.1. **Tempo de Resposta:** Tempo máximo para iniciar o atendimento após a abertura do chamado. Este tempo é crucial para garantir que o problema seja identificado e tratado rapidamente;

4.38.2. **Tempo de Resolução:** Tempo máximo para resolver o problema após a abertura do chamado. Este tempo inclui todas as etapas necessárias para restaurar o serviço ao seu estado normal;

4.38.3. **Tempo Inativo Tolerado:** Quantidade máxima de tempo por mês que o serviço pode ficar inativo sem violar o SLA. Este valor é calculado com base no percentual de SLA e representa a tolerância máxima para inatividade.

4.39. DETALHES TÉCNICOS ADICIONAIS PARA CONSIDERAÇÃO DE FALHAS

4.39.1. **Monitoramento Proativo:** Implementação de sistemas de monitoramento proativo para detectar e alertar sobre falhas antes que elas afetem os usuários finais;

4.39.2. **Redundância:** Uso de redundância em nodes críticos para garantir que, em caso de falha, o serviço possa ser mantido por meio de um sistema alternativo;

4.39.3. **Manutenção Preventiva:** Programação de manutenção preventiva regular para minimizar o risco de falhas inesperadas;

4.39.4. **Escalonamento de Suporte:** Definição de um processo claro de escalonamento para garantir que problemas críticos sejam rapidamente levados ao conhecimento de equipes de suporte de nível superior.

4.39.5. Os prazos estão alinhados com os padrões de atendimento estabelecidos nos Acordos de Nível de Serviço (SLAs), garantindo uma resposta rápida e eficiente para minimizar o impacto dos incidentes na operação do sistema. Essa agilidade é fundamental para assegurar a continuidade dos serviços e a satisfação do usuário final.

4.40. ACOMPANHAMENTO DOS CHAMADOS

4.40.1. **Aberto:** Nesta fase, o chamado é registrado no sistema de Service Desk, porém ainda não foi atribuído a um técnico específico para resolução. Este estágio marca o início do ciclo de vida do chamado.

4.40.2. **Atribuído:** Após o registro, o chamado é designado a um técnico ou equipe responsável. Neste estágio, ocorre o levantamento de requisitos e a coleta de informações relevantes necessárias para o início do atendimento.

4.40.3. **Em andamento:** Aqui, o técnico responsável pelo chamado está ativamente engajado na resolução do problema. Este estágio é caracterizado pela execução das ações necessárias para solucionar o incidente ou atender à solicitação do usuário.

4.40.4. **Pendente:** Se o chamado requer informações adicionais, autorização do usuário ou outros pré-requisitos antes que o trabalho possa ser retomado, ele entra neste estado temporário de espera. O chamado permanece pendente até que esses requisitos sejam atendidos.

4.40.5. **Aguardando usuário:** Nesta fase, o técnico aguarda uma resposta ou ação por parte do usuário antes de continuar o trabalho no chamado. Isso pode incluir aguardar a confirmação de que uma solução proposta está funcionando corretamente ou aguardar feedback adicional do usuário. No caso de houver interação por parte do usuário no ticket ou requisição num prazo máximo de 5 dias uteis o chamado será fechado automaticamente;

4.40.6. **Resolvido:** Após a conclusão bem-sucedida da resolução do problema, o chamado é marcado como resolvido. Isso significa que o incidente foi solucionado e está pronto para ser fechado;

4.40.7. **Fechado:** Finalmente, quando todas as etapas do processo de atendimento foram concluídas e o usuário está satisfeito com a solução fornecida, o chamado é oficialmente fechado. Este é o estágio final do ciclo de vida do chamado, marcando o encerramento formal do incidente ou solicitação.

4.41. SERVIÇOS DE HOTSPOT

4.41.1. CONEXÃO WI-FI EM UNIDADES ADMINISTRATIVAS E ESPAÇOS PÚBLICOS

4.41.1.1. Os serviços de conexão Wi-Fi (Hotspot) serão disponibilizados através de um conjunto integrado de hardware e software para gestão e controle de acesso. Estes serão implantados em nodes internos (indoor) nas unidades administrativas, bem como em nodes outdoor (Hotspots) em espaços públicos, como praças, calçadões e orlas marítimas;

4.41.1.2. Os pontos de acesso deverão ser interconectados a Rede Metropolitana de fibra óptica, utilizando blocos de IPs do ASN da Prefeitura de Balneário Camboriú para garantir a identificação e rastreabilidade das conexões;

4.41.1.3. É obrigatório o fornecimento de todos os equipamentos, peças, acessórios e cabeamento necessários para a implementação e manutenção da rede Wi-Fi, incluindo poste padrão de energia da Concessionária local (CELESC). Ademais, será necessário prover um sistema de controle de acesso conforme as localidades especificadas no TERMO DE REFERÊNCIA.

4.41.2. PLACAS DE IDENTIFICAÇÃO DE PONTOS DE ACESSO WIFI

4.41.2.1. **Nos espaços internos:** Deverão ser instalados no mínimo 2 (duas) placas de identificação em locais que a DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO irá informar e as mesmas deverão serem construídas em material ACM com medidas especificadas em 210 mm x 290 mm e no mínimo 3 mm de espessura, confeccionadas com lâminas de alumínio de mínimo 0, 21mm;

4.41.2.2. **Nos espaços externos:** Deverão ser instalados no mínimo 2 (duas) placas de identificação por AP instalado em locais que a DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO irá informar e as mesmas deverão serem construídas em material ACM com medidas especificadas em 300 mm x 420 mm e no mínimo 3 mm de espessura, confeccionadas com lâminas de alumínio de mínimo 0, 21mm;

4.41.2.3. **Material gráfico:** Referente as placas de sinalização deverão ser entregues de acordo com o manual de marcas da Prefeitura Municipal e arte fornecida pela área competente do município.

4.41.3. SISTEMA DE CONTROLE DE ACESSOS DO TIPO WIFI-HOSPOT

4.41.3.1. Permitir o acesso à Internet através de autenticação prévia;

4.41.3.2. Para realizar o acesso, o software deverá exigir que o usuário insira seus dados pessoais;

4.41.3.3. O Software deverá permitir limitar a velocidade e o tempo de navegação, exigindo novo login após o tempo definido;

4.41.3.4. Após o login, o Software deverá permitir direcionar os usuários a URLs específicas;

4.41.3.5. O software deverá possuir interface de gestão em nuvem, permitindo gerenciar configurações, exibir gráficos e emitir relatórios;

4.41.3.6. Toda a base de dados da Solução do portal deverá ser armazenada em nuvem;

4.41.3.7. Todos os recursos computacionais do projeto serão alocados no Brasil, provendo desta forma baixa latência e menor tempo de resposta;

4.41.3.8. A interface de gerência deve permitir a criação de usuários administradores com permissões de acesso customizadas;

4.41.3.9. A Solução deverá ser fornecida licenciada para utilização dos APS de forma simultâneas;

4.41.3.10. Deve estar em conformidade com o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD);

4.41.3.11. Deve ser compatível com a Controladora Wireless e Access Points propostos pela empresa contratada e o parque legado de pontos acesso wireless da Prefeitura Municipal, sendo em sua grande maioria Ubiquiti e Intelbras;

4.41.3.12. Deve possuir recurso de mapa de calor, exibindo de forma dinâmica em mapa interativo os Access Points e a representação da quantidade de dispositivos conectados em cada um deles;

4.41.3.13. Deve armazenar estatísticas dos usuários que usam a plataforma, coletando no mínimo os seguintes dados: idade do usuário, gênero, localização e frequência de uso da rede;

4.41.3.14. A solução deverá enriquecer o perfil do usuário à medida que mais acessos são feitos;

4.41.3.15. A solução também deve personalizar a navegação de acordo com o local de instalação do Access Point;

4.41.3.16. A solução deve permitir o envio de campanhas e pesquisas de forma global ou direcionada para os usuários que se conectarem;

4.41.3.17. Deve permitir integração com bases de dados externas;

4.41.3.18. Deve ser configurado um método de autenticação para os usuários que desejam acessar a rede. Isso pode incluir autenticação baseada em senha, autenticação de rede social, autenticação baseada em SMS ou outras opções de autenticação. A autorização também é configurada para permitir ou negar o acesso a determinados recursos ou serviços com base nas credenciais do usuário;

4.41.3.19. A página de login deve ser personalizada para corresponder à identidade visual desejada. Ela pode incluir logotipos, cores, texto e outras informações relevantes;

4.41.3.20. Quando os usuários se conectarem à rede, eles são redirecionados automaticamente para o portal de autenticação;

4.41.3.21. O portal de autenticação permitirá ser integrado a sistemas existentes, como um servidor de autenticação central ou um sistema de gerenciamento de usuários;

4.41.3.22. Registros de log completos com IP, cadastro do usuário por cpf, mac address e data/hora;

4.41.3.23. Relatórios completos com filtros: histórico (visitantes, navegação), dias com mais visitas, páginas mais visitadas, download, upload, visitantes online, visitantes com acessos recorrentes, visitantes cadastrados por dia, densidade por Ap, relatório por campanha, devem ser exportados em formatos csv, ou xls, ou pdf;

4.41.3.24. O Monitoramento do serviço deverá ser 24 horas por dia, 7 dias da semana e 365 dias por ano;

4.41.3.25. O Backup será de responsabilidade da Contratada onde o mesmo deverá ser mantido por 365 dias;

4.41.3.26. O armazenamento do backup realizado em serviços específicos com disponibilidade e durabilidade de 99.99%;

4.41.3.27. Cadastro próprio de usuário, independentemente de Facebook, Google e etc. - através de Captive Portal, com as seguintes informações: Nome completo, CPF (com algoritmo de validação para CPF), data de nascimento, contatos de telefone e e-mail (com algoritmo para validar o número de telefone por código enviado por SMS ou o e-mail, por envio de link de confirmação), cadastro de senha;

4.41.3.28. Permitir exibição de mídia externa servidas por servidores de mídia nos formatos VAST/VPAID;

4.41.3.29. Não deverá permitir múltiplos cadastros com o mesmo CPF ou E-mail;

4.41.3.30. Bloqueio de usuários e dispositivos;

4.41.3.31. Pesquisa de satisfação personalizada;

4.41.3.32. Inserir e customizar termo de uso;

4.41.3.33. Idiomas: Português - Brasil, Inglês e Espanhol;

4.41.3.34. Layout responsivo, (dispositivos móveis e desktop);

4.41.3.35. RADIUS Authentication e Accounting. Deverá suportar servidor de autenticação RADIUS redundante, isto é, na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;

4.41.3.36. Deverá permitir o Accounting do servidor RADIUS, inclusive com suporte ao parâmetro Framed-IP-Address, permitindo a identificação de um usuário e seu respectivo endereço IP associado;

4.41.3.37. Deverá suportar RADIUS CoA (Dynamic Change of Authorization);

4.41.3.38. Login único (SSO) via Microsoft Azure AD, Entra ID, Google Workspace, Google for Education;

4.41.3.39. Deverá permitir autenticação via Voucher, definido pelo Cliente, de forma que possa autorizar o acesso por meio de um código previamente definido, com opção de impressão para distribuição de senhas ao público;

4.41.3.40. A solução deverá permitir que o administrador cadastre manualmente um determinado dispositivo/usuário;

4.41.3.41. Os Data Centers devem possuir certificações ISO 27001, SSAE-16, SOC 1, 2 e 3. Além disso, devem possuir um SLA (Service Level Agreement) de 99.9% de disponibilidade da rede;

4.41.3.42. Os Data Centers devem possuir certificações ISO 27001 e SSAE 16 (ou SSAE 18);

4.41.3.43. Além disso, devem possuir um SLA (Service Level Agreement) de 99.9% de disponibilidade da rede;

4.41.3.44. Possui cadastro único, o usuário deverá ser reconhecido automaticamente na segunda conexão;

4.41.3.45. Exigir que o usuário aceite/concorde com o “Termo de Uso da Rede” e termo de Cadastro em conformidade com a LGPD;

4.41.3.46. Deve disponibilizar pelo menos 03 (três) níveis de acesso à Console de Gerenciamento Web;

4.41.3.47. A contratada deverá disponibilizar, através da solução fornecida, no mínimo, os seguintes relatórios:

4.41.3.47.1. Total de visitas do dia;

4.41.3.47.2. Tempo médio de conexão;

4.41.3.47.3. Total de tráfego de dados no mês (visível por download e upload);

4.41.3.47.4. Total de sessões no mês;

4.41.3.47.5. Tráfego médio por usuário único;

4.41.3.47.6. Tráfego médio por sessão;

4.41.3.47.7. Total de sessões por dia;

4.41.3.47.8. Tráfego por ponto de acesso;

4.41.3.47.9. Quantidade de sessões;

4.41.3.47.10. Histórico de tráfego mensal;

4.41.3.47.11. Histórico de sessões diárias;

4.41.3.47.12. Informações de Acessos do Mês;

4.41.3.47.13. Quantidade de visitantes online em tempo real;

4.41.3.47.14. Aniversariantes;

4.41.3.47.15. Ranking de visitantes que mais trafegam dados por período;

4.41.3.47.16. Ranking de visitantes que mais tempo ficam conectados por período;

4.41.3.47.17. Ranking de visitantes que mais se conectaram por período;

4.41.3.47.18. A solução deverá permitir a definição de horário de funcionamento da rede WiFi.

4.41.4. A solução deverá permitir que todos os pontos de acesso sejam agrupados em grupos e subgrupos, possibilitando a visualização desses de forma organizada;

4.41.5. A solução deverá possibilitar o gerenciamento de campanhas, definições de regras de cadastro/acessos, bem como geração de relatórios, podem ser referentes a um ponto específico, ou simultaneamente a um grupo;

4.41.6. A solução deverá permitir pesquisar visitantes por formulário com dados cadastrais;

4.41.7. A solução deverá permitir editar dados cadastrais do visitante;

4.41.8. A solução deverá permitir apresentar o histórico de acessos do visitante;

4.41.9. A solução deverá possuir a gestão que identifique as campanhas visualizadas

4.41.10. A solução deverá permitir gerenciar campanha por vídeo (upload do arquivo);

4.41.11. A solução deverá permitir gerenciar campanha por banner (upload do arquivo);

4.41.12. A solução deverá possibilitar a opção para iniciar, pausar e finalizar campanha;

4.41.13. A solução deverá permitir que as perguntas possam ser indexadas e condicionadas a respostas anteriores do usuário (fluxograma sequencial de enquetes);

4.41.14. A solução deverá possibilitar a definição para data/hora início e fim automático de campanha;

4.41.15. A solução deverá permitir redirecionar usuário a um site após autenticação;

4.41.16. A solução deverá permitir a definição de tempo limite de navegação diária por usuário;

4.41.17. A solução deverá permitir a opção de alteração de senha por e-mail;

4.41.18. Deverá possuir portal de autosserviço que permita que os próprios usuários visitantes da rede sem fio façam a solicitação de acesso por meio de preenchimento de formulários (selfregistration), com possibilidade de aprovação manual realizada por operadores credenciados no sistema.

