Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

ESTUDO TÉCNICO PRELIMINAR

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. O PRODERJ, instituição vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro, na forma do art. 3º, do Decreto nº 48.997/2024, que altera a estrutura organizacional do Poder Executivo e reestrutura o Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC.

1.2. É missão do PRODERJ atuar na inovação, na garantia da regulação e provimento de soluções tecnológicas que garantam segurança, autenticidade, integridade, padronização e validade jurídica de documentos e transações eletrônicas, respeitando o cidadão, a sociedade e o meio ambiente.

1.3. O Governo do Estado do Rio de Janeiro necessita de uma rede de comunicação de alta velocidade e com alta capacidade de resiliência com capacidade de prover dados, voz, vídeo e imagens para atender às necessidades do exercício da sua missão institucional proporcionando elevado padrão de qualidade, atendendo as necessidades de comunicação e acesso a novas tecnologias que possam suprir as demandas de infraestrutura tecnológica.

1.4. No contexto da Conectividade de Rede de Dados, alta capacidade de resiliência pode ser alcançada com a duplicação de componentes essenciais que aumentam a confiabilidade e segurança de determinado sistema, aplicação e base de dados, assim como sua disponibilidade

1.5. Em outras palavras, a duplicação de um link oferece mais de um “caminho” para que a conectividade entre dois sites remotos se mantenha sempre ativa e – assim, caso um desses caminhos esteja congestionado ou interrompido, não haverá indisponibilidade de serviço e consequentemente perda de produtividade.

1.6. A Diretoria de Infraestrutura Tecnológica identificou a necessidade de garantir a conectividade segura, moderna e eficiente entre as unidades descentralizadas da Administração Pública Estadual e a sede do Governo. Essa conectividade deve viabilizar, de forma confiável e com desempenho adequado, o acesso aos serviços corporativos hospedados no ambiente centralizado de TIC, a comunicação entre os órgãos e secretarias estaduais, bem como o acesso à Internet institucional.

1.7. Além disso, há demanda por soluções que assegurem conectividade em localidades remotas, de difícil acesso ou em constante mobilidade, como regiões com infraestrutura limitada ou operações realizadas em deslocamento. Tais necessidades incluem garantir comunicação de dados em contextos onde a infraestrutura terrestre não é suficiente ou inexistente, visando assegurar a continuidade das atividades administrativas em quaisquer condições geográficas ou operacionais.

1.8. A necessidade da comunicação entre Órgãos do Governo do Estado do Rio de Janeiro, formando a topologia da rede corporativa (Rede IP Governo), o que permite disponibilizar sistemas e serviços para os componentes da Rede IP Governo, garantindo maior segurança por meio da redução nos riscos de vazamentos de informação, além de redução de custos com melhor uso da tecnologia.

1.9. Os pontos de atendimento da Rede IP Governo Principal, de Contingência, Satelital e 4G/5G se distribuem por todo o território geográfico do Estado do Rio de Janeiro e Brasília (Representação do Governo), devido às diferenças na infraestrutura disponível ao longo dessa mesma área geográfica, a qualidade de serviço oferecida não será a mesma.

1.10. Os dados gerados pelo tráfego de conectividade, bem como dos incidentes de rede e de segurança da informação precisam ser armazenados de forma estruturada, e disponibilizados em forma de painéis de controle (dashboards), gráficos e relatórios, garantindo a formação de um histórico que permita análise quantitativa e qualitativa de um único circuito de dados ou de forma global de toda a rede corporativa.

1.11. O PRODERJ tem como uma de suas missões institucionais, prevista na Lei nº 4.480/2004 no art. 2º, VI: "planejar e coordenar a implantação de uma solução de rede multisserviço que suporte tráfego integrado de voz, dados e imagens, para as diversas demandas de comunicações, inclusive telefonia, no âmbito do governo estadual, com capilaridade e capacidade adequadas para evitar a

duplicação de esforços na criação de sub-redes paralelas distintas".

1.12. Necessidade na redução de custos da rede, aproveitando a evolução tecnológica das soluções computacionais e de telecomunicações e o fomento à participação do máximo de empresas que tenham reais condições de prestar os serviços sem perda na qualidade dos níveis mínimos exigidos. A presente contratação trata de despesas de custeio, ou seja, aquelas indispensáveis à prestação contínua de serviços e à manutenção das atividades operacionais da Administração Pública. A demanda justifica-se pela essencialidade dos serviços a serem contratados, os quais atendem diretamente ao interesse público e são imprescindíveis para o regular funcionamento das unidades do PRODERJ, bem como de demais entes públicos estaduais. Historicamente, tais serviços sempre foram prestados por concessionárias, dada sua natureza específica e insubstituível, sendo, portanto, indispensáveis à continuidade das ações institucionais.

2. RESULTADOS PRETENDIDOS

2.1. A presente demanda tem por objetivo atender à necessidade de garantir conectividade de dados de forma contínua, segura e com desempenho adequado às unidades da Administração Pública Estadual. Essa conectividade deve suportar a expansão, a modernização e a resiliência da rede corporativa governamental, possibilitando o acesso a serviços institucionais, à Internet e à comunicação entre os órgãos públicos, mesmo em cenários de contingência ou em localidades com limitações de infraestrutura.

2.2. O atendimento a essa necessidade deve considerar, ainda, aspectos como a escalabilidade da rede, a disponibilidade de suporte técnico qualificado, a capacidade de monitoramento e a adequação da infraestrutura de comunicação de dados às diferentes realidades operacionais da Administração Pública Estadual. Os requisitos técnicos detalhados, bem como as condições, quantidades e obrigações das contratadas, serão definidos nos artefatos técnicos da contratação.

2.3. Com esta contratação, busca-se atender à necessidade de ampliação da disponibilidade e confiabilidade dos meios de comunicação de dados utilizados pela Administração Pública Estadual. A iniciativa visa garantir que os órgãos e entidades públicas disponham de conectividade robusta e resiliente para acesso aos sistemas corporativos, mesmo em cenários de falha, indisponibilidade de infraestrutura local ou atuação em regiões remotas ou com mobilidade operacional.

2.4. Essa contratação deverá possibilitar o atendimento a diferentes contextos operacionais, promovendo maior continuidade dos serviços públicos digitais e mitigando os riscos de interrupção no acesso às plataformas governamentais.

2.5. Prover alta disponibilidade de acesso à rede corporativa do Governo do Estado do Rio de Janeiro com no mínimo os atuais níveis de serviços prestados;

2.6. Permitir o provisionamento de redundância entres os sites remotos das Secretarias e Órgãos públicos estaduais mediante duas operadoras de telecomunicações distintas;

2.7. Permitir o acesso ininterrupto aos sistemas de informação hospedados pelo PRODERJ e demais órgãos da administração pública direta e indireta aos servidores públicos e cidadãos;

2.8. Ampliar a eficiência operacional e a disponibilidade da rede corporativa utilizada pela Administração Pública Estadual, de forma a assegurar a continuidade dos serviços públicos e a sustentação das atividades críticas dos órgãos governamentais. Também se busca criar condições para que essa infraestrutura de rede possa evoluir e suportar a implantação de novos serviços e aplicações institucionais, alinhados às demandas atuais e futuras da transformação digital no setor público.

2.9. Evitar problemas relacionados à indisponibilidade dos sistemas, bases de dados e aplicações, ocasionados por problemas nos serviços das operadoras ou da própria infraestrutura do PRODERJ;

2.10. Prover acesso móvel à Internet, nas modalidades Satelital de baixa órbita, geoestacionário e 4G/5G.

3. RELATO DESCRITIVO DE CONTRATAÇÕES ANTERIORES DE NECESSIDADE IDÊNTICA OU SEMELHANTE, CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

3.1. A Rede IP Governo atualmente é mantida pelo PRODERJ através de dois contratos principais que disponibilizam a espinha dorsal da rede corporativa, que são as interconexões privadas e seguras entre os órgãos e secretarias aos serviços hospedados no PRODERJ e ao acesso à Internet. Contratos Nº 004/2021 e Nº 005/2021 (E-04/171/221/2018).

