ANEXO DE EDITAL

ANEXO I - ESPECIFICAÇÃO DO OBJETO
SOLUÇÃO INTEGRADA E GERENCIADA DE INFOVIA MUNICIPAL

1. OBJETO

1.1. Este Anexo especifica a rede de dados, as classes permanentes C1 a C5, a conectividade temporária C6, a extensão C7 de resiliência sob demanda e a telefonia IP/VoIP sob demanda, bem como as informações municipais necessárias à validação do escopo. Rede, eventos e telefonia possuem dimensionamento, acionamento, testes e medição próprios, sob responsabilidade integrada de execução.

1.2. A escolha técnica institucional estabelece arquitetura, requisitos por classe e critérios de operação aplicáveis a diferentes projetos, inclusive à Prefeitura de Maringá. Quantidades, cobertura, expansão e demanda de serviços serão definidas no projeto específico. Os parâmetros técnicos por classe e os níveis de serviço permanecem como referência institucional.

1.3. O projeto integra serviços, recursos e fornecedores sob responsabilidade técnica coordenada da executora. O resultado esperado é a continuidade verificável dos serviços públicos, com capacidade fim a fim, segurança, interoperabilidade, documentação e evidências de implantação e operação.

1.3.1. Os destinatários da solução são exclusivamente entes e entidades da Administração Pública direta e indireta, nos limites legais e estatutários do InPACTA. O atendimento ao cidadão por conectividade pública ocorre sob demanda e contratação do ente público.

1.4. O Cadastro do Projeto orienta a formação da relação de unidades, localidades e circuitos de cada implantação. Cada registro deverá identificar sua fonte e evidência de validação. O projeto executivo relacionará unidades e circuitos aos nodes efetivos, justificará repetições e complementará os dados por vistoria, sem equiparar automaticamente endereço, equipamento e node.

2. DEFINIÇÕES E RESPONSABILIDADES

2.1. A parceria técnica institucional, o projeto municipal e a ativação de serviços constituem níveis distintos. A qualificação de uma ou mais parceiras será técnica e institucional, com pontuação e sem apresentação de proposta econômica. A avaliação observará o edital e o Anexo II, com registro individual da conformidade e da aderência técnica. As referências a preços, custos, medição financeira, faturamento, reajuste e glosas disciplinam eventual execução remunerada de projetos municipais, mediante instrumento próprio, e não constituem documentos ou critérios econômicos da seleção institucional. A definição de cada projeto precede o compromisso de execução; a Ordem de Serviço ativa somente parcelas abrangidas por instrumento eficaz. A escala municipal documentada não se converte em demanda global do portfólio. A parceria institucional não autoriza adesão ou contratação automática pela Prefeitura. Cada atendimento dependerá de procedimento municipal próprio, com fundamento, competência, planejamento, recursos e instrumento adequados ao regime aplicável.

2.2. O suporte de primeiro nível (N1) será prestado pelo InPACTA, compreendendo recepção, registro, triagem, orientação operacional padronizada, acompanhamento, comunicação com os usuários e escalonamento. A executora responderá pelo suporte especializado N2/N3, pelo diagnóstico e restabelecimento técnico, pela manutenção e pela coordenação das operadoras e demais prestadores de sua cadeia.

2.3. A Central de Situação será operada pelo InPACTA para acompanhar proativamente disponibilidade, capacidade, alertas, chamados, incidentes, níveis de serviço e riscos, organizar evidências e coordenar a comunicação institucional. A executora disponibilizará painéis, registros, alertas e integrações com perfis de acesso autorizados. A Central não substitui o NOC, o SOC e as equipes técnicas da executora nem as competências de fiscalização e aceite do município.

Responsável	Responsabilidade
Executora	Projeto, integração, operação técnica, licenciamento, N2/N3, NOC/SOC, manutenção, equipes de campo, coordenação de terceiros e evidências.
InPACTA	Estruturação e governança da parceria, suporte N1, operação da Central de Situação, comunicação institucional e acompanhamento de resultados.
Município demandante	Necessidades, condições locais, interlocução, acessos, janelas e atos de sua competência.

2.4. DEFINIÇÕES TÉCNICAS

2.4.1. ASN: número de Sistema Autônomo utilizado para identificação de redes que participam do roteamento BGP.

2.4.2. BGP multihoming: uso de sessões eBGP independentes com mais de uma prestadora ou caminho para ampliar resiliência e controle de roteamento.

2.4.3. CPE: equipamento terminal instalado no ponto atendido, fornecido e mantido pela EXECUTORA como parte do serviço.

2.4.4. DDoS: ataque distribuído de negação de serviço destinado a consumir capacidade ou recursos de rede, sistema ou aplicação.

2.4.5. Hotspot: ponto de conectividade Wi-Fi pública, segregado da rede administrativa e operado com controle, monitoramento e segurança.

2.4.6. NOC: Centro de Operações de Rede responsável pelo monitoramento, gestão de incidentes, chamados, escalonamento e acompanhamento dos serviços.

2.4.7. Node: unidade técnica de entrega e medição da Infovia, classificada de C1 a C7 conforme finalidade e criticidade.

2.4.8. RPKI e ROA: mecanismos de validação criptográfica de autorização de origem de prefixos IP no roteamento BGP.

2.4.9. SCM: Serviço de Comunicação Multimídia, prestado no regime privado, destinado à oferta de capacidade de transmissão, emissão e recepção de informações multimídia a partir de estações fixas.

2.4.10. SOC: Centro de Operações de Segurança responsável pelo monitoramento de eventos, vulnerabilidades, incidentes e controles de segurança.

2.4.11. VRF: instância lógica de roteamento utilizada para segregação de tráfego e domínios de rede.

2.4.12. Backbone: segmento de alta capacidade da infraestrutura de telecomunicações responsável pela interligação entre pontos de presença, núcleos de rede, áreas de agregação e domínios principais de transporte.

2.4.13. Backhaul: segmento intermediário de transporte que conecta redes de acesso, pontos de agregação ou regiões atendidas ao backbone ou ao núcleo da solução.
2.4.14. Última milha: segmento de acesso compreendido entre o ponto de presença, nó de distribuição ou infraestrutura de agregação e a interface de entrega instalada no endereço atendido.
2.4.15. Rota principal MPLS: serviço de transporte corporativo segregado utilizado como rota primária dos nodes C1 e C2, com capacidade simétrica de 10 Gbps, qualidade de serviço, rastreabilidade, monitoramento e integração à arquitetura lógica da Infovia.
2.4.16. Domínio de falha: conjunto de elementos físicos, lógicos, elétricos, prediais ou operacionais cuja falha comum possa interromper simultaneamente caminhos ou componentes considerados redundantes.
2.4.17. Rota de proteção GPON: caminho de contingência dos nodes C1 e C2 fornecido por tecnologia GPON, com perfil integral de referência, independência de domínio de falha, monitoramento, comutação automática e medição por sentido. A tecnologia GPON também é utilizada como rota única dos nodes C5, no perfil específico da classe.
2.4.18. Rotas ópticas C3 e C4: par de caminhos primário e secundário em tecnologia óptica ativa ou passiva, admitida qualquer combinação entre as duas rotas, desde que cada caminho entregue 100% da capacidade mínima da classe, possua independência física e operacional e seja provido por fornecedor distinto do outro caminho.
2.4.19. CDR: registro detalhado de chamada contendo dados técnicos, temporais, tarifários e de roteamento necessários à auditoria do consumo e do faturamento.
2.4.20. DDR e DID: recursos de numeração que permitem o encaminhamento direto de chamadas públicas a ramais ou destinos internos.
2.4.21. PABX IP: plataforma de comunicação baseada em protocolos IP para controle de ramais, chamadas, filas, unidades de resposta audível e demais recursos corporativos.
2.4.22. SIP: protocolo de sinalização utilizado para estabelecimento, alteração e encerramento de sessões de comunicação multimídia.
2.4.23. SBC: controlador de borda de sessão responsável por segurança, interoperabilidade, controle e continuidade das sessões de voz.
2.4.24. Softphone: aplicação autorizada que permite utilizar um ramal institucional em computador ou dispositivo móvel.
2.4.25. Tronco SIP: serviço de interconexão entre a plataforma corporativa e a rede pública de telefonia por protocolo IP.
2.4.26. Telefonia sob demanda: parcela prevista no escopo técnico da parceria institucional, cuja execução dependerá da formalização do projeto municipal e de Ordem de Serviço específica. Preços e condições de remuneração serão definidos no instrumento de execução, sem proposta econômica na seleção institucional.
2.4.27. VoIP: transmissão de voz e recursos associados por redes baseadas em protocolo IP.
2.4.28. Lote único integrado: unidade de disputa e adjudicação composta por itens de medição tecnicamente individualizados, porém funcionalmente coordenados, cuja execução é atribuída a uma única EXECUTORA responsável pelo resultado fim a fim, sem impedir subcontratações parciais autorizadas nem a utilização de infraestrutura de terceiros.

2.5. INTERFACES E RESPONSABILIDADES DO MUNICÍPIO
2.5.1. Indicar os nodes, prioridades, responsáveis locais e janelas de intervenção;
2.5.2. Disponibilizar acesso físico, energia e condições internas sob sua responsabilidade;
2.5.3. Manter a LAN interna, servidores, aplicações e políticas internas, salvo previsão expressa;
2.5.4. Analisar planos, projetos, testes, relatórios, medições e solicitações;
2.5.5. Comunicar falhas e fornecer informações necessárias à solução dos incidentes;
2.5.6. Gerenciar ordens de serviço, acréscimos, supressões e aceite;
2.5.7. Designar gestor e fiscais e manter interlocução formal com a EXECUTORA;
2.5.8. Preservar credenciais, equipamentos e acessos sob sua guarda;
2.5.9. Cumprir suas responsabilidades relativas a dados pessoais e segurança.
2.5.10. Emitir a Ordem de Serviço da telefonia com quantitativos, unidades, números, janelas, responsáveis, critérios de aceite e autorização orçamentária;
2.5.11. Disponibilizar o inventário, os aparelhos legados, as faturas, os registros disponíveis, os responsáveis locais e as informações necessárias à portabilidade e ao planejamento;
2.5.12. Aprovar o plano de numeração, a estratégia de migração, as janelas de mudança, os perfis de acesso, a política de gravação e os critérios de retenção de dados.

3. COMPONENTES DA SOLUÇÃO
3.1. A solução combina transporte, acesso, Internet, segurança, voz e operação em uma cadeia integrada. A segregação lógica dos domínios, as interfaces e a responsabilidade por cada componente deverão constar do projeto executivo. A instalação de um componente isolado não comprova o resultado fim a fim. O diagrama conceitual apresentado ao final deste documento ilustra os domínios de transporte, segurança e serviços, sem substituir o dimensionamento e a definição das interfaces de cada projeto municipal.
3.1.1. A extensão C7 e a preparação dos nodes para redundância satelital e radioenlace observarão o item 27, com integração à arquitetura e aos requisitos das classes existentes.

Componente	Escopo integrado
Transporte C1/C2	MPLS 10 Gbps principal e proteção GPON no perfil indicado; domínios de falha e serviços prioritários.
Transporte C3/C4	Duas rotas ópticas independentes, fornecedores distintos e capacidade integral por rota.
Campo C5	GPON 50 Mbps simétricos, segurança, monitoramento e medição do sentido de subida.
Internet	Acessos institucionais e públicos com perfis de capacidade, endereçamento, diversidade e proteção definidos na especificação; quantidade e implantação por projeto.
WiFi C4	Hotspots permanentes, cobertura, autenticação e segregação conforme item 5.6.
C6	Conectividade temporária por evento com satélite como meio principal, conforme item 5.7.
Telefonia	Parcela sob demanda, com Ordem de Serviço, dimensionamento, ativação, testes e medição próprios, conforme item 25.
Operação	NOC, SOC, Service Desk, suporte, monitoramento e documentação.

C7	Resiliência fixa, transportável ou veicular sob demanda, com preparação obrigatória dos nodes conforme item 27. Preservar classes, capacidades e proteções existentes.

3.2. ARQUITETURA DA SOLUÇÃO INTEGRADA

3.2.1. A solução compreenderá implantação, operação, gerenciamento, monitoramento, manutenção, suporte, segurança, medição e evolução de rede municipal de transporte de dados, utilizando infraestrutura própria, compartilhada ou contratada de terceiros, sob responsabilidade integral da EXECUTORA.

3.2.2. A solução deverá incluir os equipamentos, licenças, plataformas, enlaces, serviços, materiais, acessórios, deslocamentos, equipes, ferramentas e integrações necessários ao atendimento das capacidades, interfaces, locais e condições expressamente definidos para a proposta. Componentes auxiliares inerentes à solução ofertada integrarão o preço, ainda que não individualizados. Essa obrigação não autoriza presumir novos locais, volumes, serviços ou adequações municipais sem delimitação no escopo. A proponente identificará componentes, dependências e premissas de dimensionamento; lacunas com impacto técnico ou econômico deverão ser esclarecidas antes da apresentação da proposta correspondente.

3.2.3. A prestação não compreende a construção de rede óptica externa para incorporação ao patrimônio municipal nem a transferência dessa rede ao MUNICÍPIO DEMANDANTE. As intervenções externas necessárias à prestação serão realizadas pela EXECUTORA ou por seus terceiros, sob sua responsabilidade, conforme o item 8.11.1. Eventuais adequações locais acessórias necessárias à instalação deverão ser incluídas no preço e previamente autorizadas quando afetarem a infraestrutura do MUNICÍPIO DEMANDANTE.

3.2.4. A EXECUTORA será a única responsável perante o Município pelos serviços próprios e subcontratados, pelos níveis de serviço, pela continuidade, pela segurança, pela coordenação de terceiros e pela correção de falhas.

3.2.5. O Município permanecerá responsável por sua LAN interna, servidores, aplicações, políticas internas, endereçamento privado, VLANs internas e sistemas finais, salvo atividade expressamente atribuída à EXECUTORA.

3.2.6. A parcela de telefonia compreenderá plataforma corporativa de telefonia IP/VoIP e comunicações unificadas, em versão estável e suportada, com capacidade para chamadas simultâneas totais dimensionada no projeto, ambiente logicamente segregado, alta disponibilidade, administração centralizada, troncos SIP redundantes, portabilidade, numeração pública, ramais ativos, softphones dimensionados no projeto, filas, unidades de resposta audível, grupos, relatórios, CDR, APIs documentadas, suporte, segurança, backup, treinamento, migração e operação assistida, com capacidade de integração com ambiente privado de processamento de inteligência artificial e reconhecimento automático de fala. A capacidade de integração será demonstrada por interfaces documentadas, formatos de dados e controles de segurança compatíveis. O fornecimento, o licenciamento e a ativação da gravação, transcrição e análise de chamadas dependerão de previsão na proposta e de acionamento específico, conforme item 25.0.

3.2.7. Os aparelhos legados disponibilizados pela Prefeitura serão integrados por interconexão lógica, avaliação de compatibilidade, provisionamento, configuração, registro seguro, associação ao plano de numeração, testes e homologação.

3.2.8. A EXECUTORA permanecerá como ponto único de responsabilidade perante o Município e coordenará a prestadora autorizada da parcela regulada de telefonia pública, as integrações, os caminhos de voz, a portabilidade, o suporte e a conciliação do faturamento.

3.2.9. A solução será especificada por requisitos funcionais, de capacidade, desempenho, disponibilidade, segurança, interoperabilidade, suporte, integração, mensuração e transição. Não será exigida marca, fabricante, modelo, edição comercial, nível de parceria, credenciamento comercial ou certificação vinculada a fabricante como condição de habilitação ou aceitação, ressalvadas as certificações regulatórias ou técnicas de produto previstas em lei e diretamente relacionadas ao objeto. Quando admitida equivalência, a proponente relacionará requisito, solução oferecida, função preservada, capacidade, desempenho, interfaces, limitações e evidência verificável. A avaliação será fundamentada nesses elementos; equivalência não dispensa mínimos, diversidade de rotas ou condições expressamente exigidos para a classe.

4. INTEGRAÇÃO COM AMBIENTES COMPUTACIONAIS E BACKUP

4.1. A operação da rede externa é prestada como serviço e não pressupõe incorporação patrimonial municipal. Integração com data center não inclui automaticamente nuvem, administração de aplicações ou migração integral desses ambientes.

4.2. O transporte deverá permitir acesso, coexistência, sincronização, backup e replicação entre ambientes municipais existentes e futuros. O diagnóstico definirá destinos, interfaces e janelas. Não se impõe prestação de nuvem ou administração irrestrita desses ambientes.

4.3. A abrangência de cada projeto identificará endereços, interfaces e destinos computacionais. O desenho dos caminhos deverá demonstrar percursos ópticos, meios próprios, compartilhados ou de terceiros e domínios de falha até o destino técnico. Identificadores distintos de circuitos não demonstram, isoladamente, independência física.

4.4. A validação do legado deverá identificar as interfaces e dependências a preservar. Adaptação, coexistência, migração e reversão deverão ser examinadas antes de reduzir requisito estruturante. Quando necessária à continuidade, a validação do destino, das janelas e do retorno precederá a desativação da origem.

4.5. AMBIENTES COMPUTACIONAIS E INTERFACES CORRELATAS

4.5.1. Podem ser correlatas as contratações de ativos e serviços internos do Município que utilizem a Infovia como meio de transporte, tais como rede local, servidores, sistemas corporativos, câmeras, sensores, equipamentos IoT, energia, climatização e adequações prediais.

4.5.2. Essas contratações não reduzem a responsabilidade da contratada pela solução de conectividade e segurança contratada e não transferem à contratada a administração dos sistemas finais ou da rede interna municipal.

4.5.3. Também são correlatos os projetos de segurança da informação, backup e recuperação, videomonitoramento, serviços em nuvem, interoperabilidade, servidores descentralizados e futuro data center municipal. O planejamento da Infovia considera que esses projetos utilizarão a rede de transporte e poderão alterar quantitativa e qualitativamente os fluxos durante a vigência.

4.5.4. São correlatas à telefonia as redes locais, alimentação elétrica por Ethernet, switches, diretório institucional, gestão de identidades, dispositivos dos usuários, salas de atendimento, políticas de segurança e adequações internas das unidades. Essas parcelas não reduzem a responsabilidade da contratada pelas interfaces e resultados expressamente incluídos na solução.

4.5.5. São interdependentes, entre outros, os projetos de ampliação do videomonitoramento, OCR, sinalização semafórica conectada, sensores urbanos, IoT, mobilidade, telemetria, fiscalização, segurança, data center, governo digital e demais soluções que utilizarão a Infovia como infraestrutura de transporte.

4.5.6. A Infovia deverá ser contratada e implantada em sequência anterior às soluções finais que dependem de conectividade, evitando que esses projetos sejam limitados por falta de capacidade, ausência de interfaces padronizadas ou necessidade de contratação emergencial de enlaces.

4.5.7. Não foi identificada contratação interdependente indispensável à modelagem inicial, além das condições locais mínimas de energia, espaço, acesso físico e interface de rede sob responsabilidade municipal.

4.5.8. A ausência de condição local deverá ser registrada e tratada sem faturamento do node não ativado.

4.5.9. Embora a contratação da Infovia não dependa da conclusão prévia desses projetos, sua arquitetura deverá admitir a integração progressiva dos ambientes e a expansão formal de capacidade, evitando que a evolução de segurança, processamento, armazenamento e continuidade de negócios seja limitada pela rede de transporte.
4.5.10. A telefonia depende da implantação da Infovia, da qualidade de serviço e das condições locais de rede, energia e acesso, mas deverá possuir contingência para preservar os serviços críticos durante falhas isoladas de caminho ou componentes.
5. CLASSES SERVIÇOS E ESPECIFICAÇÕES FUNCIONAIS
5.1. Os parâmetros a seguir descrevem o cenário municipal. Classes de node, capacidade nominal de interface, capacidade útil, número de usuários, simultaneidade e numeração pública são grandezas distintas e deverão ser demonstradas separadamente no projeto, no licenciamento e nos testes.
5.2. C3 e C4 utilizarão duas rotas ópticas independentes, ativas ou passivas, de fornecedores distintos, cada rota com 100% da capacidade da classe: 1 Gbps simétrico para C3 e 500 Mbps simétricos para C4. Essa especificação orienta também os testes, o monitoramento, a medição e o tratamento de incidentes.

Perfil	Especificação institucional
C1 e C2	Rota principal MPLS de 10 Gbps simétricos; proteção GPON com taxas nominais de linha de 2,48832 Gbps de descida e 1,24416 Gbps de subida e capacidade útil garantida conforme o item 5.8.12.
C3	Duas rotas ópticas independentes, ativas ou passivas, de fornecedores distintos; cada rota com 1 Gbps simétrico e capacidade integral da classe.
C4	Duas rotas ópticas independentes, ativas ou passivas, de fornecedores distintos; cada rota com 500 Mbps simétricos e capacidade integral da classe.
C5	Rota única GPON de 50 Mbps simétricos, túnel criptografado, monitoramento e medição de subida.
C6	Conectividade temporária por evento, com satélite como meio principal, cobertura, simultaneidade, mobilização, testes e desmobilização conforme item 5.7. Não integra os nodes permanentes.
Internet institucional	Perfil de referência de 6 Gbps por acesso, IPv4 /25, IPv6, diversidade e mitigação DDoS. Quantidade e distribuição por projeto.
Internet pública	Perfil de referência de 4 Gbps, IPv4 /29, IPv6, segregação e proteção de borda. Dimensionamento agregado por projeto.
Telefonia	Parcela sob demanda, com Ordem de Serviço, dimensionamento, ativação, testes e medição próprios, conforme item 25.
Implantação e expansão	Sem quantitativo institucional prefixado. Cadastro e memória de dimensionamento específicos para cada atendimento.
C7	Resiliência fixa, transportável ou veicular sob demanda, com preparação obrigatória dos nodes conforme item 27. Preservar classes, capacidades e proteções existentes.

5.3. DIMENSIONAMENTO E CAPACIDADE
5.3.1. A base de implantação será identificada no projeto específico por unidade, endereço, classe, capacidade, prioridade, dependências e sequência de ativação. A classificação C1 a C7 indica a função técnica de cada componente e não predetermina a quantidade de unidades.
5.3.2. A relação individualizada dos nodes, com unidade, órgão, endereço, classe, capacidade, finalidade e prioridade, integrará o processo e será disponibilizada em planilha técnica própria para formação das propostas e planejamento da implantação.
5.3.3. A quantidade física de nodes não representa, isoladamente, a volumetria total da rede. O dimensionamento deverá considerar simultaneidade, fluxos entre órgãos, backup, replicação, segurança, contingência, crescimento e novos projetos.
5.3.4. Somente serão medidos nodes e serviços formalmente solicitados, ativados, testados, monitorados e aceitos.
5.3.5. A expansão será dimensionada em cada projeto, com limites tecnicamente justificados, capacidade estrutural e condições de ativação. A previsão de crescimento não representa consumo mínimo, receita garantida ou pagamento por capacidade ociosa.
5.3.6. A previsão quantitativa dos nodes de expansão não obriga o MUNICÍPIO DEMANDANTE a solicitar, instalar ou consumir a totalidade estimada. A mera disponibilidade de capacidade estrutural, portas, interfaces, equipamentos em estoque, licenças, materiais ou recursos reservados pela EXECUTORA não autorizará cobrança de implantação, mensalidade, indenização, compensação ou receita mínima. A implantação será faturada somente após a instalação e o aceite do respectivo node, e a mensalidade será devida exclusivamente a partir de sua entrada efetiva em produção, integração ao monitoramento e aceite técnico.
5.3.7. A cobrança da implantação dependerá da instalação e do aceite. A mensalidade somente será devida após a entrada do node em produção, integração ao monitoramento e aceite técnico.
5.3.8. Nodes não solicitados, não instalados, não testados ou não aceitos não serão faturados e não gerarão direito a indenização ou receita mínima.
5.3.9. A relação técnica de cada projeto individualizará os nodes de implantação inicial e distinguirá as expansões sob demanda. O cadastro será atualizado por Ordem de Serviço, sem antecipar instalação não autorizada.
5.3.10. Para fins de memória de cálculo, a quantidade de nodes será conciliada mensalmente com o inventário, enquanto capacidade, volume e throughput serão mensurados por enlace, sentido, classe e camada.
5.3.11. A arquitetura central deverá suportar a escala e o crescimento definidos no projeto específico, com modularidade, gestão de capacidade e preservação dos componentes estruturantes sempre que tecnicamente viável. Recursos não ativados não gerarão faturamento automático.
5.3.12. O node C5 representa ponto ou célula de transporte de campo e poderá atender uma ou mais câmeras, equipamentos OCR, controladores semafóricos, sensores, dispositivos IoT ou ativos equivalentes, conforme capacidade, segregação e projeto executivo.
5.3.13. A aplicação dos C5 a câmeras, videomonitoramento, OCR, semáforos, sensores e outros dispositivos será definida pelo levantamento do projeto municipal. O diagnóstico identificará o parque existente, suas limitações, as ampliações necessárias e as dependências de conectividade, sem presumir insuficiência ou estágio de implantação comum a todos os municípios.
5.3.18. A expansão física dependerá de Ordem de Serviço e dos limites formalizados no projeto específico. A existência de capacidade disponível não autoriza ativação ou cobrança automática.
5.3.19. O planejamento de capacidade utilizará dados próprios da Infovia, registros de monitoramento, inventário atualizado, séries históricas, percentil 95, picos, filas, descartes, latência, perda, variação de atraso, criticidade e crescimento efetivamente observado nos serviços municipais.

5.3.20. A arquitetura deverá suportar a escala definida no projeto e sua expansão modular, preservando capacidade, redundância, segurança, monitoramento, gerenciamento e níveis de serviço.
5.3.21. O acompanhamento da carga da rede será separado da quantidade de nodes e utilizará capacidade nominal, capacidade disponível, utilização média e de pico, percentil 95, latência, perda, variação de atraso, descartes, filas, simultaneidade, criticidade e tendência de saturação por enlace, sentido, classe e camada.
5.3.22. Os valores de 30% e 40% no percentil 95 serão gatilhos iniciais de análise e planejamento, especialmente no núcleo e na agregação, sem gerar ampliação automática. O gatilho definitivo considerará redundância, contingência, horizonte de implantação e criticidade. Esses percentuais expressam a utilização da capacidade de referência pelo tráfego P95; não alteram o percentil estatístico adotado, que permanece 95, conforme item 5.8.15.
5.3.26. Os parâmetros de crescimento e capacidade serão revisados anualmente e sempre que houver desvio acumulado superior a 15%, saturação recorrente, degradação de SLA, ativação de projeto relevante ou mudança material da arquitetura. A série histórica municipal prevalecerá sobre a taxa inicial de planejamento quando possuir qualidade e abrangência suficientes.
5.3.27. Nenhuma curva produzirá ativação, aquisição, reserva remunerada ou faturamento automático. Toda expansão dependerá de necessidade demonstrada, disponibilidade orçamentária, Ordem de Serviço, implantação, teste e aceite.

5.4. TRANSPORTE ÓPTICO E CLASSES DE NODES

5.4.1. Os nodes C1 e C2 deverão possuir rota principal MPLS de 10 Gbps simétricos e rota de proteção por tecnologia GPON no perfil integral de referência. Os nodes C3 deverão possuir duas rotas ópticas, primária e secundária, cada uma com no mínimo 1 Gbps simétrico. Os nodes C4 deverão possuir duas rotas ópticas, primária e secundária, cada uma com no mínimo 500 Mbps simétricos. Para C3 e C4 serão admitidas tecnologias ópticas ativas ou passivas e qualquer combinação entre os caminhos, desde que haja independência física e operacional e fornecedor distinto entre as duas rotas. Os nodes C5 serão atendidos por rota única GPON de 50 Mbps simétricos.
5.4.2. O transporte deverá suportar IPv4 e IPv6, segregação lógica por VRF ou mecanismo equivalente, VLAN 802.1Q, qualidade de serviço, preservação de marcações DSCP, roteamento estático e dinâmico quando aplicável, multicast quando necessário e monitoramento por protocolos abertos.
5.4.3. Para C1 e C2, a rota principal será entregue por MPLS L2VPN, MPLS L3VPN ou modalidade funcionalmente compatível, e a proteção GPON utilizará túnel criptografado ponta a ponta, roteamento dinâmico e detecção rápida de falhas. Para C3 e C4, as duas rotas serão ópticas, ativas ou passivas, com integração lógica segura, roteamento dinâmico e detecção rápida de falhas, independentemente da combinação tecnológica. Para C5, a rota única GPON utilizará túnel criptografado, roteamento e detecção de falhas.
5.4.4. O uso de infraestrutura própria, compartilhada ou de terceiros não afastará a responsabilidade da EXECUTORA nem autorizará redução de SLA, transferência de atendimento ao Município ou fragmentação da gestão das rotas.
5.4.5. A EXECUTORA será responsável pela integração fim a fim entre a rota principal MPLS e a proteção GPON dos C1 e C2, entre as duas rotas ópticas dos C3 e C4 e pela entrega fim a fim da rota única GPON dos C5, incluindo segmentação, criptografia quando aplicável, roteamento, detecção de falhas, comutação quando aplicável, monitoramento, capacidade, estabilidade, medição e documentação.
5.4.6. A proteção ou rota secundária dos nodes C1 a C4 e a rota única dos nodes C5 deverão abranger o serviço desde a interface de entrega até o ponto de concentração, destino técnico ou domínio central definido no Projeto Executivo, considerando acesso, agregação, backbone, backhaul e última milha.
5.4.7. Nos nodes C1 a C4, as duas rotas deverão possuir diversidade física, lógica e operacional suficiente para evitar falha simultânea. Nos C3 e C4, a rota secundária deverá ainda ser provida por fornecedor distinto da rota primária. Não será aceita redundância que compartilhe integralmente cabo crítico, duto, equipamento de agregação, ponto de presença, alimentação elétrica, árvore óptica, OLT ou outro domínio de falha comum, conforme a tecnologia aplicável.
5.4.8. Compartilhamentos inevitáveis deverão ser identificados por elemento, trecho e impacto no serviço. Sua aprovação exigirá análise técnica e medidas de mitigação, sem afastar a diversidade de fornecedor dos C3/C4 ou a segregação dos sites C1 prevista no item 5.4.22. A aceitação de compartilhamento não poderá tornar uma falha simples comum capaz de interromper simultaneamente os caminhos cuja independência é exigida. Impedimento ao atendimento será resolvido antes da proposta correspondente, mediante definição formal de solução compatível.
5.4.9. Para os nodes C1 e C2, a proteção terá perfil GPON integral de referência, com taxas nominais de linha de 2,48832 Gbps no sentido de download e 1,24416 Gbps no sentido de upload. Essas taxas identificam o meio físico e não representam, por si, throughput útil garantido ao node. Antes da proposta do projeto, serão estabelecidos os mínimos úteis por sentido e as condições de concorrência, encapsulamento e criptografia aplicáveis ao serviço, conforme item 5.8.12.
5.4.10. Para os nodes C3, cada uma das duas rotas deverá entregar, individualmente, no mínimo 1 Gbps simétrico, correspondente a 100% da capacidade mínima da classe, independentemente da tecnologia óptica empregada. Para os nodes C4, cada uma das duas rotas deverá entregar, individualmente, no mínimo 500 Mbps simétricos, correspondente a 100% da capacidade mínima da classe, independentemente da tecnologia óptica empregada. Para os nodes C5, a rota única GPON entregará no mínimo 50 Mbps simétricos na interface de serviço.
5.4.11. Nos C1 e C2, serão demonstradas separadamente a taxa nominal de linha, a capacidade agregada da porta PON e da árvore óptica, o perfil reservado ao node e a capacidade útil entregue. Nos C3 e C4, o projeto executivo e o aceite comprovarão, em cada rota, os mínimos úteis simétricos de 1 Gbps e 500 Mbps, respectivamente, considerando overhead e utilização concorrente. Nos C5 será comprovado o mínimo útil de 50 Mbps simétricos.
5.4.12. Nos nodes C1 a C4, a comutação entre a rota primária e a rota secundária e o retorno à rota preferencial ocorrerão automaticamente, mediante BGP com BFD ou mecanismos funcionalmente equivalentes. Nos nodes C5, o roteamento e a detecção de falhas deverão gerar alarmes e evidências da disponibilidade e do desempenho da rota única.
5.4.13. A integração das rotas deverá preservar confidencialidade, integridade e rastreabilidade. Nos C1 e C2 e na rota única C5, a rota GPON será transportada por túnel criptografado ponta a ponta ou mecanismo equivalente. Nos C3 e C4, será admitido mecanismo de integração segura compatível com a tecnologia óptica utilizada. A exigência será funcional e não imporá produto, fabricante ou implementação específica.
5.4.14. Nos nodes C1 e C2, a operação pela proteção GPON será classificada como condição degradada, e não como indisponibilidade, somente enquanto forem mantidos os serviços essenciais, os pisos de capacidade aplicáveis, a segurança, o roteamento e o monitoramento. Nos nodes C3 e C4, a operação pela rota secundária não caracterizará degradação nem indisponibilidade quando forem preservados 100% da capacidade mínima da classe e os demais níveis de serviço. Nos nodes C5, falha da rota única será apurada como indisponibilidade conforme o SLA da classe.
5.4.15. A distinção entre acessos à Internet e rotas de transporte dos nodes, inclusive a vedação de substituir a proteção de transporte por redundância de Internet, observará o item 5.5.7.
5.4.16. Os nodes C1 deverão entregar rota principal MPLS com capacidade mínima de 10 Gbps simétricos e integrar o domínio central de transporte ou a borda estratégica da Infovia. Os firewalls que atendem aos nodes C1 dos sites principal e de continuidade deverão integrar a arquitetura de segurança de borda em alta disponibilidade, efetivamente implantada e operacional, conforme os itens 11.5.5 a 11.5.7. A distribuição dos membros entre os sites e os caminhos protegidos deverá assegurar a continuidade dos serviços abrangidos após falha de um membro, com as políticas de segurança mantidas e capacidade remanescente conforme o item 5.8.14. A redundância dos enlaces, isoladamente, não atende a essa exigência.