4.41.19. CONFIGURAÇÕES MINIMAS PARA EQUIPAMENTOS NAS CELULAS DE WIFI

4.41.20. INDOOR

4.41.20.1. Ponto de Acesso de rede Wireless de sexta geração - WI-FI 6 (802.11ax);

4.41.20.2. Permitir funcionamento em modo gerenciado por controladora WLAN física ou virtual, podendo ela ser instalada tanto em nuvem como on premise para configuração de seus parâmetros wireless, VLAN, gerenciamento de políticas de segurança, QoS e monitoramento de RF;

4.41.20.3. Access point dual radio 802.11ax, com suporte a operação em 2.4GHz e 5GHz, contendo 2 x 2 (MU-MIMO e OFDMA) em 2.4GHz e 2 x 2 (MU-MIMO e OFDMA) em 5 GHz;

4.41.20.4. Permitir simultaneamente usuários em 2.4 GHz e 5 GHz com largura de canal de 160Mhz;

4.41.20.5. Suportar velocidade de 574 mbps em modo 2.4GHz e 2402 mbps em modo 5GHz;

4.41.20.6. Possuir 01 Porta Gigabit Ethernet (RJ-45) 100/1000Mbps e 01 Porta Combo SFP Multi Gigabit 2,5G;

4.41.20.7. Possuir alimentação via padrão PoE 802.3af PoE através de uma única interface de rede, sem perda de funcionalidades e de desempenho;

4.41.20.8. Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/b/g/n/ac/ax com padrão de irradiação omnidirecional e ganho mínimo por antena de 5.0 dbi para 2.4 GHz e 5.0 dbi para 5.0 GHz;

4.41.20.9. Possuir potência de transmissão superior à 26 dBm em 2.4 GHz e 26 dBm em 5.0 GHz;

4.41.20.10. Suportar protocolo IPv4/IPv6;

4.41.20.11. Implementar VLANs conforme padrão 802.1q;

4.41.20.12. Permitir restrição de banda por usuário (QoS);

4.41.20.13. Suportar isolamento de tráfego para visitantes;

4.41.20.14. Permitir a criação de 32 SSID;

4.41.20.15. Possuir a funcionalidade Beamforming;

4.41.20.16. Suportar a tecnologia Load Balance;

4.41.20.17. Suportar a funcionalidade de band steering;

4.41.20.18. Suportar a tecnologia Reboot Schedule;

4.41.20.19. Suportar capacidade máxima de até 1024 clientes/dispositivos associados simultaneamente;

4.41.20.20. Consumo máximo de 13W;

4.41.20.21. Possuir no mínimo 01 (um) led multicolorido indicativo do estado de operação do equipamento;

4.41.20.22. Temperatura de Operação -10°C até 50°C;

4.41.20.23. Suportar os padrões de segurança WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3);

4.41.20.24. Implementar, em conjunto com a controladora wlan, padrões abertos de gerência de rede SNMP v1, v2c e v3, incluindo a geração de traps;

4.41.20.25. Suportar o padrão 802.1x;

4.41.20.26. Suportar os padrões de Roaming 802.11k/v/r;

4.41.20.27. Suportar Roaming de camada 3;

4.41.20.28. Permitir a configuração de contas RADIUS;

4.41.20.29. Possuir conectividade bluetooth 5.1.

4.41.21. CONFIGURAÇÕES MINIMAS PARA EQUIPAMENTOS NAS CELULAS DE WIFI OUTDOOR

4.41.21.1. Ponto de Acesso de rede Wireless de sexta geração - WI-FI 6 (802.11ax).

4.41.21.2. Permitir funcionamento em modo gerenciado por controladora WLAN física ou virtual, podendo ela ser instalada tanto em nuvem como on premise para configuração de seus parâmetros wireless, VLAN, gerenciamento de políticas de segurança, QoS e monitoramento de RF;

4.41.21.3. Access point dual radio 802.11ax, com suporte a operação em 2.4GHz e 5GHz, contendo 2 x 2 (MU-MIMO e OFDMA) em 2.4GHz e 2 x 2 (MU-MIMO e OFDMA) em 5 GHz;

4.41.21.4. Permitir simultaneamente usuários em 2.4 GHz e 5 GHz;

4.41.21.5. Suportar velocidade de 574 mbps em modo 2.4GHz e 2402 mbps em modo 5GHz;

4.41.21.6. Possuir 01 Porta Gigabit Ethernet (RJ-45) suportando PoE af/at, 01 porta SFP Gigabit 1000Mbps e 01 porta RJ45 console para gerenciamento;

4.41.21.7. Possuir alimentação via padrão PoE 802.3af PoE através de uma única interface de rede, sem perda de funcionalidades e de desempenho;

4.41.21.8. Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/b/g/n/ac/ax com padrão de irradiação omnidirecional e ganho mínimo por antena de 3.5 dbi para 2.4 GHz e 5.5 dbi para 5.0 GHz;

4.41.21.9. Possuir potência minima de transmissão de 28 dBm em 2.4 GHz e 25 dBm em 5.0 GHz;

4.41.21.10. Possuir conectividade bluetooth 5.0;

4.41.21.11. Possuir potência máxima de transmissão bluetooth de 10dBm

4.41.21.12. Suportar os protocolos IPv4 e IPv6 simultaneamente;

4.41.21.13. Implementar VLANs conforme padrão 802.1q;

4.41.21.14. Permitir restrição de banda por usuário (QoS);

4.41.21.15. Suportar isolamento de tráfego para visitantes;
4.41.21.16. Permitir a criação de 32 SSID;
4.41.21.17. Possuir certificação IP68 e proteção anti-corrosão;
4.41.21.18. Possuir a funcionalidade Beamforming;
4.41.21.19. Suportar a tecnologia Load Balance;
4.41.21.20. Suportar a funcionalidade de band steering;
4.41.21.21. Suportar a tecnologia Reboot Schedule;
4.41.21.22. Suportar no mínimo 1024 clientes/dispositivos associados simultaneamente;
4.41.21.23. Consumo máximo de 13W;
4.41.21.24. Possuir no mínimo 01 (um) led multicolorido indicativo do estado de operação do equipamento;
4.41.21.25. Suportar os padrões de segurança WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3);
4.41.21.26. Implementar, em conjunto com a controladora wlan, padrões abertos de gerência de rede SNMP v1, v2c e v3, incluindo a geração de traps;
4.41.21.27. Suportar o padrão 802.1x;
4.41.21.28. Suportar os padrões de Roaming 802.11k/v/r;
4.41.21.29. Suportar Roaming de camada 3;
4.41.21.30. Permitir a configuração de contas RADIUS.

4.41.22. CONCENTRADOR PARA GERENCIAMENTO DE HOTSOPT

4.41.22.1. Deve possuir pelo menos 2 portas Ethernet 10G SFP+.
4.41.22.2. Deve possuir pelo menos 4 portas Ethernet 1G/2.5G Base-T.
4.41.22.3. Deve possuir pelo menos 4 portas Ethernet 10/100/1000 Base-T.
4.41.22.4. Deve suportar no máximo 9 portas WAN.
4.41.22.5. Deve suportar uma taxa de transferência de pelo menos 4 Gbps com pacotes de 1518 bytes, com NAT+Auditoria.
4.41.22.6. Deve suportar pelo menos 1500 clientes LAN concorrentes.
4.41.22.7. Deve suportar pelo menos 1000 clientes PPPoE quando operando como servidor PPPoE.
4.41.22.8. Deve suportar uma taxa de transferência IPSEC VPN de pelo menos 900 Mbps.
4.41.22.9. Deve suportar pelo menos 1000 túneis IPSEC VPN.
4.41.22.10. Deve possuir pelo menos 4 GB de RAM.
4.41.22.11. Deve possuir pelo menos 128 MB de Nand Flash.
4.41.22.12. Deve possuir pelo menos 8 GB de EMMC.
4.41.22.13. Deve suportar disco rígido SATA3.0 de 2,5 polegadas.
4.41.22.14. Não possuir ventoinha para refrigeração.
4.41.22.15. Deve suportar OSPF v2/v3.
4.41.22.16. Deve suportar RIP/RIPng.
4.41.22.17. Deve suportar Roteamento baseado em Políticas (PBR).
4.41.22.18. Deve suportar balanceamento de carga WAN.
4.41.22.19. Deve suportar modo de interface ativa/espera na falha da porta WAN.
4.41.22.20. Deve suportar balanceamento de carga baseado no IP de origem.
4.41.22.21. Deve suportar balanceamento de carga baseado em sessão.

4.41.22.22. Deve suportar balanceamento de carga em tempo real baseado em carga.

4.41.22.23. Deve suportar IPSec VPN Servidor/Cliente.

4.41.22.24. Deve suportar L2TP VPN Servidor/Cliente.

4.41.22.25. Deve suportar PPTP VPN Servidor/Cliente.

4.41.22.26. Deve suportar OpenVPN VPN Servidor/Cliente.

4.41.22.27. Deve suportar identificação de aplicações L7 DPI.

4.41.22.28. Deve suportar bloqueio de aplicações.

4.41.22.29. Deve suportar bloqueio de websites.

4.41.22.30. Deve suportar políticas baseadas em tempo, IP e usuário.

4.41.22.31. Deve suportar SNMP V1/V2/V3.

4.41.22.32. Deve suportar autenticação de portal baseada em nuvem e independente.

4.41.22.33. Deve suportar autenticação por nome de usuário/senha.

4.41.22.34. Deve suportar autenticação por voucher.

4.41.22.35. Deve suportar autenticação com um clique.

4.41.22.36. Deve suportar personalização da página do portal.

4.41.22.37. Deve suportar integração com portais de terceiros utilizando Wi-Fi Dog e WISPr.

4.41.22.38. Deve suportar o gerenciamento local de pelo menos 1000 APs.

4.41.22.39. Deve suportar o gerenciamento local de pelo menos 1000 switches.

4.41.22.40. Deve suportar a descoberta e provisionamento automáticos de APs e switches.

4.41.22.41. Deve suportar gerenciamento local via web.

4.41.22.42. Deve suportar gerenciamento via nuvem.

4.41.22.43. Deve suportar gerenciamento via aplicativo móvel.

4.41.22.44. Deve suportar gerenciamento via nuvem pública. Todas as licenças relacionadas devem estar incluídas, caso necessitem de compra adicional.

4.42. RELATÓRIOS

4.42.1. O OPERADOR deverá fornecer mensalmente, no dia útil do mês, os seguintes relatórios ao MUNICÍPIO:

4.42.2. RELATÓRIO DE IMPLANTAÇÃO

4.42.2.1. Durante o período de implantação da infraestrutura, o OPERADOR deverá fornecer uma lista (relatório) de NÓS (NODES) incorporados à REDE METROPOLITANA e de eventuais problemas encontrados;

4.42.3. RELATÓRIO DE QUALIDADE DE SERVIÇO DA REDE METROPOLITANA

4.42.3.1. Deverá estar disponível para apresentação a qualquer momento, mediante solicitação, a visualização de painéis, emissão de relatórios e quaisquer informações relacionadas a chamados técnicos e sua linha do tempo, desde a abertura até o fechamento definitivo. Isso deve ser acessível através de um helpdesk por um funcionário devidamente cadastrado e identificado;

4.42.3.2. Disponibilidade média mensal da comunicação de dados e do sistema de gerenciamento;

4.42.3.3. Relação dos principais NÓ (NODE) concentradores e críticos, incluindo tráfego médio e de pico;

4.42.3.4. Relação de incidentes de segurança e ações tomadas;

4.42.3.5. Observações sobre identificação de enlaces sobrecarregados ou subutilizados;

4.42.3.6. Os relatórios devem ser entregues em formato eletrônico à Divisão de Tecnologia da Informação do Município.

4.42.4. Relatório de Disponibilidade e Dashboards

4.42.4.1. Deverá disponibilizar pelo menos 2 (duas) telas de no mínimo 40” devidamente instaladas junto a Contratante para verificação da disponibilidade em tempo real;

4.42.4.2. Deverá permitir acesso da contratante aos relatórios de disponibilidade a qualquer tempo, sempre que a contratante julgar necessário.

4.42.5. PENALIZAÇÃO DO OPERADOR POR INDISPONIBILIDADES NA REDE METROPOLITANA

4.42.5.1. Sempre que ocorrerem indisponibilidades por parte do OPERADOR na operação, gerenciamento, atendimento técnico ou fornecimento de relatórios de qualidade, o OPERADOR estará sujeitos às penalidades a serem aplicadas pelo MUNICÍPIO, conforme segue:

Recurso	Disponibilidade (Tempo ao mês)	Penalidade
NÓ CORE	Inferior a 99, 5 %	10 % do valor do NÓ (NODE) para cada hora de indisponibilidade
NÓ ANEL	Inferior a 99, 0 %	8 % do valor do NÓ (NODE) para cada hora de indisponibilidade
NÓ DISTRIBUIÇÃO	Inferior a 98, 5 %	Desconto do valor mensal do NÓ (NODE)
NÓ HOTSPOT	Inferior a 98, 0 %	Desconto do valor mensal do NÓ (NODE)
NÓ DISPOSITIVO IoT	Inferior a 97, 5 %	Desconto do valor mensal do NÓ (NODE)

4.42.5.2. O valor/hora da penalidade por indisponibilidade de cada recurso foi definido em função da criticidade de sua disponibilidade, da significância relativa da operação de cada um deles na estrutura da REDE METROPOLITANA e do valor mensal total do contrato respeitado os tempos limites de tolerância concedidos ao OPERADOR para correção e resolução de eventuais problemas que possam ocorrer;

4.42.5.3. O valor total das penalidades a que o OPERADOR estará sujeito, caso deixe de cumprir a taxa mínima de nível de serviço estabelecida para cada recurso identificado, deverá ser descontado pelo MUNICÍPIO no mês imediatamente posterior ao das ocorrências.

4.43. PRAZOS DE IMPLANTAÇÃO

4.43.1. Os serviços deverão ter início imediato a partir da assinatura do contrato;

4.43.2. Os serviços deverão ser prestados de segunda a sexta-feira, das 8 horas às 18 horas, atendendo as necessidades previstas neste TERMO DE REFERÊNCIA;

4.43.3. Quando da assinatura do Contrato deverá ser construído (pela contratada) cronograma inicial, com os NÓS (NODES) iniciais que deverão ser instalados, sendo que esse primeiro cronograma deve ser totalmente implementado em 60 (sessenta) dias e validado pela contratante;

4.43.4. Os NÓ (NODE) não inclusos dentro do cronograma inicial, deverão ser instalados sempre no prazo máximo de 5 dias úteis após a solicitação de instalação, independente do seu tipo;

4.43.5. No caso de não cumprimento do cronograma estabelecido, O OPERADOR estará sujeito às penalidades previstas no edital por inexecução parcial ou total do contrato;

4.43.6. Os pagamentos no período de implantação serão proporcionais ao percentual de NÓ (NODE) integrados à rede considerando os pesos utilizados no cálculo de disponibilidade.