4. INDICAÇÃO DO ALINHAMENTO ENTRE A CONTRATAÇÃO E OS PLANOS ESTRATÉGICOS DO PRODERJ

4.1. A solução pretendida está prevista no plano de contratações anual.

4.1.1. **ID PCA no PNCP**: 42498600000171-0-000041/2025

4.1.2. **Data de publicação no PNCP**: 01/08/2024

ID do item no PCA: Vide tabela do item 10

4.2. A solução pretendida também está alinhada com o Plano Estratégico e Diretor de Tecnologia de Informação e Comunicação do PRODERJ-2024 (PEDTIC), conforme abaixo:

PROGRAMA	AÇÕES	INICIATIVA 0157 Desenvolvimento da Estrutura de TIC no Estado do Rio de Janeiro	
		PRODUTOS	DESCRIÇÃO DOS PRODUTOS
0493 Gestão da Tecnologia da Informação e Governo Digital	1293 Atualização Tecnológica do Parque Computacional	6814	Data Center modernizado
		6881	Tecnologia VOIP implantada em órgão estadual
		8815	Rede governo modernizado
		8816	Solução Educacional implantada
	4133 Gerenciamento de Processamento de Dados	8246	Atualização tecnológica hardware e software para desktop realizada
		8817	Solução de e-mail realizada
		8818	Solução para Digitalização e Guarda de documentos realizada

5. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. Requisitos de Negócios

5.1.1. A topologia da Rede IP Governo deve permitir que os dados trafegados sejam auditáveis, que haja detecção de incidentes e gargalos e capacidade de otimização de funcionamento. Esses requisitos contribuem para a atividade de resposta aos incidentes na Rede IP Governo.

5.1.2. Ao oferecer alta disponibilidade de link, estabilidade da conexão há um aumento na qualidade do serviço administrado, mantido e operado pelo PRODERJ.

5.1.3. A contingência é um dos fatores fundamentais para a garantia de que o negócio sempre terá os seus recursos de rede disponíveis. Considerando que a Nuvem Híbrida do Estado do Rio de Janeiro é uma realidade crescente, a garantia de continuidade desses serviços torna-se essencial.

5.1.4. As ameaças críticas para redes mudaram muito com o passar dos anos e, hoje, se concentram em esforços como os ataques DDoS. Esses ataques volumétricos de negação de serviços distribuídos cresceram mais do que nunca nos últimos anos, acometendo várias empresas ao redor do mundo em um intervalo de poucos dias.

5.1.5. As redes que não estavam preparadas para lidar com esse tipo de ataque foram as que mais sentiram o problema. Desde então, houve um investimento massivo em duplicidade de serviços, redundância de links e outras tecnologias mitigadoras de ataques DDoS para garantir a alta disponibilidade de serviços entregue aos usuários.

5.1.6. A operação 24 horas por dia, 7 dias na semana e em todos os dias do ano por si só não garantem a disponibilidade dos serviços. Sem uma rede com contingência de links, a falha de um único dispositivo é capaz de afetar a prestação dos serviços por vários dias.

5.1.7. Além disso, a Rede Conect@.RJ tem caráter essencial, subsidiando os principais serviços e atividades do Governo do Estado do Rio de Janeiro, tais como: sistemas de telecomunicações, sistemas corporativos, correio eletrônico, acesso à Internet e à Intranet, transferência de arquivos, autenticação de usuários, integração de sistemas, gerência e segurança da informação, aplicações web, todos indispensáveis para a sua operacionalização e para o atendimento das metas e objetivos de governo.

5.1.8. Cada órgão do Estado deve ter a possibilidade de requisitar, ao longo do tempo, os enlaces que forem necessários para atender às suas demandas de links de dados.

5.1.9. A manutenção da alta disponibilidade da Rede Conect@.RJ necessita do provimento de links de comunicação de dados principal e de contingência para garantir a continuidade dos serviços prestados pelo PRODERJ a todas as Secretarias e Órgãos públicos estaduais.

5.1.10. Há também a necessidade de atendimento às demandas de acesso à Internet de forma itinerante, com soluções desmontáveis e transportáveis e também aquelas fixas para funcionamento mesmo em movimento em altas velocidades, embarcadas em veículos automotores, por exemplo. Além disso, há presença do Estado em locais de difícil acesso ou sem as facilidades físicas dos enlaces de rede tradicionais (Ex. fibra ótica). Todos estes cenários são atendidos com redes satelitais ou 4G/5G.

5.1.11. Assim, para evitar problemas relacionados à indisponibilidade dos sistemas, bases de dados e aplicações, ocasionados por problemas nos serviços das operadoras, esta contratação deverá considerar essencialmente os requisitos pertinentes para garantir alta capacidade de resiliência na operação e na disponibilidade dos acessos corporativos e à Internet.

5.1.12. Portanto, no caso de qualquer indisponibilidade nos links da operadora principal, o acesso aos

sistemas e aplicações será automaticamente encaminhado para o link de contingência garantindo assim que não haja interrupções na prestação de serviços de governo eletrônico.

5.1.13. Este documento tem por objetivo registrar a necessidade de contratação de serviços de comunicação de dados que viabilizem a conectividade entre unidades remotas da Administração Pública Estadual, garantindo desempenho, confiabilidade e disponibilidade adequados às demandas institucionais. A contratação deverá atender às diversas realidades geográficas e operacionais dos órgãos e secretarias estaduais, contemplando cenários em que a infraestrutura de conectividade convencional é limitada ou inexistente.

5.1.14. Espera-se que a solução a ser contratada permita a comunicação eficiente entre os entes públicos, suportando a operação de serviços críticos e possibilitando o monitoramento, gestão e suporte técnico adequados. As especificações técnicas, condições de fornecimento, níveis de desempenho e demais exigências serão detalhados nos artefatos técnicos da contratação.

5.1.15. O link de comunicação de dados principal e de contingência entre os sites remotos deverá permitir o transporte de grandes quantidades de informação (voz, dados, vídeo, etc.) consolidando a totalidade de suas comunicações em um único canal de transmissão em interface Ethernet. Todo o tráfego proveniente de múltiplos serviços da rede local deverá ser transportado através de uma VLAN dentro do Backbone da CONTRATADA, com segurança e performance garantidas.

5.1.16. Este serviço deverá ser prestado sobre uma rede Carrier Ethernet, ou seja, utilizando redes Ethernet para áreas Metropolitanas e Geograficamente distribuídas. A solução deverá estar configurada sobre backbone óptico metropolitano do Estado do Rio de Janeiro. Os circuitos propostos devem possuir velocidade de 30 (trinta) Mbps ou superior, interconectando as localidades onde encontram-se as Secretarias e Órgãos públicos estaduais, que seguirão como anexo do Termo de Referência.

5.2. Requisitos de Capacitação

5.2.1. Não se aplica para a presente contratação.

5.2.2. Requisitos Legais

5.2.2.1. **Aplicáveis ao objeto:**

5.2.2.2. **Lei Geral de Telecomunicações (Lei nº 9.472/1997) :** Esta lei estabelece as normas para organização dos serviços de telecomunicações, incluindo os serviços de transmissão de dados.

5.2.2.3. **Marco Civil da Internet (Lei nº 12.965/2014):** Define princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo regras sobre neutralidade de rede e responsabilidade dos intermediários.

5.2.2.4. **Regulamentação da Anatel (Agência Nacional de Telecomunicações) :** A Anatel estabelece regulamentos específicos para a prestação de serviços de telecomunicações, que também se aplicam aos serviços de link de dados.

5.2.2.5. **Resoluções da Anatel:** Normas específicas podem ser encontradas nas resoluções da Anatel, que detalham requisitos técnicos, operacionais e comerciais para os serviços de telecomunicações.

5.2.2.6. **Lei do SeAC (Serviço de Acesso Condicionado - Lei nº 12.485/2011) :** Regula o serviço de televisão por assinatura, mas também pode ter aplicabilidade em casos de transmissão de dados relacionados à distribuição de conteúdo audiovisual.

5.2.2.7. **Normas da ABNT (Associação Brasileira de Normas Técnicas):** Em alguns casos, normas técnicas da ABNT podem ser referenciadas para padronização e qualidade dos serviços de telecomunicações.

5.3. Requisitos de Manutenção

5.3.1. A CONTRATADA deverá fornecer os serviços de manutenção preventiva, corretiva, evolutiva e adaptativa para todos os acessos contratados, incluindo os links SD-WAN principal e de contingência, os acessos via satélites de baixa órbita e geoestacionários, as soluções baseadas em 4G/5G, bem como os acessos VSAT, abrangendo antenas e receptores satelitais (IDU), assegurando a continuidade e a qualidade do serviço.

5.3.2. A CONTRATADA deverá proceder com a implementação de melhorias e otimizações nos equipamentos e sistemas fornecidos, visando a atualização tecnológica e o aprimoramento do desempenho, desde que previamente acordadas entre as partes.

5.3.3. A CONTRATADA deverá proceder com os ajustes necessários para adequação dos equipamentos e serviços a novas normativas regulatórias, requisitos técnicos ou mudanças nas condições operacionais da CONTRATANTE.

5.3.4. As manutenções deverão ser realizadas preferencialmente no local de instalação dos equipamentos, exceto nos casos em que a complexidade do reparo exija a remoção do item para manutenção em laboratório ou outro ambiente apropriado, hipótese em que a CONTRATADA deverá providenciar um equipamento reserva para garantir a continuidade do serviço.