5.4.17. Cada node C1 deverá possuir rota de proteção GPON no perfil de referência com taxas nominais de linha de 2,48832 Gbps de download e 1,24416 Gbps de upload e capacidade útil garantida conforme o item 5.8.12, túnel criptografado, roteamento dinâmico, detecção rápida de falhas, monitoramento contínuo e capacidade de manter os serviços prioritários durante falha da rota principal.
5.4.18. A proteção não será comprovada por simples declaração. A EXECUTORA deverá apresentar topologia funcional, identificação dos domínios de falha, perfil GPON configurado, estado do túnel e das sessões de roteamento e detecção, além de evidência de teste de comutação e capacidade por sentido.
5.4.19. O node C1 que atende ao site de continuidade, distinto do node do site principal, deverá ser implantado em local fisicamente e operacionalmente diverso do site principal, com rotas, energia, infraestrutura predial e dependências de telecomunicações segregadas de modo a reduzir risco de falha simultânea.
5.4.20. A definição do site de continuidade deverá considerar latência, diversidade de rotas, disponibilidade de trânsito IP, acesso a pontos de presença, resiliência, capacidade de expansão e custo total de operação, com comprovação no projeto executivo.
5.4.21. Não haverá indicação obrigatória de endereço, prestadora, participante de ponto de troca ou data center específico. A arquitetura proposta deverá comprovar objetivamente diversidade, desempenho, capacidade e continuidade.
5.4.22. O site de continuidade não poderá compartilhar com o site principal o mesmo prédio, sala, alimentação principal, duto crítico, rota física, ponto de presença, equipamento de agregação ou domínio operacional capaz de produzir falha simultânea.
5.4.23. O projeto executivo dos C1 deverá demonstrar os percursos funcionais da rota principal MPLS e da proteção GPON, os domínios de falha, a capacidade em contingência, os mecanismos de criptografia, roteamento, detecção e comutação, os pontos de monitoramento e os testes de aceite, preservados os dados sensíveis da infraestrutura da prestadora. A demonstração incluirá a localização e a função dos membros de firewall que atendem aos C1, sua distribuição entre os sites, as dependências de sincronização e os percursos do tráfego em operação normal e em falha, em correspondência com os itens 11.5.5 a 11.5.7 e 21.5.10.
5.4.24. Os nodes C2 deverão entregar rota principal MPLS com capacidade mínima de 10 Gbps simétricos e rota de proteção GPON no perfil de referência com taxas nominais de linha de 2,48832 Gbps de download e 1,24416 Gbps de upload e capacidade útil garantida conforme o item 5.8.12, comutação automática, monitoramento e escalonamento prioritário.
5.4.25. A solução deverá permitir baixa latência e estabilidade para hospitais, estruturas de segurança, secretarias críticas, serviços descentralizados, servidores e demais unidades classificadas nessa categoria.
5.4.26. Embora os nodes C1 e C2 possuam a mesma capacidade nominal na rota principal e o mesmo perfil de proteção GPON, as classes permanecem distintas em razão da função arquitetural, da criticidade, da posição na topologia, da priorização operacional e dos critérios de aceite aplicáveis.
5.4.27. Cada C2 deverá ser submetido a teste individual da rota principal MPLS, da proteção GPON, do túnel criptografado, do roteamento dinâmico, da detecção de falha e da comutação, sem que a proteção seja presumida pela simples existência de VLAN, VRF, protocolo de roteamento ou infraestrutura compartilhada.
5.4.28. Os nodes C3 deverão entregar rota primária em tecnologia óptica ativa ou passiva, com capacidade mínima de 1 Gbps simétrico para unidades administrativas e serviços públicos, com qualidade de serviço, monitoramento e suporte da classe.
5.4.29. Cada C3 deverá possuir rota secundária em tecnologia óptica ativa ou passiva, fisicamente distinta e de fornecedor distinto da rota primária, com capacidade mínima de 1 Gbps simétrico, correspondente a 100% da capacidade da classe, admitida qualquer combinação tecnológica entre as duas rotas, com roteamento dinâmico, detecção rápida de falhas, comutação automática e medição por sentido.
5.4.30. A operação do C3 pela rota secundária será tratada como contingência e não caracterizará degradação nem indisponibilidade enquanto forem preservados 1 Gbps simétrico, a segurança, o roteamento, o monitoramento e os demais níveis de serviço da classe.
5.4.31. Os nodes C4 deverão entregar rota primária em tecnologia óptica ativa ou passiva, com capacidade mínima de 500 Mbps simétricos para hotspot público, segregada da rede administrativa e dimensionada segundo ambiente, cobertura, usuários ativos e experiência de navegação.
5.4.32. Cada C4 deverá possuir rota secundária em tecnologia óptica ativa ou passiva, fisicamente distinta e de fornecedor distinto da rota primária, com capacidade mínima de 500 Mbps simétricos, correspondente a 100% da capacidade da classe, admitida qualquer combinação tecnológica entre as duas rotas, com roteamento dinâmico, detecção rápida de falhas, comutação automática e monitoramento.
5.4.33. A contingência deverá preservar captive portal, autenticação quando aplicável, segregação, segurança, registros operacionais e navegação compatível com a finalidade do hotspot.
5.4.34. Os nodes C5 deverão entregar rota única GPON com capacidade mínima de 50 Mbps simétricos para câmeras, sensores, IoT, telemetria e pontos de campo, sem transferência automática à EXECUTORA da responsabilidade pelo sistema final conectado.
5.4.35. A rota única GPON dos C5 deverá utilizar túnel criptografado, roteamento, detecção de falhas, monitoramento contínuo, alarmes, medição por sentido e restauração sob SLA, sem exigência de rota secundária.
5.4.36. Quando um C5 atender múltiplos dispositivos, a EXECUTORA deverá demonstrar que o tráfego agregado, especialmente de upload, permanece compatível com a capacidade mínima de 50 Mbps simétricos, a agregação, o armazenamento e o SLA da classe.
5.4.37. A EXECUTORA deverá definir e comprovar parâmetros de latência, perda de pacotes e variação de atraso para as rotas principal e de proteção, adequados ao domínio técnico, à distância, à classe e à condição normal ou degradada.
5.4.38. Para o tráfego metropolitano entre nodes C1 e C2, os parâmetros de latência, perda de pacotes e jitter serão os estabelecidos no Instrumento de Medição de Resultado, preservadas a baixa latência e a estabilidade necessárias à voz, ao vídeo, aos sistemas críticos, ao backup e à replicação.
5.4.39. A solução deverá disponibilizar classes de QoS suficientes para tráfego crítico, voz e vídeo, sistemas corporativos, backup e tráfego de menor prioridade, com preservação de marcações e mecanismos contra monopolização da banda.
5.4.40. O Instrumento de Medição de Resultado do projeto integrará a base disponibilizada antes da proposta. Definirá, por classe e componente, limites de latência, perda e jitter aplicáveis, detecção e comutação, resposta e restauração, tempo máximo em condição degradada, serviços prioritários, perda de resiliência, janelas e exclusões admitidas, fontes de medição e faixas de glosa. Os critérios distinguirão falha de caminho, degradação e indisponibilidade do serviço. O projeto executivo detalhará a implantação e os ensaios sem alterar esses limites.
5.4.41. A EXECUTORA deverá monitorar utilização, percentil 95, picos, filas, descarte de pacotes, latência, perda, sessões, utilização dos equipamentos, armazenamento de logs e demais elementos capazes de produzir gargalo.
5.4.42. O relatório mensal deverá identificar tendências, elementos próximos da saturação e ações preventivas. O risco de esgotamento deverá ser comunicado antes de afetar os serviços públicos.
5.4.43. A arquitetura deverá suportar crescimento gradual dos nodes, dos acessos à Internet, dos serviços de segurança e dos fluxos de data center sem substituição generalizada do núcleo.
5.4.44. A coleta deverá utilizar IPFIX ou mecanismo funcionalmente equivalente baseado em padrão aberto ou amplamente adotado, com médias de cinco minutos, janela móvel de 30 dias e apuração do percentil 95 por enlace e por sentido.
5.4.45. Os valores de 30% e 40% no percentil 95 serão adotados como gatilhos iniciais de análise e planejamento, especialmente nas camadas de núcleo e agregação, sem autorizar ampliação ou faturamento automáticos. Os limiares definitivos deverão considerar velocidade, sentido, camada, classe, criticidade,

filas, latência, perda, tendência, capacidade da rota principal e perfil contratado da proteção GPON. Os percentuais de 30% e 40% referem-se à razão entre o tráfego P95 e a capacidade de referência identificada para o enlace e sentido, conforme item 5.8.15; não significam percentis 30 ou 40.

5.4.46. Os gatilhos não autorizam expansão ou faturamento automáticos. A EXECUTORA deverá apresentar análise de tendência, causa, criticidade, impacto, prazo de esgotamento e plano de capacidade.

5.4.47. O planejamento físico será definido por projeto. A capacidade por node e por camada será dimensionada pelos dados efetivos de utilização, percentil 95, simultaneidade, criticidade, filas, perdas, tendência de saturação e requisitos de contingência.

5.4.48. Para câmeras, OCR, sensores, telemetria, backup e demais aplicações intensivas em subida, o projeto executivo deverá dimensionar separadamente o upstream com base em dados efetivos, perfis de codificação, retenção, simultaneidade, criticidade, margem operacional e capacidade disponível.

5.4.49. Desvio acumulado superior a 15%, saturação recorrente, degradação de SLA ou entrada de projeto relevante exigirá revisão do plano de capacidade. A série histórica municipal será utilizada como base primária para o redimensionamento.

5.5. INTERNET BGP E ENDEREÇAMENTO

5.5.1. Os acessos dedicados à Internet serão simétricos, sem franquia, com trânsito IP integral e proteção DDoS a montante. Aplicam-se os perfis mínimos do quadro de aceite do item 21: 6 Gbps e bloco IPv4 público exclusivo /25 por acesso institucional; 4 Gbps e bloco IPv4 público exclusivo /29 por acesso público; todos com suporte a IPv6. O projeto identificará quantidade, destino, redundância e capacidade de cada acesso antes da proposta, sem confundir capacidade por acesso com capacidade agregada.

5.5.2. Os acessos institucionais redundantes deverão terminar em sites distintos e utilizar prestadoras, ASNs, rotas físicas, pontos de presença e dependências imediatas de trânsito independentes, de modo a evitar falsa redundância.

5.5.3. A EXECUTORA deverá disponibilizar sessões eBGP independentes quando tecnicamente aplicável, permitir anúncio de prefixos próprios do Município e manter rotas de contingência coerentes com a política aprovada.

5.5.4. Até a obtenção de recursos próprios pelo Município, serão utilizados blocos exclusivos disponibilizados pelas prestadoras. Os blocos não poderão utilizar CGNAT ou compartilhamento que impeça publicação de serviços, VPN, NAT ou DNS reverso.

5.5.5. A EXECUTORA deverá prestar apoio técnico e documental para futura solicitação de ASN e recursos IPv4 e IPv6 em nome do Município, incluindo plano de endereçamento, justificativa de multihoming, diligências, configuração eBGP, RPKI, ROAs e DNS reverso, sem garantia de aprovação pelos órgãos competentes.

5.5.6. A substituição de bloco ou alteração relevante de roteamento dependerá de justificativa, plano de migração, testes e aprovação do MUNICÍPIO DEMANDANTE, salvo emergência comprovada.

5.5.7. Os acessos institucionais e públicos, as sessões BGP externas, o peering e a saída pública são serviços distintos das rotas de transporte dos nodes. A redundância dos acessos à Internet não substituirá a rota de proteção dos C1/C2, a rota secundária dos C3/C4 nem a rota única dos C5.

5.6. WIFI PÚBLICO E HOTSPOTS

5.6.1. Cada node C4 deverá incluir conectividade, equipamentos, instalação, configuração, cabeamento local tecnicamente necessário, licenças, portal cativo, monitoramento, manutenção, suporte e segurança. Os pontos de acesso fornecidos para os hotspots C4 deverão implementar, no mínimo, Wi-Fi 6 (IEEE 802.11ax), com operação simultânea nas bandas de 2,4 GHz e 5 GHz. Serão aceitos pontos de acesso Wi-Fi 6E ou Wi-Fi 7 que atendam integralmente a esse mínimo. Equipamentos limitados a Wi-Fi 5 (IEEE 802.11ac) ou gerações anteriores não atenderão ao fornecimento mínimo, sem impedir o atendimento de terminais legados compatíveis.

5.6.2. O dimensionamento de cada hotspot demonstrará área de cobertura, ambiente interno ou externo, obstáculos, interferência, bandas utilizadas, canais, potência e capacidade dos enlaces de retorno. Identificará quantidade e distribuição dos pontos de acesso, usuários simultaneamente ativos e perfil de tráfego, distinguindo capacidade de associação, capacidade de rádio e capacidade útil de acesso à Internet. A solução suportará gerenciamento centralizado, ajuste de canais e potência, balanceamento, direcionamento entre bandas (band steering) e roaming assistido quando aplicável. O aceite registrará os locais de medição e verificará cobertura, autenticação, navegação e estabilidade sob a carga concorrente definida para o local; a velocidade nominal do rádio não comprovará a experiência do serviço. O projeto executivo identificará alimentação PoE, cabeamento, interfaces Ethernet, capacidade de uplink e licenças necessários aos modelos ofertados e à integração com Wi-Fi 7. A exigência de integração não pressupõe conversão de rádio Wi-Fi 6 em Wi-Fi 7 por atualização de software. O uso de 6 GHz e de funcionalidades exclusivas de Wi-Fi 7 dependerá de hardware, terminais, configuração e condições regulatórias aplicáveis, expressamente identificados na proposta.

5.6.2.1. Cada ponto de acesso deverá suportar no mínimo 200 dispositivos simultaneamente associados, dos quais pelo menos 100 simultaneamente ativos, com comprovação em ensaio de carga de 60 minutos. O perfil mínimo de ensaio será de 3 Mbps de download e 1 Mbps de upload de tráfego útil por dispositivo ativo, simultaneamente, totalizando pelo menos 300 Mbps e 100 Mbps, respectivamente, por AP. Dispositivo associado é o terminal conectado à rede; dispositivo ativo é o terminal com tráfego no ensaio. Pessoas, dispositivos e sessões TCP/UDP serão contabilizados separadamente; múltiplas sessões de um terminal não representarão múltiplos dispositivos.

5.6.2.2. Os APs serão de classe corporativa, próprios para operação contínua e alta densidade, com suporte e atualizações de segurança durante a vigência, OFDMA, MU-MIMO e operação simultânea em 2,4 GHz e 5 GHz. O rádio de 5 GHz 4×4:4 constitui a arquitetura de referência. Será admitida arquitetura distinta em Wi-Fi 6, 6E ou 7 mediante comprovação documental e atendimento integral ao mesmo ensaio de capacidade, segurança e gerenciamento, com terminais Wi-Fi 6 e sem depender de banda de 6 GHz, clientes de geração superior ou funções proprietárias dos terminais para cumprir o mínimo. A equivalência não reduzirá os mínimos de 200 associados e 100 ativos, nem as taxas e demais critérios de aceite. Cada AP terá interface de uplink de pelo menos 2,5 GbE e alimentação PoE compatível com todas as funções exigidas. Cabeamento, portas de acesso e orçamento de potência serão dimensionados para evitar limitação do desempenho contratado.

5.6.2.3. O Projeto Executivo adotará inicialmente até 50 dispositivos ativos por rádio de atendimento em 5 GHz como referência conservadora de planejamento, admitido ajuste mediante levantamento de radiofrequência e comprovação do desempenho no local. A aprovação de 100 ativos em laboratório não autoriza utilizar esse número automaticamente como capacidade permanente de toda célula. A quantidade de APs considerará cobertura, aplicações, simultaneidade, interferência, distribuição por banda e capacidade conjunta dos enlaces. Nos C4, a rota de proteção de 500 Mbps não será somada automaticamente à principal; a soma do tráfego dos APs e os recursos compartilhados deverão ser compatibilizados com o serviço de acesso contratado. O perfil do ensaio local não constitui garantia irrestrita de banda de Internet por usuário em toda a rede.

5.6.2.4. Os valores de capacidade e as condições de ensaio desta especificação constituem requisitos mínimos obrigatórios da solução ofertada, aplicáveis à seleção e à comprovação técnica nos respectivos marcos previstos. Não representam demanda presumida de um local nem capacidade garantida apenas pela designação Wi-Fi 6, 6E ou 7. O atendimento será comprovado por documentação técnica e pelos ensaios previstos, sem redução dos mínimos em razão do porte de cada projeto. As variáveis de implantação serão dimensionadas por projeto conforme o subitem seguinte; essa definição integra a execução da parceria e não constitui pendência desta especificação mínima.

5.6.2.5. Cada projeto terá dimensionamento próprio, elaborado pela parceira e submetido à aprovação técnica do InPACTA antes da respectiva implantação ou ativação, a partir da demanda formalizada e do levantamento do local. Serão identificados unidades, quantidades, áreas e pontos de cobertura, ambiente interno ou externo, obstáculos, aplicações, dispositivos associados e ativos previstos, tráfego por sentido, enlaces compartilhados, energia e

responsabilidades. A memória de dimensionamento justificará quantidade e posicionamento dos APs, capacidade dos enlaces e condições de cobertura e desempenho, com pontos de medição e critérios de aceite vinculados aos requisitos contratados. Para C6, abrangerá duração, montagem, retirada, capacidade útil do enlace e simultaneidade dos eventos. A parceira levantará as variáveis de campo, sem presumir demanda a partir do limite de catálogo. A seleção verificará os requisitos mínimos comuns; os parâmetros específicos serão formalizados no projeto e na respectiva ordem de serviço, observadas as condições de contratação e de remuneração, sem criar obrigação adicional gratuita ou flexibilizar os mínimos. A aprovação do dimensionamento é etapa de execução, não requisito de apresentação antecipada de todos os futuros projetos.

5.6.3. A quantidade teórica de dispositivos associados ao equipamento não será utilizada como único indicador de capacidade. A fiscalização considerará usuários ativos, taxa de autenticação, latência, perda, consumo, falhas e estabilidade. Aplicam-se os mínimos de 200 dispositivos associados e 100 ativos por AP, conforme itens 5.6.2.1 a 5.6.2.3, com ensaio nos termos dos itens 21.5.3.1 a 21.5.3.3.

5.6.4. Os hotspots serão segregados da rede administrativa e possuirão isolamento entre clientes, controle de sessão e proteção contra pontos de acesso não autorizados. Os mecanismos de segurança utilizarão WPA2-AES ou WPA3 e 802.1X quando aplicável ao perfil de acesso, vedada a adoção de mecanismos legados como padrão de novos ambientes. O portal cativo utilizará HTTPS, identidade visual e política de uso aprovadas, com autenticação quando definida. O teste verificará tentativa de acesso entre clientes, acesso indevido a domínios corporativos, expiração de sessão e preservação das políticas após reconexão. Registros e coleta de dados observarão a finalidade do serviço e a minimização de dados pessoais. O portal incluirá as funcionalidades de comunicação e participação dos itens 5.6.4.1 a 5.6.4.6. Poderá ser nativo ou integrado à gestão dos APs por interfaces documentadas e suportadas, com responsabilidade da executora pela solução completa. A exigência de plataforma de gerenciamento do fabricante dos APs não impõe o mesmo fabricante para o portal externo. A proposta identificará produto, versão, módulos, integração, licenças e limites incluídos, sem restrição a marca específica ou comprovação baseada apenas em nome comercial.

5.6.4.1. O portal deverá permitir criar, editar, pré-visualizar, agendar, publicar, pausar e encerrar campanhas institucionais, com texto, imagens, banners e links para serviços públicos. A programação contemplará início e término, fuso horário, seleção de hotspot, grupo de pontos ou evento e controle de repetição por sessão conforme configuração documentada. A aplicação de regras por local e período não dependerá de perfil comportamental do usuário. O conteúdo será responsivo e utilizável por teclado, com rótulos de campos e alternativas textuais para imagens informativas.

5.6.4.2. A solução deverá disponibilizar enquetes de pergunta única e questionários com múltiplas perguntas, admitindo escolha única, múltipla escolha, escala de avaliação e resposta textual com limite configurável. Deverá permitir ordenar perguntas, configurar campos obrigatórios apenas dentro da participação voluntária, validar respostas e apresentar confirmação de envio. Serão controlados prazo de participação e duplicidade de submissão por mecanismo documentado e proporcional, sem prometer identificação inequívoca de pessoas por endereço MAC ou dispositivo. A proposta explicitará o alcance e as limitações desse controle.

5.6.4.3. O portal deverá oferecer avisos institucionais, pesquisas de satisfação, avaliação de serviços e links ou chamadas para canais digitais oficiais, com configuração por local ou evento. A apresentação de conteúdo e as interações serão separadas da política de autenticação e liberação da conectividade. Indisponibilidade do módulo de campanhas ou pesquisa não bloqueará a navegação nem as novas autenticações quando os serviços de acesso permanecerem disponíveis, devendo o fluxo de contingência preservar as regras de segurança. A falha será monitorada e registrada sem concessão indevida de acesso.

5.6.4.4. O painel permitirá acompanhar, por campanha, formulário, versão, local e período, exibições, aberturas, participações iniciadas, respostas concluídas e abandonos, distinguindo métricas efetivamente observadas de estimativas. As taxas terão fórmula e denominador informados; dispositivos, sessões e pessoas não serão tratados como contagens equivalentes. Resultados agregados e respostas autorizadas serão exportáveis em CSV ou JSON, com identificador da campanha, versão, campos e referência temporal. Acesso a respostas individuais dependerá de perfil autorizado; pesquisas anônimas serão exportadas sem identificadores de autenticação ou correlação individual.

5.6.4.5. A administração do portal distinguirá autoria, aprovação, publicação e consulta de resultados por permissões. O InPACTA e os responsáveis municipais designados aprovarão conteúdos e públicos por local, finalidade dos formulários e acesso aos resultados, conforme suas competências. A executora disponibilizará configuração, integração, suporte e capacitação, sem assumir autorização editorial. Serão registrados autor, aprovador, versão, alteração, publicação, pausa, encerramento e exportação. Alteração de pergunta em campanha publicada gerará versão identificável, preservando a interpretação das respostas anteriores.

5.6.4.6. A proposta comprovará que campanhas, enquetes, questionários, relatórios e integração estão disponíveis na versão ofertada e incluídos nas licenças da capacidade contratada. Serão declarados limites de portais, locais, administradores, campanhas simultâneas, formulários, respostas, armazenamento e consultas de API quando fornecida, sem cobrança adicional para funcionalidades ou volumes já abrangidos pelo escopo. Em cada projeto serão configurados identidade visual, locais, conteúdos, formulários, perfis, volumes e política de dados antes da ativação, dentro dos recursos contratados. A PoC utilizará campanha e pesquisas de teste; a integração e a contingência serão novamente verificadas no ambiente implantado, sem exigir publicação real de campanha municipal antes da formalização.

5.6.5. A solução minimizará dados pessoais e não coletará conteúdo de navegação ou perfis comportamentais para segmentação das interações. Autenticação, registros operacionais e respostas a pesquisas terão finalidades e controles separados. Enquetes e questionários terão participação voluntária, com possibilidade de pular ou encerrar sem impedir o acesso à Internet nas condições autorizadas. A publicação dependerá da definição institucional de finalidade, campos, acesso, retenção, descarte e informação ao participante; respostas identificadas ou anônimas serão distinguidas expressamente. Não se exigirá dado pessoal desnecessário nem autorização genérica para publicidade como condição de conectividade. A opção por pesquisa anônima impedirá sua vinculação posterior à identidade de acesso nos relatórios ou exportações.

5.6.6. A plataforma deverá disponibilizar indicadores agregados de utilização, disponibilidade, autenticações, usuários ativos, consumo, falhas e capacidade, sem exposição indevida de dados pessoais. A plataforma de gerenciamento ofertada deverá suportar a operação conjunta de pontos de acesso Wi-Fi 6 e Wi-Fi 7 (IEEE 802.11be), com provisionamento, inventário, políticas de acesso e segurança, segmentação, portal cativo, monitoramento e alarmes integrados. A proposta identificará modelos, versões de software e licenças compatíveis, com documentação do fabricante de funcionalidades já disponíveis; promessa de desenvolvimento futuro não comprovará atendimento. A capacidade de integração deverá estar incluída na solução, com explicitação das licenças e dos custos de expansão por ponto de acesso. A instalação de pontos Wi-Fi 7 adicionais dependerá dos quantitativos e condições de acionamento contratados.

5.6.6.1. Os APs deverão ser gerenciados por solução corporativa de gerenciamento centralizado e aplicação de políticas, oficialmente fornecida e suportada pelo fabricante dos APs, admitida arquitetura local, em nuvem ou híbrida. A proposta identificará os componentes responsáveis pelo gerenciamento, controle, autenticação, autorização e encaminhamento do tráfego, suas versões, licenças e dependências. Deverá explicitar o modo de encaminhamento utilizado e os pontos de aplicação das políticas, demonstrando o atendimento aos requisitos funcionais, de segurança, capacidade e continuidade previstos nesta especificação. A arquitetura adotada não dispensará qualquer requisito mínimo obrigatório. Deverão estar disponíveis provisionamento centralizado, inventário, configuração em massa, distribuição de políticas, atualização de firmware, gerenciamento de canais e potência, VLANs, suporte a autenticação IEEE 802.1X com serviço RADIUS compatível, políticas de acesso, isolamento, portal cativo, monitoramento por dispositivo, histórico, alertas e relatórios. O suporte a 802.1X será comprovado em perfil de teste corporativo; sua existência não obriga o usuário do hotspot público a possuir credencial corporativa. O perfil público terá fluxo de acesso e autenticação próprio, documentado na proposta quanto às funcionalidades disponíveis e configurado em cada projeto

antes da ativação, com portal HTTPS e segregação. A proteção do portal e a proteção do enlace sem fio serão identificadas separadamente. A designação comercial SDN ou um painel em nuvem, isoladamente, não comprovará atendimento.

5.6.6.1.1. A solução deverá permitir aplicar modelos de configuração por local, grupo de APs e SSID, com atribuição dos equipamentos aos respectivos grupos. Deverá registrar a versão ou revisão da configuração, o resultado de sua distribuição e as divergências entre configuração prevista e aplicada, identificando APs sem comunicação ou com falha de aplicação. Deverá oferecer procedimento suportado para restaurar a última configuração válida. A segregação administrativa distinguirá os ambientes municipais e as permissões de gestão e consulta do InPACTA, conforme as atribuições institucionais.

5.6.6.1.2. O gerenciamento de radiofrequência deverá permitir seleção automática e ajuste manual de canal e potência, além de configuração da largura de canal por rádio e banda suportada. Os ajustes automáticos respeitarão os canais permitidos, limites de potência e condições de operação aplicáveis ao equipamento e ao local. A solução deverá apresentar ocupação dos canais, interferência observável e retransmissões, registrando as mudanças de canal e potência. O projeto definirá os parâmetros locais antes da ativação; sua configuração não reduzirá os mínimos de capacidade e desempenho exigidos.

5.6.6.1.3. O diagnóstico deverá distinguir AP, rádio, SSID e sessão, permitindo consultar sinal recebido, relação sinal/ruído, taxas físicas de conexão, utilização do canal, retransmissões e falhas de associação e autenticação, com identificação da fonte e referência temporal. Taxa física negociada não será apresentada como vazão útil comprovada. A segmentação deverá associar SSIDs às VLANs e políticas de acesso, separar o tráfego de gerenciamento e impedir acesso indevido à rede administrativa. O isolamento entre clientes do perfil público será verificado no mesmo AP e entre APs distintos, considerando os pontos de aplicação da política na solução completa.

5.6.6.1.4. A atualização de firmware deverá permitir programação por grupos de APs, com identificação prévia da compatibilidade entre equipamento, versão, plataforma e funcionalidades utilizadas. A executora registrará a versão anterior e a pretendida, a janela de manutenção, os resultados por AP e o procedimento de recuperação de falhas oficialmente suportado. A recuperação não dependerá de reversão para versão não suportada pelo fabricante. Atualizações serão escalonadas conforme o plano aprovado, para controlar a interrupção da cobertura e respeitar os níveis de serviço contratados.

5.6.6.1.5. O portal poderá ser nativo ou externo, integrado por mecanismo documentado e suportado, sem obrigação de pertencer ao fabricante dos APs, conforme itens 5.6.4.1 a 5.6.4.6. A proposta identificará o componente que autoriza o acesso, o protocolo ou API de integração, os registros de início, atualização e término de sessão e o mecanismo de expiração e encerramento. A solução deverá demonstrar redirecionamento, autorização, contabilização e encerramento efetivo do acesso. Os destinos permitidos antes da autenticação serão limitados aos serviços necessários ao fluxo autorizado. Suporte genérico a API ou RADIUS não comprovará a integração ofertada; o método IEEE 802.1X do perfil corporativo será identificado e testado separadamente do fluxo público.

5.6.6.2. A plataforma deverá oferecer perfis administrativos, trilha de auditoria, API documentada e exportação de dados, com gestão conjunta de APs Wi-Fi 6 e Wi-Fi 7. A proposta apresentará documentação oficial, versões, dependências e matriz funcional de compatibilidade. Licenças, hospedagem quando necessária, suporte e atualizações estarão incluídos para toda a capacidade efetivamente contratada durante a vigência, com custos de expansão explicitados. O projeto dimensionará APs, sites, dispositivos e autenticações simultâneas separadamente. Será documentado e testado o comportamento durante perda de comunicação com a plataforma e recuperação, incluindo preservação das configurações, continuidade das sessões locais que não dependam de serviço externo indisponível e tratamento de novas autenticações. Não se exigirá fabricante determinado. A matriz de compatibilidade vinculará cada função ao modelo de AP, firmware, plataforma, modo de operação e licença ofertados. Documentação de outra família ou geração não comprovará atendimento sem correspondência oficial para a combinação proposta. Os recursos mínimos deverão estar disponíveis na solução ofertada, ficando o dimensionamento e os parâmetros locais sujeitos ao projeto aprovado.

5.6.6.3. A API documentada deverá permitir consultar inventário e estado dos APs, versões, utilização, contagens de dispositivos associados e ativos, alarmes e eventos operacionais. A documentação informará autenticação, permissões, campos, unidades, timestamps, paginação e limites de consulta. A fiscalização terá acesso institucional de consulta e exportação, com privilégio mínimo e trilha de auditoria. Relatórios e registros autorizados serão exportáveis em formato aberto e legível por máquina, como CSV ou JSON, preservados significado e referência temporal. A solução oferecerá configuração da retenção e exportação por categoria de registro. A proposta declarará faixas de configuração, granularidade, capacidade de armazenamento e licenças incluídas. Em cada projeto, a parceira documentará o perfil de retenção, acesso e descarte, aprovado pelo InPACTA antes da ativação, dentro dos recursos contratados e das obrigações aplicáveis. Não se exigirá identificação pessoal para métricas agregadas nem coleta de conteúdo de navegação.

5.6.6.4. A proposta apresentará matriz de dependências que diferencie gerenciamento, encaminhamento de tráfego, portal, autenticação, DNS, DHCP e acesso à Internet. O teste de perda da plataforma deverá isolar sua comunicação, mantendo disponíveis os demais serviços necessários, e verificar preservação das configurações e continuidade das sessões locais independentes da plataforma. Para novas associações e autenticações, a matriz indicará serviços locais e remotos, continuidade ou bloqueio seguro, sem liberar acesso indevido por falha. Restabelecida a comunicação, a solução deverá retomar a gestão, sincronizar o inventário e identificar lacunas de telemetria, sem reconfiguração manual dos APs. Serão registrados os tempos efetivamente observados e as interrupções por função. A aprovação funcional dependerá da comprovação desses comportamentos; os limites de disponibilidade e recuperação seguirão os níveis de serviço expressamente contratados. O projeto documentará as dependências e os procedimentos de contingência pertinentes à implantação, sem presumir continuidade de função dependente de serviço externo indisponível. As indisponibilidades da gestão, do portal e do serviço de autenticação serão avaliadas separadamente, preservando os demais componentes necessários em cada cenário. O resultado distinguirá sessões já autorizadas, novas associações, novas autenticações e expiração de sessões. A falha do módulo de interatividade observará a continuidade prevista no item 5.6.4.3; a indisponibilidade de um serviço indispensável à autorização não permitirá liberação indevida de novos acessos.

5.6.7. A Infovia deverá permitir conexão de sensores, câmeras, telemetria e dispositivos relacionados a iniciativas de cidade inteligente, sem que isso implique fornecimento automático dos sistemas finais.

5.7. CONECTIVIDADE TEMPORÁRIA C6

5.7.1. O C6 atenderá eventos, operações temporárias, contingências e locais sem infraestrutura permanente disponível, mediante ordem de serviço.

5.7.2. A solução deverá utilizar conectividade satelital como meio principal, admitida contingência complementar por rede móvel, rádio, fibra temporária ou combinação equivalente quando necessária à continuidade.

5.7.3. Cada evento deverá incluir mobilização, instalação, conectividade, roteador de borda, pontos de acesso e antenas necessários, segurança, monitoramento, suporte, relatório, desmobilização e todos os custos associados. Os pontos de acesso Wi-Fi fornecidos para C6 também deverão atender ao mínimo Wi-Fi 6 e à integração com Wi-Fi 7 dos itens 5.6.1, 5.6.2 e 5.6.6. A comprovação seguirá o item 21.5.3 e o Anexo V, item 12.1, preservados o dimensionamento e o aceite próprios de cada evento. Os APs fornecidos para C6 atenderão também aos requisitos corporativos de capacidade por AP, uplink e gerenciamento centralizado previstos no item 5.6.6, aplicáveis aos C4. O ensaio de capacidade do AP será local e independente do enlace satelital. O dimensionamento do evento distinguirá público, dispositivos associados, ativos e capacidade útil do enlace, sem converter automaticamente a capacidade do AP em garantia de Internet por participante.