4.44. ENTREGA DO AS-BUILT E DOCUMENTAÇÃO TÉCNICA DA REDE

4.44.1. A empresa vencedora deverá entregar a Prefeitura Municipal cópia do requerimento formal ou protocolo para construção de rede junto a CELESC, em nome da Operadora e da Contratante, constando projeto de engenharia com detalhamento técnico, percurso da rede, incluindo mapas e especificações de cabos e infra necessária, antes do início da execução, além do As-Built da construção da rede após a conclusão dos serviços. Este documento deve incluir os seguintes elementos detalhados:

4.45. MAPA DETALHADO DA REDE:

4.45.1. Representação gráfica precisa da rede de fibra óptica, incluindo todas as rotas de cabos;

4.46. LOCALIZAÇÃO DE ELEMENTOS DA REDE:

4.46.1. CABOS: Especificação dos tipos de cabos utilizados, comprimento de cada segmento e localização exata, identificação das fibras;

4.46.2. POSTES: Identificação e localização dos postes utilizados para sustentação da infraestrutura;

4.46.3. CAIXAS DE EMENDA: Localização das caixas de emenda, com detalhes das conexões e tipos de emenda realizadas;

4.46.4. RESERVAS TÉCNICAS: Locais de reserva de cabos para manutenções futuras ou expansões da rede;

4.46.5. PONTOS DE ACESSO: Localização e especificação dos pontos de acesso da rede.

4.47. DESENHOS E ESQUEMAS TÉCNICOS:

4.47.1. Esquemas detalhados de instalação e interligação dos componentes da rede, incluindo diagramas de fiação e conexões;

4.47.2. Desenhos técnicos dos elementos físicos instalados.

4.48. DOCUMENTAÇÃO EM MEIO DIGITAL:

4.48.1. Toda a documentação deve ser fornecida em formato digital, compatível com softwares de CAD (Computer-Aided Design) ou GIS (Geographic Information System), facilitando a consulta e a integração com sistemas de gerenciamento de infraestrutura.

4.49. DETALHAMENTO DA ROTA DOS CABOS:

4.49.1. Indicação dos percursos dos cabos e das principais referências geográficas;

4.49.2. Indicação das fibras que atenderão a todas as unidades da Prefeitura Municipal, devidamente mapeadas e identificadas;

4.50. UTILIZAÇÃO, INCORPORAÇÃO E TRANSFERÊNCIA DE ATIVOS E PASSIVOS DE REDE

4.50.1. Caso a contratante prorrogue o contrato anualmente e atinja o prazo máximo de 120 (cento e vinte) meses permitido por Lei, todos os dispositivos de rede, equipamentos eletrônicos e infraestrutura de fibra óptica, incluindo as 16 fibras ópticas utilizadas no backbone, backhaul utilizadas para atender o final de milha em todos os pontos de presença conectados às portas da OLT, que foram empregados na execução e manutenção dos

serviços durante a vigência contratual, deverão ser incorporados ao patrimônio da contratante ao término do contrato;

4.50.2. A incorporação incluirá, além dos dispositivos e equipamentos físicos, as 16 fibras ópticas, assegurando a manutenção de todos os nodes ativos da rede. Toda a infraestrutura de fibra óptica instalada e utilizada, com garantia de funcionalidade contínua dos nodes, será transferida formalmente à contratante;

4.50.3. A transferência de ativos e passivos de rede, incluindo 16 fibras ópticas e demais infraestruturas de fibra, que atendem a toda rede metropolitana, será formalizada por meio de termo de doação, devidamente protocolado na Diretoria de Patrimônio da Secretaria Municipal de Gestão Administrativa, em conformidade com a Lei nº 14.133/2021 e demais disposições legais vigentes;

4.50.4. A formalização dessa doação deverá seguir todos os procedimentos legais, garantindo o registro adequado dos bens incorporados e a continuidade dos serviços, preservando o interesse público.

4.51. SIGILO E RESTRIÇÕES

4.51.1. CONFIDENCIALIDADE E SIGILO: A contratada deverá tratar como estritamente confidenciais todas as informações, dados e documentos que venha a ter conhecimento em decorrência da prestação dos serviços objeto desta contratação. A contratada se compromete a zelar pelo sigilo dessas informações, em conformidade com as normas e políticas de segurança da informação estabelecidas pelo Município, bem como pelas disposições da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD). A contratada deverá instruir e orientar seus empregados, subcontratados e prepostos a respeito dessas obrigações, sob pena de responsabilidade civil, penal e administrativa;

4.51.2. RESPONSABILIDADE POR DANOS: A contratada será responsável por todos os danos físicos e/ou materiais que, por ação ou omissão de seus empregados, subcontratados ou prepostos, venham a ser causados ao Órgão Contratante ou a terceiros, decorrentes de imperícia, negligência, imprudência ou desrespeito às normas de segurança aplicáveis. Essa responsabilidade inclui a reparação integral dos danos causados, sem prejuízo de outras sanções previstas em lei;

4.51.3. PENALIDADES PELO DESCUMPRIMENTO: O descumprimento das obrigações de confidencialidade e sigilo pela contratada, seus empregados, subcontratados ou prepostos, sujeitará a contratada às penalidades administrativas, civis e penais previstas na legislação vigente, incluindo, mas não se limitando a multas, rescisão contratual, e indenizações por perdas e danos;

4.51.4. CONFORMIDADE COM A LGPD: A contratada deverá seguir rigorosamente todas as normas e diretrizes estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), garantindo a proteção e privacidade dos dados pessoais tratados no âmbito desta contratação. A contratada se compromete a implementar todas as medidas técnicas e administrativas necessárias para proteger os dados pessoais contra acesso não autorizado, perda, alteração, e quaisquer outras formas de tratamento inadequado ou ilícito;

4.51.5. TERMO DE CONFIDENCIALIDADE: Para formalizar o compromisso de confidencialidade exigido neste contrato, a contratada deverá assinar o Termo de Confidencialidade

específico, comprometendo-se a respeitar todas as obrigações relativas à segurança e proteção das informações pertencentes à contratante. O Termo de Confidencialidade deverá abranger todas as ações ou omissões, intencionais ou acidentais, que possam resultar na divulgação, perda, destruição, inserção, cópia, acesso ou alterações indevidas das informações, independentemente do meio em que estejam armazenadas, do ambiente em que estejam sendo processadas ou da forma como trafeguem.

5. OBRIGAÇÃO DA CONTRATADA

5.1. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

5.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.3. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.4. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

5.8. Quando houver, deverá ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados à Administração;

5.9. Executar os serviços conforme especificações deste edital e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste TERMO DE REFERÊNCIA e em sua proposta;

5.10. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

5.11. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

5.12. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

5.13. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

5.14. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

5.15. Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

5.16. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução dos serviços, durante a vigência do contrato;

5.17. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este TERMO DE REFERÊNCIA, no prazo determinado;

5.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

5.19. Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo;

5.20. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

5.21. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

5.22. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

5.23. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

5.24. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação.

5.25. Assegurar que todos os componentes e serviços da rede estejam em conformidade com as normas e regulamentações técnicas aplicáveis.

5.26. Adesão aos padrões estabelecidos pela ANATEL e outras regulamentações locais e internacionais relevantes, garantindo a qualidade e a segurança dos serviços prestados.

5.27. Pontos de acesso compatíveis com IEEE 802.11ac ou superior, capacidade de suportar múltiplos usuários simultâneos, e implementação de protocolos de segurança WPA3.

5.28. Garantir a segurança de todos os dados trafegados na rede, implementando medidas de proteção contra-ataques cibernéticos.

5.29. A contratada deverá configurar toda a rede, assegurando a conectividade e a comunicação eficiente entre todas as unidades administrativas do município, garantindo que todas as operações sejam realizadas de forma fluida e segura.

5.30. As configurações abrangem desde a integração e o funcionamento eficiente dos dispositivos na ponta até o pleno funcionamento da rede, independentemente de serem dispositivos da contratante ou de outras empresas contratadas. A contratada deve garantir que todos os componentes estejam corretamente configurados e integrados, se necessário a contratada deverá manter o contato com outras até a configuração, funcionamento do dispositivo conectado à rede;

5.31. A contratada deverá fornecer e instalar todos os equipamentos de rede necessários, incluindo roteadores, switches, pontos de acesso WiFi e servidores, assegurando que os equipamentos utilizados sejam de alta qualidade e atendam aos padrões técnicos exigidos pelo município.

5.32. A Contratada deverá registrar junto a Companhia de Energia (CELESC) autorização para uso dos postes por onde passam as fibras sem nome da Contratante e da Contratada;

5.33. A Contratada deverá fornecer todas as licenças de sistemas utilizados em nome da Contratante ou ter uma carta de autorização da fabricante relativos à cedência ao final do contrato dos sistemas utilizados;

5.34. A autenticação dos usuários do sistema deve ocorrer através de integração com a base de usuários da rede corporativa do CONTRATANTE através do protocolo LDAP, Active Directory onpremisses e Microsoft Entra ID ou Azure AD da contratante;

5.35. A solução deverá estar aderente aos aspectos de segurança dispostos nos seguintes instrumentos regulatórios: Norma ABNT NBR 27002, LGPD, NIST 800-53 e SOC 2 Tipo 2.

5.36. A contratada deverá atender toda a legislação vigente e suas atualizações determinadas sejam elas demandadas por Órgãos Federal, Estadual e Municipal assim como Agências Reguladoras vinculadas e demandas solicitadas pela contratante independentemente dos requisitos mínimos elencados neste Edital e seus Anexos;

5.37. Quando houver, a contratada deverá ter e/ou desenvolver rotinas de envios automáticos no sistema atendendo a legislações vigentes sejam elas de Órgãos Federal, Estadual e Municipal assim como Agências Reguladoras vinculadas e/ou sistemas internos ou externos;

5.37.1. Quando constatado que o não atendimento a estas determinações, por parte da contratada, ocasionou a geração de multa para a contratante, esta multa será imputada à contratada, por não cumprimento da demanda, sem nenhum ônus para a contratante.

5.38. Estão compreendidos nos serviços de suporte operacional (garantia de funcionalidade e operabilidade dos softwares objeto da licitação) a resolução de dúvidas operacionais nos softwares aos usuários da CONTRATANTE;

5.39. Esse tipo de serviço deve ser realizado para esclarecimentos de dúvidas do(s) servidor(es), sempre acompanhada por responsável que estará no ambiente interno da CONTRATANTE;

5.40. O Serviço de Suporte Técnico deverá ocorrer sem custos adicionais e incluir, no mínimo:

5.40.1. Orientações e esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução;

5.40.2. Orientação e apoio às questões relacionadas à integração de dados e sistemas;

5.40.3. Interpretação da documentação dos softwares fornecidos;

5.40.4. Orientações para identificar a causa de falha ou defeito de software e a solução destes; Orientação para solução de problemas de performance e de ajustes das configurações dos softwares ofertados;

5.40.5. Orientação quanto às melhores práticas para parametrização e customização da solução;

5.40.6. Construção de relatórios não disponíveis dentro do sistema;

5.40.7. Extração de dados em arquivos, quando não passíveis de fazer diretamente pelo usuário através do sistema;

5.40.8. Cadastro de usuários e parametrização de permissões dentro do sistema, quando solicitado pela CONTRATANTE;

5.40.9. Auxiliar na Elaboração de quaisquer atividades técnicas relacionadas à utilização dos sistemas após a implantação e utilização dos mesmos, como: gerar/validar arquivos para Órgão Governamental, Instituição Bancária, Gráfica, Tribunal de Contas, auxílio na legislação, na contabilidade e na área de informática, entre outros;

5.40.10. Instalar o sistema nos terminais dos usuários caso necessário.

5.40.11. A CONTRATANTE disponibilizará o acesso ao Sistema ITSM onde todas as solicitações de serviço e incidentes em uma única plataforma, facilitando o gerenciamento, acompanhamento e a priorização dos chamados, para isto:

5.40.11.1. A CONTRATADA deve assegurar que todos os incidentes sejam gerenciados de acordo em ferramenta de Gerenciamento de Solicitações da CONTRATANTE.

5.40.11.2. A CONTRATADA deve registrar cada solicitação no Sistema ISTM (Information Tecnology Service Management) da Contratante, independentemente do meio pelo qual a demanda seja recebida (telefone, e-mail, mensageiro instantâneo ou presencialmente).

5.40.11.3. A CONTRATADA deve responder a todas as solicitações e incidentes diretamente no Sistema ISTM da Contratante. Isso é essencial para fins de verificação e validação.

5.40.11.4. A CONTRATADA deve garantir que todas as respostas e atualizações de status sejam registradas prontamente no Sistema ISTM da Contratante. Isso permitirá uma visão unificada e centralizada da abertura e do gerenciamento de chamados.

5.40.11.5. A CONTRATADA poderá de empregar seu de Sistema ISTM, desde que esta esteja devidamente integrada e seja capaz de inserir as informações necessárias em relação às solicitações geradas pela Contratante em sua própria ferramenta.

5.40.11.6. A CONTRATANTE disponibilizará as credenciais de acesso para integração junto ao Sistema ISTM o qual é o GLPI (Gestionnaire Libre de Parc Informatique).

5.40.11.6.1. As informações para integração poderão ser localizadas junto a detentora oficial da licença GLPI, TecLib;

5.40.11.6.2. A API deve suportar operações de CRUD (Create, Read, Update, Delete) para os principais módulos do GLPI, como chamados, ativos, usuários, entre outros.

5.40.11.6.3. Cada aplicação que acessa a API do GLPI deve usar um cliente de API diferente para granularização e auditoria dos acessos.

5.40.11.6.4. Deve ser possível configurar clientes de API com permissões específicas.

5.40.12. A CONTRATADA deverá promover a contínua atualização legal dos sistemas fornecidos e possíveis releases, de forma que o objeto deste edital atenda a legislação federal, estadual, municipal vigente e das normas e procedimentos dos órgãos fiscalizadores, sem custo adicional para a contratante;

5.41. A fim de garantir a sustentação da Solução para a Administração Municipal durante e após a vigência contratual, em função de eventual interrupção do contrato por qualquer motivo ou futura transição contratual decorrente de nova licitação para o mesmo objeto, a CONTRATADA deve:

5.41.1. Assegurar ao CONTRATANTE, mediante cláusula contratual, o uso do produto sucessor em caso de descontinuidade do produto contratado;

5.41.2. Assegurar ao CONTRATANTE, mediante cláusula contratual, transferência de todas as obrigações contratuais ao sucessor em caso de venda da empresa CONTRATADA ou incorporação por novos controladores;

5.41.3. Garantir o acesso à última versão do produto e da respectiva documentação, mesmo após a vigência do contrato e por no máximo 3 (três) meses, para possibilitar que as informações lançadas possam continuar a ser consultadas, independentemente se as entidades estejam ativas ou inativas na Solução, em virtude de mudanças, na estrutura do CONTRATANTE.

5.42. O CONTRATANTE se reserva ao direito de efetuar conexão da Solução a produtos de outros fornecedores, seja hardware ou software, e desde que tal iniciativa não implique em incompatibilidade com a Solução. A efetivação de tal medida, não poderá, sob qualquer hipótese, servir de pretexto para a CONTRATADA desobrigar-se da prestação de manutenção e suporte técnico e demais compromissos previstos em contrato.