5.3.5. Além disso, a CONTRATANTE será responsável pelos custos de reparação de danos aos equipamentos da CONTRATADA instalados em veículos, caso decorram de acidentes automotivos.

5.4. **2. Manutenção corretiva**

5.4.1. A Manutenção Técnica Corretiva contempla os serviços de reparo com a finalidade de eliminar todos os defeitos existentes nos equipamentos identificados por meio de diagnóstico, bem como da correção de anormalidades, da realização de testes e ajustes que sejam necessários para garantir o retorno do equipamento e/ou link de comunicação de dados às condições normais de funcionamento, e também na substituição do equipamento sem que haja prejuízo ao funcionamento do sistema;

5.4.2. Caberá à CONTRATADA manter a conectividade em perfeitas condições de uso durante todo o período de duração do contrato, comprometendo-se a reparar ou substituir, se for o caso, os acessórios ou componentes que apresentarem falhas e que caracterizam ou não perda das funções básicas do acesso;

5.4.3. As falhas constatadas deverão ser sanadas de imediato, observando os prazos previstos no acordo de nível de serviço que integrará o Termo de Referência;

5.4.4. A manutenção técnica corretiva não ensejará quaisquer custos adicionais ao CONTRATANTE, sendo parte integrante da prestação de serviços contratada.

5.5. **3. Manutenção preventiva**

5.5.1. Contempla os serviços efetuados para manter os equipamentos e links funcionando em condições normais, tendo como objetivo diminuir as possibilidades de paralisações, compreendendo:

a) manutenção do bom estado de conservação, substituição ou reparo de componentes que comprometam o bom funcionamento, atualizações de software, configuração de patches ou quaisquer modificações necessárias com objetivo de manter update dos equipamentos, limpeza, ajustes, inspeção e simulação de testes mecânicos e eletroeletrônicos em todo a rede, entre outras ações que garantam que o conjunto dos equipamentos e links estejam em permanente condição de operação;

b) a manutenção técnica preventiva deve ser executada periodicamente, com frequência não superior a 180 (cento e oitenta) dias;

A CONTRATADA deverá elaborar e entregar ao Gestor/Fiscal de Contrato da CONTRATANTE, após a execução de cada manutenção preventiva e/ou corretiva, um relatório do serviço prestado onde deverá constar:

a) a data da manutenção, os itens verificados, as anomalias encontradas, medidas corretivas adotadas (quando for o caso), peças ou equipamentos substituídos, nome do técnico responsável pela manutenção, bem como outras informações julgadas relevantes durante o procedimento;

b) a manutenção técnica preventiva não ensejará quaisquer custos adicionais ao CONTRATANTE, sendo parte integrante da prestação de serviços contratada.

5.6. **Disposições gerais relacionadas ao serviço de manutenção técnica**

5.6.1. Para a gestão dos serviços de manutenção preventiva e corretiva, a CONTRATADA deverá utilizar de sistema de gerenciamento que permita:

a) abertura de chamados de manutenção;

b) acompanhamento do planejamento e execução das manutenções preventivas e corretivas;

c) flexibilidade e simplicidade na organização dos dados e informações;

d) apresentação de resultados em formas de tabelas e gráficos;

e) diversas consultas e relatórios com recursos de ordenação, filtro e localização;

f) criação de relatórios personalizados;

g) distinção de níveis de permissão.

5.6.2. A execução do objeto da contratação se dará em conformidade com as cláusulas, condições, garantias, obrigações e responsabilidades entre as partes, conforme Termo de Referência e instrumento contratual a ser elaborado, que terá como base o presente Estudo Técnico Preliminar e requisitos técnicos constantes neste documento;

5.6.3. Fornecimento de todos os equipamentos, materiais e insumos necessários para a prestação dos serviços constantes no objeto da presente contratação, podendo ser realizado em regime de COMODATO, que nada mais é do que o empréstimo gratuito ao CONTRATANTE dos equipamentos, materiais e insumos necessários para a adequada prestação dos serviços pretendidos e se conclui com a entrega do objeto devidamente instalado nas localidades definidas pela CONTRATANTE;

5.6.4. O prazo do COMODATO, quando cabível, será igual à vigência do contrato a ser celebrado, decorrente do processo licitatório;

5.6.5. Findada a vigência contratual, os equipamentos cedidos em comodato deverão ser totalmente desinstalados e retirados de todas as dependências da CONTRATANTE, às expensas exclusivamente da CONTRATADA, no prazo de 30 (trinta) dias corridos;

5.6.6. Aplicam-se, no que couber, as demais regras de COMODATO previstas no Código Civil Brasileiro, Lei nº 10.406/2002 e alterações e demais dispositivos legais pertinentes.

5.7. Requisitos temporais

5.7.1. O prazo de entrega completa da solução será de até 180 (cento e oitenta) dias corridos após emissão da ordem de serviço, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Contratações Públicas.

5.8. Requisitos de Segurança da Informação

5.8.1. A CONTRATADA, quando da assinatura do contrato, por meio de seu representante, assinará o Termo de Confidencialidade e Sigilo em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação. O termo visa assegurar que a CONTRATADA manterá sigilo, sob pena de responsabilidade civil, penal e administrativa:

a) Sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, devendo orientar seus empregados e prepostos nesse sentido.

b) Sobre todas as informações relativas à prestação dos serviços, incluindo documentação, procedimentos, configurações de equipamentos, softwares, políticas e quaisquer informações obtidas pela CONTRATADA em função da prestação dos serviços, mesmo após o término do prazo de vigência ou rescisão do contrato.

c) Sobre a política de segurança adotada pela CONTRATANTE e as configurações de hardware e de softwares decorrentes.

d) Sobre o processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos.

e) Sobre o processo de implementação, no ambiente da CONTRATANTE, dos mecanismos de criptografia e autenticação.

5.8.2. A CONTRATADA não poderá efetuar, sob qualquer pretexto, a transferência de qualquer responsabilidade que lhe compete para outras entidades, sejam fabricantes, técnicos, subempreiteiros etc, sem a anuência expressa da CONTRATANTE.

5.8.3. A CONTRATADA deverá, ainda, submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pela CONTRATANTE, durante o tempo de permanência nas suas dependências.

5.8.4. O fornecedor não poderá armazenar consigo qualquer documento técnico que contemple configurações e regras de segurança aplicadas nos equipamentos implantados na rede da CONTRATANTE.

5.8.5. Todos os perfis de acesso e caixas postais eventualmente concedidos ao CONTRATADA deverão ser imediatamente excluídos após o término do contrato.

5.8.6. A CONTRATANTE terá propriedade sobre todos os dados, documentos e procedimentos operacionais produzidos no escopo da presente contratação.

5.8.7. A CONTRATADA deverá respeitar as normas de segurança estabelecidas na Política de Segurança da Informação e da Lei Geral de Proteção de Dados Pessoais durante a realização de atividades nas dependências da CONTRATANTE.

5.8.8. Não será permitida intervenção nas bases de dados, a menos que haja autorização expressa e formal da área gestora dos sistemas.

5.8.9. A inclusão de componentes de software proprietários sem prévia e expressa autorização da CONTRATANTE é vedada em qualquer das etapas de execução dos serviços.

5.9. **Requisitos de Privacidade e Proteção de Dados Pessoais**

5.9.1. Competirá à CONTRATADA, na qualidade de CONTROLADORA, estar em conformidade com as diretrizes contempladas na Lei nº 13.709/18, assegurando os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural durante a realização de quaisquer operações enquadradas no preceito de tratamento de dados pessoais.

5.9.2. O objeto deverá ser implantado e executado em observância aos direitos dos titulares, nos moldes do Art. 18 da LGPD.

5.9.3. Para concretização dos resultados explicitados no Item 2 - Resultados Pretendidos – não haverá a coleta e/ou armazenamento de dados pessoais.

5.9.4. A solução não apresenta funcionalidades que se enquadrem em tratamento de dados pessoais.

5.9.5. A parte CONTRATADA contará como mecanismo de segurança a solução firewall camada 7, podendo ser substituída por soluções semelhantes que alcancem idêntico escopo.

5.9.6. As partes contratadas deverão ajustar as obrigações e responsabilidades na hipótese de realização superveniente de operações de tratamento de dados pessoais, observando as previsões explicitadas na Lei Federal nº 13.709/18.

5.10. **Requisitos de Sustentabilidade Ambiental**

5.10.1. A contratada deverá observar a legislação e princípios de responsabilidade socioambiental (Lei nº 12.305/2010), bem como obedecer aos critérios previstos no capítulo I do Decreto 43.629/2012, por meio dos artigos 1º e 2º, in verbis:

Art 1º - As especificações para a aquisição de bens, contratação de serviços e obras por parte dos órgãos e entidades da Administração Pública Estadual Direta e Indireta, a fixação de critérios de julgamento e a execução e fiscalização dos respectivos contratos, observarão critérios de sustentabilidade ambiental, na forma deste Decreto.