5.7.4. O dimensionamento do C6 distinguirá público total, dispositivos conectados e usuários simultaneamente ativos. Para a formação do preço por evento completo, o projeto disponibilizará duração de operação, janelas de montagem e retirada, área e condições de cobertura, simultaneidade, aplicações, capacidade útil mínima por sentido, contingência exigida, suporte presencial quando previsto, antecedência de mobilização e eventos concomitantes. A proponente dimensionará os recursos para essas condições. Eventos com condições distintas deverão ter seu enquadramento de preço explicitado; a Ordem

de Serviço não poderá ampliar os limites precificados sem o tratamento formal pertinente.
5.7.5. A executora demonstrará capacidade operacional para o calendário e a simultaneidade dos eventos formalizados em cada projeto, sem consumo mínimo garantido.
5.7.6. O pagamento será por evento completo, homologado e aceito, vedada cobrança adicional por diária, deslocamento, instalação, equipamentos, franquia ou desmobilização já abrangidos pelo preço unitário.
5.7.7. O relatório de cada evento C6 deverá identificar o evento, período, local, Ordem de Serviço e node temporário, registrar disponibilidade do serviço, conectividade, volume de tráfego, consumo por período, quantidade de usuários e dispositivos conectados quando tecnicamente disponível, picos de simultaneidade, desempenho do enlace principal, utilização dos pontos de acesso, indisponibilidades, incidentes, chamados, ações de suporte, cobertura, qualidade e evidências suficientes à fiscalização, medição e aceite, observadas a LGPD e a minimização de dados pessoais.
5.7.8. A unidade de medição da classe C6 é o evento completo, identificado por ID próprio e Ordem de Serviço. O node temporário é vinculado ao evento e não compõe o estoque mensal dos nodes permanentes C1 a C5. Reutilização do mesmo equipamento em eventos diferentes não altera essa unidade de medição.
5.7.9. A requisição municipal de C6 deverá informar local e coordenadas, área de cobertura, datas e horários de montagem, teste, operação e retirada, público estimado, usuários simultaneamente ativos, aplicações, necessidades de upload e download, energia, acesso e responsável pelo evento. A solicitação incompleta será diligenciada antes da confirmação da mobilização.
5.7.10. Os requisitos de desempenho do evento serão definidos antes da proposta correspondente: capacidade útil por sentido, simultaneidade, cobertura, perfil de tráfego, latência e perda admissíveis, eventual franquia e tratamento de esgotamento. O projeto executivo detalhará QoS, distribuição dos pontos de acesso, visada satelital, obstruções, fixação, alimentação e condições ambientais, preservados os requisitos precificados. Antes da abertura do evento, os ensaios confrontarão os resultados com esses requisitos e registrarão os pontos de medição, a carga aplicada e as condições ambientais observadas.
5.7.11. A contingência complementar será dimensionada conforme a criticidade e a viabilidade do local. O projeto identificará meio, gatilho de acionamento, aplicações preservadas e capacidade disponível durante contingência. A classificação C6 não pressupõe duas rotas ópticas nem herda as capacidades de C3 ou C4.
5.7.12. A executora demonstrará disponibilidade de terminais satelitais, roteadores, pontos de acesso, licenças, equipes e suporte para os eventos simultâneos autorizados. O calendário consolidado deverá impedir dupla alocação de recursos incompatível com a execução.
5.7.13. A liberação técnica ocorrerá antes da abertura do evento, mediante testes de conectividade, cobertura, simultaneidade prevista, segregação, segurança, monitoramento e contingência contratada. O relatório final confrontará os parâmetros autorizados com os resultados e registrará incidentes, suporte e desmobilização, para aceite e pagamento por evento completo.

5.8. ENGENHARIA AVANÇADA DA REDE E COMPROVAÇÃO

5.8.1. O projeto executivo deverá conter diagramas físico e lógico, pontos de demarcação, tabela de interfaces e matriz de fluxos. Para cada circuito serão registrados ID, classe, endereço, caminho, provedor, capacidade por sentido, meio de acesso, domínio de falha, destino de concentração, VLAN ou VRF e responsabilidade operacional. A versão aprovada será a referência de configuração e de aceite. A executora elaborará e assumirá a responsabilidade técnica pelo projeto executivo da parcela contratada, após a formalização e a autorização da etapa de elaboração. O InPACTA verificará a compatibilidade com o escopo e as interfaces institucionais; a equipe municipal validará suas interfaces e condições locais. A aprovação será expressa pelos agentes competentes designados no instrumento, antes da implantação ou migração da parcela correspondente. Vistorias e levantamentos autorizados poderão anteceder essa aprovação. A aprovação não afastará a responsabilidade técnica da executora nem autorizará alteração de escopo, preço ou prazo.
5.8.2. A memória de capacidade decomporá acesso, agregação, backhaul, backbone, concentração, túneis e segurança de borda. Para cada elemento identificará capacidade útil por sentido, carga prevista, simultaneidade, recursos já comprometidos e capacidade residual em operação normal e após falha simples. Explicitará overhead, criptografia, inspeção, compartilhamento dos uplinks e perfil de contingência da classe. A proponente demonstrará o percurso completo do fluxo e o componente que limita sua capacidade, sem somar capacidades de rotas alternativas como se fossem simultaneamente utilizáveis. O ensaio utilizará os mesmos pontos de entrega, perfis, funções habilitadas e condições de concorrência adotados no dimensionamento.
5.8.3. A independência das rotas será demonstrada por matriz de domínios de falha que confronte cabo, duto, entrada predial, posteamento crítico, OLT ou agregador, ponto de presença, alimentação, backhaul e núcleo. Fornecedores distintos não comprovam, por si, percursos independentes. Compartilhamentos inevitáveis exigem identificação, análise de impacto, mitigação e aprovação técnica, preservadas as exigências da classe.
5.8.4. Para IPv4 e IPv6, a matriz de roteamento deverá identificar vizinhos, interfaces, prefixos permitidos, políticas de importação e exportação, preferência de caminhos e comportamento de retorno. O projeto documentará prevenção de vazamento entre VRFs, rotas não autorizadas e loops. A conectividade entre domínios será permitida somente pela matriz de fluxos aprovada.
5.8.5. O BGP com BFD, ou mecanismo funcionalmente equivalente admitido, terá parâmetros de detecção e reconvergência documentados. Os tempos máximos admissíveis serão definidos para cada classe e condição de falha antes da proposta correspondente, em coerência com os níveis de serviço exigidos. O ensaio distinguirá perda física, falha de encaminhamento com interface ativa e falha do destino monitorado. Registrará o instante de indução da falha, detecção, retirada da rota, restabelecimento do tráfego e estabilização, além da perda de pacotes. Sessão de roteamento restabelecida não comprova, isoladamente, recuperação do serviço. A aprovação do procedimento de teste não poderá alterar os limites contratados.
5.8.6. A política de retorno à rota preferencial deverá prever estabilidade e controle de oscilações. O aceite incluirá falha e retorno de cada caminho, manutenção planejada e perda das dependências compartilhadas identificadas. O resultado será aferido por fluxo de aplicação e por sentido, além do estado da sessão de roteamento.
5.8.7. O plano de segmentação deverá relacionar VLANs, VRFs ou mecanismos equivalentes, sub-redes, gateways e regras de comunicação entre rede administrativa, serviços públicos, campo, gestão e voz quando ativada. Serão testados os fluxos autorizados e a negação dos fluxos não previstos, inclusive entre clientes e entre usuários de hotspots.
5.8.8. A memória de MTU deverá contabilizar cabeçalhos de transporte, túneis e criptografia em cada caminho. O aceite verificará transmissão de diferentes tamanhos de pacote, descoberta de MTU do caminho, mensagens de controle necessárias e comportamento em contingência, evitando descarte silencioso e fragmentação incompatível com a aplicação. Ajustes de MSS, quando utilizados, serão documentados.
5.8.9. A política de QoS deverá identificar classes, marcação DSCP, fronteira de confiança, classificação, filas, limites, reserva e tratamento de excesso. O teste utilizará tráfego concorrente para verificar proteção dos serviços prioritários e ausência de monopolização. Os perfis serão demonstrados também na capacidade reduzida da proteção C1/C2. A habilitação da classe de voz não implica contratação ou ativação de telefonia.
5.8.10. Os túneis e mecanismos de integração segura deverão ter pares, algoritmos e versões suportados, autenticação, gestão de chaves, renovação, revogação e monitoramento documentados, sem divulgação de segredos em relatórios. O teste verificará tráfego útil com criptografia habilitada, renovação de sessão, falha do túnel e recuperação sem violação da segregação.
5.8.11. Na infraestrutura óptica compartilhada, a memória identificará porta PON, árvore óptica, terminais atendidos, razão de divisão óptica (split ratio), capacidade dos uplinks e perfil reservado a cada serviço. O orçamento óptico apresentará potências de transmissão e recepção, perdas estimadas em fibra,

divisores, emendas e conectores e margem disponível, confrontadas com os limites operacionais dos componentes. Serão registrados os níveis efetivamente medidos e os alarmes pertinentes. A memória de tráfego distinguirá capacidade da porta, compartilhamento, alocação dinâmica de banda e capacidade útil por sentido, considerando concorrência, overhead e criptografia. Nos C3/C4, cada rota manterá o mínimo simétrico integral; no C5, será demonstrado o atendimento simultâneo dos dispositivos e o mínimo de 50 Mbps simétricos. A proteção C1/C2 observará o perfil útil definido no item 5.8.12.

5.8.12. A proteção GPON C1/C2 observará as taxas nominais de linha do item 5.4.9. A base do projeto disponibilizada antes da proposta fixará, por sentido, a capacidade útil mínima garantida na interface de serviço, a camada de medição, o perfil de concorrência e os serviços prioritários preservados. A memória de capacidade demonstrará reserva e compartilhamento, overhead, criptografia e ausência de gargalos; o aceite aferirá o throughput útil nas condições contratadas. Não será aceita comprovação baseada apenas na velocidade da porta ou na taxa nominal do meio. Essa proteção não equivale a uma segunda rota MPLS de 10 Gbps.

5.8.13. Os acessos à Internet terão política de eBGP, prefixos, endereçamento, contingência e proteção DDoS documentada. A verificação abrangerá anúncio e retirada de prefixos, alcance IPv4/IPv6, DNS reverso e utilização dos blocos autorizados. RPKI e ROAs serão tratados na implantação dos recursos próprios quando aplicáveis, sem pressupor ASN ou blocos já concedidos.

5.8.14. A segurança de borda será dimensionada com as funções efetivamente contratadas habilitadas e com o perfil de tráfego do projeto. A memória identificará throughput inspecionado, sessões concorrentes, novas sessões, túneis, carga de CPU e memória, geração e exportação de logs e capacidade remanescente após falha de membro. A demonstração de alta disponibilidade verificará continuidade do encaminhamento e aplicação das políticas, além do estado dos equipamentos. O relatório registrará as funções ativas durante a medição; valores de encaminhamento sem inspeção não comprovarão desempenho com IPS, controle de aplicações e demais funções exigidas. Inspeção de tráfego criptografado seguirá política aprovada, com escopo e exceções identificados. A capacidade remanescente após falha de um membro deverá atender integralmente à carga e aos mínimos contratados para os serviços que utilizam o conjunto de segurança, com inspeção, VPN, registros e demais funções exigidas habilitadas. Não será admitido somar capacidades de membros que não permaneçam disponíveis no cenário de falha ensaiado.

5.8.15. O monitoramento correlacionará serviço, interface, caminho, classe, alarme e chamado, com relógios sincronizados e identificação de fonte e coleta. O percentil 95 (P95) é o valor abaixo ou igual ao qual se encontram aproximadamente 95% das amostras válidas ordenadas. Será apurado por enlace e sentido, sobre médias de cinco minutos em janela móvel de 30 dias, separando download e upload. O relatório explicitará método de cálculo, quantidade de amostras, cobertura temporal e lacunas. O P95 será apresentado em taxa de tráfego e, quando percentual, como razão entre essa taxa e a capacidade de referência explicitada. Não corresponde a 95% de disponibilidade nem a uma média ou máximo. Picos, filas, descartes, latência, perda e indisponibilidade continuarão registrados e avaliados. Lacunas não serão convertidas em tráfego zero ou disponibilidade comprovada. Os dados exportáveis permitirão reproduzir o cálculo.

5.8.16. Cada ensaio identificará requisito, unidade ou circuito, condição inicial, topologia, pontos de medição, ferramentas e versões, funções habilitadas, carga, duração, tamanhos de pacote, limite de aceitação, resultado e evidência. Serão verificados capacidade útil bidirecional, latência, perda, jitter quando aplicável, segregação, QoS sob carga, falha e retorno. A base para a proposta fixará os mínimos e as condições de ensaio que influenciem dimensionamento ou preço; o protocolo executivo detalhará sua execução, sem reduzir a exigência nem introduzir obrigação material não prevista. Medições unidirecionais indicarão a sincronização dos relógios; medições de ida e volta serão identificadas como tais. Resultado sem condição de teste ou evidência reproduzível não comprovará atendimento.

5.8.17. O cadastro de configuração deverá incluir cópias recuperáveis, versões, inventário, licenças, políticas, procedimentos de restauração e acesso administrativo segregado. Mudanças de rota, provedor, equipamento, política de QoS ou túnel exigirão análise de impacto, plano de reversão e reteste dos requisitos afetados. O diagrama conforme implantado deverá corresponder à configuração em produção.

6. SERVIÇOS TÉCNICOS SOB DEMANDA

6.1. A expansão de rede e os eventos C6 dependerão de Ordem de Serviço específica. A telefonia será acionada exclusivamente conforme o item 25. A separação técnica das parcelas não altera, por si, a forma de contratação aprovada nem autoriza faturamento por prontidão não acionada.

6.2. A especificação, o licenciamento e a operação da telefonia constam do item 25.

6.3. A Ordem de Serviço de telefonia distinguirá ramais, chamadas simultâneas, troncos externos, licenças e unidades efetivamente ativadas, conforme o item 25.

6.4. Gravação e processamento inteligente de chamadas dependem de autorização própria, conforme o item 25, sem impedir o funcionamento da voz quando não ativados.

7. OPERAÇÃO ASSISTIDA E IMPLANTAÇÃO

7.1. Cada projeto definirá inventário, interfaces, acessos, energia, acomodação, dependências, janelas e responsáveis. A migração será planejada com piloto, coexistência, ondas, reversão e verificação da conectividade de destino antes da desativação da origem.

7.2. A operação integrará o N1 e a Central de Situação do InPACTA ao NOC, SOC, suporte especializado N2/N3 e equipes de campo da executora, com sistema de chamados compartilhado ou integrado. Cobertura, canais, recursos e presença física serão dimensionados por criticidade, território e níveis de serviço no plano de mobilização, sem exigir instalação preexistente para participação.

7.3. A implantação deverá ser concluída em 90 dias, contados do marco inicial expressamente definido no instrumento do projeto. Antes da proposta correspondente, esse instrumento identificará o evento que inicia a contagem, a forma de registro, as condições de acesso e infraestrutura necessárias e os prazos específicos da telefonia. O cronograma indicará planejamento, mobilização, implantação, testes e aceite, com responsáveis e dependências. Impedimento municipal será registrado por unidade, com data, evidência, atividade afetada e providência necessária; seus efeitos e eventual reprogramação dependerão de decisão formal, sem suspensão automática de todo o cronograma ou alteração unilateral de prazo.

7.4. IMPLANTAÇÃO MIGRAÇÃO COEXISTÊNCIA E EXPANSÃO

7.4.1. O plano deverá conter arquitetura, cronograma, matriz de responsabilidades, relação de subcontratadas críticas, plano de endereçamento, segurança, monitoramento, testes, migração, coexistência, comunicação, contingência, rollback, aceite e transição.

7.4.2. O cronograma deverá priorizar os nodes C1, C2, hospitais, segurança, serviços essenciais, ambientes centrais e demais pontos indicados pela Administração.

7.4.3. A implantação será organizada em piloto e ondas de ativação, com testes, estabilização e operação assistida proporcional ao risco de cada grupo.

7.4.4. Nenhum serviço legado será desligado antes do aceite do serviço substituto, salvo autorização formal do MUNICÍPIO DEMANDANTE.

7.4.5. Mudanças nas rotas principal ou de proteção dos nodes C1 a C4, na rota única dos nodes C5, na borda, no roteamento, nos túneis criptografados, no DDoS, na Internet, na segurança ou em sistemas críticos deverão possuir plano de reversão testável e homologação proporcional ao risco.

7.4.6. Os custos de coexistência, migração, testes, correções e reversão imputáveis à solução da EXECUTORA estarão incluídos nos preços.

7.4.7. Novos nodes, mudanças de classe, ampliação de capacidade, transferência de endereço e eventos C6 dependerão de ordem de serviço, disponibilidade contratual, viabilidade técnica e aceite.

7.4.8. A mudança de prestadora, infraestrutura, rota, árvore PON, OLT, ponto de presença, túnel, mecanismo de roteamento ou subcontratada crítica deverá ser formalmente comunicada. Alterações com impacto relevante nos nodes, Internet, segurança ou continuidade exigirão documentação técnica, plano de migração, testes e homologação proporcional ao risco.
7.4.9. As expansões serão executadas gradualmente por Ordem de Serviço, após validação da necessidade e do dimensionamento, dentro dos limites, preços, recursos e condições formalizados para o projeto.
7.4.10. A EXECUTORA não será obrigada a instalar antecipadamente todos os equipamentos terminais dos nodes não demandados, mas deverá manter arquitetura, licenciamento e capacidade estrutural compatíveis com o patamar mínimo de expansão.
7.4.11. Racks, gabinetes, nobreaks, UPS, PDUs, proteções, módulos, transceptores e demais componentes necessários à ativação deverão ser previstos na composição do node ou do serviço central correspondente.
7.4.12. A telefonia observará os marcos, prazos e critérios específicos do bloco de mobilização da telefonia desta especificação, integrados ao cronograma geral de mobilização, sem interferir na continuidade dos demais serviços da Infovia.
7.4.13. A Ordem de Serviço de telefonia será emitida somente após motivação administrativa, validação dos quantitativos, disponibilidade orçamentária e confirmação dos responsáveis e dependências do MUNICÍPIO DEMANDANTE.

8. EQUIPAMENTOS E FRONTEIRAS DO ESCOPO

8.1. Equipamentos, licenças e meios necessários integram a prestação como serviço no alcance contratado. Permanecem delimitadas as responsabilidades pela LAN interna, aplicações, servidores, locais, energia e autorização de acesso. Integrações não transferem automaticamente a gestão desses ativos.
8.2. A reutilização de aparelhos municipais depende de inventário, compatibilidade, configuração e teste. A propriedade dos terminais legados permanece municipal; a rede externa de prestadores não é incorporada automaticamente ao patrimônio público.

8.5. COMUTAÇÃO AGREGAÇÃO E QOS

8.5.1. A solução de comutação e agregação será dimensionada para os nodes C1 e C2 em 10 Gbps, para os acessos à Internet, para as rotas de proteção, para a expansão e para a contingência, com capacidade de encaminhamento e interfaces compatíveis.
8.5.2. Os equipamentos deverão suportar redundância de alimentação e ventilação quando aplicável, agregação de enlaces, VLAN 802.1Q, QinQ quando necessário, STP/RSTP/MSTP ou mecanismos equivalentes, proteção contra loops e jumbo frames.
8.5.3. A camada de roteamento suportará IPv4, IPv6, rotas estáticas, OSPF, BGP, VRRP ou mecanismos equivalentes, ECMP quando aplicável e multicast quando necessário. Nos gateways de borda e de concentração que atendam serviços críticos dos sites principal e de continuidade e dos nodes C1/C2, a redundância será implantada e testada por VRRP ou mecanismo equivalente, conforme o escopo e as interfaces definidos no projeto. O simples suporte ao protocolo não comprovará sua ativação. Gateways internos municipais terão sua responsabilidade e eventual adequação expressamente identificadas, sem fornecimento presumido fora do escopo.
8.5.4. A solução implementará QoS com classificação, marcação, filas de prioridade, controle de banda e preservação de DSCP, incluindo tratamento prioritário para voz, vídeo e sistemas críticos.
8.5.5. Serão disponibilizados ACL, 802.1X quando aplicável, port security, DHCP Snooping, proteção de origem, controle de tempestades, autenticação administrativa, SSHv2, HTTPS, SNMPv3, Syslog e NTP.
8.5.6. O gerenciamento será centralizado, com inventário, configuração, backup, atualização, alarmes, telemetria e exportação de dados.
8.5.7. A indisponibilidade da ferramenta de gestão não poderá interromper o encaminhamento do tráfego já configurado.

8.6. ACESSO ÓPTICO OLT ONU ONT E CPE

8.6.1. A tecnologia GPON observará a família ITU-T G.984 ou tecnologia óptica equivalente ou superior, desde que atenda às capacidades, à interoperabilidade, à segurança, à gerência e aos níveis de serviço.
8.6.2. A quantidade de OLTs, portas PON, módulos, splitters, uplinks, chassis e elementos de agregação será dimensionada no projeto executivo conforme quantidade de nodes, split ratio, oversubscription, capacidade por sentido, contingência e expansão.
8.6.3. As OLTs e seus sistemas de gerência suportarão provisionamento, perfis de serviço, alocação dinâmica de banda (DBA), QoS, autenticação de terminais, detecção de terminal não autorizado, alarmes, atualização e integração por SNMPv3 ou API. Para cada perfil, serão identificadas as bandas assegurada e máxima por sentido, a política de compartilhamento e a associação ao node e à porta PON. O teste confrontará o perfil configurado com a capacidade útil obtida sob concorrência, verificará priorização, limites e alarmes e demonstrará que a ativação de outro terminal não reduz os mínimos contratados dos serviços existentes.
8.6.4. Os uplinks ópticos deverão possuir capacidade suficiente para o tráfego agregado, a proteção, a replicação de estados e a expansão, sem concentração incompatível com os níveis de serviço.
8.6.5. ONU, ONT ou CPE deverão ser compatíveis com a arquitetura, suportar o perfil da classe, gerenciamento remoto seguro, alarmes, inventário e integração com o túnel criptografado e o roteamento previstos.
8.6.6. Não será exigido que OLT e ONU, ONT ou CPE pertençam ao mesmo fabricante. A interoperabilidade será comprovada para as combinações efetivamente ofertadas, com identificação de modelos e versões e evidências de provisionamento, autenticação, aplicação dos perfis, VLANs, QoS, alarmes, gerenciamento remoto, atualização e recuperação após reinício. A documentação comercial isolada não substituirá a demonstração de estabilidade e desempenho da combinação utilizada. Alteração de modelo ou versão que afete a interoperabilidade exigirá validação e registro antes de sua adoção em produção.
8.6.7. Funcionalidades acessórias embarcadas em terminais não substituirão pontos de acesso ou componentes expressamente exigidos para o serviço.
8.6.8. A capacidade da árvore PON e dos elementos compartilhados será demonstrada sob carga concorrente, considerando overhead e throughput útil.

8.7. SITES DE CONCENTRAÇÃO E NODES CRÍTICOS

8.7.1. O site principal e o site de continuidade serão implantados em domínios de falha distintos e não compartilharão integralmente prédio, sala, alimentação principal, duto crítico, rota, ponto de presença ou equipamento de agregação capaz de produzir falha simultânea.
8.7.2. Cada site possuirá node C1, acesso dedicado à Internet, roteamento, segurança, comutação, monitoramento e recursos de energia compatíveis com a criticidade.
8.7.3. A localização dos sites de concentração avaliará a proximidade a pontos de troca de tráfego pertinentes ao território atendido, considerando qualidade, custo, diversidade física e resiliência, sem direcionamento a endereço, participante ou prestador específico.
8.7.4. Os nodes C2 atenderão unidades críticas e serão submetidos a teste individual de rota principal, proteção, túnel, roteamento, detecção, comutação, capacidade, estabilidade e monitoramento.

8.7.5. O projeto executivo demonstrará os percursos funcionais, domínios de falha, capacidade em contingência, mecanismos de proteção, pontos de monitoramento e testes.

8.8. INTERFACES DOS NODES INSTITUCIONAIS

8.8.1. A arquitetura de transporte deverá interoperar com as interfaces municipais e suportar, conforme a classe, MPLS, GPON, rotas ópticas ativas ou passivas, IPv4, IPv6, VLAN, VRF ou equivalente, BGP, BFD ou equivalente, túneis criptografados quando aplicáveis, QoS, monitoramento e exportação de dados.

8.8.2. A base disponibilizada para a proposta identificará, por localidade, equipamento e porta de entrega, meio físico, conector, velocidade, protocolo, VLANs ou interface de roteamento e responsabilidades por alimentação, cabeamento e configuração de cada lado. O projeto executivo confirmará a integração com a LAN municipal, sem dependência proprietária indevida. A executora configurará os componentes sob sua responsabilidade e orientará e acompanhará os ajustes municipais previstos na matriz de interfaces. Intervenção em ativos municipais exigirá atribuição expressa, autorização, acesso controlado e registro da mudança. A identificação de falha após a demarcação não dispensará o diagnóstico conjunto e o apoio técnico do item 16.3.2, nem transferirá automaticamente a administração dos ativos internos à executora.

8.8.3. O aceite incluirá capacidade por sentido, estabilidade, latência, perda, proteção, comutação, alarmes, acesso ao painel e registro no Service Desk.

8.8.4. A existência do C3 não implicará fornecimento automático de hotspot, salvo previsão expressa para o endereço.

8.9. RACKS ENERGIA E CONDIÇÕES AMBIENTAIS

8.9.1. Racks, gabinetes, caixas, PDUs, aterramento, proteção, ventilação, módulos, transceptores e acessórios necessários serão fornecidos como parte do serviço correspondente.

8.9.2. Os sites principal e de continuidade e os nodes críticos terão acomodação, monitoramento ambiental e proteção compatíveis com a criticidade e a redundância.

8.9.3. A alimentação e a autonomia serão dimensionadas pela carga real dos equipamentos e pelo tempo de transição ou restabelecimento definido para o projeto. A memória identificará cargas críticas, consumo, capacidade de UPS AC, UPS DC, nobreak ou solução equivalente, autonomia prevista, condições ambientais e dependências de alimentação. Serão identificadas as cadeias de energia dos componentes redundantes, incluindo pontos comuns capazes de causar falha simultânea. A autonomia exigida e as responsabilidades pela energia municipal e pelos recursos de proteção serão estabelecidas antes da proposta do projeto; o executivo demonstrará seu atendimento.

8.9.4. A autonomia e a condição das baterias serão comprovadas por teste controlado e monitoramento periódico, com registro da carga aplicada, estado inicial, duração, alarmes e continuidade dos equipamentos críticos. O teste de transição de energia verificará a preservação do serviço e das configurações, sem exposição desnecessária da operação a risco. Desvio em relação à autonomia exigida gerará registro de não conformidade, correção e novo teste; indicação nominal de capacidade da bateria não substituirá a comprovação sob carga.

8.9.5. A existência de gerador poderá ser considerada, sem afastar proteção, condicionamento e transição de energia.

8.9.6. As instalações observarão segurança do trabalho, condições ambientais e normas técnicas aplicáveis. A comprovação documental de segurança e saúde no trabalho observará o Anexo II 7.10.5 e 7.10.6, conforme os riscos, funções e marcos das atividades.

8.11. INTERVENÇÕES FÍSICAS E LIMITES PATRIMONIAIS

8.11.1. A Prefeitura não construirá rede de telecomunicações. As intervenções externas necessárias à entrega, como lançamento de cabos, utilização de dutos, ocupação de postes, travessias, caixas, fusões e adequações de entrada, serão providenciadas pela contratada ou por seus terceiros, sob sua responsabilidade técnica, regulatória, ambiental e financeira. Os direitos de uso e autorizações pertinentes serão comprovados no marco do Anexo II 7.12.

8.11.2. As intervenções acessórias não gerarão incorporação automática dos ativos ao patrimônio municipal.

8.11.3. A documentação exigida será limitada ao necessário para comprovar interfaces, diversidade, segurança, desempenho, manutenção e continuidade, preservadas informações sensíveis da infraestrutura de terceiros.

9. REQUISITOS TRANSVERSAIS E INTEGRAÇÕES

9.1. As interfaces devem permitir segregação, roteamento, monitoramento, logs e correlação de chamados. A capacidade será demonstrada fim a fim, por sentido de tráfego, em operação normal e no perfil próprio de contingência.

9.2. C1/C2 não conservam 10 Gbps na proteção GPON. C3/C4 exigem capacidade integral em cada caminho, diversidade física e de fornecedor. C5 exige monitoramento e restauração da rota única.

9.3. Para C3 e C4 serão mantidas duas rotas ópticas independentes, ativas ou passivas, fisicamente independentes e de fornecedores distintos, cada qual com a capacidade integral da classe: 1 Gbps simétrico para C3 e 500 Mbps simétricos para C4.

9.4. A suficiência técnica será demonstrada no serviço completo. Transporte, agregação, equipamentos, licenças, filas e segurança deverão sustentar os fluxos exigidos em operação normal e no perfil de contingência de cada classe. A demonstração de uma interface de alta velocidade não substitui a capacidade fim a fim.

9.5. O projeto executivo, o inventário, a matriz de interoperabilidade e os testes deverão identificar interfaces municipais, roteamento, segregação, monitoramento e continuidade. Compartilhamentos que afetem domínios de falha deverão ser identificados para tratamento técnico; a diferença entre prestadores não dispensa evidência de independência.

9.8. INTEROPERABILIDADE PAINÉIS E DOCUMENTAÇÃO

9.8.1. A solução deverá utilizar protocolos e interfaces abertos ou amplamente adotados, incluindo IPv4, IPv6, BGP, OSPF quando aplicável, VLAN, QoS, SNMPv3, Syslog, IPFIX, NTP, HTTPS, APIs REST ou equivalentes.

9.8.2. A executora fornecerá painéis executivos e operacionais ao município e à Central de Situação do InPACTA, com disponibilidade, capacidade, chamados, incidentes, segurança, hotspots, C6 quando ativado, implantação e indicadores de SLA. Os painéis identificarão node, classe, interface, rota, fornecedor, serviço afetado, severidade, última coleta, início do evento, responsável, providência e chamado correlato. Apresentarão séries históricas, degradação, perda de redundância, tendências e situação das ações preventivas. Perfis autorizados permitirão consulta e exportação dos dados. Falta de telemetria será sinalizada como ausência de informação e gerará verificação, sem representar disponibilidade comprovada.

9.8.3. O acesso do MUNICÍPIO DEMANDANTE será realizado por contas individualizadas, autenticação multifator quando aplicável, perfis predominantemente de consulta e trilha de auditoria.

9.8.4. Deverão ser entregues inventário de nodes, interfaces de demarcação, equipamentos terminais, parâmetros de interoperabilidade, evidências de teste, relatórios de disponibilidade, chamados, procedimentos de contingência, contatos e documentação de transição. A documentação incluirá topologia lógica de integração, parâmetros aprovados, registro das mudanças e plano de monitoramento com pontos de medição, métricas, intervalos de coleta, limiares,

severidades, contatos, periodicidade de comunicação e procedimentos de resposta. Esses parâmetros serão aprovados antes do aceite operacional, respeitando os mínimos e prazos contratuais.

9.8.5. Não será exigida entrega de engenharia interna completa da rede de terceiros, mapas detalhados de rotas, postes, caixas de emenda ou informações cuja divulgação seja desnecessária e possa comprometer segurança ou segredo empresarial, ressalvadas as evidências indispensáveis à fiscalização, diversidade, continuidade e aceite.

9.8.6. A segregação será implementada por VLANs, VRFs ou mecanismo equivalente. O plano definitivo de VLANs, gateways, fronteiras de camada 2 e camada 3, QoS e endereçamento será apresentado no projeto executivo e aprovado pelo MUNICÍPIO DEMANDANTE. O plano identificará, para cada gateway e domínio de segurança, localização, interfaces, função, responsável, endereço lógico de serviço, mecanismo de redundância, membros, dependências de energia e conexão e fluxos protegidos. Distinguirá equipamentos da executora e ativos municipais. O projeto não poderá reduzir a redundância obrigatória dos componentes críticos nem deixar indefinida a responsabilidade pela integração e pelos testes.

9.8.7. A arquitetura deverá evitar extensão indiscriminada de camada 2, preservar marcações DSCP, controlar broadcasts, impedir comunicação não autorizada entre domínios e permitir expansão sem renumeração integral.

9.8.8. O DHCP corporativo permanecerá sob administração municipal, salvo atribuição expressa no projeto. A solução suportará DHCP Relay, DHCPv4 e DHCPv6 e poderá operar DHCP nos domínios de Wi-Fi público e C6 quando incluído no escopo. Serão identificados responsáveis, escopos, servidores autorizados, interfaces de relay e controles contra servidores não autorizados. O piloto verificará atribuição e renovação de endereços, segregação dos escopos e interoperabilidade com os serviços municipais. O DNS será tratado por função, distinguindo DNS interno corporativo, recursivo, autoritativo e reverso dos blocos públicos, com responsáveis e dependências explicitados na matriz de interoperabilidade.

9.8.9. Quando o DNS autoritativo integrar o escopo, deverá possuir pelo menos duas instâncias em domínios de falha distintos, IPv4 e IPv6, DNSSEC, transferência segura de zonas, controle de acesso, logs, disponibilidade mensurável, exportação integral e transição sem dependência tecnológica.

9.8.10. O DNS reverso dos blocos públicos e as alterações relacionadas ao ASN e aos prefixos municipais deverão ser documentados e coordenados com a Administração.

9.8.11. A executora apresentará Matriz de Interoperabilidade e Responsabilidades por serviço e fluxo municipal, contendo origem, destino, interfaces de demarcação, protocolo, versão, portas, criptografia, dados trafegados, periodicidade, dependências e formato de exportação. A matriz identificará quem autoriza e executa a configuração de cada lado, presta apoio, monitora, corrige e valida. Relacionará endereçamento, VLANs/VRFs, roteamento, DHCP Relay, DNS, autenticação, regras de segurança, QoS e MTU quando aplicáveis, bem como pontos de teste, critérios de aceite, contingência e reversão. O escopo municipal será identificado antes da proposta; o projeto executivo detalhará sua implementação.

9.8.12. A interoperabilidade será testada em piloto conjunto com a equipe municipal antes da implantação em massa, abrangendo os fluxos previstos na matriz: VLANs, VRFs, roteamento, DHCP Relay, DNS, autenticação, captive portal, monitoramento, logs, APIs, chamados, painéis e exportação. Serão verificados, quando aplicáveis, acesso aos sistemas corporativos, atribuição de endereços, resolução de nomes, autenticação e fluxos de backup ou replicação, em operação normal e contingência. Cada teste registrará origem, destino, condições, resultado esperado, resultado obtido e evidências. Resposta a ping ou enlace ativo, isoladamente, não comprovará funcionamento do serviço. A equipe municipal validará os serviços internos; a executora corrigirá as falhas de sua solução e apoiará o diagnóstico das demais interfaces.

9.8.13. A Matriz de Interoperabilidade e Responsabilidades deverá identificar, para C1 e C2, a rota principal MPLS e a proteção GPON; para C3 e C4, as duas rotas ópticas independentes, com capacidade integral da classe e fornecedor distinto entre os caminhos; e, para C5, a rota única GPON. A matriz deverá incluir interfaces de demarcação, mecanismos de integração segura, roteamento, detecção de falhas, alarmes, telemetria, capacidade por sentido, critérios de contingência e metodologia de teste.

9.8.14. A interoperabilidade deverá preservar a possibilidade de integração com equipamentos e sistemas municipais por padrões abertos, sem exigir que a Administração adote protocolo proprietário para consultar o estado dos caminhos, receber alarmes, extrair indicadores ou validar o aceite.

9.8.15. A compatibilidade com a infraestrutura tecnológica municipal existente será exigida exclusivamente quanto às interfaces, sistemas, aplicações e serviços que devam permanecer operacionais durante ou após a transição. Essa compatibilidade deverá assegurar interoperabilidade e continuidade, sem transformar a arquitetura legada em padrão obrigatório para a solução contratada.