5.43. A CONTRATADA compromete-se a utilizar rotas de rede otimizadas para minimizar atrasos e perdas de pacotes, garantindo o bom desempenho dos serviços hospedados na nuvem. A CONTRATADA deverá monitorar constantemente as rotas de tráfego da rede e realizar ajustes automáticos ou manuais sempre que forem detectadas rotas degradadas, lentidão ou congestionamento.

5.44. Caso necessite A CONTRATADA compromete-se a implementar mecanismos de Qualidade de Serviço (QoS) para priorizar o tráfego de rede essencial ao funcionamento do sistema do CONTRATANTE, de forma a minimizar o impacto de congestionamentos e atrasos que possam comprometer a experiência de uso dos serviços em nuvem.

5.45. A CONTRATADA compromete-se a utilizar profissionais devidamente qualificados e especializados para a execução dos serviços previstos neste contrato, assegurando que esses profissionais possuem as competências necessárias para o bom desempenho das atividades. A CONTRATADA é responsável por garantir que todos os seus empregados estejam em conformidade com as normas legais e regulamentares aplicáveis;

6. REQUISITOS DA CONTRATAÇÃO

6.1. A LICITANTE deverá apresentar:

6.1.1. Apresentar comprovante de registro ou inscrição no Conselho Regional de Engenharia, Arquitetura e Agronomia (CREA) da jurisdição da empresa. Este comprovante deve

evidenciar que a empresa realiza atividades relacionadas ao objeto licitado e deve identificar um responsável técnico registrado;

6.1.2. A licença de SCM (Serviço de Comunicação Multimídia) outorgado pela ANATEL;

6.1.3. Atestado de capacidade técnica devem ser emitidos por empresas de direito público ou privado. Esses atestados devem comprovar a execução de serviços com quantitativos iguais a 150 pontos de fibra ópticas instalados relacionados aos itens 3, 4 e 5 da cláusula 7.10 do ETP, com características técnicas similares ou superiores ao objeto licitado.

6.1.4. A empresa declarada vencedora deverá apresentar no prazo máximo de 05 (dias) dias corridos, a documentação em meio digital e com timbre da empresa, conforme abaixo relacionada para avaliação técnica:

6.1.5. Cronograma Físico e Financeiro;

6.1.5.1. Memorial descritivo do projeto da rede de dados, composto por:

6.1.5.2. Plano de Endereçamento IP;

6.1.5.3. Relação das tecnologias empregadas;

6.2. Na proposta deverão conter fabricante, modelo, part number, descrição técnica, quantidade e preço unitário, conforme Acordão TCU nº 1.432/2024. Neste caso uma planilha detalhada;

6.2.1. Tecnologia e fornecedor do enlace;

6.2.2. Velocidades nominais de entradas e saídas;

6.2.3. Velocidade mínima garantida de entrada e saída;

6.2.4. Tempo previsto para implantação;

6.2.5. Topologia da rede integrada (Diagrama);

6.2.6. Entrega de Certificações e descrições detalhadas oficiais dos Fabricantes, visando garantir a qualidade, conformidade e especificações técnicas dos produtos a serem utilizados na rede:

6.2.7. **CERTIFICAÇÕES DE PRODUTOS:** Fornecer documentação referente aos produtos a serem instalados na rede: Documentos oficiais que certificam a qualidade e conformidade dos produtos com normas técnicas e especificações técnicas;

6.2.8. **DESCRIÇÕES DOS FABRICANTES:** Fornecer informações detalhadas dos fabricantes dos produtos, extraídas de seus sites oficiais, incluindo características técnicas, funcionalidades e compatibilidade;

6.2.9. **ATIVOS E PASSIVOS DE REDE:** Descrição completa dos equipamentos ativos (como firewall, switches, roteadores, olt, pontos de acesso, etc) e passivos (como cabos, conectores, racks, etc) de rede a serem utilizados;

6.2.10. **EQUIPAMENTOS DE INFORMÁTICA:** Descrição dos computadores, notebooks, servidores e outros equipamentos de informática que serão utilizados, incluindo especificações técnicas;

6.2.11. **LICENÇAS DE SOFTWARE:** Cópias das licenças de software que serão utilizadas na composição da central de operações, garantindo a legalidade e conformidade com as normas;

6.2.12. **PLANO DE MANUTENÇÃO PERIÓDICA:** Entregar plano de manutenção periódica da rede, limpeza e testes, com cronograma contendo no mínimo as seguintes informações:

Periodicidade, Atividades no processo (inspeção visual, testes de continuidade, medições de potência);

6.2.13. Entregar a demonstração da exequibilidade econômica da execução de forma detalhada;

6.2.14. **DESCRIÇÃO DA CENTRAL DE OPERAÇÕES:** A Central de Operações é um componente essencial para garantir a qualidade e eficiência dos serviços de rede e transporte de dados oferecidos e construídos para a Prefeitura Municipal de Balneário Camboriú. Detalhamos as características técnicas e operacionais que devem constar na composição os seguintes itens:

6.2.15. Descrever os sistemas que compões o sistema de gerenciamento e monitoramento, sito, hardware, software e recursos humanos organizados para o monitoramento e gerenciamento de rede e informações. Define-se níveis de serviço, uso de recursos computacionais e indicativos de criticidade ou indisponibilidade para identificar riscos e problemas, iniciando o tratamento necessário;

6.2.16. A contratada deverá possuir centro de operações para atendimento técnico e monitoramento proativo no raio de 15Km da base situada a rua Dinamarca, 320 para atendimento as SLAs. A empresa terá o prazo de 30 (trinta) dias após a assinatura do contato para formalizar o centro e operações. Justifica-se esta necessidade considerando a necessidade de garantir a qualidade e a eficiência dos serviços prestados, é imprescindível que a contratada possua um escritório para atendimento técnico dentro de um raio de 15km da nossa base situada na Rua Dinamarca, 320. Esta exigência é justificada por várias razões:

6.2.16.1. **Resposta Rápida a Incidentes:** A proximidade física permite uma resposta imediata a problemas técnicos e incidentes, minimizando a interrupção dos serviços essenciais.

6.2.16.2. **Cumprimento das SLAs:** Com um escritório próximo, a contratada pode garantir tempos de resposta dentro dos padrões acordados, assegurando a conformidade com os Service Level Agreements.

6.2.16.3. **Eficiência na Gestão de Recursos:** Menos tempo gasto em deslocamentos significa mais tempo disponível para atividades produtivas, aumentando a eficiência geral da operação.

6.2.16.4. **Redução de Custos Operacionais:** A proximidade diminui os custos relacionados a deslocamentos e logística, resultando em economias significativas para ambas as partes.

6.2.16.5. **Manutenção da Qualidade dos Serviços:** Um escritório próximo garante que os padrões de qualidade sejam mantidos, transmitindo maior confiança aos clientes.

6.2.16.6. **Melhora na Comunicação:** Facilita a comunicação entre a equipe técnica e os gestores locais, possibilitando uma coordenação mais eficaz das atividades.

6.2.16.7. **Sustentabilidade:** Menos deslocamentos resultam em menor emissão de carbono, contribuindo para práticas ambientais mais sustentáveis.

6.2.16.8. **Apoio ao Cliente:** Clientes sentem-se mais seguros sabendo que há uma equipe técnica próxima, pronta para resolver quaisquer problemas de maneira rápida e eficaz.

6.2.16.9. **Adaptação Rápida a Mudanças:** Facilita a implementação de mudanças ou atualizações nos serviços, garantindo que quaisquer necessidades emergentes sejam atendidas prontamente.

6.2.16.10. **Conformidade com Regulamentações:** A manutenção de um escritório próximo assegura que todos os requisitos legais e regulamentares sejam cumpridos, incluindo normas de segurança e ergonomia no ambiente de trabalho.

6.2.17. Portanto, a exigência de um escritório para atendimento técnico próximo à contratante é uma prática estratégica que beneficia ambas as partes - a empresa contratante e a contratada, garantindo a prontidão, eficiência e qualidade dos serviços prestados, especialmente no contexto das SLAs.

6.2.18. Além disso, a Central de Operações deve contar com conectividade segura e redundante com a infraestrutura de rede da prefeitura, incluindo acesso a fontes de energia seguras, com sistemas de backup de energia dedicados;

6.2.19. A infraestrutura física deve atender a todos os requisitos legais de segurança e ergonomia no ambiente de trabalho, conforme a Norma Regulamentadora nº 17 (NR-17), garantindo condições adequadas de saúde e segurança para os operadores e colaboradores envolvidos.

6.2.20. Descrição da equipe técnica dedicada para atendimento à Prefeitura Municipal, sediada na central de operações. A equipe deve estar habilitada para receber e resolver demandas por telefone, internet, mensageiro instantâneo ex.: WhatsApp, tickets e chat, tanto remotamente quanto presencialmente, identificando e descrevendo as funções de atendente de helpdesk, analista de suporte nível I, Analista de suporte nível II, Técnico de Campo Nível II, III para suporte a redes de fibra óptica, Gerente de Projetos, Gerente Técnico Operacional e a quantidade de profissionais de cada função;

6.2.21. Entregar plano de Atendimento e qualidade, elementos são essenciais para garantir a eficiência, qualidade e conformidade com as normas nos serviços de atendimento, contribuindo para a satisfação dos usuários e a melhoria contínua dos processos, contemplando os seguintes aspectos:

6.2.22. Descrição clara dos horários de funcionamento do serviço de atendimento, incluindo horários de expediente, plantões e atendimento emergencial;

6.2.23. Descrição dos procedimentos a serem seguidos para o atendimento de chamadas, incluindo o escalonamento de problemas de acordo com a gravidade e a complexidade;

6.2.24. Processo para o registro, acompanhamento e resolução de chamadas e ocorrências, com definição de responsabilidades e prazos;

6.2.25. Método para coleta e análise de dados estatísticos relacionados ao atendimento, com o objetivo de identificar tendências e áreas de melhoria;

6.2.26. Estratégia para a criação e atualização de uma base de conhecimento com informações úteis, como questões frequentes, recomendações e manuais de uso;

6.2.27. Detalhamento dos documentos a serem produzidos e mantidos, incluindo manuais de procedimentos, guias de atendimento e registros de ocorrências;

6.2.28. A avaliação técnica será realizada pela Divisão de Tecnologia da Informação em até 5 dias úteis, contados da convocação do Agente de Contratação, sito, a equipe técnica do

MUNICÍPIO, para fins de análise, aprovação e finalização de entendimentos sobre a implantação do projeto (documentação da REDE METROPOLITANA, prioridades de instalação dos NÓ (NODE), cronograma de implantação etc.). Deverá ser emitido memorando aprovando ou reprovando as especificidades técnicas em 100% de seus itens;

6.2.29. Após a avaliação técnica, e caso a empresa licitante classificada em primeiro lugar deixe de atender integralmente aos requisitos da licitação, as demais empresas serão convocadas para prosseguimento do processo de avaliação técnica, de acordo com a ordem de classificação de suas propostas.

6.2.30. Será considerada vencedora da licitação a empresa que atender integralmente todos os requisitos do edital e tiver sua proposta aprovada na sequência de avaliações técnicas que venham a ser realizadas pelo MUNICÍPIO.

6.3. ENTREGA DO AS-BUILT E DOCUMENTAÇÃO TÉCNICA DA REDE

6.3.1. Requerimento Formal e Projeto de Engenharia: A empresa vencedora deverá encaminhar formalmente à Celesc o projeto de construção da rede de fibra óptica, contendo todas as especificações técnicas e informações necessárias, e entregar à Prefeitura de Balneário Camboriú um comprovante desse envio à Celesc até o início da execução do projeto. Para assegurar a confirmação da entrega, o documento deverá ser enviado à Celesc por Aviso de Recebimento (AR), entregue em mãos, ou comprovado através do sistema de Protocolo Digital disponível no site da Celesc;

6.3.2. Conformidade com Normas Técnicas: A empresa contratada deve seguir as normas de construção mais estritas, de acordo com as regulamentações técnicas nacionais e locais, assegurando o cumprimento de todas as exigências legais. O cabeamento utilizado deve ser registrado e certificado, não sendo permitido o uso de cabos adquiridos de forma ilícita ou sem comprovação de origem legal. A rastreabilidade dos materiais é fundamental para garantir a legalidade e a qualidade dos insumos empregados;

6.3.3. Entrega do As-Built: Após a conclusão dos serviços, a empresa deverá entregar o As-Built da construção da rede, contendo todos os ajustes e modificações realizados durante a execução do contrato. O As-Built deve incluir os seguintes elementos:

6.3.3.1. **Mapa Detalhado da Rede:** Representação gráfica precisa da rede de fibra óptica, detalhando todas as rotas dos cabos, com especial atenção para os segmentos A e B que compõem o anel bidirecional. Esses segmentos não devem, em nenhum momento, compartilhar as mesmas rotas físicas, assegurando a resiliência da rede e a efetividade da arquitetura em anel bidirecional. A separação física das rotas dos segmentos A e B deve ser projetada para garantir a continuidade dos serviços em caso de falha em qualquer uma das rotas;

6.3.3.2. **Localização de Elementos da Rede:** Especificação completa dos tipos de cabos utilizados, seu comprimento por segmento e localização exata, incluindo:

6.3.3.3. **Postes:** Identificação e localização dos postes utilizados para sustentar a infraestrutura;

6.3.3.4. **Caixas de Emenda:** Localização das caixas de emenda, incluindo detalhes das conexões e tipos de emenda realizadas;

6.3.3.5. **Reservas Técnicas:** Locais reservados para cabos visando futuras manutenções ou expansões da rede;

6.3.3.6. **Pontos de Acesso:** Localização e especificação detalhada dos pontos de acesso da rede.

6.3.3.7. **Desenhos e Esquemas Técnicos:** Esquemas detalhados da instalação e interligação dos componentes da rede, incluindo diagramas de fiação e conexões, além de desenhos técnicos dos elementos físicos instalados.

6.3.4. Documentação em Meio Digital:

6.3.5. Toda a documentação deve ser fornecida em formato digital, compatível com softwares de CAD (Computer-Aided Design) e/ou GIS (Geographic Information System), para facilitar a consulta e integração com sistemas de gerenciamento de infraestrutura.

6.3.6. Detalhamento da Rota dos Cabos:

6.3.6.1. **Percursos dos Cabos:** Indicação clara dos percursos dos cabos e principais referências geográficas.

6.3.6.2. **Fibras Alocadas:** Indicação precisa das fibras que atenderão as unidades da Prefeitura Municipal, devidamente mapeadas e identificadas.

6.3.6.3. **Assinatura de Responsável Técnico:** Todos os documentos devem ser assinados por um responsável técnico credenciado no CREA (Conselho Regional de Engenharia e Agronomia), garantindo a conformidade com as normas técnicas e regulamentares.