Art. 2º - Consideram-se critérios de sustentabilidade ambiental, dentre outros:

- economia no consumo de água e energia;

- minimização da geração de resíduos e destinação final ambientalmente adequada dos que forem gerados;

- racionalização do uso de matérias-primas;

- redução da emissão de poluentes;

- adoção de tecnologias menos agressivas ao meio ambiente;

- implementação de medidas que reduzam as emissões de gases de efeito estufa e aumentem os sumidouros;

- utilização de produtos de baixa toxicidade;

- utilização de produtos com a origem ambiental sustentável comprovada, quando existir certificação para o produto.

5.10.2. Por se tratar de serviços de enlaces de comunicação de dados, não se faz necessário declaração de não ofertar produtos com materiais perigosos.

5.10.3. Os equipamentos devem atender todas as normativas da ANATEL, em especial quanto ao limite de emissão de ondas eletromagnéticas, possuindo selo de certificação da Agência Nacional de Telecomunicações.

5.10.4. Os equipamentos devem atender toda legislação ambiental no que tange aos equipamentos eletrônicos, sendo devidamente certificados pelos órgãos competentes, com importação regular, se for o caso.

5.11. **Requisitos de arquitetura tecnológica**

5.11.1. Todos os requisitos tecnológicos da solução estão descritos no Anexo I - Especificações Técnicas.

5.12. **Requisitos de projeto e de implementação**

5.12.1. A CONTRATADA deverá elaborar o Projeto Físico e Lógico das redes principal e de contingência, que deverá ser submetido ao CONTRATANTE para aprovação quando da implantação dos circuitos solicitados.

5.12.2. O CONTRATANTE será responsável pela configuração dos elementos de sua rede interna de forma que projeto aprovado possa ser implementado.

5.12.3. Demais requisitos de implementação estarão descritos no Anexo I - Especificações Técnicas associado a solução escolhida.

5.13. **Requisitos de garantia**

5.13.1. As soluções de hardware e software que farão parte da prestação dos serviços devem ser ofertadas com garantia do fabricante durante toda a vigência contratual, contados a partir do recebimento definitivo, a qual comporta: a garantia comumente utilizada pelo fabricante acrescida de todas as licenças/subscrições necessárias para o perfeito funcionamento da solução, e de suporte técnico.

5.13.2. A garantia durante toda a vigência contratual se justifica por se tratar de equipamentos aos quais se vislumbra ter utilização intensiva e diária, e portanto o suporte do fabricante se mostra fundamental para garantia do pleno funcionamento do item, e para mitigar os tempos de indisponibilidades permitindo rápida atuação da CONTRATADA na análise e reposição de peças, se for o caso.

5.13.3. Durante o período da garantia, no caso de qualquer um dos produtos apresentarem defeitos, precisar ser reparado ou substituído, a CONTRATADA deverá reparar ou repor o produto no mesmo local onde o mesmo encontra-se instalado.

5.13.4. Caso a CONTRATADA verifique a necessidade de encaminhar equipamento para assistência técnica, deverá providenciar a imediata reposição de outro equipamento ao CONTRATANTE, em perfeito estado de funcionamento e com características técnicas idênticas ou superiores àquelas do equipamento defeituoso, o qual o substituirá até a conclusão de seus reparos. É responsabilidade da CONTRATADA a instalação e configuração do novo equipamento, garantindo o funcionamento da solução dentro das mesmas condições anteriores ao problema. Cabe lembrar que a CONTRATADA é responsável pela garantia do sigilo das informações configuradas no equipamento.

5.13.5. Para retirada do equipamento defeituoso das dependências da CONTRATANTE, deverá a CONTRATADA relatar, por escrito, a situação ao servidor responsável pelo acompanhamento dos serviços, que, após constatar tal necessidade, autorizará a saída também por escrito.

5.13.6. O equipamento colocado em substituição ficará instalado nas dependências da CONTRATANTE até a devolução do equipamento consertado, que deverá ocorrer no prazo de até 30 (trinta) dias corridos após a sua retirada para reparos.

5.13.7. Durante a vigência da garantia, caso os equipamentos fornecidos sejam descontinuados na linha de produção do fabricante, a CONTRATADA deverá manter as condições previstas neste documento ou providenciar a substituição por outros modelos disponíveis que executem as mesmas funcionalidades exigidas, sem ônus adicionais para a CONTRATANTE. Não será permitido à CONTRATADA ofertar dispositivo(s) que possuam aviso de end of sale ou end of life por parte do fabricante.

5.13.8. As peças e componentes substituídos deverão ser entregues ao CONTRATANTE, juntamente com o equipamento consertado, salvo definição contrária pelo CONTRATANTE e qualquer substituição deverá ser acompanhada por técnico designado pela mesma.

5.13.9. Todas as peças, dispositivos ou mesmo unidades que forem substituídas durante o período de garantia terão, a partir de sua entrega, todas as garantias descritas neste item.

5.13.10. As peças/equipamentos de reposição devem ser originais do fabricante ou por empresa por ele homologada e certificada, devendo apresentar características equivalentes ou superiores.

5.13.11. A garantia do fabricante deverá contemplar reposição de peças, equipamentos e componentes defeituosos, sem ônus adicional para o CONTRATANTE, a fim de que o funcionamento do equipamento seja restabelecido de maneira completamente funcional, pelo prazo de toda a vigência contratual

5.13.12. A garantia do fabricante deve cobrir os defeitos decorrentes de projeto, fabricação, construção, montagem, acondicionamento, transporte, erros na instalação física e/ou desgaste prematuro, envolvendo, obrigatoriamente, a substituição dos componentes defeituosos, sem qualquer ônus adicional para o CONTRATANTE.

5.13.13. A CONTRATADA deverá oferecer telefone de suporte e e-mail para abertura e acompanhamento dos chamados para acionamento da garantia, comprometendo-se a manter registros

dos mesmos. O contato telefônico deverá ser do tipo 0800 ou telefone local em português do Brasil e deverá funcionar em regime 24x7 (todos os dias do ano).

5.13.14. A CONTRATADA deverá disponibilizar, via web ou impresso, relatório técnico indicando os defeitos, procedimentos realizados, data/hora e nome do colaborador responsável.

5.13.15. A empresa deverá fornecer certificados de garantia, por meio de documentos próprios, ou anotação impressa ou carimbada na Nota Fiscal respectiva.

5.13.16. Aplicar-se-á, no que couber, as disposições do Código de Proteção e Defesa do Consumidor, instituído pela Lei nº 8.078, de 11 de setembro de 1990.

5.13.17. O fabricante deverá possuir site na internet com a disponibilização de manuais, drivers, firmwares e todas as atualizações existentes relativas ao equipamento ofertado.

5.13.18. Durante toda a vigência da GARANTIA, deverá ser mantida a base de conhecimento de problemas, bem como o histórico dos reparos ou substituições para os equipamentos fornecidos.

5.13.19. Os danos provocados por imperícia ou negligência (comprovado mau uso) dos usuários estão compreendidos na hipótese de exclusão da garantia.

5.14. **De experiência e formação da equipe que executará os serviços relacionados à solução de TIC**

5.14.1. Considerando a criticidade dos serviços de comunicação de dados a serem contratados, especialmente no que tange à disponibilidade, segurança, desempenho e suporte à infraestrutura de TIC da solução ofertada, faz-se necessária a exigência de equipe técnica devidamente capacitada para a execução das atividades..

5.14.2. A exigência de qualificação técnica tem como objetivo mitigar riscos operacionais, garantir a correta execução dos serviços contratados e assegurar a continuidade dos serviços prestados à administração pública.

5.14.3. A equipe técnica para o serviço deverá possuir qualificação conforme estabelecido no Anexo I - Especificações Técnicas.

5.15. **Requisitos materiais e humanos**

5.15.1. Materiais

5.15.1.1. Para fornecimento de links de acesso à internet dedicados com segurança embarcada e rede gerenciada via software (Firewall e SD-WAN), considerando que há fornecimento de equipamentos em comodato, além de insumos, os requisitos materiais devem ser definidos conforme o § 2º do art. 25 da Lei nº 14.133/2021, que trata da necessidade de detalhamento de bens e serviços associados à contratação.

a) Firewall (NGFW) com suporte a equipamentos e políticas de segurança, inspeção de tráfego criptografado, prevenção contra ameaças e integração com SD-WAN.

b) Dispositivos SD-WAN capazes de gerenciar múltiplos links, aplicar políticas de QoS e otimizar a conectividade com balanceamento de carga e failover automático.

c) Opcionais

d) Roteadores e switches gerenciáveis, caso sejam necessários para viabilizar a integração dos links com a infraestrutura existente.

e) Insumos Necessários

f) Patch panels, cabos de fibra óptica e conectores para integração física dos equipamentos à infraestrutura da CONTRATANTE.

g) Suportes ou racks, caso a CONTRATANTE não possua em sua infraestrutura.