9.8.16. Características ou limitações do ambiente atual não constituirão teto de capacidade, requisito de replicação tecnológica, critério de rejeição da arquitetura de destino ou justificativa automática para redução de redundância, segurança, monitoramento, disponibilidade, escalabilidade ou demais requisitos desta especificação.

9.8.17. Incompatibilidades identificadas deverão constar da Matriz de Interoperabilidade e Responsabilidades com a dependência afetada, impacto, solução de integração ou transição, responsável, cronograma, teste de aceite e procedimento de reversão, priorizando adaptação, coexistência, migração ou substituição antes de qualquer proposta de alteração estrutural.

10. LICENCIAMENTO E DIREITOS DE USO

10.1. O direito de uso dos componentes e a legitimidade dos licenciamentos deverão ser demonstráveis. A prestação da rede externa não implica aquisição municipal da infraestrutura; o reaproveitamento de terminais municipais não transfere sua propriedade à executora.

10.2. A documentação e a portabilidade devem permitir fiscalização e transição. Não se presume cessão de propriedade intelectual, código-fonte ou engenharia interna de terceiros fora do escopo definido.

11. SEGURANÇA PROTEÇÃO DE DADOS E CONFORMIDADE

11.1. A segregação abrangerá redes administrativa e pública, voz, campo, gestão e ambientes computacionais. Contas individualizadas, perfis compatíveis, logs e acesso autorizado aos painéis permitirão fiscalização sem divulgação irrestrita de credenciais ou engenharia sensível.

11.2. A gravação e a análise de chamadas dependem de finalidade, autorização, retenção, acesso, exportação, descarte e informação aos envolvidos. Transcrição, sumarização, classificação e pesquisa semântica são assistivas. A indisponibilidade da camada analítica não impedirá o estabelecimento ou a manutenção de chamadas.

11.3. Versões de modelos, validação comparativa, avaliação representativa e controles contra manipulação do conteúdo transcrito integram a governança técnica. Não se fixa limiar numérico de confiança ou taxa mínima de acerto sem definição própria.

11.4. Os acessos institucionais aos painéis deverão utilizar contas individualizadas, perfis compatíveis e rastreabilidade. A demonstração de capacidade, diversidade e continuidade deverá preservar credenciais e informações sensíveis de engenharia, sem impedir a verificação do resultado. Gravação e processamento de chamadas dependem de finalidade, autorização e controles de acesso, retenção, exportação e descarte.

11.5. SEGURANÇA DE BORDA E PROTEÇÃO DDOS

11.5.1. Os acessos dedicados à Internet deverão possuir mitigação DDoS a montante, com detecção automática, capacidade de ativação sem intervenção manual do MUNICÍPIO DEMANDANTE, acompanhamento pelo NOC e SOC e preservação do tráfego legítimo.

11.5.2. A mitigação deverá contemplar ataques volumétricos, ataques de protocolo e esgotamento de estado, bem como ataques de aplicação quando

compatíveis com o serviço contratado.
11.5.3. Antes da homologação, deverão ser realizados ensaios controlados e autorizados, sem impacto a terceiros, para comprovar detecção, acionamento, continuidade, comunicação, roteamento e geração de relatório.
11.5.4. A falha no teste impedirá o aceite do componente e deverá ser corrigida e retestada sem custo adicional.
11.5.5. A segurança de borda operará em alta disponibilidade, com pelo menos dois membros ou instâncias em domínios de falha distintos, ou arquitetura equivalente que preserve o serviço após falha de um componente. O conjunto suportará o tráfego dimensionado com todas as funções exigidas habilitadas, inclusive no cenário de falha de um membro, conforme item 5.8.14. A topologia identificará dependências de energia, comutação, interfaces e conexões, eliminando pontos únicos de falha no conjunto crítico contratado. A redundância dos firewalls será articulada à dos gateways e dos caminhos de rede; enlaces redundantes isoladamente não comprovarão alta disponibilidade da segurança.
11.5.6. Serão admitidos appliances físicos, virtuais, serviço gerenciado ou arquitetura equivalente, em modo ativo/passivo, ativo/ativo ou equivalente, com isolamento, desempenho, licenciamento, suporte, rastreabilidade e responsabilidade única. A solução sincronizará configurações, políticas e estados das sessões necessários à continuidade, incluindo traduções NAT e associações de VPN quando aplicáveis. A proposta identificará os tipos de sessão preservados e os que exigem restabelecimento, demonstrando atendimento aos limites publicados para cada serviço. A perda do canal de sincronização será detectada e tratada por mecanismo que impeça atuação conflitante dos membros, divergência de políticas ou encaminhamento sem os controles de segurança exigidos.
11.5.7. A solução deverá incluir firewall de próxima geração, IPS, controle de aplicações, proteção contra malware, VPN, autenticação administrativa forte, alta disponibilidade, exportação de logs, APIs, SNMPv3 ou equivalente, IPFIX ou equivalente e integração com os sistemas de monitoramento. As políticas de filtragem, inspeção, segmentação e registro permanecerão efetivas durante a comutação. A falha de um membro não autorizará contorno automático do firewall ou liberação de tráfego vedado. O retorno do membro recuperado observará verificação de saúde, consistência das configurações e estados e estabilização, evitando alternância repetitiva e interrupções adicionais.
11.5.8. Inspeção criptográfica deverá ser aplicada por política, considerando privacidade, capacidade, riscos, exceções técnicas e legislação, não sendo presumida inspeção profunda universal de todo o transporte metropolitano.
11.5.9. Licenças, assinaturas e atualizações de segurança deverão permanecer válidas durante toda a vigência.

11.8. SIGILO E TRATAMENTO DE DADOS

11.8.1. A EXECUTORA tratará dados pessoais somente para finalidades necessárias à execução, segundo instruções documentadas do MUNICÍPIO DEMANDANTE, base legal aplicável e princípios de finalidade, adequação, necessidade, segurança e prevenção.
11.8.2. A solução deverá adotar minimização de dados nos hotspots, evitar coleta desnecessária de conteúdo de navegação e manter registros pelo prazo legal ou contratual aplicável.
11.8.3. Suboperadores, ambientes de nuvem e prestadores que tratem dados deverão ser identificados e submetidos às mesmas obrigações de segurança, sigilo, localização, retenção e resposta a incidentes.
11.8.4. A executora comunicará imediatamente o incidente de segurança aos contatos designados do município e do InPACTA, segundo os papéis e o fluxo formalizados, sem aguardar conclusão da investigação para transmitir as informações disponíveis. O registro inicial identificará momento de detecção, serviços e dados potencialmente afetados, medidas de contenção e interlocutor responsável; informações adicionais serão fornecidas à medida que confirmadas, distinguindo fatos, hipóteses e aspectos ainda sob apuração. Serão preservados registros e evidências com controle de acesso e integridade, observadas as instruções legítimas e a continuidade dos serviços. A comunicação à ANPD e aos titulares, quando exigível, caberá ao agente legalmente responsável, nos prazos e condições regulamentares. O fluxo interno permitirá o cumprimento dessas obrigações e não atribuirá à executora decisão unilateral sobre comunicação legal de responsabilidade de outro agente.
11.8.5. Credenciais, chaves, logs, configurações e dados operacionais deverão ser protegidos por controles de acesso, autenticação forte, criptografia e trilha de auditoria.
11.8.6. As obrigações de confidencialidade permanecerão após o término do contrato.
11.8.7. Os CDR, gravações autorizadas, mensagens, contatos, identificadores, credenciais e relatórios de telefonia deverão observar controle de acesso, finalidade, retenção, integridade, confidencialidade, exportação e descarte seguro.
11.8.8. O acesso da fiscalização aos registros ocorrerá na extensão necessária à medição, auditoria, segurança e apuração de incidentes, com rastreabilidade e observância das atribuições institucionais.

12. REGISTROS RETENÇÃO E CONTINUIDADE

12.1. CDR, logs, inventários e registros operacionais deverão permitir rastreabilidade e conciliação no alcance definido para cada serviço. Finalidade, acesso, retenção, exportação e descarte deverão ser compatíveis com a operação e a autorização correspondentes.
12.2. Os períodos de guarda e os papéis de tratamento exigem definição própria e conferência do fundamento aplicável. Continuidade da voz permanece independente do processamento analítico.

13. INTEGRAÇÃO ESCALABILIDADE E GOVERNANÇA

13.2. A governança de cada projeto identificará quem solicita, autoriza, executa, verifica e aceita, com recursos e acessos compatíveis. A carteira verificará capacidade residual antes de novos compromissos. O acompanhamento de um cliente não permitirá acesso indevido aos dados de outro.
13.3. A inclusão de nova demanda requer demonstrar capacidade residual de transporte, segurança, licenças, monitoramento, equipes e suporte. A capacidade já comprometida não poderá ser novamente contada como livre.

14. IMPLANTAÇÃO CONFIGURAÇÃO E ACEITE

14.2. A instalação física ou declaração de atendimento não substitui testes de capacidade, segregação, proteção, interoperabilidade e suporte. O registro deve individualizar local, classe, componente, condições e resultado. Janelas e reversão deverão preceder mudanças críticas.
14.3. A evidência de aceite deverá individualizar a entrega por local, classe e componente. A condição de serviço ativado dependerá de solicitação, implantação, monitoramento, teste e aceite no alcance formalizado. A instalação de equipamento e a mera declaração de atendimento não substituem a verificação aplicável.

14.6. INVENTÁRIOS E PROVIDÊNCIAS DE PREPARAÇÃO

14.6.1. Consolidar a relação individualizada dos nodes do projeto, com endereço, unidade, classe, capacidade, finalidade, prioridade e situação atual. O cadastro sustentará o dimensionamento, as ondas de implantação, os testes, o aceite e a fiscalização.
14.6.2. Validar a vigência, a disponibilidade orçamentária, a previsão no planejamento anual e a fonte dos recursos.

14.6.3. Realizar a consulta técnica e comercial com a mesma planilha e registrar empresas convidadas, respostas e ausências de resposta.
14.6.4. Consolidar referências públicas comparáveis e a memória de cálculo do valor estimado.
14.6.5. Definir indicadores e níveis de serviço após análise das práticas de mercado e da criticidade de cada classe.
14.6.6. Organizar acessos aos locais, janelas, responsáveis, inventário, endereçamento, VLANs e interfaces de entrega.
14.6.7. Definir a integração de chamados, os perfis dos painéis da unidade gestora do projeto e a rotina de validação da medição.
14.6.8. Designar gestor e fiscais com competências técnica, administrativa e setorial.
14.6.9. Planejar a capacitação das equipes da unidade gestora do projeto, administradores de rede, gestores e fiscais, limitada à fiscalização, aos painéis, aos chamados, aos indicadores, aos incidentes e à contingência.
14.6.10. Consolidar o inventário de telefonia com usuários, ramais, números públicos, faixas DDR, DIDs, serviços 0800, números de utilidade pública, filas, URAs, regras, gravações, aparelhos, gateways, integrações, contratos, custos e responsáveis.
14.6.11. Extrair e analisar os registros de chamadas e as faturas dos últimos 12 meses, distinguindo chamadas internas e externas, fixas, móveis, locais, nacionais, internacionais, 0800, horários de pico, simultaneidade e sazonalidade.
14.6.12. Validar a relação entre numeração pública, reserva de números e ramais efetivamente ativos, evitando equivalência indevida entre esses elementos.
14.6.13. Classificar os terminais existentes quanto à compatibilidade, possibilidade de atualização, segurança, obsolescência e aptidão para interconexão lógica, registrando o resultado no inventário.
14.6.14. Definir a política de gravação, retenção, acesso, descarte e auditoria de chamadas, mensagens e relatórios, com participação das áreas de segurança, proteção de dados, jurídica e de negócio.
14.6.15. Validar o plano de portabilidade, as janelas, os números críticos, os serviços de emergência, os canais alternativos, o piloto, a coexistência, o retorno e a comunicação aos usuários.
14.6.16. Realizar pesquisa formal de preços com cenários comparáveis de ramais, canais, tráfego, terminais, implantação, suporte e serviços especiais, incluindo análise do custo total e da economicidade em relação ao ambiente atual.
14.6.17. Atualizar o Termo de Referência, o Instrumento de Medição de Resultado, a planilha de preços, os critérios de habilitação, os testes, o plano de migração e a matriz de riscos em compatibilidade com os requisitos de telefonia do projeto.
14.6.18. Levantar o histórico de chamados, manutenções, remanejamentos, configurações, falhas de terminais, reincidências, acionamentos de prestadoras e intervenções de cabeamento, preferencialmente dos últimos 12 meses, para dimensionar equipe, criticidade e custo.
14.6.19. Consolidar a matriz de criticidade da telefonia, identificando unidades 24x7, números de emergência, atendimento ao cidadão, saúde, segurança, filas e posições cuja indisponibilidade exija equipamento temporário ou atendimento local prioritário.
14.6.20. Definir a Matriz de Responsabilidades da Telefonia, delimitando plataforma, operadora, Infovia, rede local, alimentação elétrica, aparelhos municipais, periféricos, cabeamento interno, obras e suporte ao usuário.
14.6.21. Validar, após o inventário, a necessidade e o quantitativo do banco temporário de equipamentos para posições críticas, sem assumir aquisição ou reposição irrestrita de aparelhos legados.
14.6.22. Separar na especificação do projeto as configurações lógicas rotineiras, incluídas na mensalidade, das mudanças em massa, novas integrações, novos pontos e remanejamentos físicos, sujeitos a Ordem de Serviço e preço unitário quando integrarem o objeto.
14.6.23. Organizar a composição de custos de cada projeto por comutação e agregação, acessos, capacidade simultânea, ativação de unidades, gravação autorizada, treinamento e intervenções físicas. Distinguir componentes incluídos no serviço de parcelas adicionais autorizáveis, evitando duplicidade de remuneração.
14.6.24. Recalibrar anualmente as curvas da Infovia e da telefonia, utilizando inventário, séries históricas, capacidade disponível, percentil 95, CDR, hora de maior movimento, ocupação, sazonalidade, Ordens de Serviço e novos projetos, sem converter hipóteses de planejamento em consumo mínimo ou faturamento automático.

14.7. CONTEÚDO DO PROJETO E SEQUÊNCIA DE IMPLANTAÇÃO

14.7.1. O plano deverá conter mobilização, inventário, vistorias, arquitetura, responsáveis, dependências, janelas, cópias de segurança, implantação dos serviços centrais, links, piloto, ondas, testes, critérios de sucesso, critérios de interrupção, reversão, aceite, estabilização e operação assistida. O cronograma distinguirá levantamento, elaboração, análise, correção e aprovação do projeto executivo, implantação, testes e aceite, com responsáveis e prazos definidos no instrumento do projeto. A execução por etapas exigirá aprovação prévia do detalhamento da parcela e verificação de suas dependências. A aprovação do projeto executivo não se confundirá com o aceite dos serviços implantados. Para telefonia sob demanda, será respeitado o prazo específico do item 25.21.1.
14.7.2. O cronograma será acompanhado nos painéis da unidade gestora do projeto, com informações de previsto, realizado, desvios, bloqueios, riscos e ações corretivas.
14.7.3. Alterações relevantes de prazo, sequência ou prioridade dependerão de comunicação e aprovação municipal. O cronograma priorizará os serviços centrais, os nodes C1, os nodes C2, as unidades essenciais, os demais nodes e a prontidão do C6.
14.7.4. Para a seleção da parceira, a metodologia e os compromissos de prazo serão apresentados no cronograma de referência previsto no Anexo II, itens 11.1.1 a 11.1.7. Na execução, cada projeto terá cronograma próprio, com marcos autorizados, prazos máximos compatíveis com a proposta aceita, capacidade simultânea, dependências e evidências. O dimensionamento posterior não dispensará a obrigação de agilidade assumida nem permitirá ampliar unilateralmente os prazos específicos já estabelecidos. O controle de entregas e a recuperação de atrasos observarão o mesmo protocolo, preservado o aceite técnico de cada parcela.

15. SUPORTE MANUTENÇÃO E NÍVEIS DE SERVIÇO

15.3. As metas específicas do cenário municipal deverão permanecer vinculadas ao texto técnico consolidado. Não se converte a menção a operação contínua em funcionamento contínuo do InPACTA ou em NOC obrigatório em cada nova cidade.
15.4. A executora manterá NOC, SOC, suporte especializado N2/N3, equipes de campo e os recursos tecnológicos de atendimento previstos no projeto, integrados ao N1 e à Central de Situação do InPACTA. A localização, a cobertura e a presença física serão justificadas por criticidade e território. Cada parte mobilizará sua estrutura para a execução, sem imposição de instalação prévia para participação.
15.5. O InPACTA será responsável pelo N1 e pela Central de Situação, nos termos dos itens 2.2 e 2.3. A executora manterá N2/N3 e a responsabilidade pela solução técnica. O escalonamento preservará protocolo, severidade, impacto, horários, ações e evidências, sem reiniciar ou suspender os prazos de atendimento e restabelecimento. Incidentes detectados pelo NOC/SOC serão registrados e tratados diretamente pela executora, com comunicação ao InPACTA, sem aguardar abertura pelo N1.

Classe	Disponibilidade mensal e limite de indisponibilidade (30 dias)	Escopo

C1	99,95%; até 21 min 36 s acumulados no mês de 30 dias	Rota principal MPLS de 10 Gbps, proteção GPON com capacidade útil garantida conforme o item 5.8.12 e continuidade dos serviços prioritários.
C2	99,90%; até 43 min 12 s acumulados no mês de 30 dias	Rota principal MPLS de 10 Gbps, proteção GPON com capacidade útil garantida conforme o item 5.8.12 e contingência prioritária.
C3	99,50%; até 3 h 36 min acumulados no mês de 30 dias	Duas rotas ópticas independentes de 1 Gbps simétrico cada, com fornecedor distinto entre as rotas, comutação automática e continuidade dos níveis de serviço.
C4	98,50%; até 10 h 48 min acumulados no mês de 30 dias	Duas rotas ópticas independentes de 500 Mbps simétricos cada, com fornecedor distinto entre as rotas, comutação automática e continuidade dos hotspots públicos.
C5	98,00%; até 14 h 24 min acumulados no mês de 30 dias	Rota única GPON de 50 Mbps simétricos para campo, câmeras, sensores e IoT, com monitoramento e restauração sob SLA.

15.6. NOC SOC SUPORTE PRESENCIAL E SERVICE DESK

15.6.1. A executora implantará e manterá a estrutura de NOC definida no projeto e no plano de mobilização, como obrigação de execução. Sua localização e cobertura dependerão da necessidade operacional demonstrada.

15.6.2. O NOC coordenará monitoramento, chamados, N2/N3, equipes de campo, manutenção, mudanças, incidentes, capacidade e interface com a fiscalização. A detecção de falha ou degradação acionável gerará alerta e chamado automático ou registro imediato pelo NOC, com horário da primeira evidência, impacto, severidade e responsável. A executora iniciará o tratamento sem aguardar reclamação do usuário ou encaminhamento pelo N1, notificando o InPACTA e os interlocutores municipais conforme criticidade. Correlação e agrupamento de alarmes preservarão os eventos originais. Os registros de detecção, abertura, reconhecimento, acionamento e restauração permitirão verificar os prazos contratuais, sem reinício por escalonamento.

15.6.3. O NOC operará 24 horas por dia, 7 dias por semana, monitorando os nodes, links, hotspots e serviços centrais contratados, inclusive caminhos de proteção ou redundância. Conforme o componente, coletará estado das interfaces, sessões de roteamento e túneis, capacidade e utilização por sentido, latência, perda, jitter, erros, descartes, filas, sinais ópticos e saúde dos equipamentos. O plano de monitoramento definirá intervalos, persistência dos limiares, severidades, correlação, recuperação e janelas autorizadas, compatíveis com os níveis de serviço. Serão combinadas telemetria, eventos e sondas autorizadas por serviço. Falha do coletor, perda de comunicação ou interrupção da coleta também gerará alerta e verificação. Para firewalls e gateways redundantes, o monitoramento identificará papel e saúde de cada membro, estado da sincronização, divergências de configuração, perda de redundância, comutações, falha de interface e capacidade residual. A perda de proteção gerará alerta e chamado mesmo quando o tráfego permanecer disponível, com acompanhamento pela Central de Situação.

15.6.4. A EXECUTORA deverá disponibilizar SOC 24x7, admitida estrutura remota especializada, integrado ao NOC e responsável pelo monitoramento de eventos de segurança, gestão de vulnerabilidades, correlação, resposta a incidentes, relatórios e medidas corretivas e preventivas.

15.6.5. O SOC deverá abranger os domínios de Internet, borda, hotspots, logs e componentes de segurança sob responsabilidade da EXECUTORA.

15.6.6. O InPACTA disponibilizará e coordenará sua equipe de N1. O plano de mobilização definirá dimensionamento, horários, canais, local de atuação e atendimento presencial quando previsto, considerando os projetos simultâneos. A executora indicará interlocutores N2/N3 e disponibilizará as integrações necessárias ao atendimento. A ausência de atendimento N1 em determinada janela não impedirá o acionamento direto do NOC/SOC ou do suporte especializado para incidentes críticos, nos regimes e prazos exigidos.

15.6.7. Cada parte manterá a gestão de seus profissionais. O município definirá prioridades e resultados pelos canais pactuados, sem dirigir jornada, férias, substituições ou disciplina das equipes. O atendimento presencial de engenharia, manutenção, reparo e substituição de componentes sob responsabilidade da executora será realizado por suas equipes técnicas e não se confundirá com o N1 do InPACTA.

15.6.8. A executora disponibilizará sistema de chamados ou integração com o sistema do InPACTA, com portal, telefone, correio eletrônico, API ou mecanismo equivalente, trilha de auditoria, criticidade, registro de tempos, anexos, comunicação e relatórios. O N1 do InPACTA e o N2/N3 da executora atuarão com perfis próprios e histórico compartilhado, preservando identificador único ou correlação inequívoca entre protocolos, segregação de dados e rastreabilidade de cada intervenção.

15.6.9. Durante a implantação da integração, serão admitidos mecanismos transitórios de exportação, notificações e conciliação, desde que preservada a rastreabilidade.

15.8. DISPONIBILIDADE INDICADORES E TRATAMENTO DE OCORRÊNCIAS

15.8.1. A disponibilidade será apurada mensalmente, individualmente por node, em regime de operação contínua de 24 horas por dia, durante todos os dias do mês, pela fórmula DM = ((TM - IA) / TM) x 100, em que DM é a disponibilidade mensal, TM é o total de minutos do período efetivo de medição e IA é a soma dos períodos de indisponibilidade atribuíveis à EXECUTORA, observadas as regras de contabilização e exclusão deste instrumento. Os limites da tabela correspondem a um mês de referência de 30 dias (43.200 minutos). Nos meses de duração diferente e nos períodos parciais de medição, o limite será calculado proporcionalmente ao tempo efetivo do período, pela fórmula IA máxima = TM x (1 - DM mínima / 100), preservado o percentual mínimo da classe. O limite é acumulado no período mensal e não se renova a cada incidente. A apuração observará as condições de contingência e perda de resiliência dos itens 15.8.4 a 15.8.9.

15.8.2. Manutenções programadas somente serão excluídas quando autorizadas, comunicadas no prazo, realizadas na janela aprovada e sem extrapolar os limites contratuais.

15.8.3. Não serão excluídos eventos causados por falha de subcontratada, operadora, infraestrutura de terceiros, dimensionamento inadequado, licença expirada, falta de capacidade, falha de monitoramento ou ausência de manutenção sob responsabilidade da EXECUTORA.

15.8.4. A utilização da rota secundária não constituirá, por si só, indisponibilidade. Nos C1 e C2, o período poderá ser registrado como operação degradada quando forem preservados os serviços essenciais, os pisos de capacidade aplicáveis, a conectividade, a segurança, o roteamento e o monitoramento. Nos C3 e C4, a operação pela rota secundária permanecerá em condição normal de disponibilidade quando forem mantidos 100% da capacidade mínima da classe e os demais níveis de serviço.

15.8.5. Eventos de contingência deverão possuir início, término, causa, estado das rotas, capacidades observadas, latência, perda, jitter quando aplicável, alarmes, chamados, serviços afetados e ações de restauração registrados no sistema de monitoramento e no relatório mensal. Nos C3 e C4 deverá ser registrada também a rota e o fornecedor em operação.

15.8.6. Nos C1 e C2, a operação pela proteção será convertida em indisponibilidade quando não atender ao perfil mínimo definido, interromper serviço essencial, perder segurança ou roteamento, deixar de ser monitorada ou ultrapassar o limite temporal do IMR. Nos C3 e C4, haverá degradação ou

indisponibilidade quando qualquer rota ativa não mantiver a capacidade integral da classe ou os demais parâmetros de desempenho e segurança definidos no IMR.
15.8.7. As glosas possuem natureza de ajuste da medição e não afastam multa administrativa quando houver atraso, reincidência, omissão, fraude, incidente grave ou descumprimento de obrigação autônoma.
15.8.8. A reincidência será caracterizada pelo descumprimento da mesma classe em dois meses consecutivos ou três meses alternados em seis meses, quando imputável à EXECUTORA, sem prejuízo de critério mais rigoroso definido no contrato para falhas críticas.
15.8.9. A falha ou indisponibilidade da rota secundária, ainda que a rota primária permaneça operacional, será registrada como perda de resiliência, gerará chamado e exigirá correção prioritária. As glosas específicas de perda de resiliência, restauração tardia e perda de capacidade serão detalhadas no IMR, observadas as diferenças entre a proteção GPON dos C1/C2 e a redundância de capacidade integral dos C3/C4, sem duplicidade de glosa pelo mesmo fato e período.
15.8.10. O IMR da telefonia deverá considerar disponibilidade do núcleo e dos troncos, qualidade de voz, tempos de resposta e solução, sucesso de portabilidade, exatidão do faturamento, segurança e cumprimento dos prazos de ativação.
15.8.11. O descumprimento produzirá glosa proporcional sobre o componente afetado, sem prejuízo da correção, do reteste, das sanções e da apuração de responsabilidade quando houver reincidência ou impacto relevante.
15.8.12. A indisponibilidade da plataforma de telefonia, do licenciamento necessário à operação, do serviço SIP, do FQDN, dos certificados, de controlador de borda crítico, do armazenamento obrigatório ou do mecanismo de alta disponibilidade será atribuída ao componente afetado e refletida na medição.
15.8.13. Falha de renovação, downgrade, expiração de licença ou perda de acesso ao portal que impeça operação, administração, atualização ou suporte constituirá indisponibilidade imputável à EXECUTORA.
15.8.14. A ocupação de 90% ou mais da capacidade simultânea sem plano preventivo aprovado será considerada não conformidade de capacidade, ainda que não ocorra bloqueio de chamada.
15.8.15. Serão medidos tempo de estabelecimento, taxa de atendimento, taxa de completamento, chamadas rejeitadas por capacidade, abandono de filas, falhas por código SIP, eventos de failover e tempo de restauração.
15.8.16. A perda de CDR, inconsistência de relatório, falha de backup, impossibilidade de restauração ou ausência de trilha de auditoria sujeitará a parcela afetada a glosa específica, sem duplicidade pelo mesmo fato.
15.8.17. A indisponibilidade simultânea dos dois caminhos SIP, falha generalizada de registro ou interrupção de números essenciais será classificada como incidente crítico de prioridade máxima.
15.8.18. O IMR detalhará faixas de glosa para indisponibilidade, qualidade de voz, falha de portabilidade, atraso de ativação, inconsistência de faturamento, segurança, backup, failover e relatórios.
15.8.19. A glosa não substituirá a obrigação de correção, reteste, recomposição de dados, ressarcimento ou aplicação de sanção quando cabível.

16. CAPACITAÇÃO E DOCUMENTAÇÃO OPERACIONAL

16.1. A documentação necessária à operação e à transição abrangerá inventários, configurações, interfaces, registros de atendimento, evidências e procedimentos de continuidade. Deverá permitir fiscalização e acesso no perímetro autorizado.
16.2. A executora capacitará a equipe de N1 e os responsáveis pela Central de Situação do InPACTA antes do início da operação, abrangendo uso dos painéis e chamados, triagem, orientações padronizadas, classificação de severidade, critérios de escalonamento, segurança de acesso e leitura dos indicadores. Fornecerá manuais, procedimentos operacionais e contatos de escalonamento atualizados. A capacitação preservará as responsabilidades da executora por N2/N3, implantação, manutenção e operação técnica.

16.3. CAPACITAÇÃO E TRANSFERÊNCIA DE CONHECIMENTO

16.3.1. O InPACTA indicará os profissionais de N1 e da Central de Situação que receberão a capacitação. A executora realizará exercícios de abertura, triagem, escalonamento e acompanhamento de chamados, com validação dos perfis de acesso, dos registros de tempo e da comunicação entre as equipes. As alterações relevantes na solução serão acompanhadas da atualização da documentação e da orientação às equipes afetadas.
16.3.2. A executora prestará apoio especializado às equipes municipais na implantação, migração, operação, incidentes e mudanças das interfaces entre a Infovia e os ambientes internos incluídos no projeto. O apoio abrangerá diagnóstico conjunto, validação de configurações, interpretação de alarmes, testes por serviço, análise de capacidade e acompanhamento dos ajustes autorizados. Antes de atribuir a ocorrência à LAN, ao servidor ou à aplicação municipal, apresentará evidências da localização e da causa identificada ou da hipótese técnica, com testes realizados, impacto e orientação de correção. Persistindo dúvida sobre a origem, manterá a investigação conjunta e o acompanhamento das interfaces de seu escopo. O chamado não será encerrado apenas pela indicação genérica de falha interna; registrará encaminhamento, responsável, providências e validação do restabelecimento ou tratamento formal da pendência.
16.3.3. A Prefeitura manterá a administração cotidiana de sua LAN, servidores, estações, aplicações, diretórios e impressoras, salvo atividade expressamente atribuída à executora. Essa delimitação não excluirá o apoio especializado à integração previsto no item 16.3.2. Configurações nos ativos municipais serão realizadas pela equipe municipal ou pela executora quando expressamente autorizada e responsável pela atividade, com cópia de segurança pertinente, janela, procedimento de reversão e registro. Novos serviços, adequações ou expansão fora do escopo dependerão do controle de alterações; o apoio às interfaces já contratadas integrará as obrigações de execução.
16.3.4. A solução incluirá capacitação inicial para equipes da unidade gestora do projeto, administradores de rede, gestores e fiscais, abrangendo painéis, chamados, indicadores, incidentes, medição e contingência, sem transferência da operação da contratada para o Município.

17. QUALIFICAÇÃO EQUIPE E CAPACIDADE OPERACIONAL

17.1. A comprovação de experiência abrange instalação de nós de rede sobre fibra óptica com terminação ONT ou ONU e de pontos de acesso Wi-Fi. O levantamento distinguirá três categorias: nós de rede com ONT/ONU, Wi-Fi fixo e Wi-Fi móvel, sem presumir que as três integrem toda demanda. Na habilitação institucional, serão apresentados atestados de execução satisfatória emitidos por pessoas jurídicas de direito público ou privado em nome da participante, com os documentos de comprovação do Anexo II, itens 7.3 a 7.10. Na habilitação institucional, a experiência será aferida pelos critérios objetivos do Anexo II, itens 7.1.1 a 7.1.4, sem aplicar percentual sobre demanda presumida ou sobre o acervo de uma empresa. Para cada projeto dimensionado, o mínimo técnico-operacional será de 30% da quantidade de cada categoria relevante efetivamente incluída e justificada, conforme Anexo II, item 7.8, antes da formalização executiva. Admite-se somatório de atestados compatíveis, sem duplicação e sem identidade obrigatória de município, cliente, marca ou modelo. Os demais serviços sob demanda não exigem acervo específico nesta habilitação; seus requisitos técnicos e comprovações de execução permanecem exigíveis.
17.2. A comprovação técnico-operacional e a qualificação econômico-financeira serão apresentadas no ato e prazo definidos no edital, com análises e conclusões independentes. Sua aprovação expressa antecederá a convocação à prova de conceito, quando prevista. A ausência de critério institucional previamente publicado impede a conclusão da habilitação; a inexistência de dimensionamento dos futuros municípios não constitui, por si, impedimento à

seleção institucional. Antes da formalização de cada execução municipal, será verificada a capacidade disponível para atender ao escopo efetivo, considerando compromissos simultâneos, equipe, infraestrutura, licenças e dependências. Essa verificação não altera retroativamente o resultado da qualificação institucional nem dispensa os requisitos técnicos do projeto. A simples entrega de documentos não comprova aprovação. Análise pendente ou efeito suspensivo impeditivo bloqueará a convocação. A qualificação econômico-financeira não constitui proposta econômica nem critério de pontuação.

17.3. ART ou TRT da atividade futura será apresentado antes do início da intervenção sujeita a responsabilidade profissional. Acervo profissional, experiência empresarial e registro da execução futura são objetos diferentes. A diligência esclarece prova admissível, sem criar retroativamente capacidade essencial ausente.

17.3.1. Para instrução da habilitação, aplicar os tipos documentais e a demonstração das competências da equipe previstos no Anexo II, itens 7.9 e 7.10. A tipificação das três categorias é de contagem e comprovação; não acrescenta Wi-Fi veicular ao escopo de C1 a C6, nem equipara terminal óptico isolado ao conjunto de requisitos de um node municipal. O mínimo de 30% aplica-se exclusivamente às categorias relevantes presentes e dimensionadas na demanda, antes da formalização executiva, conforme Anexo II 7.8.

18. DOCUMENTAÇÃO TÉCNICA E COMPROVAÇÕES

18.1. A documentação técnica relacionará cada requisito à arquitetura, ao componente, à versão, à licença, à evidência e à etapa de comprovação. A matriz de rastreabilidade identificará os itens desta especificação e os respectivos registros de avaliação. As declarações da interessada e as conclusões da análise terão registros separados.

18.2. MATRIZ DE CONFORMIDADE E COMPROVAÇÕES

18.2.1. A proponente apresentará matriz contendo requisito, atendimento, forma de atendimento, componente, documentação comprobatória, parcela executada diretamente e eventual subcontratação.

18.2.2. Respostas genéricas como “atende” não substituirão a identificação objetiva da evidência quando o requisito exigir comprovação documental ou teste.

18.2.3. A matriz deverá abranger integralmente este Termo de Referência e os documentos integrantes do processo, sem alterar a ordem ou a numeração dos requisitos.

18.2.4. Divergência entre proposta, matriz, documentação e demonstração será submetida a diligência nos limites legais, sem permitir modificação material da solução ofertada.

18.2.5. A aceitação de equivalência dependerá de comprovação técnica objetiva e não reduzirá a responsabilidade integral da EXECUTORA.

18.2.6. A matriz aprovada integrará o contrato e servirá de referência para o projeto executivo, os testes e a fiscalização.