6.3.7. Requisitos Legais e Normativos:

6.3.7.1. Lei nº 14.133/2021, Art. 6º, Inciso XXV: Define o projeto como o conjunto de elementos necessários e suficientes para caracterizar a obra ou serviço objeto da licitação.

6.3.7.2. Lei nº 14.133/2021, Art. 42: Determina que a execução do contrato deve ser acompanhada e fiscalizada por um representante da Administração.

6.3.8. Procedimentos de Entrega e Aceitação: A entrega do As-Built e da documentação técnica deve ser realizada antes da aceitação final dos serviços. Esta documentação será revisada pela fiscalização responsável, para garantir que todas as modificações e ajustes realizados durante a execução do projeto sejam devidamente registrados e aprovados. A entrega dessa documentação é essencial para futuras manutenções, expansões da rede e garantia da conformidade técnica e operacional da infraestrutura instalada.

6.3.9. Comprovação de possuir contratado ou empregado no quadro funcional da empresa, na data prevista para a entrega da proposta, responsável técnico, profissional de nível superior e declaração de contratação futura do profissional detentor da CAT apresentada, desde que acompanhada de declaração de anuência do profissional, em observância ao disposto no art. 67 da Lei Federal nº 14.133/2021, mediante a apresentação de um dos seguintes documentos:

6.3.9.1. Cópia da Carteira de Trabalho e Previdência Social (CTPS), contendo as folhas com o número de registro, qualificação civil e contrato de trabalho;

6.3.9.2. Ficha de Registro de Empregado, em frente e verso;

6.3.9.3. Contrato de trabalho; ou

6.3.9.4. Contrato de prestação de serviço.

6.3.10. A contratada deverá possuir centro de operações para atendimento técnico e monitoramento proativo no raio de 15Km da base situada a rua Dinamarca, 320 para atendimento as SLAs. Justifica-se esta necessidade considerando a necessidade de garantir a qualidade e a eficiência dos serviços prestados, é imprescindível que a contratada possua um escritório para atendimento técnico dentro de um raio de 15km da nossa base situada na Rua Dinamarca, 320. A contratada terá o prazo de 30 (trinta) dias, contados a partir da assinatura do contrato, para comprovar a existência do referido escritório no raio de 15 km. Esta exigência é justificada por várias razões:

6.3.10.1. Resposta Rápida a Incidentes: A proximidade física permite uma resposta imediata a problemas técnicos e incidentes, minimizando a interrupção dos serviços essenciais;

6.3.10.2. Cumprimento das SLAs: Com um escritório próximo, a contratada pode garantir tempos de resposta dentro dos padrões acordados, assegurando a conformidade com os Service Level Agreements;

6.3.10.3. Eficiência na Gestão de Recursos: Menos tempo gasto em deslocamentos significa mais tempo disponível para atividades produtivas, aumentando a eficiência geral da operação;

6.3.10.4. Redução de Custos Operacionais: A proximidade diminui os custos relacionados a deslocamentos e logística, resultando em economias significativas para ambas as partes;

6.3.10.5. Manutenção da Qualidade dos Serviços: Um escritório próximo garante que os padrões de qualidade sejam mantidos, transmitindo maior confiança aos clientes;

6.3.10.6. Melhora na Comunicação: Facilita a comunicação entre a equipe técnica e os gestores locais, possibilitando uma coordenação mais eficaz das atividades;

6.3.10.7. Sustentabilidade: Menos deslocamentos resultam em menor emissão de carbono, contribuindo para práticas ambientais mais sustentáveis;

6.3.10.8. Apoio ao Cliente: Clientes sentem-se mais seguros sabendo que há uma equipe técnica próxima, pronta para resolver quaisquer problemas de maneira rápida e eficaz;

6.3.10.9. Adaptação Rápida a Mudanças: Facilita a implementação de mudanças ou atualizações nos serviços, garantindo que quaisquer necessidades emergentes sejam atendidas prontamente;

6.3.10.10. Conformidade com Regulamentações: A manutenção de um escritório próximo assegura que todos os requisitos legais e regulamentares sejam cumpridos, incluindo normas de segurança e ergonomia no ambiente de trabalho.

6.3.11. A empresa deverá encaminhar, no prazo de até 30 (trinta) dias após a execução do serviço, os requisitos mencionados nos itens acima. Ressalta-se que se trata de um serviço contínuo de atualização.

6.4. DAS GARANTIAS

6.4.1. Exigir-se-á do licitante vencedor, no prazo máximo de 5 (cinco) dias úteis, contados a partir da data da assinatura do contrato, a prestação de garantia contratual, a ser realizada em

qualquer das modalidades previstas no § 1º do art. 96 da Lei nº 14.133/2021. O valor da garantia será de 5% (cinco por cento) do valor total do contrato e será restituído após a execução satisfatória dos serviços contratados;

6.4.2. A garantia prestada não poderá ser vinculada a outras contratações, salvo após a sua liberação formal pela Administração contratante;

6.4.3. Caso o valor do contrato seja alterado, conforme disposto no art. 124 da Lei nº 14.133/2021, a garantia deverá ser complementada, no prazo de 48 (quarenta e oito) horas, para que seja mantido o percentual de 5% (cinco por cento) do valor atualizado do contrato;

6.4.4. Nos casos em que multas ou penalidades forem descontadas da garantia, o seu valor original deverá ser recomposto pelo licitante vencedor no prazo de 48 (quarenta e oito) horas, sob pena de rescisão unilateral e administrativa do contrato.

7. JUSTIFICATIVA NOS CASOS DE LICITAÇÕES NÃO EXCLUSIVAS

7.1. O processo licitatório desta contratação não ocorrerá de forma exclusiva conforme o Decreto Municipal n. 8.981/2018, pois é factível no caso de valores acima do que aqui apresentado. Ao possibilitar a mais ampla participação e um maior alcance em uma licitação pode beneficiar o comprador ao aumentar a competição, fornecer uma gama mais ampla de opções, promover a inovação e a qualidade, reduzir riscos e garantir um processo transparente e imparcial. Quanto mais fornecedores participarem da licitação, maior será a competição, o que pode resultar em propostas mais competitivas e melhores preços para o órgão.

8. JUSTIFICATIVA PARA PERMISSÃO OU VEDAÇÃO DE CONSÓRCIOS

8.1. A formação de consórcios para a contratação deste certame está expressamente proibida.

8.2. A restrição à participação de consórcios é justificada por várias razões. Em primeiro lugar, o objeto desta contratação não exige um alto grau de complexidade técnica que poderia justificar a formação de consórcios. Além disso, a permissão para a formação de consórcios poderia potencialmente limitar a competição entre as empresas, diminuindo a disputa e possivelmente levando a preços menos competitivos. Ao proibir a formação de consórcios, evitamos a possibilidade de formação de cartéis e a manipulação de preços, promovendo assim uma concorrência justa e equitativa.

9. MODELO DE EXECUÇÃO DO OBJETO

9.1. Os serviços terão início imediato após o recebimento da Autorização de Fornecimento. A contratação ocorrerá conforme a necessidade do órgão, sendo cada serviço requisitado nos prazos e quantidades que a Prefeitura de Balneário Camboriú julgar pertinentes. A contratada deverá cumprir rigorosamente os prazos estabelecidos no Termo de Referência para a execução e entrega dos serviços.

9.2. As demandas serão encaminhadas por comunicação oficial, com a especificação do serviço pretendido e com a autorização prévia, por meio de uma Ordem de Serviço, contendo a descrição do local a ser atendido.

9.3. A critério da CONTRATANTE, a Ordem de Serviço/Autorização de Fornecimento poderá ser substituída por solicitação via comunicação oficial, a qual, contendo todas as informações relativas ao serviço a ser prestado e prazo para execução, terá o mesmo valor da Ordem de Serviço para efeitos desta licitação.

9.4. As reuniões iniciais serão no sentido de definir o passo a passo da implantação junto aos responsáveis da Divisão de TI da Prefeitura de Balneário Camboriú e a contratada, podendo as mesmas serem feitas de forma presencial ou por meio virtual, desde que previamente agendadas.

9.5. A conclusão dos serviços será finalizada em até 90 (sessenta) dias após a assinatura do contrato, nos seguintes endereços/localidades iniciais do contrato:

Secretaria	Unidade	Endereço	Bairro	Tipo	Tecnologia	Velocidade
SEGOV	Divisão De Tecnologia Da Informação	R. Pardal, 111,	Ariribá	tipo 1	Gw Anel	10 gbps
SSE	Secretaria De Segurança	Av. Marginal Oeste, 2381	Municípios	tipo 1	Gw Anel	10 gbps
SED	Secretaria Da Educação	R. Camboriú, 100	Municípios	tipo 2	Anel	10 gbps
SFA	Prefeitura De Balneário Camboriú	R. Dinamarca, 320	Nações	tipo 2	Anel	10 gbps
SSS	Secretaria De Saúde E Saneamento Municipal	R. 1500, 1100	Centro	tipo 2	Anel	10 gbps
SSS	Hospital Ruth Cardoso	R. Angelina S/N	Municípios	tipo 2	Anel	10 gbps
BC TRÂNSITO	Fumtran Anexo Obras	-26.99671, -48.65046	Estados	tipo 3	gpon	1 gbps
BC TRÂNSITO	Bctran - Bc TRÂNSITO	Av. Marginal Leste, 1450	Centro	tipo 3	gpon	1 gbps
BC TRÂNSITO	BCTran – Escola de Trânsito	Av. Santa Catarina, 701	Estados	tipo 3	gpon	1 gbps
BCPREVI	Bcprevi	R. Dinamarca, 175	Nações	tipo 3	gpon	1 gbps
COSIP	Cosip	R. Aqueduto, 30	Estados	tipo 3	gpon	1 gbps
FCBC	Teatro Municipal (Praça + Rua Lateral) Novo Interno	Av. Central & R. 300	Centro	tipo 3	gpon	1 gbps
FCBC	Biblioteca Municipal	R. 2500 & 3ª Av.	Centro	tipo 3	gpon	1 gbps
FCBC	Fundação Municipal Da Cultura	R. 300, 50 Teatro Municipal Bruno Nitz	Centro	tipo 3	gpon	1 gbps
FCBC	Escola De Arte E Artesanato - Casa Linhares (N28/114)	R. Emanoel Rebelo Dos Santos, 1079	Barra	tipo 3	gpon	1 gbps
FME	Fme - Artes Marciais Dojo	-27.00986, -48.64083	Municípios	tipo 3	gpon	1 gbps
FME	Academia Pontal Norte.	Av. Atlântica, 65	Centro	tipo 3	gpon	1 gbps
FME	Ginásio Irineu Bornhausen - Bairro Dos Estados	Av. Santa Catarina, 700	Estados	tipo 3	gpon	1 gbps
FME	Fundação Municipal Do Esporte	R. 2438, 146	Centro	tipo 3	gpon	1 gbps
FME	Centro De Artes Marciais	R. Dom Jose, 433 - Vila Real	Vila Real	tipo 3	gpon	1 gbps
FME	Ginásio Hamilton Linhares - Bairro Da Barra	R. Jardim Da Saudade, 250	Barra	tipo 3	gpon	1 gbps
FME	Ginásio Sergio Lorenzatto - Bairro Das Nações	R. Liberia, 811	Nações	tipo 3	gpon	1 gbps
FME	Centro Olimpico	R. Paraguai, 618	Nações	tipo 3	gpon	1 gbps
FUNSERVIR	Funservir - Saude Do Servidor Publico	R. 200, 500	Centro	tipo 3	gpon	1 gbps
FUNSERVIR	Funservir	R. 200, 500	Centro	tipo 3	gpon	1 gbps

GAP	Casa Dos Conselhos	R. 1822, 1510	Centro	tipo 3	gpon	1 gbps
PCIVIL	Policia Civil - Estaleirinho	-27.02991, -48.58433	Estaleiro	tipo 3	gpon	1 gbps
PMILITAR	Base Pm Barra Sul	-27.007428447762237, -48.601784160573864	Barra	tipo 3	gpon	1 gbps
PMILITAR	Pmsc - Central Regional De Emergências	R. Jose Francisco Vitor & Praca Do Pescador	Barra	tipo 3	gpon	1 gbps
PMILITAR	12º Batalhão Da Policia Militar	R. Mexico, 1191	Nações	tipo 3	gpon	1 gbps
PMILITAR	Batalhão Da Policia Militar - Central De Monitoramento	R. Noruega, 669	Nações	tipo 3	gpon	1 gbps
SED	N.E.I Santa Clara	-27.00381, -48.63999	Municípios	tipo 3	gpon	1 gbps
SED	N.E.I Cristo Luz	-27.00507, -48.63243	Municípios	tipo 3	gpon	1 gbps
SED	Polo De Altas Habilidades	-27.00626, -48.64313	Municípios	tipo 3	gpon	1 gbps
SED	N.E.I Santa Inês	-27.00690, -48.63920	Municípios	tipo 3	gpon	1 gbps
SED	C.E.A.C. Projeto Oficinas (Nei Nova Geração)	-27.00738, -48.63925	Municípios	tipo 3	gpon	1 gbps
SED	N.E.I Pão E Mel	-27.00873, -48.63020	Vila Real	tipo 3	gpon	1 gbps
SED	Ambiarte	-27.009424, -48.637517	Municípios	tipo 3	gpon	1 gbps
SED	C.E.I. Taquaras	-27.01051, -48.58006	Taquaras	tipo 3	gpon	1 gbps
SED	N.E.I Odácia Tereza Damazio	-27.01131, -48.60929	Barra	tipo 3	gpon	1 gbps
SED	N.E.I Taquaras	-27.01192, -48.58082	Taquaras	tipo 3	gpon	1 gbps
SED	N.E.I Iate Clube	-27.01459, -48.63175	Jardim Iate Clube	tipo 3	gpon	1 gbps
SED	N.E.I Nova Esperança	-27.02456, -48.61370	Nova Esperança	tipo 3	gpon	1 gbps
SED	N.E.I Pequeno Mundo	-27.02501, -48.61329	Nova Esperança	tipo 3	gpon	1 gbps
SED	C.E.I. Nova Esperança	-27.02744, -48.61166	Nova Esperança	tipo 3	gpon	1 gbps
SED	N.E.I Brilho Do Sol	-27.03081, -48.58444	Estaleiro	tipo 3	gpon	1 gbps
SED	C.E.I. Dona Lila Estaleiro	-27.03157, -48.59080	Estaleiro	tipo 3	gpon	1 gbps
SED	N.E.I Estaleirinho	-27.05109, -48.59358	Estaleirinho	tipo 3	gpon	1 gbps
SED	C.E.I. Giovania De Almeida	-27.05127, -48.59236	Estaleirinho	tipo 3	gpon	1 gbps
SED	N.E.I Vovô Alécio	Av. Dos Tucanos, 290	Ariribá	tipo 3	gpon	1 gbps
SED	C.E.I. Aririba	Av. Dos Tucanos, 60	Ariribá	tipo 3	gpon	1 gbps
SED	C.E.I. Alfredo Domingos Da Silva	Av. Hermógenes Assis Feijó, 1335	São Judas Tadeu	tipo 3	gpon	1 gbps
SED	C.E.I Nova Esperança - Hs	Av. Jose Alves Cabral, 30 - Nova Esperança	Nova Esperança	tipo 3	gpon	1 gbps
SED	C.E.I. Governador Ivo Silveira	Av. Santa Catarina, 637	Estados	tipo 3	gpon	1 gbps
SED	C.E.I. Vereador Santa	R. 2450, 420	Centro	tipo 3	gpon	1 gbps
SED	C.E.J.A Deputado Doutel De Andrade	R. 3020, 160	Centro	tipo 3	gpon	1 gbps
SED	C.A.I.C Ayrton Senna Da Silva	R. Angelina	Municípios	tipo 3	gpon	1 gbps
SED	N.E.I Sementes Do Amanha	R. Angelina, 595	Municípios	tipo 3	gpon	1 gbps