5.16. **Especificações Técnicas e Condições de Fornecimento**

5.16.1. A CONTRATADA deverá fornecer equipamentos atualizados tecnologicamente em sua última versão, não podendo estar em situação de End-of-Life ou End-of-Sale, estarem sendo suportados e recebendo atualizações de segurança do fabricante, e que atendam integralmente os requisitos técnicos que serão estabelecidos no Termo de Referência e seus Anexos, bem como realizar a substituição de qualquer componente sempre que solicitado pela CONTRATANTE, com a devida justificativa técnica.

5.16.2. Os equipamentos devem ser entregues **pré-configurados** para integração imediata à infraestrutura de TI do órgão.

5.16.3. O fornecimento deve incluir **licenciamento de software e suporte técnico** para os equipamentos durante a vigência do contrato.

5.16.4. Os equipamentos que formarão o backbone da Rede Conect@.RJ devem ser **compatíveis e interoperáveis com aqueles a serem instalados nas unidades remotas, principalmente no serviço de SD-WAN**.

5.17. **Quantitativo de usuários**

5.17.1. Com relação a mão de obra especializada, está diretamente relacionada com a garantia e instalação dos produtos, não se configurando em nenhuma hipótese de terceirização de serviços, principalmente pelo fato de que não há previsão de mão de obra residente/exclusiva no objeto da presente contratação.

5.18. **Horário de Funcionamento do Órgão em que deverão ser prestados os serviços**

5.18.1. O horário padrão de funcionamento será entre 08h e 18h, de segunda a sexta-feira. No entanto, há órgãos e secretarias com funcionamento 24x7x365.

5.19. **Restrições de área, identificando questões de segurança institucional, privacidade, segurança, medicina do trabalho, dentre outras;**

5.19.1. Todos os prestadores de serviço da CONTRATADA deverão estar devidamente identificados com crachá da empresa.

5.19.2. Disposições normativas internas

5.19.3. Os prestadores estarão sujeitos às normativas internas da CONTRATANTE, que serão disponibilizadas à CONTRATADA no momento da assinatura do contrato.

5.20. **Requisitos de suporte técnico**

5.20.1. O suporte técnico aos produtos fornecidos deverá contemplar as atividades de assistência técnica e suporte on-line para atendimento em caso de problemas identificados na infraestrutura de rede e conectividade, esclarecimentos de dúvidas técnicas (por telefone e e-mail) , atualização de firmware e software, sem limites de chamados técnicos em qualquer modalidade.

5.20.2. O suporte técnico, obrigatoriamente, deverá ser realizado pelo fabricante da solução ou pela CONTRATADA, desde que esta seja credenciada pelo fabricante.

5.20.3. O suporte técnico deverá prever o aconselhamento sobre a implementação e a melhor utilização dos produtos adquiridos.

5.20.4. Inicialmente, todo atendimento será realizado via telefone ou Internet, salvo quando uma visita técnica for julgada necessária pelos especialistas da CONTRATADA ou quando for solicitada pelo CONTRATANTE para solução de um problema. Os dias e horários de atendimento obedecerão à conveniência da CONTRATANTE;

5.20.5. Os chamados somente poderão ser fechados após concordância e autorização da CONTRATANTE;

5.20.5.1. A CONTRATADA entregará, ao final do atendimento on-site, relatório que conste, minimamente, os dados do técnico da CONTRATADA, os dados do colaborador que abriu o chamado junto à CONTRATADA, o problema descrito no ato da abertura do chamado, a avaliação e solução implementada, observações, hora de abertura e fechamento do chamado, e campo para assinatura de representantes da CONTRATADA e da CONTRATANTE;

5.20.5.2. A CONTRATADA deverá instalar e configurar todos os componentes das soluções descritas neste Estudo Técnico e seus Anexos, bem como disponibilizar garantia e suporte técnico às atividades operacionais para o atendimento de demandas da CONTRATANTE referentes aos equipamentos e softwares adquiridos, envolvendo as seguintes atividades:

a) Substituição de equipamento defeituoso;

b) Atualização de firmware/IOS;

c) Aplicação de patches de segurança em todos os ativos envolvidos;

d) Instalação e/ou atualização de licenças;

e) Recebimento e acompanhamento de alertas dos equipamentos;

f) Suporte a rotinas operacionais;

g) Suporte na resolução de problemas;

h) Atualização de versões, releases e patches aplicados nos ativos, com o devido histórico.

5.20.5.3. O suporte presencial, quando houver, deverá ocorrer nos locais definidos pela CONTRATANTE

e em todos os locais a serem definidos pela CONTRATANTE, sem ônus adicional, no que se refere à viagem, transporte, hospedagem, alimentação ou qualquer outra despesa, relacionada ou não, a prestação do respectivo suporte.

5.20.5.4. A CONTRATADA deverá disponibilizar um número único nacional não tarifado (0800) para abertura de chamados de suporte técnico, como também o Serviço de Gerência fornecido pela CONTRATADA deverá ser capaz de gerenciar os níveis de serviços acordados.

5.20.5.5. A assistência técnica on-site deverá ser prestada nas instalações da CONTRATANTE, sítios e unidades especiais conforme os prazos estipulados nos Níveis Mínimos de Serviço (NMS).

5.20.5.6. No momento de abertura do chamado deverá ser fornecido ao CONTRATANTE um número único de identificação do chamado. Os chamados somente poderão ser abertos e fechados após autorização da CONTRATANTE.

5.20.5.7. Os serviços de suporte técnico deverão incluir serviços de atualização dos equipamentos componentes da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de softwares de equipamentos.

5.20.5.8. A CONTRATADA deverá disponibilizar, ainda, um número de telefone ao CONTRATANTE para contato com a área de suporte de 2º nível para solução de problemas urgentes que necessitem a atuação imediata, tais como: reinício de interfaces de roteadores, conferência de aplicação de políticas nos roteadores, lista de acesso, ativação de modo debug de forma temporário para diagnóstico, verificação de logs, configuração de velocidade e modo de operação de interfaces, elaboração de listas de acesso temporárias e reinício de equipamentos.

5.20.5.9. A CONTRATANTE reserva-se o direito de promover, a qualquer tempo, alterações nas políticas de utilização do serviço de acesso à Internet, ficando a CONTRATADA, neste caso, será obrigada a prestar o suporte técnico necessário à implementação dessas diretrizes nos equipamentos por ela empregados na prestação os serviços, inclusive nos roteadores locados, sem prejuízo das condições de funcionamento previstas no edital.

5.20.5.10. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo CONTRATANTE.

5.20.5.11. Em caso de reiterado inadimplemento do SLA, a CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato.

6. LEVANTAMENTO DE MERCADO

6.1. Considerando as demandas crescentes por comunicação eficiente, segura e ininterrupta entre os diversos órgãos e secretarias do Estado, torna-se necessária a contratação de serviços de conectividade de dados que possibilitem a manutenção e a evolução da infraestrutura de rede institucional existente, garantindo alta disponibilidade, escalabilidade e resiliência.

6.1.1. A solução a ser contratada deverá atender a um conjunto diversificado de necessidades, incluindo:

a) Interligação de ambientes de Tecnologia da Informação e Comunicação (TIC) distribuídos geograficamente pelo território estadual, com qualidade de serviço adequada para o tráfego de dados, voz, vídeo e aplicações críticas;

b) Garantia de continuidade dos serviços de rede, mesmo diante de eventuais falhas ou indisponibilidades, por meio de uma arquitetura de alta resiliência;