19. PROVA DE CONCEITO E VALIDAÇÃO TÉCNICA

19.1. Na seleção institucional, a comprovação de todas as funcionalidades e capacidades será documental, inclusive rede, segurança, Wi-Fi, portal, telefonia, integrações, operação, resiliência, sensores e diferenciais. Testes operacionais com equipamentos constituem medida excepcional, restrita à necessidade indispensável demonstrada no processo, após análise dos documentos e diligência, conforme os itens 13.38.1 a 13.38.4 do Anexo II. A descrição de um ensaio não determina sua execução automática na seleção. Permanecem os testes exigíveis na implantação, no aceite e na operação de cada parcela. A convocação excepcional observará a aprovação prévia das habilitações do item 17.2 e as condições do Edital 25.1. Requisitos, métodos, critérios e efeitos estarão definidos previamente, com decisão individual e isonomia.

19.1.1. Quando indispensável e autorizada conforme item 19.1, a demonstração será temporária, em ambiente de laboratório, com acesso da equipe avaliadora e sem entrega definitiva, aquisição antecipada ou transferência dos equipamentos à Administração. Serão admitidos recursos próprios, compartilhados ou locados e licenças de avaliação legítimas, desde que reproduzam as funções e a capacidade exigidas para cada ensaio e amostra expressamente definidos no roteiro publicado. A demonstração funcional em escala reduzida não comprovará a capacidade fim a fim da rede municipal, a diversidade física dos enlaces ou a cobertura real, que serão verificadas na implantação e no aceite. Os ensaios específicos de capacidade dos APs manterão seus mínimos, cargas e critérios publicados, sem redução decorrente da escala do laboratório. Na seleção de parceiro, somente será convocada a participante que cumprir a fase antecedente prevista no instrumento de seleção. O roteiro publicado identificará quem será convocado, os ensaios obrigatórios, seus efeitos, prazos e regras uniformes de repetição. A demonstração de seleção, quando prevista, não substituirá o aceite de implantação e operação.

19.2. Antes de impor a demonstração, será necessário definir finalidade, requisitos e subitens, ambiente, cenários, insumos, evidências, critérios, segurança, fase, tratamento de interrupções e inconclusões, manifestações e consequências. Teste de seleção não equivale a teste de implantação ou aceite do serviço, nem confirma item não testado.

20. TRANSIÇÃO E PORTABILIDADE

20.1. A saída deverá preservar continuidade, numeração institucional, exportação de registros e configurações, documentação e cooperação necessária com a sucessora. O plano de transição delimitará interfaces, responsabilidades, acesso e evidências.

20.2. Portabilidade e direito de uso não implicam cessão de infraestrutura, propriedade intelectual ou código-fonte não compreendidos no objeto. A desativação da origem dependerá das condições de continuidade previstas.

20.3. TRANSIÇÃO DE SAÍDA E ENTREGA DE INFORMAÇÕES

20.3.1. A garantia contratual será definida no edital, em percentual proporcional aos riscos, ao valor e à duração do contrato, observados os limites legais.

20.3.2. A EXECUTORA deverá elaborar Plano de Transição de Saída com antecedência mínima de 180 dias do término, quando não houver prorrogação, ou em prazo menor determinado pela Administração em caso de extinção antecipada.

20.3.3. O plano deverá contemplar inventário, dados, configurações, contatos, chamados, relatórios, blocos, roteamento, credenciais institucionais, procedimentos, cooperação com sucessora e manutenção da continuidade.

20.3.4. Não haverá transferência de rede física externa da EXECUTORA, mas deverão ser entregues todas as informações e dados operacionais pertencentes ou necessários à Administração.

20.3.5. A transição de saída da telefonia deverá preservar a numeração e incluir cooperação com a sucessora, exportação de dados e configurações, entrega de CDR e documentação, migração controlada e continuidade dos serviços críticos.

21. CRITÉRIOS GERAIS DE ACEITE

21.1. O aceite da execução dependerá da correspondência entre solicitação, implantação, integração, monitoramento, teste e entrega no alcance formalizado. Parcela sob demanda não será considerada ativada apenas porque existe limite contratual ou previsão de crescimento.

21.2. A demonstração excepcional de laboratório na seleção, autorizada conforme item 19.1, não certificará implantação nem atendimento de requisitos não testados. O instrumento aplicável distinguirá evidências da proposta, ensaios de seleção e obrigações de implantação e operação, com critérios e consequências definidos antes das propostas. A demonstração utilizará recursos temporários, conforme item 19.1.1. Requisito reservado à execução não será declarado atendido ou descumprido apenas pela ausência da infraestrutura municipal ainda não implantada.

GRUPO	CRITÉRIOS MÍNIMOS DE ACEITE
C1	Rota principal MPLS de 10 Gbps simétricos, proteção GPON com taxas nominais de linha de 2,48832 Gbps down e 1,24416 Gbps up, aferição da capacidade útil garantida conforme o item 5.8.12, diversidade, comutação automática, operação degradada controlada, monitoramento e documentação.
C2	Rota principal MPLS de 10 Gbps simétricos, proteção GPON com taxas nominais de linha de 2,48832 Gbps down e 1,24416 Gbps up, aferição da capacidade útil garantida conforme o item 5.8.12, diversidade, comutação automática, estabilidade, monitoramento e documentação.
C3	Duas rotas ópticas, ativa ou passiva, cada uma com 1 Gbps simétrico, fisicamente distintas e com fornecedor distinto entre as rotas, comutação, estabilidade, interface, monitoramento e suporte.
C4	Duas rotas ópticas, ativa ou passiva, cada uma com 500 Mbps simétricos, fisicamente distintas e com fornecedor distinto entre as rotas, comutação, backhaul, cobertura, autenticação, segregação, segurança, gestão e relatórios.
C5	Rota única GPON de 50 Mbps simétricos, túnel criptografado, roteamento e detecção de falhas, capacidade de subida, estabilidade em campo, interface, monitoramento, suporte, disponibilidade e restauração sob SLA.
Acessos institucionais	6 Gbps, IPv4 /25, IPv6, diversidade, DDoS, roteabilidade, estabilidade e integração com a borda.
Acesso público	4 Gbps, IPv4 /29, IPv6, DDoS, segregação e processamento pela segurança de borda.
NOC e SOC	Operação técnica, canais, painéis, chamados, relatórios, integração com N1 do InPACTA, N2/N3, monitoramento, segurança e escalonamento.
C6	Conectividade temporária por evento, com satélite como meio principal, cobertura, simultaneidade, mobilização, testes e desmobilização conforme item 5.7. Não integra os nodes permanentes.
Telefonia IP/VoIP	Quando demandada: Ordem de Serviço, plataforma homologada, alta disponibilidade, dois caminhos SIP, portabilidade, chamadas internas e externas, 0800 e números especiais, qualidade de voz, segurança, CDR, faturamento conciliado, softphones, interconexão lógica dos aparelhos legados disponibilizados pela Prefeitura, suporte, documentação e operação assistida.
Operação e manutenção da telefonia	Service Desk e protocolos funcionais, severidades, manutenção preventiva e corretiva, configurações rotineiras, escalonamento de prestadoras, suporte aos terminais compatíveis, recorrência, segurança de acesso remoto, relatórios e evidências conforme IMR.
Processamento privado de IA aplicado à telefonia	Quando habilitado: limiar de confiança com revisão humana obrigatória, rastreabilidade da versão dos modelos, validação antes de atualização, avaliação de desempenho do reconhecimento de fala por variação linguística regional, controles contra manipulação do conteúdo transcrito, aviso ao cidadão, processamento privado, exportação e continuidade independente do serviço de voz.
C7	Resiliência fixa, transportável ou veicular sob demanda, com preparação obrigatória dos nodes conforme item 27. Preservar classes, capacidades e proteções existentes.

21.5. RECEBIMENTO E HOMOLOGAÇÃO

21.5.1. O recebimento provisório ocorrerá após instalação, ativação e entrega das evidências mínimas, sem autorizar faturamento recorrente até o aceite técnico previsto para o item.

21.5.2. O recebimento definitivo dependerá de validação da estabilidade, desempenho, monitoramento, documentação, segurança, integração e ausência de inconformidade impeditiva.

21.5.3. Os testes por node observarão sua classe: capacidade útil por sentido, simetria aplicável, latência, perda, jitter quando pertinente, segregação, mecanismos de segurança, roteamento, detecção de falhas, monitoramento, alarmes, painel e Service Desk. Nos C1/C2 serão testados o perfil útil da proteção GPON e a comutação; nos C3/C4, ambos os caminhos e a comutação; nos C5, a rota única e a restauração. Não se exigirá teste de rota secundária em classe que não a possui. Nos hotspots C4, será comprovado o mínimo Wi-Fi 6 e a capacidade de integração com Wi-Fi 7 exigidos nos itens 5.6.1, 5.6.2 e 5.6.6. A comprovação incluirá fichas técnicas dos pontos de acesso, matriz de compatibilidade da plataforma e registro do padrão negociado com terminal Wi-Fi 6. A integração com Wi-Fi 7 será demonstrada com amostra de pontos de acesso Wi-Fi 6 e Wi-Fi 7 sob a plataforma ofertada, verificando provisionamento, políticas, autenticação ou portal quando aplicável, segmentação, monitoramento e alarmes. Serão identificados modelos, versões, licenças, configurações e resultados. A retrocompatibilidade de um terminal Wi-Fi 7 conectado a um ponto Wi-Fi 6, isoladamente, não comprovará a integração de gestão exigida. O ensaio conjunto poderá utilizar amostra representativa em laboratório; a cobertura e o desempenho reais permanecerão sujeitos ao aceite local.

21.5.3.1. O ensaio de capacidade utilizará um AP por vez, mantendo 200 dispositivos associados, com 100 ativos durante 60 minutos contínuos, após estabilização. Cada ativo deverá obter pelo menos 3 Mbps de download e 1 Mbps de upload úteis simultâneos, aferidos individualmente em janelas de 60 segundos, sem aprovação por média que oculte terminal abaixo do mínimo. Não serão aceitos reinicialização do AP ou desconexões atribuíveis à solução durante o ensaio. Sob a mesma carga, a perda de sondas por dispositivo deverá ser de até 1% e o percentil 95 do tempo de ida e volta até o servidor cabeado local de até 50 ms.

21.5.3.2. O servidor de teste será cabeado na rede local, sem gargalo de interface ou processamento e sem dependência da Internet. Serão usadas estações Wi-Fi 6 independentes, físicas ou emuladas em radiofrequência, que reproduzam individualmente associação, autenticação, disputa pelo meio e tráfego. Emulação exclusivamente de fluxos IP em uma única estação não comprovará capacidade de clientes do AP. O perfil será de 80 ativos em 5 GHz e 20 em 2,4 GHz, com canais de 40 MHz e 20 MHz, respectivamente, RSSI entre -65 e -55 dBm e SNR mínimo de 25 dB. Os outros 100 associados permanecerão sem tráfego de aplicação gerado pelo ensaio, sendo 20 em 5 GHz e 80 em 2,4 GHz, totalizando 100 associados por banda. Tráfego de controle necessário à manutenção das associações será registrado e não será confundido com carga de aplicação. Segurança, isolamento, políticas, portal quando aplicável e monitoramento permanecerão habilitados. As condições de comparação serão equivalentes, sem exigir identidade de comandos ou da implementação interna.

21.5.3.3. O relatório identificará cada estação, banda, taxas úteis por sentido e por intervalo, latência, perda, falhas, autenticações, configuração, firmware e licenças, com evidências exportáveis. A capacidade será comprovada em amostra de cada configuração de AP ofertada. Na seleção, a capacidade será examinada por comprovação documental; o ensaio somente integrará PoC excepcional autorizada conforme item 19.1 e Anexo II 13.38.1 a 13.38.4, com

roteiro previamente publicado, prazo de preparação e condições uniformes; não será exigida implantação municipal antecipada. Na implantação, haverá validação da cobertura, carga prevista, gestão, segurança e desempenho no ambiente efetivo, além da correspondência com a configuração aprovada. A amostra de laboratório não substitui o aceite local nem o dimensionamento dos enlaces.

21.5.3.4. O tráfego útil será medido na aplicação receptora, em Mbps decimais, com TCP e uma conexão de dados por sentido por estação ativa, download e upload concorrentes. Após todas as estações concluírem associação, endereçamento e autenticação aplicável, o ensaio durará 60 minutos, em 60 janelas consecutivas e não sobrepostas de 60 segundos. Cada estação deverá atingir os mínimos por sentido em cada janela; o agregado não substituirá a aferição individual. A ferramenta deverá gerar carga suficiente para aferir os mínimos e registrar bytes úteis recebidos e duração real. A mesma família IP e MTU serão aplicadas a todas as execuções de comparação e declaradas no roteiro. A funcionalidade da outra família IP exigida no projeto será comprovada separadamente.

21.5.3.5. Durante a carga, cada estação ativa enviará uma sonda ICMP Echo por segundo ao servidor local, com 64 bytes de dados ICMP e prazo de resposta de 1 segundo. Perda será a razão entre sondas sem resposta válida no prazo e sondas enviadas, por estação, durante o ensaio. O RTT será calculado nas respostas válidas; o percentil 95 corresponderá à posição teto de 0,95 multiplicado pelo número de amostras válidas, após ordenação crescente. A perda e o RTT serão avaliados separadamente, sem substituir ausência de resposta por latência zero. Serão preservados os registros individuais e a referência temporal, aplicando-se os limites já estabelecidos de perda até 1% e RTT P95 até 50 ms.

21.5.3.6. O roteiro será disponibilizado com as regras aplicáveis antes das propostas e identificará topologia, equipamentos e versões de teste, características dos clientes e fluxos espaciais, ferramentas, endereçamento, MTU, canais, potência, localização e método de medição de RSSI e SNR, interferência externa, perfil de autenticação e matriz de funções habilitadas. A medição de sinal identificará o receptor e o sentido aferido; valores de origens distintas não serão tratados como equivalentes sem método documentado. O roteiro fixará prazo de preparação, executor, observadores, recursos fornecidos por cada parte, despesas, repetições permitidas e tratamento de falha do ambiente. Não serão alteradas condições seletivamente para aprovar participante; ocorrência externa será registrada e tratada pelas mesmas regras de repetição.

21.5.4. O aceite da resiliência dos nodes C1 a C4 exigirá teste controlado de falha do caminho primário ou condição equivalente, com comprovação da ativação automática do caminho secundário, do roteamento, da detecção de falhas e da continuidade dos serviços prioritários. Nos C1 e C2 será comprovada a proteção GPON; nos C3 e C4 será comprovada a capacidade integral da classe em cada uma das duas rotas ópticas e a diversidade de fornecedor.

21.5.5. Durante o teste deverão ser registrados, no mínimo, horário, estado dos caminhos, alarmes, perda de pacotes, latência, variação de atraso, capacidade entregue, continuidade das sessões ou aplicações de referência, chamados gerados e tempo observado de transição e estabilização. O aceite incluirá os fluxos municipais definidos na matriz de interoperabilidade e a demonstração de detecção proativa, alerta, abertura de chamado, comunicação à Central de Situação e escalonamento ao N2/N3. Serão testadas degradação, perda de redundância e perda de telemetria em condições controladas, verificando também a identificação da recuperação e a preservação do histórico e dos prazos.

21.5.6. Os testes dos C3 e C4 deverão demonstrar, em cada uma das duas rotas ópticas, capacidade mínima de 1 Gbps simétrico e 500 Mbps simétricos, respectivamente, além da independência física, do fornecedor distinto entre os caminhos, da comutação, estabilidade, monitoramento e atendimento dos níveis de serviço.

21.5.7. A comprovação de resiliência deverá incluir identificação suficiente dos domínios de falha, capacidade por rota, alarmes, eventos de comutação e restauração. Nos C1/C2, deverá incluir o perfil da proteção GPON; nos C3/C4, a capacidade integral e a diversidade de fornecedor; nos C5, a disponibilidade e o tempo de restauração da rota única.

21.5.8. Alterações relevantes de rota, ponto de presença, equipamento de agregação, prestadora ou fornecedor da rota, porta PON, OLT, backbone, backhaul ou última milha dos nodes exigirão repetição proporcional dos testes de proteção ou redundância conforme a classe e a tecnologia afetada.

21.5.9. O relatório de aceite deverá indicar as evidências técnicas suficientes para comprovar a proteção, sem obrigar a divulgação de informações de engenharia interna que não sejam necessárias à fiscalização.

21.5.10. Testes deverão ser realizados com métodos, ferramentas e servidores de referência aprovados pela fiscalização, preservando registro de data, hora, local, equipamento e resultado. Para HA de firewalls e gateways, o ensaio incluirá falhas isoladas de membro, interface, alimentação e canal de sincronização, conforme a arquitetura, seguidas de recuperação e retorno. Sob carga representativa e inspeção habilitada, serão medidos detecção, comutação, interrupção, perda de pacotes, sessões preservadas ou restabelecidas e capacidade residual, verificando NAT, VPN, roteamento e políticas aplicáveis. A base do projeto disponibilizada antes da proposta fixará valores máximos de comutação e interrupção, perda tolerada e critérios de preservação ou restabelecimento por serviço crítico. O roteiro executivo não poderá criar ou flexibilizar esses limites. Ausência de limite previamente definido impedirá a homologação do ensaio correspondente.

21.5.11. Falhas impeditivas deverão ser corrigidas e retestadas sem custo adicional. O serviço não aceito não será faturado.

21.5.12. O recebimento da telefonia será realizado por entregáveis e unidades ativadas, com aceite provisório após testes técnicos e aceite definitivo após estabilização, conciliação de faturamento e entrega documental.

21.5.13. Falha em portabilidade, alta disponibilidade, redundância, qualidade de voz, segurança, CDR, monitoramento ou conciliação impedirá o aceite da unidade afetada até correção e reteste.

21.6. HOMOLOGAÇÃO DAS CLASSES DE ACESSO

21.6.1. A homologação será realizada por node e por serviço, com testes compatíveis com a classe e a finalidade.

21.6.2. O teste de proteção dos nodes C1 e C2 deverá provocar, em janela controlada, a indisponibilidade da rota principal ou condição técnica equivalente, comprovando a ativação automática da rota GPON e o atendimento das capacidades e serviços prioritários definidos para a contingência.

21.6.3. O relatório deverá registrar topologia funcional, caminhos testados, mecanismo de criptografia, estado das sessões de roteamento e detecção de falhas, horário, duração da transição, perda observada, capacidade entregue em contingência, alarmes, chamados correlatos, estabilidade após a comutação e retorno à condição normal.

21.6.4. A repetição dos testes de proteção dos C1 e C2 após mudanças relevantes observará a regra do item 21.5.8, aplicada à classe e à tecnologia afetadas.

21.6.5. Os nodes C3 e C4 serão testados quanto às duas rotas ópticas, à capacidade integral de 1 Gbps simétrico por rota para C3 e 500 Mbps simétricos por rota para C4, à diversidade física e de fornecedor, à integração lógica, ao roteamento dinâmico, à detecção de falhas, à capacidade por sentido, à estabilidade, à interface de entrega, à comutação, ao suporte e ao monitoramento. Os nodes C5 serão testados quanto à disponibilidade, ao perfil mínimo de 50 Mbps simétricos, à capacidade de subida, ao túnel criptografado, ao roteamento, à detecção de falhas, à estabilidade, à interface de entrega, ao suporte e ao monitoramento da rota única GPON.

21.6.6. Os nodes C4 serão testados quanto a backhaul, cobertura, autenticação, segregação, capacidade de usuários, segurança, gestão e relatórios. O aceite do portal verificará também criação, aprovação, agendamento e encerramento de campanha, enquete, questionário, participação voluntária, relatório, exportação, segregação de perfis e falha do módulo de interatividade, conforme itens 5.6.4.1 a 5.6.4.6 e 5.6.5. As evidências identificarão versão, local, configuração e resultado, com dados de teste ou legitimamente autorizados. O aceite verificará também a aplicação e recuperação de configurações por grupos, os parâmetros de rádio, o diagnóstico, a segregação entre APs e a integração completa do portal, nos termos dos itens 5.6.6.1.1 a 5.6.6.1.5. A

continuidade será verificada por função e dependência, conforme item 5.6.6.4.
21.6.7. Os acessos à Internet previstos no projeto municipal serão identificados por sua função, site atendido e código de circuito e serão testados quanto à capacidade, simetria, endereçamento, roteabilidade, diversidade, proteção DDoS, estabilidade e integração com a segurança de borda.
21.6.8. O C6 será testado antes do evento quanto à conectividade, cobertura, capacidade, segurança, monitoramento, suporte e contingência.

22. RELATÓRIOS INDICADORES E RESULTADOS
22.1. Os resultados pretendidos são continuidade das unidades, capacidade compatível com os fluxos, proteção efetiva dos caminhos, suporte integrado, migração segura e preservação da comunicação por voz. A linha de base de cada atendimento deve permitir comparar os resultados sem presumir economia ou ganho percentual.
22.2. O acompanhamento relacionará disponibilidade por node, interrupções, restauração, capacidade por sentido, percentil 95, perda, latência, comutação, chamados, causa raiz, migração, numeração e registros autorizados. Indicadores agregados não substituirão a verificação de unidade crítica nem ocultarão perda de redundância. O relatório mensal demonstrará eventos detectados proativamente, tempos de detecção e resposta, causa identificada, recorrências, lacunas de coleta, desvios de capacidade e medidas preventivas, com responsável, prazo e situação. A Central de Situação acompanhará essas providências e a comunicação institucional; a executora manterá a condução técnica de N2/N3, NOC e SOC.
22.3. O acompanhamento deverá distinguir capacidade nominal, capacidade disponível e qualidade efetiva. Médias agregadas não poderão ocultar indisponibilidade de unidade crítica, perda de redundância ou descumprimento do perfil de uma classe. A demonstração de benefício depende de base de comparação consistente e de evidência por serviço.

22.6. DOSSIÊ DE MEDIÇÃO E EVIDÊNCIAS
22.6.1. O Dossiê Mensal de Medição consolidará inventário, serviços ativos, disponibilidade, desempenho, capacidade, incidentes, chamados, manutenções, segurança, glosas, alterações e evidências.
22.6.2. Os relatórios serão entregues em PDF assinado e em formatos abertos para dados tabulares, com rastreabilidade entre painel, ticket, log, CDR, Ordem de Serviço e fatura.
22.6.3. A medição mensal observará o item 22.7.10 e abrangerá os registros de todos os serviços ativos. Testes de homologação por amostragem expressamente previstos não substituem essa apuração integral.
22.6.4. Ausência, insuficiência ou inconsistência de evidências poderá suspender o aceite e a liquidação da parcela controvertida.
22.6.5. Os relatórios de capacidade indicarão tendência, risco de saturação e plano preventivo.
22.6.6. O relatório informará licença e versão, usuários e ramais, chamadas simultâneas máximas, percentis, horários de pico, alertas de 70%, 80% e 90% e tendência.
22.6.7. Serão apresentados disponibilidade do núcleo, troncos e SBCs, eventos de failover, backup, restauração, atualizações, certificados, incidentes e mudanças.
22.6.8. Serão apresentados ASR, ACD, PDD, códigos SIP, chamadas rejeitadas, abandonadas, transferidas, falhas de portabilidade, qualidade de voz e causas de degradação.
22.6.9. Serão apresentados relatórios de filas, agentes, grupos, extensões, regras de entrada, auditoria administrativa, gravações autorizadas e acessos a dados sensíveis.
22.6.10. As evidências permitirão conciliação entre CDR, tronco, fatura, Ordem de Serviço, inventário, licença, faixa ativada e documento fiscal.
22.6.11. Os relatórios C6 observarão o conteúdo mínimo do item 5.7.7.

22.7. GESTÃO MEDIÇÃO E FISCALIZAÇÃO
22.7.1. A execução será acompanhada por gestor e fiscais designados, com apoio técnico das unidades competentes, sem transferência à Administração da operação da rede da EXECUTORA.
22.7.2. A fiscalização utilizará painéis, relatórios, chamados, logs, testes, evidências de disponibilidade, auditorias e reuniões técnicas.
22.7.3. Todos os equipamentos, licenças, plataformas, manutenção, deslocamentos, suporte, testes e custos necessários deverão estar incluídos nos itens correspondentes, sem cobranças autônomas não previstas.
22.7.4. A base inicial e a expansão equivalente utilizarão os mesmos preços unitários por classe, vedada diferenciação artificial entre node inicial e node futuro com composição técnica equivalente.
22.7.5. Todos os switches de núcleo, agregação, distribuição e acesso, módulos ópticos, transceptores, fontes, licenças, software de gerenciamento, suporte, manutenção e substituições necessários ao atendimento das rotas e capacidades previstas deverão estar incluídos nos preços correspondentes, sem cobrança paralela.
22.7.6. Os custos abrangidos pelo item de switches não poderão ser novamente cobrados nos itens de implantação ou mensalidade dos nodes.
22.7.7. Os preços dos nodes deverão incluir integralmente as rotas correspondentes a cada classe: MPLS e proteção GPON para C1 e C2; duas rotas ópticas independentes de 1 Gbps simétrico cada para C3; duas rotas ópticas independentes de 500 Mbps simétricos cada para C4; e rota única GPON de 50 Mbps simétricos para C5. Em todos os casos estarão incluídos capacidade, integração lógica, roteamento, detecção, monitoramento, testes, documentação, manutenção e correção de falhas.
22.7.8. Não será admitida cobrança adicional por rota secundária, perfil óptico, túnel criptografado ou mecanismo equivalente, roteamento, detecção de falhas, comutação, reserva operacional, monitoramento, teste de contingência ou componente indispensável ao atendimento da resiliência contratada.
22.7.9. A medição será instruída por relatório de todos os nodes e serviços ativos, contendo identificação, classe, capacidade, status, disponibilidade, indisponibilidades, chamados, causa provável, manutenção, exclusões justificadas, glosas, utilização e evidências de restabelecimento.
22.7.10. Não será admitida medição baseada apenas em resumo global, amostragem ou declaração genérica de disponibilidade.
22.7.11. A ausência, insuficiência ou inconsistência das evidências poderá impedir o aceite da medição, exigir reprocessamento e gerar glosa quando a disponibilidade não puder ser comprovada.
22.7.12. Para C1 e C2, o relatório mensal indicará o estado da rota principal MPLS, da proteção GPON, do túnel, das sessões de roteamento e detecção, das comutações, da operação degradada e da capacidade por sentido. Para C3 e C4, indicará o estado das duas rotas ópticas, fornecedor em operação, comutações, capacidade integral por rota, desempenho e incidentes. Para C5, indicará disponibilidade, alarmes, desempenho, capacidade por sentido, incidentes e restauração da rota única.
22.7.13. O pagamento será realizado conforme os serviços efetivamente ativados, aceitos, disponíveis e medidos, após apresentação do documento fiscal e demais documentos exigidos, observados os prazos administrativos, retenções, glosas e sanções.
22.7.14. Nenhum node, link ou serviço recorrente será faturado antes da respectiva ordem de serviço, ativação, monitoramento, teste e aceite.

22.7.15. A medição da telefonia será segregada por Ordem de Serviço e conterá, no mínimo, núcleo ativo, ramais ativos, softphones vinculados, faixas de canais, números portados, tráfego, serviços especiais, eventos de indisponibilidade e glosas.
22.7.16. A fiscalização terá acesso aos CDR, inventários, painéis e relatórios necessários à conferência, observadas as regras de segurança e proteção de dados.
22.7.17. Divergência entre CDR, inventário, Ordem de Serviço, relatório de ativação e fatura suspenderá a liquidação da parcela controvertida até saneamento, sem prejuízo do pagamento da parte incontroversa.
22.7.18. Quando a camada analítica privada de inteligência artificial estiver habilitada por Ordem de Serviço, a medição deverá registrar os processamentos efetivamente realizados, versões dos modelos, limiares de confiança, encaminhamentos à revisão humana, falhas de transcrição e integração, indicadores de desempenho e eventos de segurança. Os custos deverão estar contemplados nos itens de telefonia correspondentes previstos na planilha, sem cobrança autônoma não prevista.

23. SUSTENTABILIDADE E CICLO DE SUPORTE

23.1. A qualificação econômico-financeira da interessada, a sustentabilidade da parceria e as condições financeiras de execução têm finalidades distintas. A qualificação será examinada e aprovada antes da convocação à PoC, conforme o Anexo I, item 17.2, sem proposta econômica, comparação de preços ou pontuação financeira na seleção institucional. Documentos, índices, fórmulas e bases de cálculo exigíveis serão motivados e definidos previamente no instrumento convocatório. Preços, remuneração, repasses e demais condições de eventual execução municipal serão estabelecidos no instrumento próprio do projeto.
23.2. Os valores deverão ser definidos mediante orçamento e aprovação próprios. O modelo deverá relacionar contribuições, custos, riscos e resultados e indicar os marcos de sua aprovação, sem substituir a pesquisa exigível da contratação municipal ou atribuir a ela efeito de seleção da parceria.
23.3. A sustentação exige identificar contribuições, custos, riscos, resultados e capacidade efetiva antes de assumir compromissos. Não se presume remuneração, margem, receitas de outros municípios ou demanda garantida.

23.4. ATUALIZAÇÕES E GESTÃO DE MUDANÇAS

23.4.1. A EXECUTORA manterá a plataforma, componentes de sistema, parâmetros de interoperabilidade com prestadores, software embarcado dos terminais suportados e integrações em versões estáveis, seguras e compatíveis.
23.4.2. Atualizações críticas de segurança serão avaliadas imediatamente e aplicadas em até 72 horas após sua validação técnica e autorização da mudança, salvo impedimento formalmente justificado e mitigado.
23.4.3. Atualizações funcionais serão aplicadas em janela autorizada, com backup, plano de testes, reversão e verificação pós-mudança, em prazo máximo de 30 dias após homologação.
23.4.4. Mudança de versão principal dependerá de matriz de compatibilidade de terminais, troncos, APIs, integrações, gravações, filas, relatórios, SBCs e regras de chamada.
23.4.5. Nenhuma atualização poderá reduzir funcionalidades, capacidade, segurança, relatórios, APIs ou interoperabilidade contratadas.

23.5. EFICIÊNCIA ENERGÉTICA E DESTINAÇÃO DE RESÍDUOS

23.5.1. A utilização de infraestrutura existente reduz obras, ocupação de postes, lançamento de cabos e intervenções em via pública.
23.5.2. A contratada será responsável pela destinação adequada de equipamentos, baterias, cabos, embalagens e resíduos gerados por sua execução, observadas as regras de logística reversa e resíduos sólidos aplicáveis.
23.5.3. A solução priorizará equipamentos com eficiência energética, dimensionamento adequado, manutenção preventiva e substituição responsável, reduzindo consumo excessivo, falhas recorrentes e descarte prematuro.

24. OBRIGAÇÕES TÉCNICAS ESSENCIAIS E CONDIÇÕES DE CONSOLIDAÇÃO

24.1. A entrega será verificada pelo desempenho do serviço completo e pela correlação entre projeto, inventário, configuração, ensaio, registro operacional e aceite. A integração de componentes de terceiros não dilui a responsabilidade pela solução assumida.
24.2. Antes da proposta correspondente, o instrumento do projeto fixará o marco inicial e os prazos de implantação, o regime de tarifação e as condições de isolamento da plataforma de voz que influenciem dimensionamento ou preço. A Ordem de Serviço acionará exclusivamente as condições já contratadas, sem completar posteriormente requisito essencial à comparação das propostas.

24.3. NEUTRALIDADE EQUIVALÊNCIA E DESEMPENHO

24.3.1. Este item estabelece os requisitos mínimos de capacidade, funcionalidade, interoperabilidade, segurança, gerenciamento, desempenho e verificabilidade dos componentes utilizados na prestação do serviço integrado.
24.3.2. Os equipamentos, softwares, licenças, plataformas, enlaces, serviços e acessórios serão fornecidos, mantidos, atualizados e substituídos pela EXECUTORA durante a vigência, sem aquisição isolada ou transferência automática de propriedade ao Município.
24.3.3. A EXECUTORA permanecerá responsável por serviços próprios, infraestrutura de terceiros e parcelas subcontratadas, inclusive para atendimento, restabelecimento, medição, glosa, sanção e transição.
24.3.4. O dimensionamento deverá demonstrar que nenhum enlace, interface, equipamento, licença, sistema de gerenciamento, plataforma, fila, tabela, sessão ou componente compartilhado constitui gargalo em operação normal, contingência ou expansão.
24.3.5. Serão admitidos componentes, arquiteturas e tecnologias equivalentes ou superiores, desde que a equivalência seja comprovada objetivamente e não reduza capacidade, segurança, interoperabilidade, suporte, rastreabilidade, continuidade ou níveis de serviço.
24.3.6. Os requisitos técnicos deverão ser interpretados como limites mínimos de resultado e desempenho. Não será admitida exigência de característica atípica, combinação incomum de interfaces, recurso proprietário, certificação de marca ou detalhe construtivo que, sem justificativa técnica formal nos autos, restrinja indevidamente o universo de soluções aptas a atender ao objeto.
24.3.7. A descrição de equipamentos e componentes limitar-se-á às características indispensáveis ao resultado contratado, especialmente capacidade, desempenho, interfaces necessárias à interconexão, protocolos, segurança, disponibilidade, gerenciabilidade, interoperabilidade e condições efetivamente pertinentes ao ambiente de execução, vedada a reprodução cumulativa de características de catálogo, ficha técnica ou arranjo construtivo que identifique ou favoreça produto específico sem motivação técnica formal nos autos.
24.3.8. Quando houver certificação, homologação ou requisito regulatório legalmente aplicável ao produto, equipamento ou serviço, a exigência será formulada de maneira impessoal e objetiva e será aceita para toda solução equivalente que comprove regularidade perante o órgão ou entidade competente, vedada sua conversão em certificação de marca, vínculo comercial ou qualificação emitida por fabricante determinado.

24.3.9. A aprovação do projeto executivo não transfere ao MUNICÍPIO DEMANDANTE a responsabilidade pelo dimensionamento, compatibilidade, desempenho, licenciamento ou suficiência da solução.
24.3.10. Todo requisito será comprovado por documentação técnica, matriz de conformidade, demonstração, teste, painel, log, relatório ou outra evidência reproduzível definida no roteiro de aceite.