SED	Projeto Oficinas Da Barra	R. Antonio Domingos Da Silva, 147	Barra	tipo 3	gpon	1 gbps
SED	N.E.I Ariribа	R. Bemtevi & R. Beija-Flor	Ariribá	tipo 3	gpon	1 gbps
SED	C.E.I. Tomaz Francisco Garcia	R. Biguacu, 841	Municípios	tipo 3	gpon	1 gbps
SED	C.E.A.C. Escola De Ingles	R. Canelinha, 139	Municípios	tipo 3	gpon	1 gbps
SED	C.E.A.C Vila Real	R. Dom Abelardo, 400 - Vila Real	Vila Real	tipo 3	gpon	1 gbps
SED	N.E.I Anjo Da Guarda	R. Dom Diniz, 350 - Vila Real	Vila Real	tipo 3	gpon	1 gbps
SED	C.E.I. Prof Armando Cesar Ghislandi	R. Dom Diniz, 450 - Vila Real	Vila Real	tipo 3	gpon	1 gbps
SED	N.E.I Pequeno Navegador	R. Dom Fradique, 100	Jardim Iate Clube	tipo 3	gpon	1 gbps
SED	C.E.I. Jardim Iate Clube	R. Dom Henrique, 903	Jardim Iate Clube	tipo 3	gpon	1 gbps
SED	C.E.I. Dona Lili	R. Fermino Taveira Cruz, 249	Barra	tipo 3	gpon	1 gbps
SED	N.E.I Carrossel	R. Grécia, 205	Nações	tipo 3	gpon	1 gbps
SED	N.E.I Crianca Esperanca	R. Isaias Serrão, 76	Nova Esperança	tipo 3	gpon	1 gbps
SED	N.E.I Sonho De Crianca	R. Itália, 1001	Nações	tipo 3	gpon	1 gbps
SED	C.E.I. Prof Antonio Lucio	R. Itália, 977	Nações	tipo 3	gpon	1 gbps
SED	N.E.I Bom Sucesso	R. Maria Joaquina Correa & R. Antônio Dos Santos	Barra	tipo 3	gpon	1 gbps
SED	N.E.I Pioneiros	R. Miguel Matte, 585 -	Pioneiros	tipo 3	gpon	1 gbps
SED	N.E.I Recanto Dos Passarinhos	R. Paquistão, 360	Nações	tipo 3	gpon	1 gbps
SED	C.E.I. Presidente Medici	R. Paraguai, 1005	Nações	tipo 3	gpon	1 gbps
SED	N.E.I Rio Das Ostras	R. Pedro Pinto Felipe, 232	São Judas Tadeu	tipo 3	gpon	1 gbps
SED	N.E.I Sao Judas Tadeu	R. Pedro Pinto Felipe, 451	São Judas Tadeu	tipo 3	gpon	1 gbps
SED	N.E.I Novo Tempo	R. Pernambuco, 500	Estados	tipo 3	gpon	1 gbps
SED	N.E.I Meu Primeiro Passo	R. Síria, 756	Nações	tipo 3	gpon	1 gbps
SFA	Procon	R. 2000, 856	Centro	tipo 3	gpon	1 gbps
SGA	Praça Da Cultura	-26.98466, -48.63471	Centro	tipo 3	gpon	1 gbps
SGA	Arquivo Intermediário	-26.99717, -48.65047	Estados	tipo 3	gpon	1 gbps
SGA	Cemitério Da Barra	-27.01298, -48.60939	Barra	tipo 3	gpon	1 gbps
SGA	Cemitério Da Barra Anexo	R. Aquiles Da Costa, 64	Barra	tipo 3	gpon	1 gbps
SGA	Departamento De Patrimônio	R. Dinamarca, 246	Nações	tipo 3	gpon	1 gbps
SGA	C.I.A.S.P - Centro Integrado Ao Servidor Publico	R. Paraguai, 401	Nações	tipo 3	gpon	1 gbps
SGA	Depósito - Marcenaria	R. São Miguel & Rua São Sebastiao	São Francisco De Assis	tipo 3	gpon	1 gbps
SGA	C.I.A.D	Rodovia Br-101, Km 131 Cep 88349-175, Av. Marginal Oeste.	Monte Alegre	tipo 3	gpon	1 gbps
SMA	Parque Ecológico - Hs	Alameda Delfim De Pádua Peixoto Filho, 122	Municípios	tipo 3	gpon	1 gbps
SMA	Secretaria Do Meio Ambiente	Alameda Delfim De Pádua Peixoto Filho, 122	Municípios	tipo 3	gpon	1 gbps

SMA	Secretaria Do Meio Ambiente	R. Angelina, 1900	Municípios	tipo 3	gpon	1 gbps
SOU	Paisagismo	-27.00933, -48.63882	Municípios	tipo 3	gpon	1 gbps
SOU	Secretaria De Obras	Av. Santa Catarina, 801	Estados	tipo 3	gpon	1 gbps
SOU	Secretaria De Obras Da Barra	R. Bento Cunha, 665	Barra	tipo 3	gpon	1 gbps
SPI	Secretaria Da Saúde (Cc Tonho Cilo)	-27.03134, -48.59159	Estaleiro	tipo 3	gpon	1 gbps
SSE	C.E.F.A.G	-26.97533741218407, -48.677192825773446	Várzea Do Ranchinho	tipo 3	gpon	1 gbps
SSE	Radio GM Morro Teleférico	-27.00037, -48.59729	Barra	tipo 3	gpon	1 gbps
SSE	Radio GM Morro Do Pinho	-27.00691, -48.58993	Praia Do Pinho	tipo 3	gpon	1 gbps
SSE	Praça Almirante, Base GM	Av. Atlântica Praça Almirante Tamandaré	Centro	tipo 3	gpon	1 gbps
SSE	Secretaria De Segurança Publica	R. Canoinhas & Av. Marginal Oeste Municípios	Municípios	tipo 3	gpon	1 gbps
SSE	Radio GM Morro Cristo Luz	R. Indonésia, 800	Nações	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Das Nações (CAS) (ESF)	-26.97884, -48.64915	Nações	tipo 3	gpon	1 gbps
SSS	UPA 24H - Nações	-26.98261, -48.64249	Nações	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Do Bairro Dos Estados (Esf)	-26.99709, -48.64921	Estados	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Do Bairro Dos Municípios (Esf)	-27.00393, -48.63504	Municípios	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Da Barra (Esf)	-27.0090067, -48.597426	Barra	tipo 3	gpon	1 gbps
SSS	Pai - Posto De Atenção Infantil	-27.00901, -48.64176	Municípios	tipo 3	gpon	1 gbps
SSS	Posto De Saude Taquaras	-27.01050, -48.58035	Taquaras	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Da Nova Esperança (Esf)	-27.02485, -48.61378	Nova Esperança	tipo 3	gpon	1 gbps
SSS	CAPS AD	5ª Av. & R. Curitibanos	Municípios	tipo 3	gpon	1 gbps
SSS	N.A.I Núcleo de Atenção ao Idoso	Alameda Delfim De Pádua Peixoto Filho	Municípios	tipo 3	gpon	1 gbps
SSS	Samu - Serviço De Atendimento Móvel De Urgência	Alameda Dos Estados Policial Luiz Carlos Rosa, 25	Estados	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Do Ariribá (ESF)	Av. Dos Tucanos, 300	Ariribá	tipo 3	gpon	1 gbps
SSS	UBS - Pioneiros	Av. Osmar Souza Nunes, 260 -	Pioneiros	tipo 3	gpon	1 gbps
SSS	Ambulatório De Especialidades Nações	Av. Palestina, 150	Nações	tipo 3	gpon	1 gbps
SSS	Secretaria Da Pessoa Idosa	R. 1822, 614	Centro	tipo 3	gpon	1 gbps
SSS	Ambulatorio De Especialidades Centro	R. 1926, 1428	Centro	tipo 3	gpon	1 gbps
SSS	CTA/CISS - Centro De Testagem E Aconselhamento	R. 2350, 560 & 4ª Av.	Centro	tipo 3	gpon	1 gbps

SSS	Caps Ii - Centro De Atenção Psicossocial	R. 916, 382	Centro	tipo 3	gpon	1 gbps
SSS	Vigilância Epidemiológica	R. 916, 535	Centro	tipo 3	gpon	1 gbps
SSS	Laboratório Municipal	R. 990, 81	Centro	tipo 3	gpon	1 gbps
SSS	Transporte E Manutenção Da Saúde	R. Acre, 139	Estados	tipo 3	gpon	1 gbps
SSS	COE - Centro Odontológico Especializado	R. Ceara & R. Sao Paulo Estados	Estados	tipo 3	gpon	1 gbps
SSS	Posto De Saúde Da Vila Real (Esf)	R. Dom Abelardo, 400 - Vila Real	Vila Real	tipo 3	gpon	1 gbps
SSS	CCPU - Centro De Controle De Pragas Urbanas	R. Dom Henrique & R. Arroio Trinta Jardim Iate Clube	Jardim Iate Clube	tipo 3	gpon	1 gbps
SSS	UPA 24H - Barra	R. Jardim Da Saudade, 1500	Barra	tipo 3	gpon	1 gbps
SSS	Farmacia Sul	R. Jardim Da Saudade, 250	Barra	tipo 3	gpon	1 gbps
SSS	Upa Barra	R. Jardim Da Saudade, 37	Barra	tipo 3	gpon	1 gbps
SSS	Ubs - Sao Judas Tadeu	R. Mauricio Venancio Cunha, 130	São Judas Tadeu	tipo 3	gpon	1 gbps
SSS	Cefir - Centro De Fisioterapia E Reabilitação	R. Mexico, 875	Nações	tipo 3	gpon	1 gbps
SSS	Nam - Núcleo De Atenção À Mulher	R. Mexico, 875	Nações	tipo 3	gpon	1 gbps
SSS	Vigilancia Sanitaria	R. Suica, 150	Nações	tipo 3	gpon	1 gbps
SSS	Ubs - Estaleiro	R. Vereador Domingos Da Fonseca - Estaleiro	Estaleiro	tipo 3	gpon	1 gbps
STC	Casa De Passagem	-26.980544799779217, -48.67781332804838	Várzea Do Ranchinho	tipo 3	gpon	1 gbps
STC	Centro Comunitário Do Bairro Dos Municípios (Casa Da Sogra)	-27.00855, -48.64088	Municípios	tipo 3	gpon	1 gbps
STC	Cras Construindo Cidadania	-27.01815, -48.60421	São Judas Tadeu	tipo 3	gpon	1 gbps
STC	Casa Do Autista	Alameda Delfim De Pádua Peixoto Filho	Municípios	tipo 3	gpon	1 gbps
STC	Casa Da Mulher E Do Voluntário	R. 2850, 285	Centro	tipo 3	gpon	1 gbps
STC	Secretaria De Desenvolvimento E Inclusão Social	R. 3100, 876	Centro	tipo 3	gpon	1 gbps
STC	Conselho Tutelar	R. 902, 566	Centro	tipo 3	gpon	1 gbps
STC	Centro Comunitário Nova Esperança	R. Alécio Domingos Linhares, 130	Nova Esperança	tipo 3	gpon	1 gbps
STC	Cras Espaço Cidadão	R. Brusque, 127	Municípios	tipo 3	gpon	1 gbps
STC	Instituição De Acolhimento - Lar Do Adolescente	R. Dom Miguel, 484 - Vila Real	Vila Real	tipo 3	gpon	1 gbps
STC	Departamento De Economia Artesanal (Dea) Colônia	R. Francisco Victor, 40	Barra	tipo 3	gpon	1 gbps
STC	Centro Comunitário Do Bairro Das Nações	R. Ilhas Marshall, 145	Nações	tipo 3	gpon	1 gbps
STC	Creas	R. Iraque, 289	Nações	tipo 3	gpon	1 gbps

STC	Centro De Convivência Da Família (Ctc)	R. Itália, 1059	Nações	tipo 3	gpon	1 gbps
STC	Centro Comunitário Da Barra.	R. Manoel Correa, 359	Barra	tipo 3	gpon	1 gbps
STC	Centro Comunitário Do Bairro São Judas	R. Pedro Pinto Felipe, 162	São Judas Tadeu	tipo 3	gpon	1 gbps
STU	Pit - Ponto De Informações Turísticas	Av. Do Estado Dalmo Vieira, 5041	Centro	tipo 3	gpon	1 gbps
STU	Passarela Da Barra (Lado Barra)	Av. Normando Tedesco, 1743	Barra	tipo 3	gpon	1 gbps
STU	Secretaria De Turismo E Desenvolvimento Econômico	R. 2850, 566	Centro	tipo 3	gpon	1 gbps
STU	Sala Do Empreendedor	R. Dinamarca, 172	Nações	tipo 3	gpon	1 gbps
	Praça Almirante Tamandaré	-26.98697, -48.63252	Centro	tipo 3	gpon	1 gbps
	Gelmar - Escoteiro Leao Do Mar	-27.00933, -48.63882	Municípios	tipo 3	gpon	1 gbps
	Associação Dos Moradores Do Estaleirinho	-27.05684, -48.59653	Estaleirinho	tipo 3	gpon	1 gbps
	Ong Viva Bicho	R. Antônio Lopes Goncalves Bastos, 1010 - Nova Esperanca	Nova Esperança	tipo 3	gpon	1 gbps
	Ong Viva Bicho - CAM	R. Antônio Lopes Goncalves Bastos, Nº 1010 - Nova Esperanca	Nova Esperança	tipo 3	gpon	1 gbps
	Compur	R. Dinamarca, 175	Nações	tipo 3	gpon	1 gbps
	Portal De Acesso Morro Do Careca	R. Virginia Ângelo Severino, 2 - Praia Dos Amores	Praia Dos Amores	tipo 3	gpon	1 gbps
SEGOV	Dog Park 4ª Avenida Com 2870	4ª Avenida Com Rua 2870	Centro	tipo 4	gpon	1 gbps
SEGOV	Praça Kurt Amann	Av Atlântica,	Centro	tipo 4	gpon	1 gbps
SEGOV	Praça Molhe Barra Sul	Av. Atlantica Molhe Da Sul	Barra Sul	tipo 4	gpon	1 gbps
SEGOV	Praça Da Cultura	Av. Da Lagoa & R. 511	Centro	tipo 4	gpon	1 gbps
SEGOV	Dog Park Do Shurastey	Av. Do Estado Dal Vieira, 4029	Nações	tipo 4	gpon	1 gbps
SEGOV	Praça Do Pescador	R. Antonio Domingos Da Silva & Praça Do Pescador	Barra	tipo 4	gpon	1 gbps
SEGOV	Praça Manoel Germano Correa	R. Paraguai & Av. Palestina	Nações	tipo 4	gpon	1 gbps
SEGOV	Dog Park Rua 1911	Rua 1911, 2	Centro	tipo 4	gpon	1 gbps
SEGOV	Dog Park Rua 3208	Rua 3208 Com Rua 3708	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.97181467293969, -48.63312080267655	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.97523817301764, -48.6349376633493	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.97743665956578, -48.63492227896578	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.98016201293991, -48.63503790695072	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.98310376031339, -48.63367508918677	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.98523528533421, -	Centro	tipo 4	gpon	1 gbps