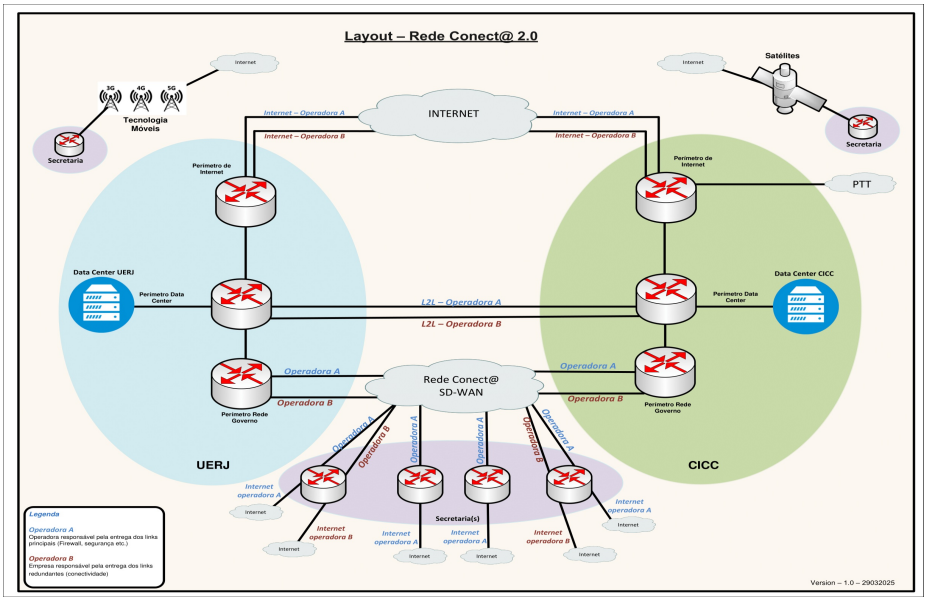
c) Capacidade de atendimento em áreas com infraestrutura limitada ou inexistente, incluindo localidades remotas e de difícil acesso;

d) Suporte às tecnologias emergentes utilizadas pela administração pública, como telefonia sobre IP (VoIP), virtualização de desktops (VDI), sistemas em nuvem, entre outros;

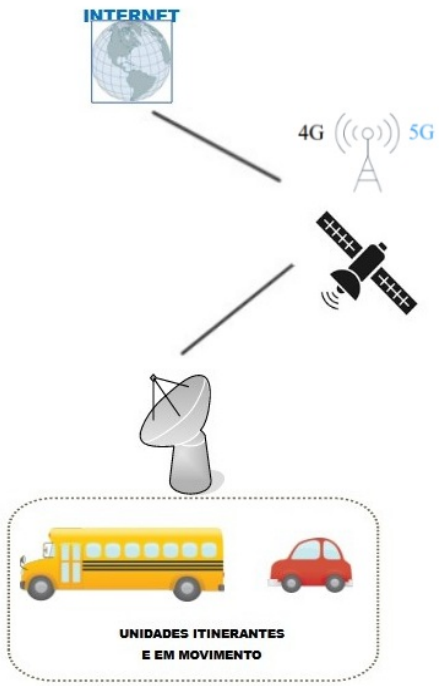
e)Monitoramento proativo, suporte técnico qualificado, e gestão integrada dos serviços prestados.

6.2. A fim de organizar a futura contratação de forma eficiente e adequada às diferentes realidades e necessidades dos órgãos públicos, o objeto deverá ser estruturado em diferentes grupos de serviços, com requisitos e metas específicas de desempenho, de acordo com a solução de mercado que melhor se adequar às necessidades da Administração.

6.3. Abaixo o desenho esquemático da **Rede Conect@.RJ**:



1. Desenho esquemático das soluções móveis



6.4. **Análise do Cenário**

6.4.1. Com o objetivo de garantir uma infraestrutura de comunicação de dados resiliente e de alta disponibilidade, o PRODERJ busca viabilizar uma plataforma de conectividade capaz de sustentar de forma contínua e confiável as atividades desempenhadas pelos usuários da rede corporativa estadual.

Essa infraestrutura deve assegurar o desempenho adequado das aplicações críticas, tráfego de dados, voz e imagens, promovendo a melhoria da qualidade dos serviços públicos prestados à sociedade.

6.4.2. Além disso, é necessário que a solução ofereça flexibilidade e escalabilidade, de modo a atender às demandas variáveis dos órgãos e secretarias estaduais, incluindo unidades descentralizadas e de características especiais, mantendo a integridade e a continuidade operacional dos sistemas, bases de dados e demais recursos tecnológicos que compõem a Rede Governo.

6.4.3. A conectividade entre os ambientes distribuídos, inclusive em regiões com baixa infraestrutura, deve ocorrer de maneira integrada e transparente, promovendo a interligação eficiente entre o backbone da rede e os diversos pontos de presença do Estado, conforme os requisitos técnicos e níveis de serviço estabelecidos.

6.4.4. Visando atender aos preceitos estabelecidos nas normativas vigentes, a contratação deverá contemplar soluções que assegurem conectividade corporativa confiável, de alto desempenho e com níveis adequados de segurança, disponibilidade e escalabilidade. A prestação dos serviços deverá atender às diversas necessidades da administração pública estadual, incluindo o acesso à internet institucional, a interligação de unidades organizacionais em diferentes localidades e a garantia de operação contínua dos serviços, inclusive em áreas com infraestrutura limitada de telecomunicações.

6.4.5. A estrutura da contratação deverá considerar a diversidade de demandas e contextos operacionais, prevendo soluções aderentes aos requisitos técnicos definidos e alinhadas aos objetivos estratégicos da administração, garantindo a continuidade e evolução da infraestrutura de rede que dá suporte aos serviços públicos.

6.4.6. Trata-se de um serviço contínuo, já contratado em ciclos anteriores, cuja natureza é essencial para a manutenção da comunicação entre os órgãos e entidades do Governo do Estado do Rio de Janeiro. A solução atualmente em operação demonstrou-se adequada ao longo do tempo, assegurando conectividade segura, com desempenho satisfatório e cobertura em todo o território estadual, atendendo às necessidades institucionais com níveis apropriados de disponibilidade e segurança.

6.4.7. Entretanto, com o avanço tecnológico e a evolução das demandas dos órgãos públicos, identificou-se a oportunidade de modernizar e otimizar os serviços atualmente contratados. A adoção de soluções mais atuais e eficientes poderá manter — e até ampliar — os padrões de qualidade alcançados, promovendo maior flexibilidade, escalabilidade e eficiência operacional, além de possibilitar, em muitos casos, a redução de custos recorrentes.

6.4.8. Dessa forma, o presente estudo considera não apenas a manutenção dos serviços já prestados, em razão de sua continuidade essencial, mas também sua evolução, alinhada às inovações tecnológicas disponíveis no mercado e às diretrizes de transformação digital da administração pública.

6.4.9. No contexto da evolução das tecnologias de conectividade, serão analisadas alternativas que possibilitem a modernização da arquitetura de rede atualmente em operação, considerando desde a manutenção do modelo vigente até a adoção de novas soluções ou, eventualmente, a convivência entre diferentes tecnologias, de forma a garantir desempenho, segurança e eficiência na prestação dos serviços.

6.4.10. Durante o levantamento de mercado, será avaliado o grau de aderência das soluções disponíveis por parte dos prestadores de serviços de telecomunicações, com base nas características técnicas e operacionais exigidas para atendimento às necessidades da administração pública estadual. Essa análise permitirá identificar o modelo mais adequado à realidade do Estado, observando aspectos como cobertura, qualidade, escalabilidade, suporte técnico e conformidade com as diretrizes legais e estratégicas da contratação pública.

6.4.11. Os potenciais fornecedores poderão utilizar as tecnologias que atendam aos requisitos técnicos mínimos e definidos no Anexo de Especificações Técnicas.

6.4.12. Outra solução que pode ser objeto deste estudo é a construção de uma rede própria, do Governo do Estado do Rio de Janeiro, a ser mantida e operada pelo PRODERJ. No entanto, tal projeto demandaria esforço e recursos financeiros incompatíveis com a realidade do Estado do Rio de Janeiro, que se encontra em Regime de Recuperação Fiscal, além da questão de prazos, pois a realização de obras em todo o estado para instalação de fibras óticas, os tempos associados e licenças municipais, de 5 (cinco) a 10 (dez) anos é o que se estima para conclusão de tal projeto.

6.5. **Levantamento das soluções de mercado**

6.5.1. **Solução 1 - Acesso através de link de banda larga internet**

6.5.1.1. Conexão de banda larga com a internet, pode-se dar através de diversos meios, a exemplo da ADSL, 4G, 5G, Rádio, entre outras. As tecnologias de rádio que compreendem 4G, 5G e Rádio não serão consideradas neste estudo, pois com elas trazemos problemas de interferência climática, física e eletromagnética, cobertura, tempo de resposta além de risco de descargas atmosféricas, ferindo o requisito de isolamento elétrico, risco esse que podem comprometer todos os equipamentos internos. O

uso de somente uma tecnologia de conectividade já foi experimentado e se mostrou limitado por falhas da operadora, ou dos equipamentos, ou devido a alta latência de comunicação, deixando as atividades da autarquia comprometidas até o restabelecimento.