24.4. OBRIGAÇÕES DE EXECUÇÃO INTEGRADA

24.4.1. Prestar integralmente os serviços, mantendo regularidade, capacidade, disponibilidade, segurança, suporte e continuidade;
24.4.2. Manter autorização SCM vigente em seu próprio nome durante toda a execução; A prova e a verificação da regularidade observarão o Anexo II 7.11.
24.4.3. Fornecer e manter equipamentos, licenças, plataformas, enlaces e recursos necessários;
24.4.4. Implantar e operar NOC físico, SOC 24x7 e suporte especializado N2/N3, disponibilizando sistema de chamados e integrações para o N1 e a Central de Situação operados pelo InPACTA;
24.4.5. Gerir operadoras, provedores, equipes de campo e subcontratadas sem transferir responsabilidades;
24.4.6. Monitorar proativamente os nodes, links, hotspots e componentes centrais contratados, identificar degradação e tendências de saturação, correlacionar eventos e agir conforme os itens 15.6.2 e 15.6.3. Comparar indicadores com a linha de base e os limiares aprovados, emitir recomendações preventivas e acompanhar sua execução. Alertas não autorizarão expansão, intervenção em ativos municipais ou custo adicional sem a aprovação cabível;
24.4.7. Apresentar relatórios completos, conciliáveis com chamados, painéis, logs e faturamento;
24.4.8. Manter gestão de capacidade e corrigir gargalos decorrentes do dimensionamento da solução;
24.4.9. Comunicar incidentes, mudanças, riscos de saturação e indisponibilidades relevantes;
24.4.10. Cumprir LGPD, Marco Civil, sigilo, segurança e retenção limitada;
24.4.11. Realizar manutenção preventiva, preditiva e corretiva sem custo adicional;
24.4.12. Substituir componentes defeituosos por equivalentes ou superiores dentro do SLA;
24.4.13. Cooperar com a migração, transição de saída e transferência de informações operacionais;
24.4.14. Manter regularidade trabalhista, fiscal, técnica, ambiental e regulatória;
24.4.15. Assumir custos decorrentes de falhas, retrabalho, retestes e correções imputáveis à sua solução.
24.4.16. Manter as rotas principais MPLS e as proteções GPON dos nodes C1 e C2, as duas rotas ópticas independentes dos nodes C3 e C4, cada qual com a capacidade integral da classe e com fornecedores distintos, e as rotas únicas GPON dos nodes C5 durante toda a vigência, inclusive durante manutenções, migrações e substituições de terceiros.
24.4.17. Monitorar continuamente as rotas, túneis e sessões de roteamento e detecção, registrar eventos de comutação, comunicar operações degradadas e apresentar evidências à fiscalização;
24.4.18. Repetir os testes de proteção após alterações relevantes e corrigir, sem custo adicional, deficiência de diversidade, capacidade, criptografia, roteamento, detecção, comutação, monitoramento ou documentação imputável à solução ofertada.
24.4.19. Manter capacidade de mobilização da telefonia durante a vigência e cumprir as Ordens de Serviço nos prazos definidos;
24.4.20. Coordenar a prestadora autorizada da telefonia pública e responder integralmente por seus serviços perante o Município;
24.4.21. Executar inventário, projeto, migração, portabilidade, interconexão lógica dos aparelhos legados, provisionamento, testes, treinamento, operação assistida e documentação;
24.4.22. Manter a alta disponibilidade, os dois caminhos independentes, a segurança, o monitoramento, os backups, os CDR e a conciliação do faturamento;
24.4.23. Preservar a numeração institucional e cooperar integralmente com a transição de saída.

25. ESPECIFICAÇÃO E ACIONAMENTO DA TELEFONIA

25.0. A telefonia constitui parcela de ativação eventual. Sua especificação e precificação serão individualizadas nos instrumentos aplicáveis; a execução, as licenças ativadas, os testes, a operação assistida e a medição dependem de Ordem de Serviço própria. A implantação da rede não autoriza automaticamente telefonia, gravação ou processamento inteligente. Aplicam-se as regras comuns deste Anexo no que couber, sem duplicação de cobrança por infraestrutura ou suporte compartilhados. A proposta identificará separadamente os recursos da telefonia e os de gravação, transcrição e análise: o que integra o preço base, o que depende de licença ou serviço adicional previsto e a respectiva unidade de medição. Demonstrar capacidade de integração não equivale a fornecer ou ativar processamento de chamadas. A Ordem de Serviço somente acionará recursos e quantidades abrangidos pelas condições contratadas.

25.1. ATIVAÇÃO DA TELEFONIA

25.1.1. A telefonia IP/VoIP integra o objeto e a proposta técnica da parceria institucional, sem apresentação de preços nessa seleção. Sua execução será iniciada somente após a formalização do instrumento próprio do projeto municipal e a emissão de Ordem de Serviço específica durante a respectiva vigência.
25.1.2. A Ordem de Serviço indicará a motivação, as unidades atendidas, os quantitativos, os números, as integrações, a capacidade de canais, o cronograma, os responsáveis, as janelas de mudança, os critérios de aceite e a autorização orçamentária.
25.1.3. A EXECUTORA deverá manter capacidade técnica, regulatória, operacional e de mobilização para atender à Ordem de Serviço dentro dos prazos desta especificação. A prontidão não acionada não gerará faturamento, indenização ou consumo mínimo.
25.1.4. Os preços unitários da telefonia e as regras de reajuste, revisão, medição e glosa serão definidos no procedimento próprio de formalização da execução municipal antes de sua contratação. Não serão exigidos nem utilizados no julgamento da seleção da parceria técnica institucional.
25.1.5. A emissão de Ordem de Serviço não alterará a natureza, o regime de execução, o julgamento, os preços unitários ou a responsabilidade centralizada do contrato, limitando-se a definir o momento, o local e as quantidades da parcela previamente contratada.
25.1.6. Demandas que ultrapassem os limites, requisitos ou condições desta especificação dependerão da análise e do instrumento jurídico cabível, vedada sua inclusão por simples Ordem de Serviço.

25.2. MATRIZ DE RESPONSABILIDADES DA TELEFONIA

25.2.1. A matriz de responsabilidades deverá indicar, para cada componente e ocorrência, quem diagnostica, autoriza, executa, fornece material, substitui, registra, testa, aceita e suporta o custo, abrangendo contratada, Município, prestadora regulada, operadora de acesso, mantenedora da rede local e demais terceiros.

25.3. CAPACIDADE E LICENCIAMENTO DA TELEFONIA

25.3.1. A capacidade contratada corresponderá ao total de chamadas internas e externas ativas simultaneamente, inclusive chamadas em filas, conferências, transbordos, gravações autorizadas e demais recursos concorrentes que consumam capacidade de processamento ou sessão da solução. Os troncos SIP e

caminhos de telefonia pública serão dimensionados dentro dessa capacidade total, vedada interpretação que resulte em capacidade externa adicional por simples soma às chamadas internas.
25.3.2. Serão disponibilizados softphones dimensionados no projeto para perfis autorizados. O softphone deverá permanecer associado a ramal ativo e integrado ao mesmo plano de numeração, inventário, políticas de segurança e suporte, sem duplicidade de licenciamento.
25.3.3. A administração deverá ocorrer por interface web controlada, com perfis, grupos, filas, horários, feriados, caixas postais, transferência, captura, conferência, permissões, classes de serviço, relatórios e trilha de auditoria.

25.4. CAMINHOS SIP E REGULARIDADE DA PRESTAÇÃO
25.4.1. O acesso à rede pública será prestado por pessoa jurídica regularmente autorizada pela Anatel para a modalidade aplicável, diretamente pela EXECUTORA ou por prestadora integrante de sua cadeia de execução.
25.4.2. A proponente indicará na proposta a estratégia regulatória e operacional da parcela de telefonia. A identificação nominal da prestadora autorizada poderá ocorrer durante a mobilização, devendo ser formalizada, documentada e aprovada antes da ativação.
25.4.3. A EXECUTORA permanecerá integralmente responsável perante o Município pela plataforma, pelos caminhos SIP, pela portabilidade, pelo suporte, pelos níveis de serviço, pela medição, pelo faturamento e pela atuação da prestadora autorizada.
25.4.4. Os dois caminhos SIP, sua capacidade e a independência dos domínios de falha atenderão aos itens 25.6.1 e 25.6.2. O dimensionamento da plataforma observará o item 25.3.1, distinguindo chamadas internas e externas dentro da capacidade total.
25.4.5. A arquitetura deverá possuir controladores de borda de sessão ou mecanismos equivalentes em alta disponibilidade, com proteção, interoperabilidade, controle de sessões, limitação de abuso, registros e failover testável.

25.5. NUMERAÇÃO PORTABILIDADE E ATENDIMENTO
25.5.1. A EXECUTORA deverá preservar ou reorganizar de forma controlada os números públicos efetivamente identificados no inventário, incluindo DIDs, faixas DDR, serviços 0800, números de utilidade pública e demais recursos autorizados.
25.5.2. A referência histórica de faixas de numeração será utilizada para inventário e planejamento, sem presunção de que todos os números estejam ativos ou gerem cobrança individual.
25.5.3. A portabilidade será executada por lotes controlados, com plano de comunicação, janelas aprovadas, coexistência, chamadas de validação, aceite e retorno documentado.
25.5.4. O plano de numeração interna será preservado sempre que viável ou reorganizado mediante aprovação, documentação, comunicação aos usuários e mapa de correspondência entre ambientes.

25.6. TRONCOS SIP CONTROLADORES DE BORDA E UNIDADES
25.6.1. Serão mantidos dois caminhos SIP independentes, cada um apto a suportar integralmente a capacidade externa ativada, sem que a soma dos caminhos amplie o limite total de simultaneidade definido no projeto.
25.6.2. Os caminhos deverão possuir diversidade de prestadora ou, quando utilizados serviços da mesma prestadora, diversidade comprovada de ponto de presença, borda, acesso, energia, rota e domínio de falha.
25.6.3. A comutação entre caminhos será automática ou operacionalmente assistida dentro do SLA, com preservação da identificação de chamada, regras de entrada e saída, DIDs, serviços especiais e registros.
25.6.4. A plataforma deverá utilizar serviços SIP tecnicamente compatíveis, comprovados por teste integral de entrada, saída, portabilidade, criptografia quando aplicável, DTMF, identificação, serviços especiais, redundância, continuidade e tarifação, sem exigência de homologação, parceria ou lista comercial de fabricante específico.
25.6.5. Unidades remotas utilizarão controlador de borda de sessão, túnel seguro ou arquitetura funcionalmente equivalente quando necessário à concentração de sinalização, segurança, continuidade, travessia controlada de NAT e interoperabilidade, conforme quantidade de terminais, criticidade e topologia.
25.6.6. Unidades críticas ou com concentração de terminais que justifique controle local de sinalização, mídia, segurança ou continuidade deverão utilizar controlador de borda de sessão dedicado ou arquitetura funcionalmente equivalente, dimensionada conforme a quantidade de terminais, chamadas simultâneas, criticidade e topologia.
25.6.7. O SBC concentrará sinalização e mídia da unidade, reduzirá dependências de NAT e firewall e será dimensionado para todos os telefones e chamadas simultâneas locais, com margem operacional.
25.6.8. A indisponibilidade, atualização, perda de registro ou saturação do SBC será monitorada pelo NOC e tratada no mesmo fluxo de incidentes da Infovia.

25.7. RECURSOS DE ATENDIMENTO E ORGANIZAÇÃO
25.7.1. A plataforma organizará usuários, filas, grupos de toque, URAs, troncos e extensões de sistema por departamentos municipais, com horários, fusos, idiomas, permissões e relatórios próprios.
25.7.2. Cada departamento poderá possuir horários de expediente, intervalos, feriados, destinos fora de horário, mensagens e regras de atendimento aprovadas.
25.7.3. Serão suportadas filas, grupos de toque, distribuição simultânea ou sequencial, estratégias de atendimento, login e logout de agentes, transbordo, tempo máximo de espera, anúncios e destinos alternativos.
25.7.4. As URAs permitirão menus, DIDs associados, atendimento por horário, entrada inválida, ausência de entrada, encaminhamento direto autorizado e arquivos de áudio em formato compatível.
25.7.5. A solução disponibilizará presença, transferência cega e assistida, captura, estacionamento, conferência, correio de voz, encaminhamento por estado, agenda, contatos, histórico e funções de recepção e supervisão.
25.7.6. Escuta, sussurro, intervenção, gravação e visualização de chamadas serão restritos a perfis autorizados e utilizados conforme finalidade, legislação e trilha de auditoria.
25.7.7. A solução deverá possuir capacidade de integração com ambiente privado de processamento de inteligência artificial para transcrição, sumarização, classificação temática, monitoria assistida da qualidade e pesquisa semântica das chamadas formalmente autorizadas, observadas finalidade, base jurídica, segurança, retenção, controle de acesso e revisão humana.

25.8. PROCESSAMENTO PRIVADO DE CHAMADAS POR INTELIGÊNCIA ARTIFICIAL
25.8.1. A solução deverá integrar a plataforma de telefonia IP/VoIP a ambiente privado de execução de modelos de inteligência artificial por APIs, interfaces documentadas ou camada intermediária de integração, sem dependência de produto, fabricante, modelo, edição comercial ou serviço externo específico.
25.8.2. A camada de inteligência artificial será funcionalmente desacoplada da telefonia. A indisponibilidade de reconhecimento de fala, processamento de

modelos, indexação, pesquisa, banco analítico, armazenamento de transcrições ou dashboards não poderá impedir o estabelecimento, recebimento, transferência, encaminhamento ou continuidade das chamadas.

25.8.3. O fluxo funcional deverá permitir correlação entre chamada, CDR, gravação autorizada, transcrição, metadados, processamento inteligente e resultado estruturado, utilizando identificador único ou mecanismo equivalente que assegure rastreabilidade ponta a ponta.

25.8.4. A conversão de voz para texto será realizada por mecanismo específico de reconhecimento automático de fala, independente do ambiente de execução de modelos de linguagem, com suporte à língua portuguesa e capacidade de processamento das chamadas habilitadas pelo MUNICÍPIO DEMANDANTE.

25.8.5. A transcrição deverá preservar referência temporal suficiente para auditoria e, quando tecnicamente suportado pelo mecanismo utilizado, diferenciação entre interlocutores, segmentação da fala e indicador de confiança do reconhecimento.

25.8.6. O ambiente privado de execução de modelos deverá receber transcrições, metadados e instruções definidas pela aplicação de integração e produzir resultados destinados às finalidades autorizadas pelo MUNICÍPIO DEMANDANTE.

25.8.7. O processamento deverá suportar, no mínimo, sumarização de chamadas, classificação por assunto e subassunto, identificação do motivo do contato, identificação do resultado do atendimento, extração estruturada de informações, monitoria assistida da qualidade, pesquisa semântica e correlação com base institucional de conhecimento.

25.8.8. A solução deverá permitir resultados estruturados em campos predefinidos e formatos processáveis por máquina, incluindo JSON ou formato aberto equivalente, possibilitando validação de esquema, armazenamento, integração, auditoria e utilização em painéis e relatórios.

25.8.9. Os critérios de monitoria da qualidade deverão ser parametrizáveis por unidade, departamento, fila ou serviço e poderão considerar identificação, cumprimento de procedimento, clareza, objetividade, resolutividade, encaminhamento, prestação de informação obrigatória, confirmação de entendimento e encerramento adequado.

25.8.10. Cada avaliação automatizada deverá permitir identificação das evidências textuais que fundamentaram o resultado e deverá admitir revisão, confirmação, alteração ou rejeição por usuário autorizado, com registro da avaliação original e da revisão realizada.

25.8.11. A solução deverá admitir estados explícitos de informação insuficiente, não identificado, não aplicável, baixa confiança ou necessidade de revisão humana, vedada a conversão automática da ausência de informação em conclusão negativa.

25.8.12. A pesquisa semântica deverá permitir representação vetorial dos conteúdos textuais e identificação de chamadas ou trechos semanticamente relacionados, sem dependência exclusiva de coincidência literal de palavras.

25.8.13. A integração com base institucional de conhecimento deverá permitir recuperar documentos ou trechos pertinentes antes do processamento analítico, mantendo referência à fonte utilizada quando a avaliação depender de procedimento, orientação ou conteúdo institucional.

25.8.14. Os modelos de inteligência artificial não serão considerados fonte primária de norma, procedimento ou orientação administrativa. Quando a análise exigir fundamento institucional, o resultado deverá estar relacionado ao conteúdo disponibilizado pelo MUNICÍPIO DEMANDANTE.

25.8.15. A solução deverá suportar execução privada dos modelos e componentes analíticos em infraestrutura dedicada, privada ou sob controle contratual, sem obrigatoriedade de transferência de gravações, transcrições ou metadados para serviços públicos externos de inteligência artificial.

25.8.16. O ambiente de processamento inteligente deverá operar em segmento protegido, sem exposição direta aos terminais de telefonia ou usuários finais, com autenticação, autorização, controle de origem, criptografia, registro de operações, limitação de requisições, gestão de segredos e monitoramento de segurança.

25.8.17. Gravações, transcrições, resumos, classificações, representações vetoriais, metadados e demais dados municipais não poderão ser utilizados pela EXECUTORA ou por terceiros para treinamento, aperfeiçoamento ou enriquecimento de modelos destinados a finalidade estranha ao objeto sem autorização formal e fundamento jurídico aplicável.

25.8.18. A solução deverá possuir filas e mecanismos de controle de processamento que permitam absorver indisponibilidades temporárias da camada analítica e processar posteriormente as chamadas pendentes, observadas as políticas de retenção e proteção de dados.

25.8.19. A capacidade de telefonia e a capacidade de processamento inteligente deverão ser monitoradas separadamente, com indicadores de disponibilidade dos componentes, quantidade de chamadas recebidas para processamento, processadas e pendentes, falhas de transcrição, falhas de integração, tempo de processamento, utilização de recursos e ocorrências encaminhadas para revisão humana.

25.8.20. A solução deverá permitir exportação das transcrições, classificações, resumos, resultados de monitoria, taxonomias, metadados e registros de auditoria em formatos estruturados e documentados, preservando portabilidade e transição para solução sucessora.

25.8.21. A habilitação das funções de gravação, transcrição e análise dependerá de política formal do MUNICÍPIO DEMANDANTE que identifique finalidade, escopo, filas ou serviços abrangidos, perfis de acesso, retenção, descarte e demais controles aplicáveis ao tratamento dos dados.

25.8.22. A solução deverá permitir a definição de limiar mínimo de confiança, parametrizável por finalidade de análise, abaixo do qual o resultado será obrigatoriamente encaminhado à fila de revisão humana antes de qualquer uso administrativo, sendo vedada a utilização de resultado abaixo do limiar sem revisão e confirmação expressa.

25.8.23. Toda atualização de versão de modelo de linguagem ou de reconhecimento de fala utilizada em produção deverá ser precedida de validação técnica documentada, comparando amostra de resultados entre a versão anterior e a nova versão, com aprovação do MUNICÍPIO DEMANDANTE antes da promoção a produção. O identificador de versão do modelo utilizado em cada processamento deverá ser registrado nos metadados de que trata o item 25.8.3, para fins de auditoria e rastreabilidade histórica.

25.8.24. A EXECUTORA deverá apresentar, na fase de homologação e periodicamente durante a execução, relatório de desempenho do reconhecimento de fala e da classificação automática segmentado por variação linguística regional representativa da população atendida, permitindo ao MUNICÍPIO DEMANDANTE identificar e tratar eventual desempenho desigual entre grupos de falantes, sem exigir coleta de atributos pessoais desnecessários à finalidade de avaliação.

25.8.25. A arquitetura de integração entre a transcrição e o ambiente de modelos de linguagem deverá adotar controles de segurança específicos contra manipulação do conteúdo transcrito com o objetivo de alterar o comportamento do modelo, contornar as instruções da aplicação ou extrair informação além do escopo autorizado da chamada, devendo a EXECUTORA descrever, no Projeto Executivo, os controles adotados e os testes realizados para essa finalidade.

25.8.26. Quando a chamada for submetida a processamento por inteligência artificial nos termos desta seção, o cidadão deverá ser informado dessa condição em momento e forma compatíveis com a informação prevista para gravação de chamadas, quando aplicável, sem prejuízo do direito a informações e demais garantias previstas na legislação de proteção de dados pessoais.

25.9. ARQUITETURA E ENGENHARIA DE TRÁFEGO DA TELEFONIA

25.9.1. A arquitetura de destino utilizará sinalização SIP, negociação de sessão por SDP, transporte de mídia RTP/RTCP, eventos DTMF por padrão interoperável e codecs G.711 A-law e ao menos um codec de menor consumo de banda, admitidos padrões equivalentes que preservem interoperabilidade, qualidade e ausência de dependência proprietária.

25.9.2. Os troncos SIP e os controladores de borda deverão suportar IPv4 e IPv6, TLS 1.2 ou superior, SRTP, certificados administráveis, normalização de sinalização, proteção contra mensagens malformadas, limitação de sessões, controle de topologia, tradução de numeração e alta disponibilidade.
25.9.3. O projeto executivo deverá apresentar memória de engenharia de tráfego com chamadas na hora de maior movimento, tentativas de chamada, duração média, simultaneidade, taxa de completamento, taxa de bloqueio e margem de crescimento. A capacidade ativada deverá manter probabilidade de bloqueio igual ou inferior a 1% e permitir expansão progressiva até o limite de simultaneidade dimensionado no projeto sem indisponibilidade prolongada.
25.9.4. A solução deverá medir e disponibilizar, no mínimo, ASR, ACD, PDD, chamadas completadas, chamadas rejeitadas, códigos de resposta SIP, ocupação simultânea, utilização por categoria, falhas de registro, jitter, perda, latência, fator R ou MOS estimado e eventos de comutação, com filtros por período, unidade, ramal, tronco e prestadora.
25.9.5. Chamadas para números de emergência, serviços de utilidade pública e números especiais deverão preservar identificação de origem, encaminhamento correto, localização administrativa do ponto originador quando tecnicamente aplicável e prioridade compatível com a criticidade do serviço.
25.9.6. A migração para 100% VoIP deverá eliminar dependências permanentes de gateways TDM, fluxos E1 e sinalizações legadas. Gateways de transição somente poderão ser utilizados durante coexistência controlada, sem gerar cobrança recorrente após o aceite da arquitetura de destino.

25.10. TERMINAIS LEGADOS E SOFTPHONES

25.10.1. Os aparelhos legados disponibilizados pela Prefeitura serão submetidos a inventário e avaliação de compatibilidade com a plataforma implantada, a conexão em nuvem, o provisionamento centralizado, os protocolos de segurança e os requisitos de qualidade. O reaproveitamento dependerá de interoperabilidade comprovada e homologação técnica documentada, sem obrigação de manter terminal inseguro, obsoleto ou incompatível.
25.10.2. A atividade compreenderá provisionamento, configuração, atualização de parâmetros, registro seguro, associação ao usuário e ao ramal, integração à VLAN de voz e ao plano de numeração, testes e homologação.
25.10.3. A EXECUTORA apresentará relatório de compatibilidade e de condições técnicas dos aparelhos inventariados, com identificação do endereço, unidade, usuário, ramal, versão, protocolo, resultado dos testes e medidas operacionais aplicáveis.
25.10.4. Os softphones serão provisionados centralmente, com autenticação, revogação, inventário, políticas de uso, proteção de credenciais e suporte aos sistemas operacionais e periféricos homologados.

25.11. TERMINAIS E PROVISIONAMENTO

25.11.1. Os terminais novos deverão suportar os protocolos, codecs, mecanismos de segurança, provisionamento, VLAN, QoS e requisitos de interoperabilidade definidos nesta especificação e possuir documentação técnica suficiente para comprovação de compatibilidade e suporte durante a vigência.
25.11.2. O provisionamento será centralizado e seguro, com inventário por MAC, número de série, unidade, usuário, ramal, firmware, endereço, VLAN, estado e data da última comunicação.
25.11.3. Senhas administrativas e de autenticação serão individualizadas, complexas e rotacionadas, vedados padrões de fábrica e credenciais comuns entre terminais.
25.11.4. Firmware de terminais será atualizado de forma controlada e compatível, com piloto, janela, reversão e registro da versão instalada.
25.11.5. Os terminais utilizarão VLAN de voz, QoS, NTP, codecs aprovados, autenticação segura, TLS e SRTP quando suportados, desativação de serviços desnecessários e restrição de acesso administrativo.
25.11.6. Serão disponibilizados cliente web e aplicações de usuário para computadores e dispositivos móveis compatíveis com os sistemas operacionais adotados pela Administração, com provisionamento, revogação, atualização e suporte durante a vigência, sem dependência de marca específica de sistema operacional.
25.11.7. Os softphones dimensionados no projeto serão vinculados a usuários e ramais ativos, com controle de dispositivos, revogação de sessões, autenticação, proteção de credenciais e inventário.
25.11.8. Dispositivo perdido, comprometido, desligado ou não autorizado terá sessão e credenciais revogadas imediatamente após comunicação ou detecção.

25.12. INTERVENÇÕES FÍSICAS E LIMITES DO ESCOPO DA TELEFONIA

25.12.1. Ajustes pontuais de conexão, conectorização, patching e correções locais indispensáveis à ativação ou ao restabelecimento do ramal poderão integrar o serviço. A implantação de novos pontos, remanejamentos físicos extensos, obras civis e ampliação de cabeamento estruturado somente integrarão o objeto quando expressamente quantificados, precificados e autorizados por Ordem de Serviço.

25.13. QUALIDADE DE SERVIÇO DA TELEFONIA

25.13.1. O tráfego de voz utilizará VLAN própria. A classificação, a preservação das marcações, as filas prioritárias e o controle de admissão observarão os itens 25.29.1 a 25.29.6, conforme a criticidade das unidades, preservadas a segregação e a segurança dos demais domínios da Infovia.
25.13.2. Para planejamento, teste e fiscalização serão adotadas metas de latência unidirecional de até 100 milissegundos no domínio metropolitano e limite máximo de até 150 milissegundos nos percursos completos, variação de atraso de até 30 milissegundos e perda de pacotes de até 1%, observados codec, percurso, criptografia, rede pública e metodologia aprovada.
25.13.3. O monitoramento da telefonia pelo NOC observará o item 25.29.7, com as metas de qualidade estabelecidas no item 25.13.2.

25.14. APIS E INTEGRAÇÕES DE VOZ

25.14.1. A plataforma deverá disponibilizar APIs documentadas para controle de chamadas, consulta de estados e administração autorizada, utilizando REST, WebSocket, JSON, OpenAPI ou padrões equivalentes, com autenticação forte, tokens revogáveis, segregação de permissões, registro de auditoria e documentação suficiente à integração com sistemas municipais.
25.14.2. As APIs serão disponibilizadas para integrações autorizadas com Service Desk, BI, automação de usuários, atendimento digital, diretórios, sistemas corporativos e aplicações futuras, sem cobrança adicional de licença já abrangida.
25.14.3. Cada integração utilizará aplicação ou principal de serviço próprio, escopo mínimo, segredo individual, expiração, rotação, trilha de auditoria e restrição de origem.
25.14.4. A documentação entregará endpoints, versões, escopos, fluxos de autenticação, campos, limites, tratamento de erro, eventos, dependências, testes e procedimento de revogação.
25.14.5. Alteração de API, descontinuidade, mudança de versão ou incompatibilidade será comunicada e tratada pela EXECUTORA, preservando as integrações contratadas ou disponibilizando mecanismo equivalente.

25.14.6. Desenvolvimento de integração específica dependerá de escopo e Ordem de Serviço quando não estiver expressamente incluído, mas a disponibilidade, licenciamento e documentação das APIs integrarão o serviço base.

25.15. LICENCIAMENTO E TITULARIDADE DA TELEFONIA

25.15.1. O licenciamento necessário à operação deverá permanecer ativo durante toda a vigência, sem redução de funcionalidades, capacidade ou níveis de serviço, sem interrupção por falta de renovação e sem transferência para conta não autorizada.

25.15.2. A chave de licença, a conta principal, o endereço eletrônico de titularidade, o FQDN, os certificados, os repositórios de backup e as credenciais institucionais serão vinculados a contas corporativas indicadas pelo MUNICÍPIO DEMANDANTE, vedada dependência exclusiva de conta pessoal ou de colaborador da EXECUTORA.

25.15.3. A EXECUTORA assumirá, nos preços ofertados, renovações, atualizações, alterações de política comercial do fornecedor tecnológico e demais custos necessários para manter a capacidade e as funcionalidades contratadas durante toda a vigência.

25.15.4. A plataforma deverá assegurar segregação lógica dos dados, configurações, credenciais administrativas e armazenamento do Município em relação a outros clientes, preservando isolamento, segurança, rastreabilidade e controle institucional, sem imposição de modalidade comercial específica de hospedagem.

25.15.5. Não serão admitidas versões experimentais, prévias, candidatas a lançamento, sem suporte vigente ou com fim de vida anunciado para período incompatível com o cronograma de implantação e a vigência contratual.

25.16. SEGURANÇA E REGISTROS DA TELEFONIA

25.16.1. Os controles de acesso, criptografia, credenciais e auditoria da plataforma observarão os itens 25.17.1 a 25.17.4, 25.17.7, 25.17.8 e 25.17.12.

25.16.2. A prevenção e a resposta a fraude e abuso observarão os itens 25.17.5 e 25.17.6.

25.16.3. A geração, o conteúdo, a exportação, a conciliação e a proteção dos CDR observarão os itens 25.28.1 a 25.28.3 e 25.28.10, conforme a finalidade e a legislação aplicável.

25.16.4. Gravações autorizadas, mensagens, contatos, relatórios e dados pessoais deverão observar finalidade, base de tratamento, acesso, retenção, segurança, descarte e auditoria definidos pelo MUNICÍPIO DEMANDANTE.

25.17. PROTEÇÃO DA PLATAFORMA DE VOZ

25.17.1. O acesso administrativo utilizará autenticação multifator, contas nominativas, menor privilégio, segregação de funções e papéis compatíveis com a organização por departamentos.

25.17.2. As atribuições municipais serão mapeadas a perfis de acesso compatíveis com a solução implantada, preservando separação entre administração técnica, gestão organizacional, supervisão de filas, acesso a relatórios e acesso a gravações.

25.17.3. Credenciais compartilhadas serão vedadas, ressalvada conta técnica de emergência mantida em cofre, com uso controlado, rotação, registro e comunicação à fiscalização.

25.17.4. O acesso administrativo remoto será restrito por VPN, rede confiável, lista de endereços autorizados ou controle equivalente, com logs e alertas de tentativa indevida. O suporte remoto utilizará autenticação forte, credenciais individuais, menor privilégio, registro de sessão e trilha de auditoria, origem autorizada, janela de mudança quando aplicável e revogação imediata de acessos incompatíveis com a função ou o contrato.

25.17.5. A solução deverá manter proteção contra força bruta, enumeração de extensões, registro SIP indevido, chamadas fraudulentas, destinos restritos, consumo anômalo e abuso de credenciais. Serão mantidos alertas e resposta integrada ao SOC.

25.17.6. As regras de saída limitarão destinos, categorias, países, horários e perfis conforme política municipal, com bloqueio padrão para destinos não autorizados.

25.17.7. A sinalização utilizará TLS e a mídia utilizará SRTP quando suportadas de ponta a ponta pelos terminais, SBCs e prestadores, sendo qualquer exceção documentada, autorizada e acompanhada de medida compensatória.

25.17.8. Certificados digitais deverão ser válidos, monitorados e renovados antes do vencimento, sem uso de certificados expirados ou não confiáveis em produção.

25.17.9. Funções de manipulação automática de SIP em dispositivos intermediários que causem alteração indevida de sinalização deverão ser desabilitadas ou configuradas de modo compatível, sendo firewall, NAT, portas e fluxos validados por testes reproduzíveis de conectividade e chamadas.

25.17.10. As portas e faixas de rede necessárias serão documentadas no projeto executivo, limitadas ao estritamente necessário e validadas após cada alteração relevante, considerando SIP, RTP, túnel, HTTPS, provisionamento, push e atualizações.

25.17.11. A plataforma permanecerá em zona de segurança própria e não terá acesso irrestrito a sub-redes sensíveis, servidores ou sistemas municipais não necessários ao objeto.

25.17.12. Tokens de API, chaves, segredos, certificados e senhas serão armazenados de forma protegida, rotacionados e revogados no desligamento de usuário, aplicação ou prestador.

25.18. CONFORMIDADE REGULATÓRIA E REMISSÕES DE SEGURANÇA DA TELEFONIA

25.18.1. A autorização e a proteção das gravações observarão os itens 25.28.8 e 25.28.9, sem habilitação indiscriminada.

25.18.2. A solução deverá manter conformidade com a regulamentação da Anatel durante toda a vigência, inclusive quanto à autenticação e identificação da origem das chamadas, portabilidade, certificação de equipamentos, combate a fraude e rastreabilidade, incorporando as adequações regulatórias obrigatórias ao serviço contratado.

25.18.3. O acesso remoto de suporte observará os controles administrativos dos itens 25.17.1 a 25.17.4.

25.19. CONTINUIDADE E RECUPERAÇÃO DA TELEFONIA

25.19.1. A plataforma deverá operar em infraestrutura de nuvem ou data center compatível com os requisitos contratuais, com segregação lógica dos dados, configurações, credenciais e administração do Município em relação a outros clientes, alta disponibilidade em domínios de falha independentes, monitoramento contínuo, backup protegido e procedimentos documentados de recuperação e retorno.

25.19.2. O núcleo da plataforma e os troncos SIP observarão disponibilidade mensal mínima de 99,95%, excluídas exclusivamente as janelas previamente autorizadas e as hipóteses de exclusão objetivamente comprovadas no IMR.

25.19.3. Os objetivos de recuperação e de perda máxima de configurações administrativas observarão os valores e a comprovação estabelecidos no item 25.20.6.

25.19.4. Endereçamento, nomes, certificados, DNS, NTP, firewall, rotas, portas, políticas, integrações e dependências deverão constar do Projeto Executivo da Telefonia.

25.20. ALTA DISPONIBILIDADE BACKUP E RECUPERAÇÃO

25.20.1. A arquitetura adotará mecanismos de alta disponibilidade distribuídos em domínios de falha independentes, com comutação, recuperação e retorno compatíveis com os objetivos de continuidade e perda máxima de dados definidos nesta especificação, sem imposição de topologia proprietária ou modalidade comercial específica.

25.20.2. Os ambientes principal e de contingência deverão possuir independência suficiente de host, armazenamento, energia, zona ou localidade e demais dependências imediatas, de modo a evitar ponto único de falha e permitir comutação e recuperação comprovadas por teste.

25.20.3. O mecanismo de continuidade deverá monitorar os serviços críticos do núcleo de telefonia, detectar indisponibilidades relevantes e executar ou permitir comutação controlada para ambiente de contingência, preservando os requisitos de chamadas, administração, integrações e registros.

25.20.4. A comutação deverá impedir concorrência indevida entre ambientes, preservar consistência de configuração, tratar atualização de resolução de nomes e rotas quando aplicável e prever retorno documentado à condição normal.

25.20.5. Serão realizados testes trimestrais de failover e retorno, além de teste semestral de restauração integral a partir de backup, com registros de tempo, perda de dados, chamadas de validação e correções.