		48.6328144467543				
SSE	Sse - Hotspot	-26.98742597087312, -48.63116240716548	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.98927860981992, -48.62900347569612	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.99156110166463, -48.62836998383209	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.99428935450317, -48.62698401745965	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.99676142376023, -48.62515197366642	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-26.99788247353347, -48.62351050545991	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-27.00096024690055, -48.62125149078776	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-27.00198729052183, -	Centro	tipo 4	gpon	1 gbps

		48.61839859999326				
SSE	Sse - Hotspot	-27.00270552596956, -48.6166223893072	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-27.00372644057709, -48.61425806804992	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-27.00501788303792, -48.61136064054314	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-27.00544055388772, -48.60592511191233	Centro	tipo 4	gpon	1 gbps
SSE	Sse - Hotspot	-27.00551842036097, -48.60741812174057	Centro	tipo 4	gpon	1 gbps
STU	Passarela Da Barra (Lado Bc)	Av. Normando Tedesco, 1743 Sul	Barra Sul	tipo 4	gpon	1 gbps
STU	Passarela Da Barra - Hs	Av. Normando Tedesco, 4950 Sul	Barra Sul	tipo 4	gpon	1 gbps
	Deck Pontal Norte	Av. Atlantica Deck Pontal Norte Inicio	Pioneiros	tipo 4	gpon	1 gbps
	Atracadouro Barra Sul	Av. Atlantica, 6006 Sul	Barra Sul	tipo 4	gpon	1 gbps
	Deck Pontal Norte Rack01	Av. Atlantica, 65 -	Pioneiros	tipo 4	gpon	1 gbps
	Hs Avenida Central	Av. Central, 128	Centro	tipo 4	gpon	1 gbps
	Estação Rodoviária	Av. Santa Catarina, 347	Estados	tipo 4	gpon	1 gbps
	Hs Patio Hospital Ruth Cardoso	R. Angelina & Hmrc Municipios	Municípios	tipo 4	gpon	1 gbps
BC TRÂNSITO	Sem 3ª Av X Av Alvin Bauer	3ª Av. & Av. Alvin Bauer	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 3ª Av X R 1500	3ª Av. & R. 1500	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 3ª Av X R 3000	3ª Av. & R. 3000	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 3ª Avenida X Rua 3122	3ª Av. & R. 3122	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 3ª Av X R 904	3ª Av. & R. 904	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 4ª Av X Av Alvin Bauer	4ª Av. & Av. Alvin Bauer	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 4ª Av X R 1500	4ª Av. & R. 1500	Centro	tipo 5	gpon	1 gbps

BC TRÂNSITO	Sem 4ª Av X R 2000	4ª Av. & R. 2000	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 4ª Av X R 2500 X R 2550	4ª Av. & R. 2500	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 4ª Av X R 3000	4ª Av. & R. 3000	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 4ª Av X R 3100	4ª Av. & R. 3100	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 4ª Av X R 904	4ª Av. & R. 904	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 5ª Av X 6ª Av X R Canoinhas	5ª Av. & 6ª Av. Municipios	Municipios	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 5ª Av X R Araquari	5ª Av. & R. Araquari Municipios	Municipios	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 5ª Av X R Chapecó	5ª Av. & R. Chapeco Municipios	Municipios	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem 5ª Av X R Dom Luiz	5ª Av. & R. Dom Luiz Vila Real	Vila Real	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Atlântica X Av Central	Av. Atlantica & Av. Central	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Belgica X R Dinamarca	Av. Belgica & R. Dinamarca	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X Av Alvin Bauer	Av. Brasil & Av. Alvin Bauer	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X Av Central	Av. Brasil & Av. Central	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 1101	Av. Brasil & R. 1101	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 1131	Av. Brasil & R. 1131	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 1500	Av. Brasil & R. 1500	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 1901	Av. Brasil & R. 1901	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 2000	Av. Brasil & R. 2000	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 2500	Av. Brasil & R. 2500	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 3000	Av. Brasil & R. 3000	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Avenida Brasil X Rua 3100	Av. Brasil & R. 3100	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 3300	Av. Brasil & R. 3300	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R 3700	Av. Brasil & R. 3700	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Brasil X R Osmar Souza Nunes	Av. Brasil & R. Osmar. Souza Nunes	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Central X Av Alvin Bauer	Av. Central & Av. Alvin Bauer	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Das Flores X Goias	Av. Das Flores & Goias Estados	Estados	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Do Estado X Alvin Bauer X São Paulo	Av. Do Estado Dalmo Vieira & Av. Alvin Bauer Estados	Estados	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Do Estado X R Isidoro Caetano	Av. Do Estado Dalmo Vieira & R. Isidoro Caetano	Pioneiros	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Do Estado X R 1131 X R Marrocos	Av. Do Estado Dalmo Vieira & R. Marrocos Nações	Nações	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Do Estado X R Protásio B. Caetano	Av. Do Estado Dalmo Vieira & R. Protasio B. Caetano	Pioneiros	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Do Estado X R Síria	Av. Do Estado Dalmo Vieira & R. Siria	Nações	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Marginal Leste X R 2500	Av. Marginal Leste & R. 2500	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Marginal Leste X R 3100	Av. Marginal Leste & R. 3100	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Martin Luther (Continuação) X Avenida	Av. Martin Luther & Av. Das Flores Estados	Estados	tipo 5	gpon	1 gbps

	Das Flores (Aqueduto)					
BC TRÂNSITO	Sem Av Martin Luther X R	Av. Martin Luther & R. Dinamarca	Nações	tipo 5	gpon	1 gbps
	Dinamarca					
BC TRÂNSITO	Sem Av Martin Luther X R Israel	Av. Martin Luther & R. Israel	Nações	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Martin Luther X R Jordânia	Av. Martin Luther & R. Jordania	Nações	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Martin Luther X R Marrocos	Av. Martin Luther & R. Marrocos	Nações	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Av Martin Luther X R Síria	Av. Martin Luther & R. Siria	Nações	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Rua 3198 X Rua 3122	R. 3198 & R. 3122	Centro	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem R Dom Henrique X R Dom Felipe	R. Dom Henrique & Dom Felipe Vila Real	Vila Real	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem R Dom Henrique X R Dom Daniel	R. Dom Henrique & R. Dom Daniel Vila Real	Vila Real	tipo 5	gpon	1 gbps
BC TRÂNSITO	Sem Rua Venezuela X Avenida Dos Tucanos	R. Venezuela & Av. Dos Tucanos	Ariribá	tipo 5	gpon	1 gbps
BCPREVI	Cam Bcprevi	R. Dinamarca, 175	Nações	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 936	Av. Atlantica & R. 1601	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 2390	Av. Atlantica & R. 1900	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 4144	Av. Atlantica & R. 3850	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Pontal Norte	Av. Atlantica Corpo De Bombeiros Pbs	Pioneiros	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 1310	Av. Atlantica, 1310	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 1576	Av. Atlantica, 1576 & R. 1001	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica - Praca Alm. Tamandaré	Av. Atlantica, 2554	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 3030	Av. Atlantica, 3030	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 3675	Av. Atlantica, 3675 & R. 3300	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 4740	Av. Atlantica, 4740	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Barra Sul	Av. Atlantica, 48 Sul	Barra Sul	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 5443	Av. Atlantica, 5443	Centro	tipo 5	gpon	1 gbps
SITE-PRAIA	Cam Obra - Atlantica 640	Av. Atlantica, 640 -	Pioneiros	tipo 5	gpon	1 gbps
SSE	Cam Gm Secretaria Do Meio Ambiente - Laboratorio	Alameda Delfim De Padua Peixoto Filho, 122	Municipios	tipo 5	gpon	1 gbps
SSE	Cam Gm Secretaria Do Meio Ambiente - Sede	Alameda Delfim De Padua Peixoto Filho, 122	Municipios	tipo 5	gpon	1 gbps
SSE	Cam Almirante Tamandare	Av. Atlantica Praca Almirante Tamandare	Centro	tipo 5	gpon	1 gbps
SSE	Cam Gm Praça Da Biblia	Av. Da Lagoa & R. 511	Centro	tipo 5	gpon	1 gbps
SSE	Cam Gm Bc TRÂNSITO	Av. Santa Catarina, 701	Estados	tipo 5	gpon	1 gbps
SSE	Cam Gm Secretaria De Obras	Av. Santa Catarina, 801	Estados	tipo 5	gpon	1 gbps
SSE	Cam Gm Posto De Saude Central	R. 1500, 1100	Centro	tipo 5	gpon	1 gbps
SSE	Cam Gm Secretaria Da Saude - Central Veiculos	R. 1500, 1100	Centro	tipo 5	gpon	1 gbps

SSE	Cam Gm Funservir	R. 902, 566	Centro	tipo 5	gpon	1 gbps
SSE	Cam Gm Hospital Ruth Cardoso 02	R. Angelina, 168	Municípios	tipo 5	gpon	1 gbps
SSE	Cam Gm Hospital Ruth Cardoso 01	R. Angelina, 208	Municípios	tipo 5	gpon	1 gbps
SSE	Cam Gm Secretaria De Obras Da Barra	R. Bento Cunha & R. Bento Cunha	Barra	tipo 5	gpon	1 gbps
SSE	Cam Gm Secretaria Da Educação	R. Camboriu, 100	Municípios	tipo 5	gpon	1 gbps
SSE	Cam Gm Upa 24 Horas - Bairro Das Nações 01	R. Israel, 205	Nações	tipo 5	gpon	1 gbps
SSE	Cam Gm Upa 24 Horas - Bairro Das Nações 02	R. Israel, 205	Nações	tipo 5	gpon	1 gbps
SSS	Farmácia Municipal E Farmácia De Medicamentos Excepcionais	4ª Av. & R. 2438	Centro	tipo 5	gpon	1 gbps
	Cam Upa Barra	R. Jardim Da Saudade, 1500	Barra	tipo 5	gpon	1 gbps

9.5.1. Poderão ocorrer alterações de endereços entre os pontos listados e os pontos necessários nesta primeira etapa considerando a dinâmica do município, neste caso será fornecida nova listagem de pontos essenciais a serem executados dentro dos 90 dias.

9.5.2. Os demais pontos que não estão nesta lista deverão ser instalados em até:

9.5.2.1. Nó (Nodes) Distribuição e Eventos: em até 5 dias úteis;

9.5.2.2. Nó (Node) HotSpot: 10 dias úteis;

9.5.2.3. Nó (Node) Dispositivos IoT: 15 dias úteis.

9.5.3. A não execução de instalação dentro dos prazos acarretará em 2% (dois por cento) do valor do item por ocorrência;

9.5.4. Instalação da solução no ambiente virtual, disponibilizado pela Contratada para os sistemas.

9.5.5. A contratada deverá entregar relatório de cada etapa da implantação, assim como a documentação final, onde deverá conter todos os detalhes de configuração e instalação.

9.5.6. As entregas para compor a solução devem ocorrer em até 90 (sessenta) dias úteis após a emissão da nota de empenho e deverá ocorrer na Divisão de TI da Prefeitura de Balneário Camboriú.

9.5.7. Não haverá a possibilidade de subcontratação de parte do objeto, sendo que a contratada que deverá realizar as etapas dos serviços ou o próprio fabricante da solução.

9.5.8. A finalização do contrato se dará após o fim da garantia.

9.6. Mecanismos formais de comunicação:

9.6.1. O mecanismo formal de comunicação é o registro de abertura de chamado. Isto não impede que sejam usados canais informais de comunicação instantâneo ou e-mail.

9.7. Manutenção de Sigilo e Normas de Segurança:

9.7.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei,

independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

10. MODELO DE GESTÃO DO CONTRATO

10.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

10.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostilamento.

10.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

10.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

10.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

10.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

10.7. A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste TERMO DE REFERÊNCIA, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

10.8. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos itens contratados para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

10.9. A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

10.10. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis, além dos fatores redutores, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas neste TERMO DE REFERÊNCIA.

10.11. Os responsáveis quanto a fiscalização desta contratação serão os:

10.11.1. Gestor do Contrato: Leandro Arthur Rodrigues da Silva, Matrícula 56.114;

10.11.2. Fiscal Administrativo: Bruna Emerenciana Alves Diniz da Silva, Matrícula 52.063;

10.11.3. Fiscal Setorial: Sandro Aparecido da silva Andrade, Matrícula 56.673;

10.11.4. Fiscal Técnico: Murilo Allan Sodré de Souza, Matrícula 56.750.

11. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

11.1. Os serviços e materiais fornecidos deverão estar em conformidade com as especificações técnicas descritas no Estudo Técnico Preliminar. A aceitação do objeto será realizada após a verificação da conformidade dos serviços e materiais fornecidos com as especificações técnicas e a realização de testes de funcionamento.

11.2. Disponibilidade dos Serviços:

11.3. A disponibilidade mínima mensal do serviço é de:

11.4. Nós (Nodes) Core: Mínimo 99,5% 11.5 Nós (Nodes) Anel: Mínimo 98,5% 11.6 Nós (Nodes) Distribuição: Mínimo 98% 11.7 Nós (Nodes) HotSpot Externo: Mínimo 99,5% 11.8 Nós (Nodes) Dispositivos e IoT: Mínimo 97%

11.5. O percentual de disponibilidade é calculado com base no tempo em que o serviço permanece em condições normais de funcionamento durante um mês.

11.6. Descontos por Indisponibilidade:

11.7. Sempre que a disponibilidade do link estiver abaixo dos limites mínimos:

Recurso	Disponibilidade (Tempo ao mês)	Penalidade
NÓ CORE	Inferior a 99, 5 %	10 % do valor do NÓ (NODE) para cada hora de indisponibilidade
NÓ ANEL	Inferior a 99, 0 %	8 % do valor do NÓ (NODE) para cada hora de indisponibilidade
NÓ DISTRIBUIÇÃO	Inferior a 98, 5 %	Desconto do valor mensal do NÓ (NODE)
NÓ HOTSPOT	Inferior a 98, 0 %	Desconto do valor mensal do NÓ (NODE)
NÓ DISPOSITIVO IoT	Inferior a 97, 5 %	Desconto do valor mensal do NÓ (NODE)

11.8. Taxa de Erro:

11.8.1. A contratada deve medir a taxa de erro na rede.

11.8.2. O retardo máximo permitido é de 110 ms.

11.9. Tempo de Solução:

11.9.1. O tempo máximo para solução ou reparo é de 6 horas (exceto para configurações de roteamento e QoS, que são de 4 horas).