6.5.1.2. **Analisando o cenário é possível observar os seguintes pontos:**

a) A saída da comunicação da localidade será única, mantendo um ponto de falha da operadora e caso esta falhe a prestação jurisdicional é comprometida.

b) A navegação de internet será de forma direta não precisando passar pela capital;

c) Equipamentos de segurança serão necessários nos sites remotos, pois o tráfego de autenticação de usuários nas estações de trabalho precisam chegar até o Data Center

d) Em linhas gerais, esta solução por si só não trará muitos benefícios, pelo contrário, a complexidade da rede aumentará e vários pontos de controle adicionais precisarão ser implementados.

e) Prós: Baixo custo, simplicidade na instalação do ponto remoto e diversidade de fornecedores, otimizada para serviços em nuvem.

f) Contras: Complexidade lógica, instabilidade, baixo nível de segurança e controle e baixa confiabilidade.

6.6. **Solução 2: Acesso através de link MPLS**

6.6.1. O Multiprotocol Label Switching é um mecanismo em redes de telecomunicações de alto desempenho que direciona dados de um nó da rede para o próximo nó baseado em rótulos de menor caminho em vez de endereços de rede longos, evitando consultas complexas em uma tabela de roteamento. Essa tecnologia é atualmente utilizada no PRODERJ. O MPLS tem alta capacidade de entrega de pacotes e oferece alta qualidade de serviço (QoS). A solução é satisfatória em gerenciar e evitar perda de pacotes, mantendo o fluxo do tráfego mais importante. O MPLS é um protocolo de rede que controla o fluxo de tráfego entre dois locais. Então, as redes MPLS são redes privadas dedicadas e usam protocolos de roteamento avançados para enviar vários tipos de tráfego pela rede usando caminhos diferentes. Por exemplo, vídeo e voz precisam de uma rota de baixa latência para garantir que o desempenho seja alto, contudo, o tráfego geral da internet pode seguir uma rota mais congestionada porque o atraso não é um problema. Portanto, a vantagem do MPLS é que ele garante entrega de pacotes rápida e confiável, tornando-o ideal para aplicativos de alto desempenho ou em tempo real.

6.6.2. **Analisando o cenário é possível observar os seguintes pontos:**

a) Solução é usada há mais de 15 anos no PRODERJ e já é bem conhecida;

b) Possui somente um ponto de conexão com o Data Center, tanto para navegação da Internet quanto para conexão interna;

c) A estrutura atual já está toda preparada para esta solução.

d) Esta solução, por mais funcional que esteja hoje, não está mais atendendo os novos requisitos de velocidade e disponibilidade exigidos pelo período pós pandemia. Com o advento das videoconferências, caso a conectividade falhe as transmissões não podem ser realizadas, causando remarcações e atrasos impactando assim o trabalho remoto.

e) Prós: Melhor performance, estabilidade, confiabilidade e segurança, otimizada para o modelo cliente-servidor

f) Contras: Limitação de localidades e velocidade, maior custo por Mbps e ponto único de falha.

6.7. **Solução 3: Acesso através links MPLS + de Internet IP Dedicados + Serviço SD-WAN Seguro**

6.7.1. SD-WAN (Software-Defined Wide Area Network) é uma tecnologia que permite a administração de uma rede de larga escala de maneira mais simplificada e flexível. Em vez de depender de hardware específico e configurações complexas, a SD-WAN usa software para controlar e gerenciar a rede, o que permite que os usuários façam alterações rapidamente e de maneira mais fácil. O SD-WAN é uma forma de se agregar diversas conexões, e as utilizarem de forma concomitante, possibilitando também que exista redundância.

6.7.2. A tecnologia SD-WAN permite o uso racional das conexões de dados, garantindo a qualidade de comunicação, independentemente da tecnologia utilizada nos meios de transporte, com gerenciamento centralizado, garantindo um maior desempenho para as aplicações e ajudando a diminuir os riscos de interrupções de tráfego altamente sensível ao desempenho.

6.7.3. Proporciona também uma eficiente visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de qualidade de serviços (QoS), tipo de aplicação, desempenho e latência, com a

utilização de túneis VPN (Virtual Private Network) para comunicação entre os sites.

6.7.4. O SD-WAN Seguro é a tecnologia SD WAN agregada com soluções de segurança da informação. Os equipamentos possuem a capacidade de gerenciar as diversas conexões de rede e realizar a segurança dos usuários que as utilizam, contendo firewalls e outras tecnologias que previnem ataques cibernéticos. O SD- Wan Seguro pode proporcionar alta velocidade, redundância e segurança para as conexões das unidades do interior do estado.

6.7.5. É oportuno destacar que o PRODERJ possui solução em modelo-cliente servidor que necessitam de baixa latência, em especial, o banco de dados Oracle, a fim de que possam funcionar de maneira adequada. Além disso, há um crescimento das soluções baseadas em nuvem. Desta forma, para o modelo cliente-servidor a tecnologia MPLS é mais adequada, enquanto para o modelo em nuvem a rede Internet apresenta maior vantagem.

6.7.6. **Analisando o cenário é possível observar os seguintes pontos:**

a) A redundância de equipamentos e caminhos é priorizada para atender aos novos requisitos de disponibilidade dos sites remotos;

b) A junção das tecnologias de Internet e MPLS apresentam maior flexibilidade em cada um dos seus pontos positivos;

c) Fica facilitada a expansão da rede, com suporte a múltiplos provedores de Internet, aumentando a resiliência operacional;

d) Possibilidade de priorização de tráfego crítico (voz, vídeo, aplicações de missão crítica) sem necessidade de reconfiguração manual em cada site.

e) Possibilidade de utilizar múltiplos links simultaneamente (Internet IP Simétrica, 4G/5G, satélite), garantindo continuidade dos serviços em caso de falha de um provedor.

f) Roteamento dinâmico e balanceamento de carga automático entre links para evitar interrupções.

g)SD-WAN oferece criptografia de ponta a ponta, garantindo a integridade dos dados em redes públicas.

h) Roteamento otimizado para aplicações na nuvem, melhorando a experiência de uso de serviços como Microsoft 365, Google Workspace, AWS, Azure, etc.

i) A solução proposta tende a mitigar o risco de indisponibilidade por falhas nas conexões e lentidão durante a realização de transmissões e videoconferências.

j) Prós: Melhor performance, estabilidade, redundância, alta disponibilidade, alta confiabilidade e segurança.

k) Contras: Maior custo.

6.8. **Existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016:**

6.8.1. Não se aplica.

6.9. **As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis:**

6.9.1. Não se aplica.

6.10. **Análise comparativa de custos (TCO)**

6.11. **Cálculo dos Custos Totais de Propriedade - Memória de Cálculo**

6.12. **Solução considerada inviável**

6.13. **Solução 1 - Acesso através de link banda larga**

6.13.1. A opção existente além do link MPLS e de acesso à Internet, é a conexão de banda larga. A tecnologia de banda larga possui um custo menor de aquisição, porém não apresenta banda estável, conforme Resolução ANATEL nº 717, , de 23 de dezembro de 2019), ele pode variar entre 60% e 80% no download e 20% a 40% no upload. Além disso, o SLA da banda larga não atende os requisitos da solução (SLA da banda larga é de 48 horas).

6.14. **Solução 2: Acesso através de link MPLS**

a Principal

Órgão		Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
TRF4	LIGGA TELEC. S.A.	18/2022	01/05/2024	300	R$ 2.102,23	R$ 7,01
ANAC	CLARO	22/2020 - TA1	09/11/2023	192	R$ 1.799,60	R$ 9,37
CJF	ALGAR	29/2020	20/07/2023	200	R$ 1.700,00	R$ 8,50
TRE-TO	ZAP TELEC. LTDA	30/2022	13/07/2023	500	R$ 4.900,00	R$ 9,80
PREF. SALVADOR	TELEMAR	36/2020	24/06/2023	10000	R$ 52.612,79	R$ 5,26
PROPOSTA	OI			350	R$ 12.560,00	R$ 35,89
				Mediana por Mb		**R$ 8,94**
				Qtd	Qtd MB	
			SEDE	1	350	R$ 3.127,76
				Valor Mensal		**R$ 3.127,76**

s Remotos

Órgão		Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
TRF4	LIGGA TELEC. S.A.	18/2022	01/05/2024	50	R$ 576,29	R$ 11,53