25.20.6. O RTO máximo será de 15 minutos e o RPO de configurações administrativas será de uma hora, comprovados em aceite e acompanhados pelo IMR.

25.20.7. Os backups serão criptografados, armazenados fora da instância produtiva e enviados a repositório aprovado, por protocolo seguro de transferência, compartilhamento de arquivos autenticado, armazenamento de objetos ou mecanismo equivalente que assegure confidencialidade, integridade, versionamento e restauração.

25.20.8. A rotina mínima compreenderá backup diário, cópia anterior a mudança relevante, retenção de pelo menos 30 cópias diárias e 12 cópias mensais, salvo política superior definida antes da proposta. Para cumprir o RPO de uma hora das configurações administrativas, a solução manterá cópias incrementais, registros recuperáveis de alterações ou mecanismo equivalente com frequência suficiente. Replicação não substituirá backup protegido. O teste de restauração comprovará o ponto recuperável e a perda efetiva de configurações, além do prazo de recuperação.

25.20.9. Falha de backup, restauração, replicação ou teste de failover gerará chamado automático, correção prioritária e registro no relatório mensal.

25.21. MOBILIZAÇÃO DA TELEFONIA

25.21.1. O Projeto Executivo da Telefonia deverá ser apresentado em até 10 dias corridos da Ordem de Serviço.

25.21.2. O inventário, a validação de tráfego, o plano de numeração, o desenho de migração e o piloto deverão ser concluídos em até 30 dias corridos da Ordem de Serviço.

25.21.3. A primeira ativação completa deverá ser concluída em até 90 dias corridos da Ordem de Serviço, ressalvadas dependências de portabilidade ou autorizações de terceiros devidamente comprovadas, sem afastar a obrigação de planejamento preventivo e mitigação.

25.21.4. A ativação de novos ramais e softphones dentro da capacidade instalada ocorrerá em até 10 dias úteis da Ordem de Serviço.

25.21.5. A ampliação de faixas de canais ou a implantação em nova unidade ocorrerá em até 30 dias corridos da Ordem de Serviço, observadas as dependências técnicas formalmente registradas.

25.21.6. A implantação e a migração serão executadas por piloto em unidades de perfis distintos e por ondas, abrangendo inventário, backup validado, mapa de correspondência entre ambientes, coexistência temporária, portabilidade por janelas controladas, critérios de avanço, comunicação, plano de retorno, treinamento, documentação e operação assistida por no mínimo 30 dias após a migração geral.

25.22. INTEGRAÇÃO DAS ETAPAS DE IMPLANTAÇÃO DA TELEFONIA

25.22.1. A sequência de implantação e migração observará o item 25.21.6. A operação assistida será verificada conforme o item 25.26.8, e o aceite documental observará o item 25.26.9.

25.23. SUPORTE E INCIDENTES DA TELEFONIA

25.23.1. O fluxo integrado de atendimento, registro e escalonamento da telefonia observará os itens 25.24.1 e 25.24.3 e a regra comum do item 15.5.

25.23.2. Incidentes críticos com indisponibilidade generalizada, perda de chamadas essenciais, falha dos dois caminhos ou comprometimento de segurança serão atendidos no regime 24x7 do item 25.24.1, conforme os tempos do IMR.

25.23.3. Na transição de saída, a EXECUTORA deverá cooperar com a sucessora e entregar numeração, usuários, ramais, filas, unidades de resposta audível, regras, CDR, gravações autorizadas, inventário, configurações, documentação e procedimentos necessários à continuidade.

25.24. OPERAÇÃO SUPORTE E MANUTENÇÃO DA TELEFONIA

25.24.1. A executora prestará suporte especializado N2/N3 da telefonia, integrado ao N1 do InPACTA e ao sistema de chamados da Infovia. Manterá atendimento técnico 24x7 para incidentes críticos, gestão de problemas, manutenção, atualização, relatórios e indicadores, com interlocutor responsável pela solução técnica e pelo acionamento de sua cadeia de prestadoras. O atendimento será integrado à Central de Situação do InPACTA, ao NOC e ao SOC da executora, com registro único ou protocolos correlacionados, comunicação, evidências e acompanhamento até a solução.

25.24.2. A parcela de telefonia incluirá gestão operacional de ponta a ponta durante o período em que estiver ativada, abrangendo plataforma, troncos SIP, controladores de borda, numeração, portabilidade, serviços 0800 e especiais, ramais, softphones, integrações, registros de chamadas, monitoramento, suporte e coordenação das prestadoras e subcontratadas envolvidas.

25.24.3. O N1 do InPACTA receberá incidentes, requisições e solicitações de configuração pelos canais de atendimento definidos no projeto. O registro conterá protocolo, data e hora, solicitante, unidade, serviço afetado, severidade, ações, escalonamentos, causa, solução, evidências e aceite do encerramento. As configurações técnicas e a correção de falhas caberão à executora, observados o acionamento direto para incidentes críticos e a preservação dos prazos previstos no item 15.5.

25.24.4. A manutenção preventiva compreenderá, no mínimo, revisão mensal da saúde da plataforma, alta disponibilidade, troncos, registros, certificados, cópias de segurança, capacidade, filas, alarmes, integrações, segurança, versões suportadas, consistência dos CDR e situação dos terminais e componentes críticos incluídos no inventário.

25.24.5. A manutenção corretiva será realizada remotamente ou no local, conforme a natureza da falha, e compreenderá diagnóstico, solução de contorno, correção de configuração, atualização corretiva, restauração, substituição de componentes de responsabilidade da contratada, testes e confirmação do restabelecimento.

25.24.6. Nos aparelhos legados compatíveis disponibilizados pelo Município, estarão incluídos inventário, diagnóstico, provisionamento, reconfiguração, testes e correções tecnicamente viáveis. Reparos físicos e substituições definitivas dependerão da disponibilidade de peças, da economicidade e da delimitação estabelecida na especificação do projeto, vedada obrigação aberta de manutenção de equipamento obsoleto, sem suporte ou incompatível.

25.24.7. Para posições críticas, o Termo de Referência poderá prever banco técnico de equipamentos equivalentes para substituição temporária, sem transferência de propriedade, enquanto o aparelho municipal estiver em diagnóstico ou reparo. O quantitativo, a distribuição, os prazos e a composição do custo deverão ser definidos após o inventário.
25.24.8. As operações rotineiras de criação, exclusão, bloqueio, desbloqueio e alteração de ramal, usuário, perfil, grupo, fila, unidade de resposta audível, permissão, desvio, rota, regra de menor custo, horário e destino deverão integrar o preço do ramal ou do núcleo ativo, sem cobrança individual por chamado.
25.24.9. As alterações lógicas rotineiras deverão ser concluídas em até 48 horas úteis, salvo prazo inferior estabelecido pelo Instrumento de Medição de Resultado, criticidade do serviço, necessidade de portabilidade, janela autorizada ou dependência comprovada de terceiro. Mudanças em massa, projetos de reorganização e novas integrações dependerão de Ordem de Serviço e planejamento específico.
25.24.10. A contratada será responsável pela abertura, acompanhamento, escalonamento e encerramento dos chamados junto às prestadoras de telefonia e demais terceiros utilizados, sem transferir à Administração a coordenação operacional ou a investigação da causa raiz.
25.24.11. Os incidentes serão classificados, no mínimo, em crítico, significativo e normal, considerando abrangência, indisponibilidade total ou parcial, impacto sobre serviços essenciais, existência de contingência, quantidade de usuários, números públicos afetados e risco à segurança. Os tempos de resposta, recuperação remota, atendimento local e solução serão definidos na especificação do projeto e no Instrumento de Medição de Resultado.
25.24.12. A reabertura do mesmo incidente ou a recorrência tecnicamente correlata em até 48 horas deverá elevar sua prioridade, preservar o histórico do chamado e acionar gestão de problemas, análise de causa raiz e plano de ação corretiva definitiva.
25.24.13. O relatório mensal da telefonia apresentará níveis de atendimento, disponibilidade, tempos por severidade, reincidências, causas, alterações executadas, falhas de terceiros, utilização de contingência, terminais indisponíveis, substituições temporárias, manutenção preventiva, capacidade, segurança e plano de melhoria.

25.25. ENSAIOS DA TELEFONIA

25.25.1. O escopo do piloto e as funcionalidades a validar observarão o item 25.26.2.
25.25.2. Os testes deverão comprovar alta disponibilidade, comutação dos caminhos SIP, recuperação do núcleo, segurança, qualidade de voz, ocupação de canais, CDR, portabilidade, faturamento, monitoramento, backup e retorno.
25.25.3. A homologação da portabilidade por lote observará o item 25.26.5.
25.25.4. A documentação e as condições de aceite final observarão o item 25.26.9.
25.25.5. Quando a Ordem de Serviço abranger processamento inteligente das chamadas, o aceite deverá comprovar integração entre telefonia, CDR, gravação autorizada, reconhecimento automático de fala, ambiente privado de execução de modelos, saída estruturada, rastreabilidade, limiar de confiança, revisão humana obrigatória abaixo do limiar, governança e registro de versões dos modelos, avaliação de desempenho do reconhecimento de fala, controles contra manipulação do conteúdo transcrito, informação ao cidadão, segurança, exportação e continuidade da telefonia durante indisponibilidade da camada analítica.

25.26. HOMOLOGAÇÃO DA OPERAÇÃO DA TELEFONIA

25.26.1. Após a emissão da Ordem de Serviço de telefonia, a contratada apresentará projeto executivo com arquitetura, domínios de falha, capacidades, caminhos SIP, prestadores autorizados, integrações, VLANs, qualidade de serviço, controladores de borda, numeração, plano de migração, cronograma, responsáveis, dependências e critérios de retorno, observando o prazo de mobilização definido na especificação do projeto.
25.26.2. O piloto abrangerá unidades de perfis distintos e validará chamadas internas, fixas, móveis, longa distância, internacionais quando aplicáveis e autorizadas, 0800, números de utilidade pública, filas, unidades de resposta audível, transferência, conferência, transbordo, softphones, aparelhos legados interconectados e integrações.
25.26.3. Os testes de continuidade provocarão falhas controladas da instância principal, de um caminho SIP, de controlador de borda e de acesso de dados, verificando tempo de detecção, comutação, restabelecimento de novas chamadas, preservação da numeração, alarmes, registros e retorno à condição normal.
25.26.4. Os testes de qualidade medirão latência, variação de atraso, perda, ocupação de canais, registro SIP, fator R ou MOS estimado, tempo de estabelecimento, taxa de atendimento, duração média, códigos de resposta SIP, estabilidade e comportamento durante pico e contingência, com metodologia, amostragem, horários e resultados reproduzíveis.
25.26.5. A portabilidade será homologada por lote de números, com chamadas originadas e recebidas, identificação correta, serviços 0800, números especiais, emergência, encaminhamentos e plano de retorno. Nenhum grupo crítico será desligado antes da confirmação do aceite.
25.26.6. O faturamento será testado por amostragem e conciliação entre ordens de serviço, inventário, CDR, faixas de canais, ramais ativos, números, tráfego, tarifas, impostos e documento fiscal, vedada cobrança por chamadas internas ou recursos não ativados.
25.26.7. A gravação de chamadas, quando autorizada, será testada quanto à informação, acesso, criptografia, integridade, retenção, exportação, auditoria e descarte. A ausência de autorização impedirá sua ativação.
25.26.8. O aceite da operação assistida prevista no item 25.21.6 verificará o cumprimento do período mínimo e a correção de regras, filas, URAs, terminais, permissões, integrações, faturamento, qualidade e documentação, sem prejuízo do suporte continuado.
25.26.9. O aceite final dependerá da entrega do inventário, diagramas, credenciais institucionais, backups, procedimentos, relatórios de testes, registros de portabilidade, matriz de responsabilidades, evidências de treinamento e plano de continuidade e transição. A homologação será formalizada em termo próprio.
25.26.10. Antes do aceite operacional serão testados os canais de atendimento, a atuação do N1 do InPACTA, o escalonamento ao N2/N3 da executora, a classificação por severidade, o atendimento remoto, o acionamento local e a integração com prestadoras. Os testes comprovarão histórico compartilhado, preservação dos prazos, acesso da Central de Situação aos indicadores e acionamento técnico direto para incidentes críticos.
25.26.11. Serão executadas amostras de criação, alteração, bloqueio, desbloqueio e exclusão de ramais, usuários, filas, unidades de resposta audível, permissões, desvios e rotas, verificando prazo, autorização, auditoria, resultado e ausência de cobrança paralela.
25.26.12. O plano de manutenção preventiva será homologado com checklist, periodicidade, responsáveis, fontes de evidência, tratamento de alertas, correções, segurança, backup, capacidade e relatório mensal. Incidentes recorrentes deverão demonstrar fluxo de gestão de problemas e análise de causa raiz.
25.26.13. Quando houver banco temporário de equipamentos, o aceite verificará disponibilidade, compatibilidade funcional, inventário, cadeia de custódia, prazo de mobilização, higienização, configuração segura, devolução e ausência de transferência patrimonial.
25.26.14. Intervenções físicas incluídas no objeto serão aceitas somente após Ordem de Serviço, identificação do ponto, materiais empregados, teste, etiquetagem, atualização do inventário, registro fotográfico quando pertinente e validação da unidade.
25.26.15. Quando o processamento inteligente estiver abrangido pela Ordem de Serviço, o aceite deverá validar o limiar mínimo de confiança por finalidade, o encaminhamento automático dos resultados abaixo do limiar para revisão humana e o bloqueio de uso administrativo antes da confirmação expressa.

25.26.16. O aceite deverá validar o registro da versão dos modelos de linguagem e de reconhecimento de fala e o procedimento documentado de comparação entre versões antes de atualização em produção.
25.26.17. O reconhecimento de fala e a classificação automatizada serão avaliados em amostra representativa das variações linguísticas regionais relevantes ao atendimento, com registro da metodologia, dos resultados, das limitações identificadas e das medidas corretivas quando aplicáveis.
25.26.18. Serão realizados testes controlados de resiliência a manipulação do conteúdo transcrito, verificando que instruções contidas na fala não permitam alterar indevidamente o comportamento do modelo, exceder o escopo autorizado ou acessar conteúdo institucional não pertinente à chamada.
25.26.19. O aceite verificará a implementação do aviso ao cidadão quando houver processamento por inteligência artificial, conforme a política aprovada pela Administração e a legislação aplicável.

25.27. MEDIÇÃO E CONCILIAÇÃO DA TELEFONIA

25.27.1. Chamadas internacionais serão cobradas por minuto e destino ou região tarifária. Serviços 0800, números especiais, utilidade pública e demais componentes específicos serão medidos separadamente quando aplicável.
25.27.2. Chamadas internas entre ramais do sistema não serão tarifadas por minuto como tráfego da rede pública.
25.27.3. A medição mensal conciliará Ordem de Serviço, inventário, ramais ativos, softphones, faixas de canais, números, CDR, tarifas, impostos, eventos, SLA e documento fiscal.
25.27.4. A cobrança do núcleo da plataforma, dos ramais, das faixas de canais e dos serviços recorrentes somente começará após a ativação e o aceite. A implantação e a portabilidade serão pagas após a homologação do respectivo entregável.
25.27.5. A planilha de preços deverá separar implantação, núcleo da plataforma, ramal ativo, faixa de canais, tráfego, serviços especiais, portabilidade, treinamento e demais unidades mensuráveis, impedindo sobreposição ou cobrança duplicada.
25.27.6. Quando houver cobrança específica pela camada de processamento inteligente, a planilha de preços deverá identificar de forma separada e auditável as unidades de medição relacionadas a processamento, transcrição, armazenamento e demais recursos efetivamente contratados, vedada cobrança duplicada com licenças, ramais, chamadas, gravações ou infraestrutura já remunerados em outro item.

25.28. CDR RELATÓRIOS GRAVAÇÕES E AUDITORIA

25.28.1. O mecanismo de CDR será habilitado e configurado para gerar arquivos, registros individuais ou transmissão por interface documentada, conforme integração definida, sem impedir exportação integral dos dados.
25.28.2. Os CDR conterão, no mínimo, identificadores de chamada, origem, destino, número discado, data e horários de início, atendimento e término, duração, motivo de encerramento, rota, tronco, cadeia de transferência, categoria, tarifa e custo quando aplicável. Para os componentes tarifados, serão discriminados duração real, duração tarifada, preço unitário e valor, com proteção segundo a finalidade e a legislação aplicável.
25.28.3. Os CDR serão conciliados com inventário, Ordem de Serviço, portabilidade, tarifas, faturas e registros do NOC, preservando rastreabilidade de chamadas transferidas e transbordadas.
25.28.4. A plataforma fornecerá logs de chamadas, chats quando utilizados, ações administrativas, regras de entrada, filas, agentes, grupos, extensões, chamadas abandonadas, tempos de espera e duração.
25.28.5. Relatórios programados serão disponibilizados em formato visual e CSV ou formato aberto equivalente, apto a integração com ferramenta de inteligência de negócios.
25.28.6. O relatório mensal incluirá ocupação das chamadas simultâneas, percentis, picos, horários de maior movimento, ASR, ACD, PDD, chamadas completadas, rejeitadas, abandonadas, falhas por código SIP e tendência de capacidade.
25.28.7. Alertas de capacidade serão gerados quando a ocupação atingir 70%, 80% e 90% da faixa ativada, acompanhados de análise de tendência, causa, risco de bloqueio e providência.
25.28.8. A gravação de chamadas permanecerá desabilitada por padrão e será ativada apenas por política formal, por usuário, fila, grupo ou tipo de chamada, com informação aos envolvidos quando aplicável. A política dependerá de finalidade formalmente definida e autorização administrativa.
25.28.9. Gravações autorizadas serão armazenadas em repositório protegido, com acesso restrito, logs, criptografia, retenção limitada por categoria, descarte seguro, monitoramento de capacidade e exportação.
25.28.10. Usuários não poderão excluir gravações, alterar CDR ou apagar registros de auditoria sem autorização expressa e controle de privilégio.

25.29. REDE DE VOZ E QUALIDADE DE SERVIÇO

25.29.1. A rede deverá preservar a qualidade de serviço da telefonia desde o terminal, controlador de borda de sessão ou ponto de ingresso até a plataforma corporativa de telefonia e os troncos SIP, abrangendo LAN sob responsabilidade definida, CPE, MPLS, proteção, borda, Internet e infraestrutura de hospedagem.
25.29.2. A mídia RTP será classificada com DSCP EF e a sinalização SIP com classe separada, CS5 ou classificação tecnicamente equivalente, admitida classificação equivalente tecnicamente justificada e aprovada.
25.29.3. As marcações serão preservadas fim a fim, submetidas a policiamento na borda e associadas a filas prioritárias com largura de banda suficiente, vedada remarcação indiscriminada ou competição com tráfego de menor prioridade.
25.29.4. A capacidade de voz será calculada por codec, intervalo de pacotização, cabeçalhos IP, UDP, RTP, criptografia, encapsulamento, redundância, chamadas simultâneas e margem operacional.
25.29.5. O projeto executivo demonstrará a banda reservada por unidade, enlace e sentido para a simultaneidade dimensionada, preservando as aplicações críticas da Infovia.
25.29.6. A admissão de novas chamadas deverá respeitar a capacidade disponível, prevenindo congestionamento da classe de voz e bloqueando expansão automática que ultrapasse a banda ou a licença ativada.
25.29.7. O NOC monitorará latência, jitter, perda, descarte em filas, utilização da classe de voz, registros SIP, RTP, ocupação simultânea, falhas de registro e qualidade percebida. O acompanhamento abrangerá também disponibilidade, caminhos ativos e eventos de comutação.
25.29.8. A operação utilizará baselines por unidade e horário, identificará deterioração progressiva e acionará correção antes do descumprimento do SLA.
25.29.9. A rota secundária dos nodes C1 a C4 deverá preservar a classe de voz e a capacidade mínima necessária aos serviços prioritários durante contingência, observados o perfil GPON dos C1/C2 e a capacidade integral das duas rotas dos C3/C4.
25.29.10. Alterações de codec, pacotização, criptografia, tronco, SBC, rota, QoS ou firewall serão testadas quanto a qualidade, interoperabilidade e consumo de banda antes de implantação ampla.
25.29.11. Em teste controlado, a qualidade objetiva deverá atingir MOS-LQO igual ou superior a 4,0 nas condições de referência para os codecs aprovados, ou resultado equivalente segundo metodologia reconhecida, sem afastar as metas de latência, jitter e perda.

25.29.12. O relatório mensal apresentará, por domínio e unidade crítica, desempenho da voz, eventos de degradação, causas, correções, capacidade e tendência.

25.30. DIMENSIONAMENTO E CAPACIDADE DA TELEFONIA

25.30.1. A telefonia será dimensionada pelo inventário e pelo estudo de tráfego de cada projeto. A Ordem de Serviço definirá as unidades, a capacidade licenciada e a ativação efetivamente necessárias, após validação administrativa e disponibilidade de recursos.

25.30.2. Os quantitativos e as faixas de capacidade orientarão o planejamento, a escalabilidade, o dimensionamento e a avaliação da capacidade técnica de atendimento. A pesquisa de preços e a avaliação econômica de eventual execução municipal ocorrerão no procedimento próprio do projeto. O faturamento dependerá de instrumento eficaz, Ordem de Serviço, ativação, testes, homologação e aceite da unidade correspondente.

25.30.3. A ativação inicial e a expansão dos ramais observarão o dimensionamento e a autorização previstos no item 25.30.1, sem obrigação de utilização integral da capacidade estrutural disponível.

25.30.4. Os softphones dimensionados no projeto serão ativados sob demanda e vinculados a ramais ativos, sem cobrança duplicada de licença pelo mesmo usuário, ramal ou funcionalidade.

25.30.5. O planejamento de ramais utilizará inventário, usuários, CDR, simultaneidade e perfil de chamadas efetivamente observados. Taxas de crescimento e limites de expansão serão justificados no projeto e recalibrados por evidências.

25.30.6. A capacidade simultânea será dimensionada separadamente do número de ramais, abrangendo chamadas internas, externas, filas, conferências, transbordos, gravações autorizadas e demais recursos concorrentes. As faixas de ativação serão estabelecidas no projeto específico.

25.30.7. A faixa ativa será definida por CDR e medições da hora de maior movimento, considerando tentativas, duração média, intensidade de tráfego, taxa de completamento, probabilidade de bloqueio, distribuição entre chamadas internas e externas e margem técnica, por Erlang B ou método equivalente.

26. PROTOCOLO DE ENTREGA E CONSOLIDAÇÃO DO PROJETO

26.1. A prefeitura demandante formalizará a solicitação por projeto, designará coordenador e responsáveis técnicos e setoriais e apresentará o Cadastro do Projeto com evidências. A requisição fixará data de entrega, canal oficial, destinatário, versão e escopo. Antes de solicitar a proposta executiva do respectivo projeto municipal, o InPACTA consolidará e disponibilizará às participantes dessa etapa a mesma base de locais, quantidades ou faixas, capacidades, interfaces, responsabilidades, condições de implantação, medição e requisitos de aceite necessários à avaliação. Informações reservadas necessárias ao dimensionamento serão disponibilizadas em procedimento controlado com condições uniformes de acesso. Não será exigida proposta econômica na seleção da parceria técnica institucional. A instrução econômica de eventual execução municipal utilizará o escopo validado no procedimento próprio do projeto. Na seleção institucional, a comparação utilizará as premissas e o cenário de referência publicados no edital, sem exigir o levantamento antecipado de todos os futuros municípios. O levantamento e o dimensionamento de cada implantação permanecerão sujeitos à validação antes da liberação da parcela correspondente. Havendo mais de uma parceira qualificada apta ao escopo, comparar orçamentos uniformes e escolher o menor preço integralmente conforme, observado o edital, itens 24.3 a 24.5.

26.2. O conjunto mínimo de rede compreenderá relação individualizada de localidades e nodes C1 a C5, endereços e coordenadas, criticidade, aplicações, usuários, circuitos, contratos vigentes, topologia disponível, interfaces, endereçamento, VLANs, condições de energia e infraestrutura local, fluxos entre unidades e ambientes computacionais, medições de tráfego e necessidades de expansão. Dados não conhecidos serão identificados como pendência, com responsável e providência de levantamento. Serão identificados os serviços internos que dependem da Infovia, seus fluxos críticos, responsáveis, requisitos de continuidade, pontos autorizados de teste e condições de acesso ao monitoramento. O levantamento distinguirá apoio à integração, administração municipal e intervenções atribuídas à executora. O inventário identificará firewalls e gateways existentes, respectivos responsáveis, topologia, membros redundantes, versões, licenças, interfaces, políticas de integração e necessidades de continuidade. Para os serviços críticos, a base validada fixará os limites de interrupção, comutação e recuperação de sessões que orientarão dimensionamento e aceite, sem presumir capacidades do legado. Para os hotspots, a Prefeitura entregará identidade visual, canais oficiais, responsáveis pela aprovação de conteúdo, objetivos das campanhas, locais e períodos, modelos de perguntas, volumes estimados, perfis de acesso e regras de tratamento das respostas. O InPACTA consolidará e validará essas definições com a área municipal responsável antes da ativação das interações, sem transferir à executora a decisão sobre finalidade ou publicação de conteúdo institucional.

26.3. Os eventos C6 terão cadastro próprio por evento ou programação estimada, conforme item 5.7, separado dos nodes permanentes. A prefeitura deverá declarar expressamente se há demanda por C6 e identificar os períodos de simultaneidade, as necessidades de cobertura, o público e as condições locais.

26.4. A telefonia terá declaração própria de demanda. Se solicitada, a prefeitura entregará inventário de ramais, usuários, terminais, softphones, numeração pública e titularidade, contratos e portabilidade, filas e URAs, serviços críticos, CDR e medições de tráfego disponíveis, integrações, janelas e responsáveis. Ausência de demanda formal manterá a telefonia sem ativação e sem medição.

26.5. Cada informação deverá ter identificador, responsável municipal, data de referência e evidência verificável. As bases serão entregues em formato editável e estruturado, com unidades de medida e chaves de relacionamento. Fotografias, plantas, relatórios e autorizações serão vinculados aos registros correspondentes. Credenciais e dados sensíveis serão transmitidos em canal restrito, somente quando necessários e autorizados.

26.6. O recebimento será protocolado com relação de arquivos e versões. A equipe técnica do InPACTA verificará completude, consistência, duplicidades, vinculação de IDs, quantidades e condições locais. O recebimento de arquivos não equivale à validação técnica ou à aprovação do projeto.

26.7. A diligência de complementação identificará dado ou evidência faltante, responsável, impacto no dimensionamento e data de resposta acordada. O coordenador municipal acompanhará as pendências e encaminhará à autoridade demandante os atrasos que impeçam a definição do escopo. Alteração do prazo será registrada com justificativa e impacto no cronograma.

26.8. Pendências essenciais de locais, quantidades, capacidade, interfaces, responsabilidade, energia, acesso, autorização ou demanda impedirão a consolidação e a liberação da parcela afetada. Quando influenciarem viabilidade, dimensionamento ou preço, deverão ser resolvidas antes da solicitação da proposta correspondente; não serão transferidas à proponente como obrigação indeterminada. Não se presumirão valores, capacidade, gratuidade ou aceite por silêncio. Atividades independentes poderão prosseguir com delimitação expressa. O projeto executivo detalhará a solução para o escopo definido e não substituirá a definição prévia dos requisitos necessários à comparação das propostas.

26.9. A consolidação exigirá declaração municipal de conferência dos dados, relação das evidências, versão do cadastro, validação técnica do InPACTA e aprovação expressa do escopo pela autoridade competente. A declaração municipal não substitui vistoria, análise técnica ou responsabilidade da executora pelo projeto executivo. A Prefeitura instruirá e aprovará seu planejamento conforme o regime aplicável, incluindo ETP, TR ou documentos técnicos exigíveis. Quando exigido, o ETP fundamentará necessidade, alternativas e viabilidade; o TR definirá objeto, quantidades, capacidades, obrigações, níveis de serviço e aceite. O projeto executivo será o detalhamento de implantação da solução contratada, elaborado pela executora conforme Anexo I, item 5.8.1, sem substituir esses documentos ou definir posteriormente requisitos essenciais à comparação das propostas. Eventual dispensa de documento de planejamento dependerá de fundamento e decisão formal no processo municipal.

26.10. O Termo de Validação do Escopo identificará projeto e versão, localidades e quantidades por classe, base e expansão, eventos C6, telefonia solicitada ou não, interfaces, exclusões, condições de início, pendências remanescentes sem efeito impeditivo e responsáveis. As assinaturas ou referências aos atos

de aprovação serão registradas antes da liberação da contratação ou execução da parcela correspondente.
26.11. Após a validação, mudança de local, classe, quantidade, capacidade, integração ou telefonia será submetida a controle de alterações, com motivo, impacto técnico, econômico e de prazo, responsável, aprovação e nova versão. Cadastro, especificação, matrizes, preços, cronograma e Ordem de Serviço serão atualizados de forma coerente.
26.12. A emissão de Ordem de Serviço dependerá de escopo aprovado, condições de acesso e infraestrutura confirmadas, autorização competente e recursos formalizados. A OS identificará os itens, unidades, quantidades, prazos, critérios de aceite e responsáveis. A confirmação das condições municipais não afasta a obrigação da executora de verificar tecnicamente a implantação e apontar impedimentos.

27. RESILIÊNCIA MODULAR E REDUNDÂNCIAS SOB DEMANDA

27.1. A extensão C7 de resiliência integra a Infovia nas modalidades fixa C7-F, transportável C7-T e veicular C7-V, para continuidade de comunicações prioritárias, atendimento público temporário e sensoriamento pertinente à missão. Seu fornecimento e implantação ocorrerão somente sob demanda autorizada. Os requisitos de C1 a C6, dos acessos dedicados, da segurança e da telefonia permanecem íntegros. Entrega integralmente enquadrável em C6 conservará esse enquadramento; a mesma entrega não será contabilizada novamente como C7.
27.2. Todos os nodes C1, C2 e C3 deverão ser entregues preparados para redundância satelital: interface WAN disponível e compatível, física ou logicamente segregada; capacidade residual de roteamento, túneis seguros, detecção de falhas, seleção de rota, retorno controlado, VLAN/VRF ou equivalente, QoS, registros e supervisão. As funções e licenças necessárias à preparação estarão disponíveis na entrega, sem substituição dos equipamentos principais para obtê-las. Identificar portas, versões, espaço, energia e passagem de cabos. Terminal, acessórios específicos, instalação, serviço satelital e ativação serão fornecidos somente na demanda correspondente.
27.3. Todos os nodes integrantes do anel, independentemente da classe, deverão possuir equipamentos preparados para incorporar radioenlace de contingência em caso de indisponibilidade da fibra. Identificar interfaces, capacidade residual, funções, licenças, espaço, energia e passagem de cabos, sem substituição dos equipamentos principais para obter a integração. Rádios, antenas, suportes, infraestrutura específica, implantação e ativação dependerão de demanda autorizada e estudo do percurso. Preparação não comprova enlace instalado, ativo ou viável em qualquer trajeto.
27.4. C7-F atenderá instalação essencial, centro de coordenação ou base de contingência. Reunirá roteamento, distribuição local, conjunto satelital solicitado, energia e supervisão; APs corporativos serão incluídos quando houver atendimento público. DNS, autenticação, gestão e aplicações protegidas deverão alcançar ambiente disponível fora do domínio de falha. Reaproveitamento de rack, energia, roteamento ou APs dependerá de capacidade, autonomia e segurança comprovadas.
27.5. C7-T atenderá abrigo, posto temporário ou local isolado após liberação de acesso seguro. Reunirá os componentes previstos para a missão, distribuição elétrica, bateria, caixas, suportes, cabeamento inventariado e identificação. Dividir a carga em volumes compatíveis com a equipe e o acesso; informar massas, dimensões, ferramentas, área de montagem e limites de chuva e vento. O tempo de deslocamento será separado do tempo de instalação. Posição verificada no início de cada implantação poderá substituir receptor GNSS dedicado, com registro rastreável.
27.6. C7-V atenderá equipe embarcada e distribuição pública móvel com veículo estacionado. Reunirá roteador WAN veicular, GNSS, distribuição multigigabit, terminal satelital compatível com o regime solicitado, AP corporativo quando aplicável, bateria auxiliar, conversão DC-DC e proteções. Operação em movimento dependerá de equipamentos, serviço e instalação adequados. AP externo deverá comprovar adequação veicular. Rádio direcional convencional somente operará com veículo estacionado, estabilizado e alinhado.
27.7. A composição modular observará o quadro M0 a M9. C7-F compreende M0, M1, M3, M4 e M9; C7-T acrescenta acondicionamento e instalação temporária; C7-V acrescenta M8. M2, M5, M6 e M7 dependerão da finalidade solicitada. M4 poderá usar a telemetria nativa e a plataforma existente. M5 não exige computador adicional quando gateway e serviços disponíveis comprovarem processamento, armazenamento e autonomia funcional. Preparação dos C1/C2/C3 não implica fornecimento de C7 completo.

ID	Conteúdo	Acionamento
M0	Roteamento, firewall, segregação, inventário e supervisão.	Comum a todas as unidades; pode reutilizar ativos validados.
M1	Terminal satelital, suporte, cabos, plano e franquia compatíveis.	Fornecimento e ativação sob demanda; integra o C7 solicitado e a redundância opcional de C1/C2/C3.
M2	Pontos de acesso externos e política de acesso público.	Quando houver área de atendimento à população.
M3	Bateria, carregadores, conversores, distribuição e proteções.	Obrigatório no C7 contratado; capacidade por carga e autonomia.
M4	Posicionamento, mapa, telemetria e histórico.	Obrigatório no C7 contratado; GNSS contínuo quando necessário.
M5	Sensores, gateway, servidor IoT e processamento local.	Por missão; sensores de saúde do próprio node integram a base.
M6	Radioenlace licenciado completo, com as duas pontas.	Implantação sob demanda; nodes do anel obrigatoriamente preparados. Viabilidade por percurso.
M7	Conectividade celular e antenas.	Opcional; não conta como independente de infraestrutura terrestre.
M8	Integração veicular, suportes e gestão de energia da frota.	Exclusivo do C7-V.
M9	Prontidão, suporte, treinamento, testes e logística.	Comum; extensão de cobertura e prazos definidos por demanda.

27.8. A seleção dos equipamentos será por funções, capacidade e interoperabilidade comprovadas, sem indicação de marca ou modelo de referência. O CPE deverá suportar as interfaces WAN/LAN, túneis seguros, QoS, segregação e supervisão sob carga. Quando suas interfaces forem insuficientes, a distribuição utilizará switch gerenciável multigigabit e alimentação compatível. O firewall do CPE não substitui as funções, o desempenho ou a alta disponibilidade da borda institucional. Identificar versão, licenças, suporte, garantia e manutenção da composição ofertada.