11.10. Paradas Programadas:

11.10.1. A contratada deve comunicar com antecedência, no mínimo sete dias, as paradas programadas para manutenção preventiva e adaptações na rede;

11.10.2. O limite anual para paralisações é de 24 horas.

11.11. Suporte Técnico:

11.11.1. O suporte deve estar disponível 24 horas por dia, todos os dias da semana, independentemente de feriados ou finais de semana.

11.12. Para Pagamentos: As notas fiscais deverão ser protocoladas diretamente via web, no sistema Comunicação 1DOC, onde serão encaminhadas para os setores responsáveis darem o devido seguimento.

11.13. O procedimento para protocolo consistirá em:

11.13.1. 1º Passo: Acessar o Site (sítio eletrônico) da Prefeitura e a opção "Protocolos Eletrônicos";

11.13.2. 2º Passo: Criar um login de acesso em nome da empresa usando CNPJ;

11.13.3. 3º Passo: No campo "Assunto" escolher a opção: " Notas Fiscais e Contratos com a Divisão de TI (DITI)";

11.13.4. 4º Passo: Informar o número dos empenhos e anexar os documentos pertinentes.

11.14. Cada protocolo deverá conter:

11.14.1. Apenas uma nota fiscal;

11.14.2. Certidão Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União;

11.14.3. Certidão Negativa Estadual;

11.14.4. Certidão Negativa Municipal;

11.14.5. Certificado de Regularidade de FGTS;

11.14.6. Certidão Negativa de Trabalhistas;

11.15. O Pagamento será efetuado em até 30 dias após protocolo, caso não haja solicitação de documentos adicionais.

12. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR

12.1. A opção pela contratação com menor valor se justifica especialmente quando se dispõe de informações precisas sobre o objeto a ser executado. Essa abordagem possibilita que a administração pública tenha uma margem de precisão mais apurada na definição dos custos envolvidos, culminando em uma contratação potencialmente mais econômica;

12.2. O julgamento tipo MENOR VALOR GLOBAL, busca a agilidade nos serviços de fiscalização na prestação de serviços (efetuada pela empresa contratada) dos itens que fazem parte da especificidade do objeto a ser contratado, bem como trazer segurança, para que nossos servidores possam exercer suas funções, sem que sejam interrompidas pela falta de organização, adequação e má prestação de serviços;

12.3. Sob essa perspectiva, a aglutinação de serviços em lote único, conjugada à adoção de julgamento pelo menor preço global, não se revela fator impeditivo à competitividade desejada entre todos os fornecedores, aptos a prestar o serviço de forma integrada;

12.4. Considerando que a prestação dos serviços será realizada nas dependências da Administração Municipal, incluindo quaisquer gastos ou despesas com mão de obra, materiais e produtos necessários, EPI's, transporte, deslocamentos, hospedagem, alimentação, tributos, ônus previdenciários e trabalhistas, seguros e outros encargos ou despesas incidentes. Esta contratação gera economicidade proporcional pela redução de custos e despesas podendo uma equipe apenas atender o objeto do contrato;

12.5. Vale ainda ressaltar que a contratação por preço global é adequada quando existem informações precisas sobre o objeto a ser executado;

12.6. A empreitada por preço global deve ser adotada quando for possível definir previamente no projeto, com boa margem de precisão, as quantidades dos serviços a serem executados; enquanto que a empreitada por preço unitário deve ser preferida para objetos que, por sua natureza, não permitam a precisa indicação dos quantitativos orçamentários." TCU. Informativo de Licitações e Contratos nº 162/2013 (Acórdão 1978/2013-Plenário).

13. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

13.1. O valor estimado da contratação é de R$ 3.856.849,75 (Três milhões oitocentos e cinquenta e seis mil oitocentos e quarenta e nove reais e setenta e cinco centavos);

13.2. Não foi encontrado no painel de preços a contratação do objeto pretendido, conforme demonstrado no documento anexo.

14. CRONOGRAMA FÍSICO E FINANCEIRO

14.1. Cronograma Físico das instalações dos nós de rede

Tipo	Descrição	Vel	30 dias	60 dias	90 dias	Total
1	Instalação NODES CORE (gateways) Concentradores. Criticidade 0, Disponibilidade 99,5%	10 Gb	2			2
2	Instalação NODES ANEL Secretarias. Criticidade 1, Disponibilidade 98,5%	10 Gb	4			4
3	Instalação NODES DISTRIBUIÇÃO Unidades Administrativas Criticidade 2, Disponibilidade 98%	1 Gb	60	60	40	160
4	Instalação NODES HOTSPOT EXTERNOS. Criticidade 3, Disponibilidade 98%	1 Gb	9	8	20	37
5	Instalação NODES DISPOSITIVOS IOT Criticidade 4, Disponibilidade 97%	1 Gb		55	55	110

15. CRONOGRAMA DE PAGAMENTO

Tipo	Descrição	Qtde	Valor Instalação e Mensal	1º mês	2º mês	3º mês	4º mês	5º mês	6º mês	7º mês	8º mês	9º mês	10º mês	11º mês	12º mês	1º ano
1	Instalação NODES CORE (gateways). Concentradores. Criticidade 0, Disponibilidade 99,5%	2	R$ 14.000,00	R$ 28.000,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
2	Instalação NODES ANEL Secretarias. Criticidade 1, Disponibilidade 98,5%	4	R$ 671,25	R$ 2.685,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
3	Instalação NODES DISTRIBUIÇÃO Unidades Administrativas Criticidade 2, Disponibilidade 98%	160	R$ 394,25	R$ 23.655,00	R$ 23.655,00	R$ 15.770,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
4	Instalação NODES HOTSPOT EXTERNOS. Criticidade 3, Disponibilidade 98%	37	R$ 294,25	R$ 2.648,25	R$ 2.354,00	R$ 5.885,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
5	Instalação NODES DISPOSITIVOS IOT Criticidade 4, Disponibilidade 97%	110	R$ 294,25	R$ 0,00	R$ 16.183,75	R$ 16.183,75	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00	R$ 0,00
6	Instalação NODES EVENTOS que possuem as mesmas características dos **NÓS (NODES) Item 3.** Sob Demanda, Instalação em 5 Dias	50	R$ 324,25	R$ 0,00	R$ 0,00	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 16.212,50

7	Instalação NODES HOTSPOT que possuem as mesmas características dos **NÓS (NODES) Item 4**. Sob Demanda, Instalação em 10 Dias	50	R$ 324,25	R$ 0,00	R$ 0,00	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 1.621,25	R$ 16.212,50
8	Instalação NODES DISPOSITIVOS IOT que possuem as mesmas características dos **NÓS (NODES) Item 5**. Sob Demanda, Instalação em até 15 Dias	100	R$ 294,25	R$ 0,00	R$ 0,00	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 2.942,50	R$ 29.425,00
9	Transferência de NODE de local	160	R$ 147,50	R$ 0,00	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,45	R$ 2.145,50	R$ 23.600,00
10	Suporte NODES CORE (gateways). Concentradores. Criticidade 0, Disponibilidade 99,5%	240	R$ 10.875,00	R$ 0,00	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,27	R$ 23.727,30	R$ 261.000,00
11	Suporte NODES ANEL Secretarias. Criticidade 1, Disponibilidade 98,5%	480	R$ 5.155,00	R$ 0,00	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,54	R$ 22.494,60	R$ 247.440,00
12	Suporte NODES DISTRIBUIÇÃO Unidades Administrativas. Criticidade 2, Disponibilidade 98%	19200	R$ 1.215,00	R$ 0,00	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,72	R$ 212.072,80	R$ 2.332.800,00
13	Suporte NODES HOTSPOT EXTERNOS similares aos do Item 3. Criticidade 3, Disponibilidade 98%	444	R$ 835,00	R$ 0,00	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,63	R$ 33.703,70	R$ 370.740,00
14	Suporte NODES DISPOSITIVOS IOT. Criticidade 4, Disponibilidade 97%	1320	R$ 320,00	R$ 0,00	R$ 0,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 42.240,00	R$ 422.400,00

15.1.1. Valores máximos mensais/anuais, considerando as solicitações e demandas de instalação de pontos, transferência de node, Instalação NODES EVENTOS que possuem as mesmas características dos NÓS (NODES) Item 3. Sob Demanda, Instalação em 5 Dias, Instalação NODES HOTSPOT que possuem as mesmas características dos NÓS (NODES) Item 4. Sob Demanda, Instalação em 10 Dias e Instalação NODES DISPOSITIVOS IOT que possuem as mesmas características dos NÓS (NODES) Item 5. Sob Demanda, Instalação em até 15 Dias. Estes pontos possivelmente não serão utilizados em sua totalidade pois, é de acordo com a necessidade da Administração.

15.1.2. O contrato terá vigência de 12 (doze) meses, renováveis por igual período dentro dos limites estabelecidos pela Lei Federal nº 14.133/2021.

16. PESQUISA DE MERCADO

16.1. Considerando a singularidade desta contratação, onde se trata de condições exclusivas para a implementação da rede metropolitana (MAN), é fundamental justificar a escolha com base em alguns fatores essenciais:

16.1.1. A análise de mercado indicou que os preços praticados para a implementação da rede metropolitana estão compatíveis com os padrões de mercado. A contratação foi analisada considerando todas as especificações técnicas e serviços inclusos, resultando em um custo benefício favorável.

16.1.2. Foram pesquisados preços de diferentes fornecedores nacionais. A análise comparativa revelou que a forma de orçamento selecionada oferece condições mais vantajosas, tanto em termos de preço quanto de qualidade dos serviços e equipamentos fornecidos, assegurando compatibilidade com as necessidades da Administração.

16.1.3. As condições oferecidas pelos orçamentos, incluindo prazos de entrega, qualidade dos materiais e suporte técnico, são superiores às encontradas em outras propostas. A quantidade de equipamentos e serviços demandados foi especificada de acordo com as necessidades precisas do projeto, garantindo adequação plena ao escopo definido.

16.1.4. A consulta ao portal de compras públicas não identificou soluções equivalentes disponíveis em termos de quantidade e descrição técnica que atendessem aos requisitos do projeto da rede metropolitana. A análise demonstrou a inexistência de alternativas compatíveis, justificando a singularidade e a exclusividade da contratação.

16.1.5. A especificidade dos equipamentos e serviços necessários para a rede metropolitana não foi atendida por soluções disponíveis no mercado em quantidade suficiente ou com as descrições técnicas exigidas. Isso reforça a necessidade de orçamento direcionado, que contemple todas as demandas técnicas e operacionais do projeto.

16.2. Dessa forma, a justificativa para esta contratação em condições exclusivas se baseia em uma análise detalhada e criteriosa de mercado, assegurando que os preços são compatíveis, que as condições oferecidas são as melhores possíveis, e que não há soluções disponíveis no mercado que atendam plenamente às especificações exigidas.

17. ADEQUAÇÃO ORÇAMENTÁRIA

17.1. Por se tratar de um Pregão, as despesas ocorrerão por conta das dotações orçamentárias do Departamento Solicitante ou Secretaria que solicitar a contratação.

18. MATRIZ DE RISCO

Categoria	Risco	Descrição	Impacto	Probabilidade	Ação Mitigadora
Implementação	Atrasos no cronograma	Atrasos na instalação da infraestrutura e equipamentos	Alto	Média	Planejamento detalhado e cronograma rigoroso
Implementação	Falhas na instalação	Erros na instalação dos equipamentos e infraestrutura	Alto	Média	Treinamento adequado para a equipe de instalação e supervisão contínua

Segurança	Vulnerabilidades cibernéticas	Possíveis ataques cibernéticos e falhas de segurança	Alto	Média	Medidas de segurança robustas, como firewalls, criptografia e auditorias periódicas
Segurança	Acesso não autorizado	Acesso não autorizado à rede por terceiros	Alto	Média	Implementação de autenticação multifator e controle rigoroso de acessos
Financeiro	Estouro de orçamento	Custos não previstos excedendo o orçamento inicial	Médio	Média	Incluir margem de contingência e monitorar custos continuamente
Financeiro	Atrasos em pagamentos	Atrasos nos pagamentos aos fornecedores, afetando a continuidade dos serviços	Médio	Baixa	Estabelecer cronograma de pagamentos e reservar fundos para pagamentos pontuais
Conformidade	Falta de conformidade	Não conformidade com regulamentações e normas técnicas	Alto	Baixa	Garantir conformidade com normas locais e internacionais
Operacional	Falhas de desempenho dos equipamentos	Falhas nos dispositivos instalados comprometendo a operação	Médio	Média	Selecionar equipamentos de alta qualidade e realizar testes exaustivos
Operacional	Falta de redundância	Falta de sistemas redundantes para garantir a continuidade do serviço	Alto	Média	Implementação de soluções redundantes e sistemas de backup
Treinamento	Insuficiência de treinamento	Falta de capacitação para operação eficiente da rede	Médio	Média	Planejar e executar programas abrangentes de treinamento e capacitação
Fornecedores	Desempenho inadequado dos fornecedores	Fornecedores não cumprirem os prazos ou especificações técnicas	Médio	Média	Seleção criteriosa de fornecedores e acompanhamento contínuo do desempenho
Tecnológico	Obsolescência tecnológica	Tecnologias utilizadas tornarem-se obsoletas rapidamente	Alto	Média	Escolha de tecnologias escaláveis e atualizáveis
Manutenção	Falhas na manutenção preventiva e corretiva	Problemas não identificados ou corrigidos prontamente	Alto	Média	Contratos de manutenção preventiva e corretiva com SLA definidos
Ambiental	Impacto ambiental da instalação	Danos ao meio ambiente durante a instalação da infraestrutura	Médio	Baixa	Realizar avaliações de impacto ambiental e seguir diretrizes de sustentabilidade
Comunicação	Falha na comunicação com	Falta de informações claras para todas as partes envolvidas	Médio	Alta	Estabelecer canais de comunicação claros e

	as partes interessadas				frequentes com todas as partes interessadas
Legal	Problemas jurídicos e de conformidade legal	Questões legais imprevistas relacionadas à contratação	Alto	Baixa	Consultoria jurídica contínua para garantir conformidade legal
Logística	Problemas logísticos na entrega e instalação dos equipamentos	Atrasos na entrega e dificuldades na instalação dos equipamentos	Médio	Média	Planejamento logístico detalhado e parcerias com fornecedores confiáveis
Reputacional	Danos à reputação	Falhas no projeto podem	Alto	Média	Comunicação transparente
		causar danos à reputação do município e das partes envolvidas			com a comunidade e gestão de crises eficiente
Usabilidade	Interface do usuário inadequada	Interfaces de usuário mal projetadas dificultando a utilização da rede	Médio	Média	Testes de usabilidade e design centrado no usuário