27.9. Os APs de C7 atenderão integralmente ao item 5.6 e seus subitens: Wi-Fi 6 mínimo, 2,4/5 GHz simultâneos, uplink de pelo menos 2,5 GbE, PoE e cabeamento compatíveis, gestão oficial suportada pelo fabricante e operação conjunta Wi-Fi 6/7. Aplicam-se a referência 5 GHz 4×4:4 ou equivalência integral comprovada, o planejamento inicial até 50 ativos por rádio de 5 GHz e as condições de comprovação existentes. Wi-Fi integrado ao roteador não substitui AP corporativo conforme. Capacidade limitada do satélite não reduz os requisitos locais de acesso, gestão, portal ou segurança.

27.10. No roteamento veicular, dimensionar capacidade sob VPN, interfaces para os meios solicitados, GNSS, antenas, tensão de entrada e alimentação protegida para a instalação efetiva. A conectividade celular, quando solicitada, deverá atender à tecnologia e ao desempenho definidos na demanda; não constitui independência da infraestrutura terrestre. Não presumir que interface nominal ou rádio integrado atendam à capacidade da solução completa.

27.11. A conectividade satelital, inclusive por constelação de baixa órbita quando solicitada, deverá ter terminal, acessórios e perfil de serviço compatíveis com o uso fixo, transportável ou veicular, compartilhamento e operação em movimento quando requerida. Identificar cada ponto no cadastro da demanda, sem quantitativo fixo institucional. Verificar obstruções, visão do céu, fixação, cabos, aterramento, surtos e energia da configuração completa. Alimentação em corrente contínua dependerá de comprovação de tensão, potência, conversão e proteções.

27.12. O radioenlace transporta dados entre duas extremidades da Infovia e depende de contraponto operacional; não fornece internet isoladamente. Um enlace direto 1+0 compreenderá duas unidades de rádio, duas antenas compatíveis, suportes, terminações e alimentação nas duas pontas. Proteção 1+1, repetidores e diversidade de percurso terão dimensionamento próprio, sem presumir duplicação de todos os componentes ou do consumo total.

27.13. Cada percurso de rádio terá coordenadas, alturas, perfil de terreno, obstáculos, zona de Fresnel, interferências, chuva, margem de desvanecimento, modulação, capacidade útil por sentido e disponibilidade calculada, segundo metodologia pertinente da UIT-R P.530. Verificar estruturas, vento, aterramento, surtos, limites ambientais, cotas de instalação e energia em ambas as pontas. Ensaio pontual não comprova disponibilidade anual. Identificar responsável pelo contraponto, disponibilidade dos serviços de destino e regularização aplicável.

27.14. A escolha de proteção 1+0 ou 1+1 será justificada por criticidade, falhas cobertas e risco residual, com identificação dos elementos compartilhados. Dois canais no mesmo equipamento ou equipamentos no mesmo suporte e fonte não demonstram independência de infraestrutura. Chuva, dano estrutural, alagamento, alimentação compartilhada e perda do destino podem afetar simultaneamente fibra, rádio e satélite. Registrar ameaças comuns, medidas de redução e risco residual.

27.15. A integração seguirá AP ou sensor, VLAN/VRF correspondente, CPE, túnel seguro pelo meio disponível, terminação autorizada no site principal ou de continuidade, segurança de borda e destino. Preservar IPv4/IPv6, VLAN 802.1Q, VRF ou equivalente, DSCP, rotas, detecção, MTU/MSS, criptografia, gestão de chaves e registros, conforme a arquitetura existente. Evitar loops, oscilação e vazamento de rotas. CGNAT dependerá de solução comprovada para os fluxos exigidos e não substituirá os blocos públicos exclusivos dos acessos dedicados. O rádio poderá contornar apenas o trecho óptico afetado.

27.16. Segregar rede institucional, gestão, sensores e acesso público. Priorizar coordenação, mensagens, sistemas essenciais e voz tecnicamente validada; telemetria e comunicação pública básica terão perfis definidos. Aplicações volumosas poderão ser limitadas pela política aprovada. QoS local não assegura prioridade no provedor satelital; continuidade de sessões e endereços dependerá da arquitetura e de ensaio. A solução não substitui rádio de missão crítica. Telefonia solicitada utilizará plataforma, SBC, troncos SIP e parâmetros do item 25, sem PABX paralelo.

27.17. Cada node terá código único, modalidade, coordenadas, fonte, precisão estimada, horário de atualização, estado, responsável e recursos disponíveis. Node fixo poderá usar levantamento de campo; transportável atualizará a posição em cada implantação; veicular utilizará GNSS e histórico controlado. Cada sensor remoto terá localização própria. Posição e leitura antigas serão sinalizadas com a idade do registro, sem apresentação como dado atual.

27.18. O sensoriamento ambiental será incorporado por finalidade: temperatura e umidade, chuva, nível, umidade do solo, fumaça ou gases e outros fenômenos pertinentes ao risco. Identificar fenômeno, unidade, faixa, precisão declarada, exposição, calibração quando aplicável e intervalo de aquisição. Sensores de saúde do node abrangerão energia, bateria, gabinete, entrada de água e violação conforme os riscos. Motor, escapamento e movimento poderão afetar as leituras embarcadas. Partículas não comprovam incêndio; sensores ambientais não substituem detecção e alarme de proteção à vida.

27.19. Sensores, gateway, servidor de rede e aplicação constituirão cadeia completa quando utilizada arquitetura LoRaWAN. Comprovar protocolo, radiofrequência aplicável, proteção ambiental, interface e integração. Câmeras utilizarão transporte de maior capacidade. APIs documentadas e exportação em formato aberto permitirão integração ao mapa e às plataformas; avaliar OGC SensorThings quando pertinente. Armazenar origem, qualidade, horário de aquisição, recepção e sincronização; evitar duplicação após recuperação.

27.20. A continuidade local deverá demonstrar recepção e armazenamento dos dados durante perda de WAN e sincronização posterior, com lacunas identificadas. A indisponibilidade da Central ou nuvem não elimina políticas locais. Testar separadamente portal, DNS/DHCP, autenticação, sessões existentes, novos ingressos e expiração, conforme 5.6.6.4 e Anexo V. Preservar campanhas, enquetes, questionários, aprovação institucional e continuidade previstos no item 5.6; não utilizar acesso aberto sem controles como contingência.

27.21. A memória de energia abrangerá toda a carga necessária ao serviço, inclusive rádios, terminais satelitais solicitados, roteamento, switches, conversores, segurança, supervisão e dependências de cada extremidade. Declarar potência medida por item, regime, picos, perdas, eficiência, fração utilizável, temperatura e envelhecimento. Evitar dupla contagem de componentes já incluídos no consumo de um conjunto. Conferir PoE por norma, tensão, pinagem, potência por porta, total e partida; PoE passivo exige compatibilidade comprovada.

27.22. Dimensionar bateria nominal em Wh pela potência média completa em W multiplicada pela autonomia em horas, dividida pela fração utilizável e eficiência, com margens justificadas para temperatura e envelhecimento. Dimensionar banda por sentido pela soma das aplicações simultâneas e reserva justificada; distinguir usuários associados de ativos e medir upload, VPN, filas, perda e latência. Taxa nominal de interface, AP ou linha GPON não é capacidade útil garantida. Memória de armazenamento e tráfego dos sensores considerará tamanho, frequência, retenção e recuperação dos registros.

27.23. A referência de autonomia do C7 é de 8 horas; ampliação, inclusive para 12 horas, dependerá de definição expressa na demanda. Aplicar a autonomia especificada à carga completa de cada extremidade necessária, sem intervenção humana durante esse período, e identificar a autonomia dos serviços de destino. Para duração superior, prever recarga, geração ou reposição, responsáveis, acesso, combustível quando aplicável, mobilização e limites de continuidade. Não se presume autonomia universal de 12 horas ou continuidade de 72 horas.

27.24. O ensaio de autonomia desligará a energia da rede elétrica, utilizará carga real representativa e registrará continuamente tensão, corrente, estado de carga e alarmes, sem interrupção dos serviços protegidos pelo período exigido. Ensaio equivalente dependerá de justificativa, equivalência demonstrável e aprovação prévia da fiscalização competente. Comprovar recarga após retorno da energia, tempo de recuperação e condições de nova contingência, preservada a segurança elétrica e operacional.

27.25. O aceite verificará fixação ao vento, aterramento, surtos, proteção ambiental, exposição a alagamento e cotas previstas no projeto executivo. No veículo, preservar bateria de partida e alternador, prever bateria auxiliar, conversão DC-DC e gestão de bateria compatíveis, picos, fusíveis, bitolas, temperatura, conexão externa e desconexão segura. A montagem, a sustentação e as limitações operacionais deverão ser comprovadas para a configuração efetivamente instalada.

27.26. A demanda identificará localidades, modalidades, unidades, módulos, percursos, simultaneidade, serviços prioritários, capacidade útil por sentido, autonomia, período operacional, mobilização, dependências, responsabilidades e critérios de aceitação antes do detalhamento executivo e da implantação. Os exemplos de composição unitária não fixam frota, quantidade mínima institucional ou acervo. Reaproveitamento de ativos depende de validação; componentes integrados não serão contados duas vezes. A unidade de rádio será o percurso completo, com duas extremidades e eventuais repetidores justificados.

27.27. Como parâmetros de referência da extensão C7, adotar na base da demanda comutação C7-F de até 60 segundos para novas sessões prioritárias com reserva já ativa, montagem C7-T de até 30 minutos após chegada e liberação segura e ativação C7-V de até 15 minutos após posicionamento seguro, com conjunto pré-instalado e serviço ativo. Separar deslocamento de montagem e registrar configuração, condições, horários, aplicações e perdas. Esses parâmetros não relaxam os mínimos de C1 a C6 e não asseguram preservação de todas as sessões existentes.

27.28. O ensaio local dos APs de C7 observará 200 dispositivos associados e 100 ativos por AP, durante 60 minutos, com 3 Mbps de descida e 1 Mbps de subida por ativo, conforme item 5.6 e Anexo V 12.1. A carga agregada local de 300/100 Mbps por AP será verificada independentemente do acesso satelital, cujo dimensionamento será próprio. Cobertura e qualidade da área atendida serão comprovadas no aceite. A plataforma de gestão, o portal e a segurança permanecerão sujeitos aos ensaios existentes.

27.29. Na entrega dos nodes, comprovar preparação por documentação do fabricante, matriz de interfaces, versões e licenças e ensaio de integração com caminho de teste. Tal prova não demonstra serviço satelital ou rádio operacional. Depois da demanda, testar por ponto ou percurso o meio real, vazão por sentido, latência, perda, túnel, qualidade dos serviços, falha, retorno, alarmes e energia da carga completa. Rádio exigirá registros de propagação, margem, modulação e capacidade útil; satélite exigirá obstruções, condição do céu e perfil de serviço.

27.30. A comprovação distinguirá documentação institucional, demonstração funcional em ambiente controlado, detalhamento executivo, implantação, aceite e operação. A análise documental aplica-se a todas as funções desta extensão; somente pontos de extrema necessidade, motivados conforme Anexo II 13.38.1 a 13.38.4 e selecionados no roteiro previamente publicado, integrarão a PoC excepcional, sem construção antecipada de rede, percurso de rádio definitivo ou frota operacional. Obrigações de campo permanecem exigíveis na parcela implantada, sem aprovação presumida pelo laboratório. As matrizes registrarão requisito, evidência, fase, conclusão e fundamento; a extensão não altera os quatro diferenciais facultativos ou sua pontuação.

27.31. O InPACTA coordenará a integração institucional ao N1 e à Central de Situação; a executora responderá pela implantação, N2/N3, NOC/SOC, operação técnica, manutenção e evidências; o município indicará prioridades, locais, acesso e articulação com Defesa Civil e serviços essenciais, conforme suas atribuições. Relacionar eventos, alarmes, chamados, node, percurso, demanda e município, preservando os prazos existentes. Definir limiares, persistência, histerese, confirmação e escalonamento pertinentes, retenção e acesso por finalidade. Alertas públicos, sirenes e atuação automática de segurança dependerão de projeto específico e atribuição expressa de responsabilidades.

27.32. A falta de energia da rede elétrica, isoladamente, não afasta a obrigação de autonomia especificamente prevista e aceita. Falhas da reserva serão examinadas por causa, limites de projeto, responsabilidades e evidências, sem exclusão ou responsabilidade automática pelo rótulo de desastre. Eventos além dos limites serão examinados conforme o instrumento e a matriz de riscos. Manter internet via satélite não restaura aplicações hospedadas em destino indisponível; comprovar o ambiente de continuidade necessário.

27.33. O planejamento técnico contemplará capacidade das equipes, volumes transportáveis, logística, guarda, recarga, manutenção, sobressalentes, treinamento e testes periódicos. Compartilhar recursos somente com simultaneidade comprovada. Quando exigida prontidão, os recursos e a conectividade estarão disponíveis e testados antes do acionamento. A simples preparação dos equipamentos ou o fornecimento sob demanda não garante atendimento imediato durante desastre; registrar os prazos e condições da parcela autorizada.

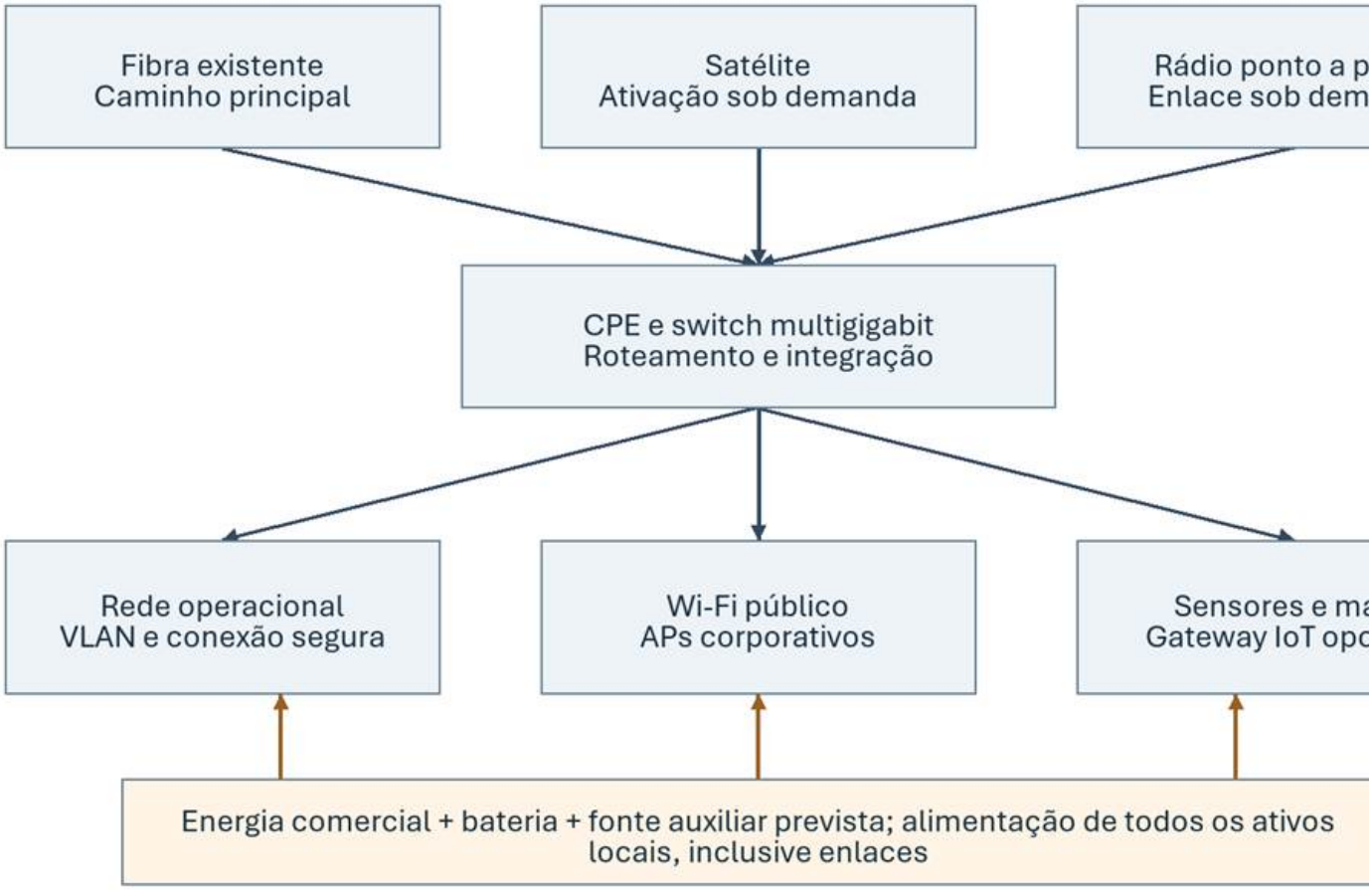
27.34. A proposta técnica apresentará matriz por módulo com função, composição ofertada, versões, licenças, interfaces, consumo, dependências, evidências e limitações, topologias de dados e energia, matriz de falhas, capacidade em contingência, operação sem nuvem e mobilização. O levantamento municipal registrará dados e evidências no Cadastro e nos formulários, com situação informada, vistoriada, medida ou validada. Dados essenciais não definidos impedem a liberação da parcela afetada, sem exigir dimensionamento antecipado de todos os municípios na qualificação institucional.

27.35. Comprovar homologação dos equipamentos e regularidade de serviço, espectro e estações conforme aplicáveis, nos marcos pertinentes. Autorização SCM não substitui as demais verificações. Comprovar uso satelital em movimento e distribuição pública compatíveis com o serviço. A extensão não cria exigência de vínculo comercial com fabricante, marca específica, acervo próprio de satélite, rádio ou sensores, nem quantitativo adicional de habilitação; permanecem os critérios do Anexo II.

27.36. A contingência de capacidade inferior à fibra terá prioridades e limitações explícitas; não repõe integralmente a banda nem afasta níveis de serviço originais. Distinguir falha de caminho, perda de resiliência, degradação e indisponibilidade conforme 5.4.40 e 15.8.4 a 15.8.9. Registrar separadamente o atendimento C7 e a falha original. Rotas de emergência serão autorizadas, documentadas e integradas aos sites principal e de continuidade; não concederão acesso direto à LAN administrativa nem substituirão proteções ópticas e acessos dedicados.

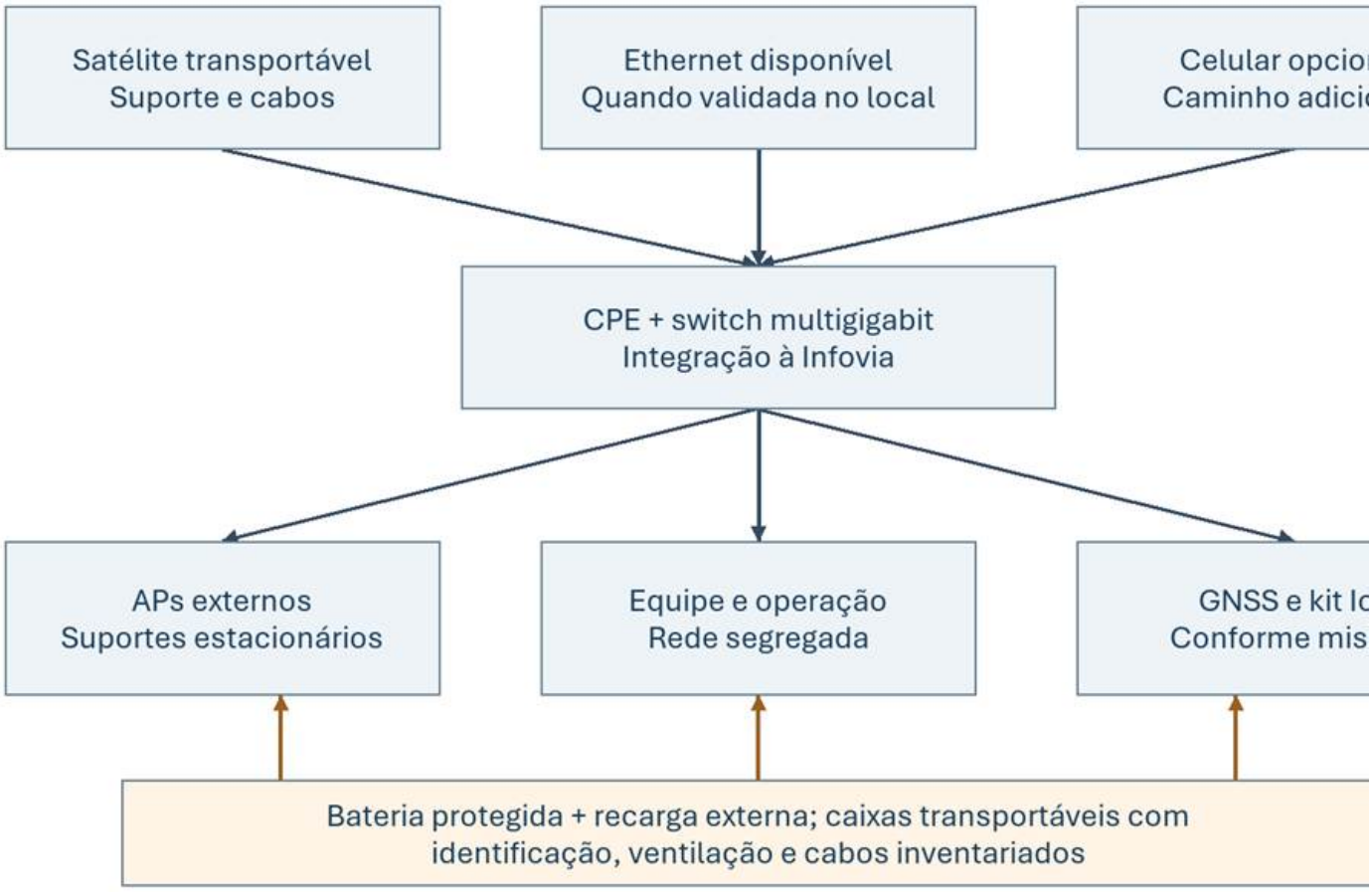
27.37. DIAGRAMAS FUNCIONAIS DA EXTENSÃO

C7 fixo



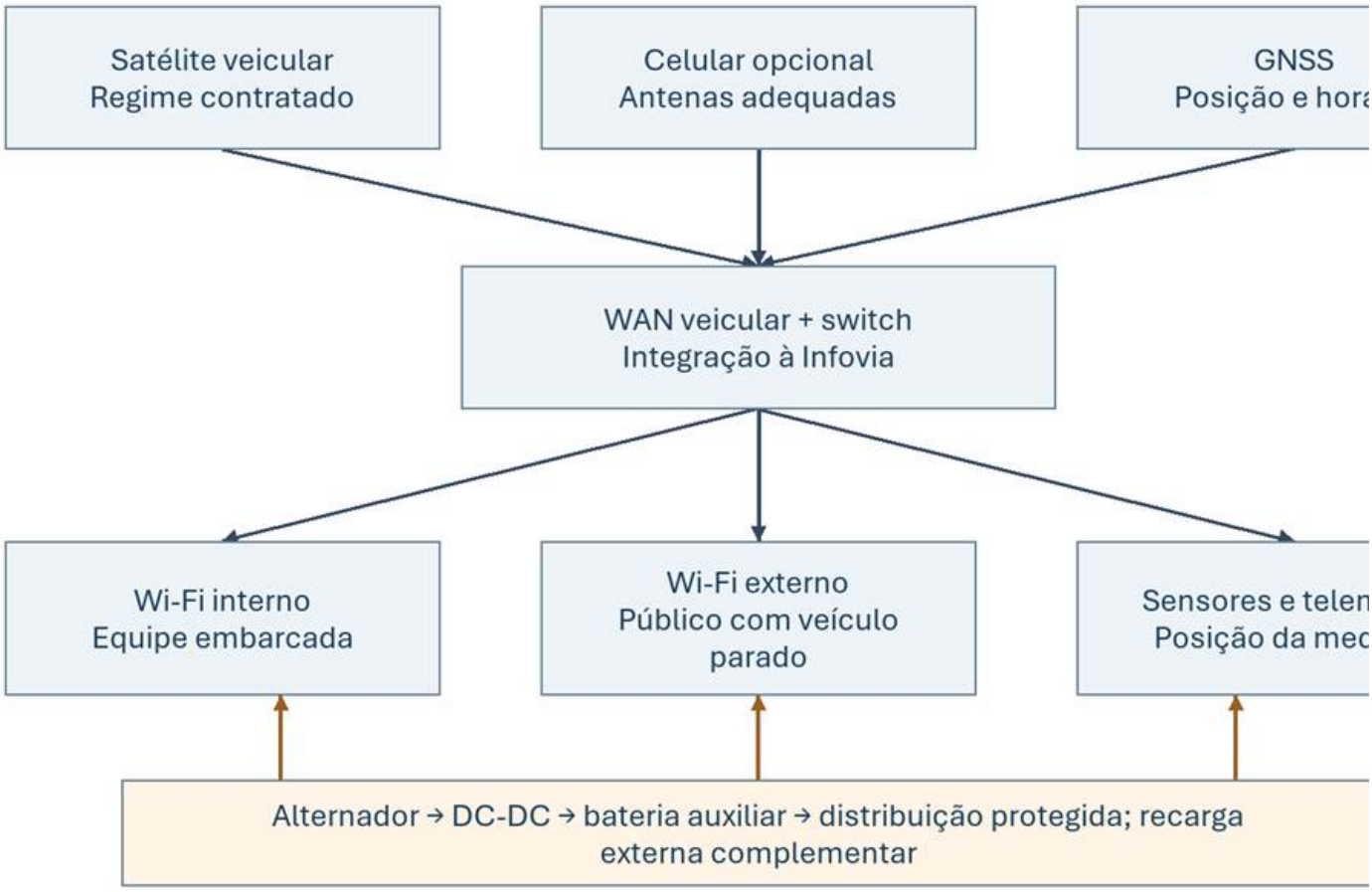
Representação funcional: não fixa quantidade, local ou percurso. Preparação dos nodes não equivale a redundância ativa. Os recursos de rádio e satélite dependem da demanda autorizada, de destino operacional e de energia nas extremidades necessárias.

C7 transportável



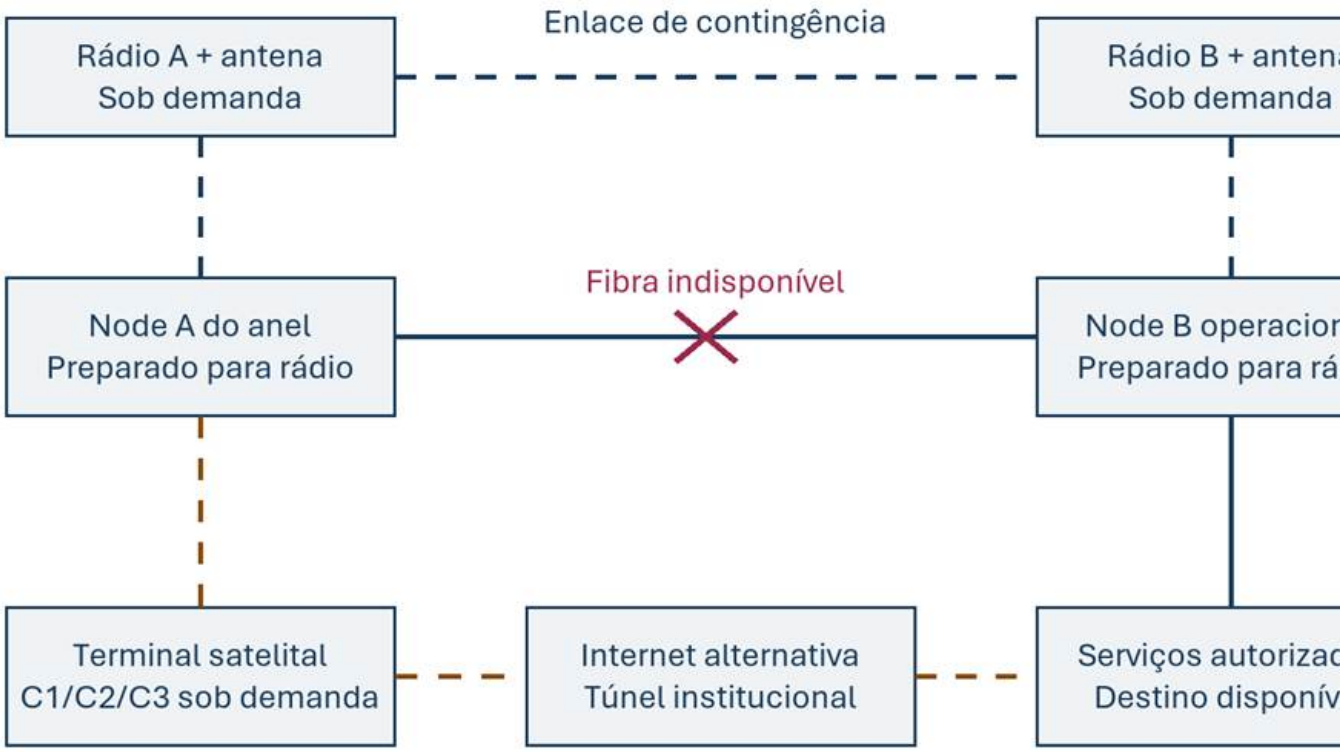
Representação funcional: não fixa quantidade, local ou percurso. Preparação dos nodes não equivale a redundância ativa. Os recursos de rádio e satélite dependem da demanda autorizada, de destino operacional e de energia nas extremidades necessárias.

C7 veicular



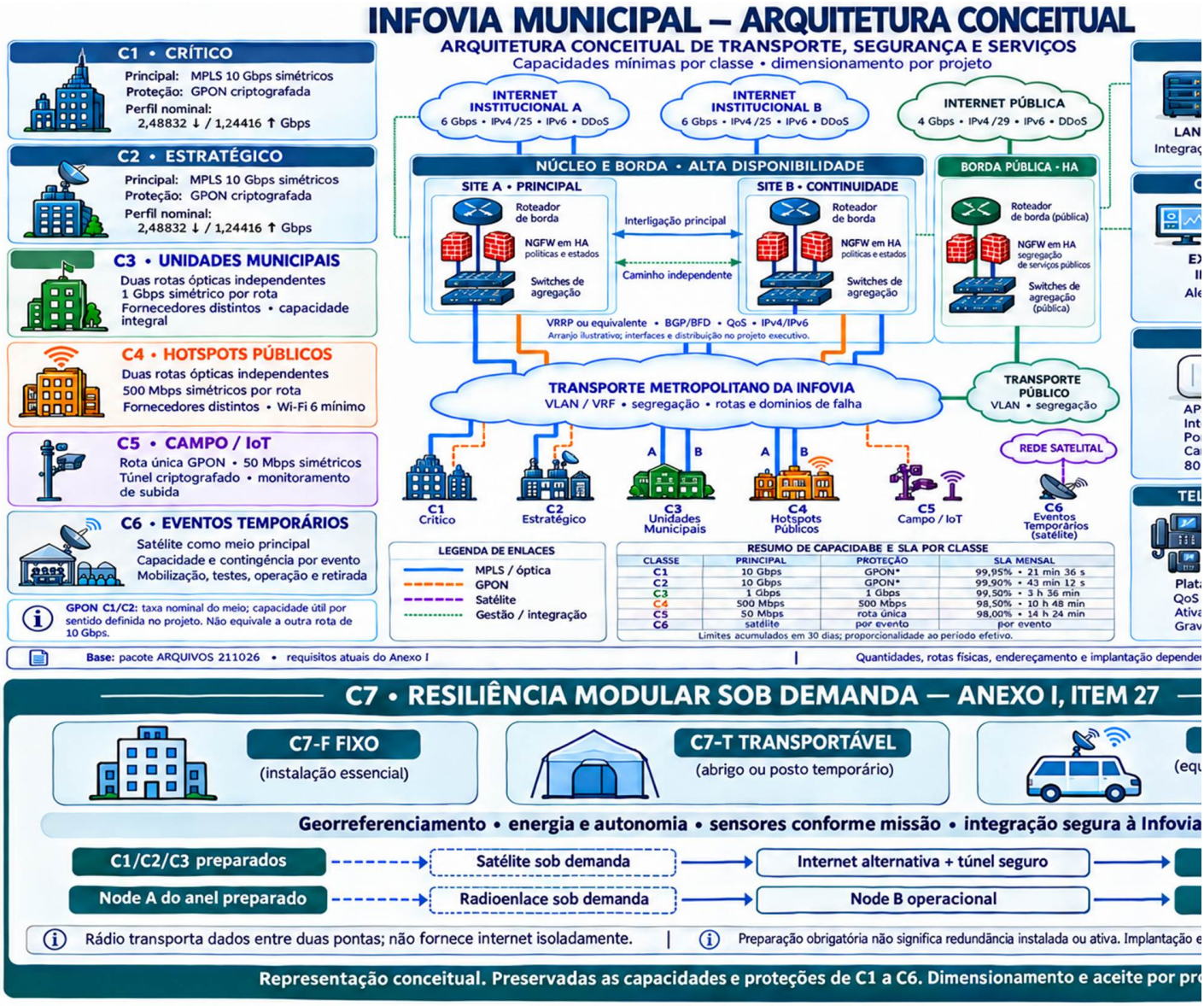
Representação funcional: não fixa quantidade, local ou percurso. Preparação dos nodes não equivale a redundância ativa. Os recursos de rádio e satélite dependem da demanda autorizada, de destino operacional e de energia nas extremidades necessárias.

Separação entre contingência por rádio e acesso satelital



Tracejado: recurso a implantar e ativar sob demanda.

Representação funcional: não fixa quantidade, local ou percurso. Preparação dos nodes não equivale a redundância ativa. Os recursos de rádio e satélite dependem da demanda autorizada, de destino operacional e de energia nas extremidades necessárias.



Representação conceitual aplicável aos municípios demandantes, conforme o escopo de cada projeto. Ícones, posição dos componentes e traçado das conexões são ilustrativos; não fixam quantitativos, locais, interfaces ou rotas físicas. Prevalecem os requisitos da especificação técnica e o projeto executivo aprovado.

Documento assinado eletronicamente por **Cristiane Regina de Camargo Hasegawa**, **Diretor(a)-Presidente do INPACTA**, em 10/11/2026, às 18:12, conforme horário oficial de Brasília, com fundamento na Medida Provisória nº 2200-2, de 24 de agosto de 2001 e Decreto Municipal nº 871, de 7 de julho de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.maringa.pr.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **10002009** e o código CRC **51126AF5**.

Referência: Processo nº 43.04.00000202/2026.44 SEI nº 10002009