TRF4	LIGGA TELEC. S.A.	18/2022	01/05/2024	35	R$ 514,63	R$ 14,70
TJ / MT	OI	05/2021	01/10/2022	200	R$ 5.600,00	R$ 28,00
TJ / MT	OI	05/2021	01/10/2022	200	R$ 4.550,00	R$ 22,75
TJ / MT	OI	05/2021	01/10/2022	50	R$ 2.500,00	R$ 50,00
TJ / MT	Brasil Digital	04/2021	26/09/2022	200	R$ 4.334,10	R$ 21,67
TJ / MT	Brasil Digital	04/2021	26/09/2022	50	R$ 7.000,00	R$ 140,00
TJ / MT	REDE EXS	03/2021	03/10/2022	50	R$ 3.300,00	R$ 66,00
TJ / MT	REDE EXS	03/2021	03/10/2022	200	R$ 5.900,00	R$ 29,50
ANAC	CLARO	22/2020 - TA1	09/11/2023	46	R$ 1.276,24	R$ 27,74
ANAC	CLARO	22/2020 - TA1	09/11/2023	24	R$ 631,75	R$ 26,32
CJF	ALGAR	29/2020	20/07/2023	100	R$ 1.200,00	R$ 12,00
PREF. SALVADOR	TELEMAR	36/2020	24/06/2023	50	R$ 2.219,67	R$ 44,39
TRE-TO	ZAP TELEC. LTDA	30/2022	13/07/2023	100	R$ 1.150,00	R$ 11,50
PROPOSTA	OI			30	R$ 4.300,00	R$ 143,33
PROPOSTA	OI			50	R$ 5.100,00	R$ 102,00
				Mediana por Mb		**R$ 27,87**
				Qtd	Qtd MB	
			VARA	17	30	R$ 14.214,81
			FORO	5	50	R$ 6.968,04
				Valor Total Mensal		**R$ 21.182,85**

Custo por MB para o serviço MPLS: R$ 18,41

Cálculo: Valor por MB Porta Principal + Valor por MB Sites Remotos / 2

6.15. **Acesso através de Link MPLS + IP Simétrico Dedicado + Serviço SD-WAN Seguro**

Porta Principal - Link 1 Internet

Órgão	Operadora	Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
PGE-RJ	CLARO S.A	34/2020	21/05/2024	100	R$ 874,00	R$ 8,74
TSE	OI	49/2022	06/12/2024	2000	R$ 14.989,29	R$ 7,49
TRE-TO	FORTEL FORTALEZA TELECOMUNICAÇÕES S/A	29/2022	13/07/2023	1000	R$ 3.800,00	R$ 3,80
TRE-MT	OI	15/2021	26/08/2026	500	R$ 2.500,00	R$ 5,00
TRT-ES	Brasil Digital Telecomunicações	06/2021	09/03/2026	300	R$ 2.634,00	R$ 8,78
TRE-MS	ACESSOLINE TELECOMUNICAÇÕES LTDA	25/2022	02/08/2024	500	R$ 2.900,00	R$ 5,80
PROPOSTA	TITANIA			500	R$ 15.000,00	R$ 30,00
PROPOSTA	OI			500	R$ 8.560,00	R$ 17,12
				Mediana por Mb		**R$ 8,12**
				Valor Mensal 500 Mb		**R$ 4.058,66**

Sites Remotos - Internet

Órgão	Operadora	Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
TRT-18	BRASIL DIGITAL	38/2020	07/04/2023	50	R$ 1.138,00	R$ 22,76
FUFMT	GIGA BYTE TELEC. LTDA	10/2021	21/06/2023	300	R$ 5.090,36	R$ 16,97
FUFMT	SET SOLUCOES TEC E INF LTDA	14/2022	15/03/2022	800	R$ 14.600,00	R$ 18,25
PROPOSTA	TITANIA			100	R$ 3.000,00	R$ 30,00
PROPOSTA	TITANIA			150	R$ 5.000,00	R$ 33,33

TRT-16	FORTEL FORTALEZA TELECOMUNICAÇÕES S/A	18/2021	20/04/2024	200	R$ 650,00	R$ 3,25
				Mediana por Mb		**R$ 20,51**
				Qtd	Qtd MB	
			VARA	17	100	R$ 34.858,50
			FORO	5	150	R$ 15.378,75
				Valor Mensal		**R$ 50.237,25**

Porta Principal - SD-WAN

Órgão	Operadora	Contrato	Vigência	Qtd	Valor	Valor total
PROPOSTA	OI			1	R$ 12.500,00	R$ 12.500,00
CJF	ALGAR	29/2020	20/07/2023	1	R$ 1.500,00	R$ 1.500,00
				Mediana		**R$ 7.000,00**
				Valor Mensal		**R$ 7.000,00**

Sites Remotos - SD-WAN

Órgão	Operadora	Contrato	Vigência	Qtd	Valor	Valor por Equip.
PROPOSTA	OI			22	R$ 57.200,00	R$ 2.600,00
CJF	ALGAR	29/2020	20/07/2023	22	R$ 33.000,00	R$ 1.500,00
INSS	TELEBRAS	31/2022	25/11/2024	22	R$ 25.366,22	R$ 1.153,01
				Mediana		**R$ 1.500,00**
				Valor Mensal		**R$ 1.500,00**

Porta Principal - Link 2 Internet

Órgão	Operadora	Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
PGE-RJ	CLARO S.A	34/2020	21/05/2024	100	R$ 874,00	R$ 8,74
TSE	OI	49/2022	06/12/2024	2000	R$ 14.989,29	R$ 7,49
TRE-TO	FORTEL FORTALEZA TELECOMUNICAÇÕES S/A	29/2022	13/07/2023	1000	R$ 3.800,00	R$ 3,80
TRE-MT	OI	15/2021	26/08/2026	500	R$ 2.500,00	R$ 5,00
TRT-ES	Brasil Digital Telecomunicações	06/2021	09/03/2026	300	R$ 2.634,00	R$ 8,78
TRE-MS	ACESSOLINE TELECOMUNICAÇÕES LTDA	25/2022	02/08/2024	500	R$ 2.900,00	R$ 5,80
PROPOSTA	TITANIA			500	R$ 15.000,00	R$ 30,00
PROPOSTA	OI			500	R$ 8.560,00	R$ 17,12
				Mediana por Mb		**R$ 8,12**
				Valor Mensal 500 Mb		**R$ 4.058,66**

Porta Principal - MPLS

Órgão		Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
TRF4	LIGGA TELEC. S.A.	18/2022	01/05/2024	300	R$ 2.102,23	R$ 7,01
ANAC	CLARO	22/2020 - TA1	09/11/2023	192	R$ 1.799,60	R$ 9,37
CJF	ALGAR	29/2020	20/07/2023	200	R$ 1.700,00	R$ 8,50
TRE-TO	ZAP TELEC. LTDA	30/2022	13/07/2023	500	R$ 4.900,00	R$ 9,80
PREF. SALVADOR	TELEMAR	36/2020	24/06/2023	10000	R$ 52.612,79	R$ 5,26

PROPOSTA	OI			350	R$ 12.560,00	R$ 35,89
				Mediana por Mb		**R$ 8,94**
				Qtd	Qtd MB	
			SEDE	1	350	R$ 3.127,76
				Valor Mensal		**R$ 3.127,76**

Sites Remotos - MPLS

Órgão		Contrato	Vigência	Qtd MB	Valor Total	Valor por MB
TRF4	LIGGA TELEC. S.A.	18/2022	01/05/2024	50	R$ 576,29	R$ 11,53
TRF4	LIGGA TELEC. S.A.	18/2022	01/05/2024	35	R$ 514,63	R$ 14,70
TJ / MT	OI	05/2021	01/10/2022	200	R$ 5.600,00	R$ 28,00
TJ / MT	OI	05/2021	01/10/2022	200	R$ 4.550,00	R$ 22,75
TJ / MT	OI	05/2021	01/10/2022	50	R$ 2.500,00	R$ 50,00
TJ / MT	Brasil Digital	04/2021	26/09/2022	200	R$ 4.334,10	R$ 21,67
TJ / MT	Brasil Digital	04/2021	26/09/2022	50	R$ 7.000,00	R$ 140,00
TJ / MT	REDE EXS	03/2021	03/10/2022	50	R$ 3.300,00	R$ 66,00
TJ / MT	REDE EXS	03/2021	03/10/2022	200	R$ 5.900,00	R$ 29,50
ANAC	CLARO	22/2020 - TA1	09/11/2023	46	R$ 1.276,24	R$ 27,74
ANAC	CLARO	22/2020 - TA1	09/11/2023	24	R$ 631,75	R$ 26,32
CJF	ALGAR	29/2020	20/07/2023	100	R$ 1.200,00	R$ 12,00
PREF. SALVADOR	TELEMAR	36/2020	24/06/2023	50	R$ 2.219,67	R$ 44,39
TRE-TO	ZAP TELEC. LTDA	30/2022	13/07/2023	100	R$ 1.150,00	R$ 11,50
PROPOSTA	OI			30	R$ 4.300,00	R$ 143,33
PROPOSTA	OI			50	R$ 5.100,00	R$ 102,00

				Mediana por Mb		**R$ 27,87**
				Qtd	Qtd MB	
			VARA	17	30	R$ 14.214,81
			FORO	5	50	R$ 6.968,04
				Valor Mensal		**R$ 21.182,85**

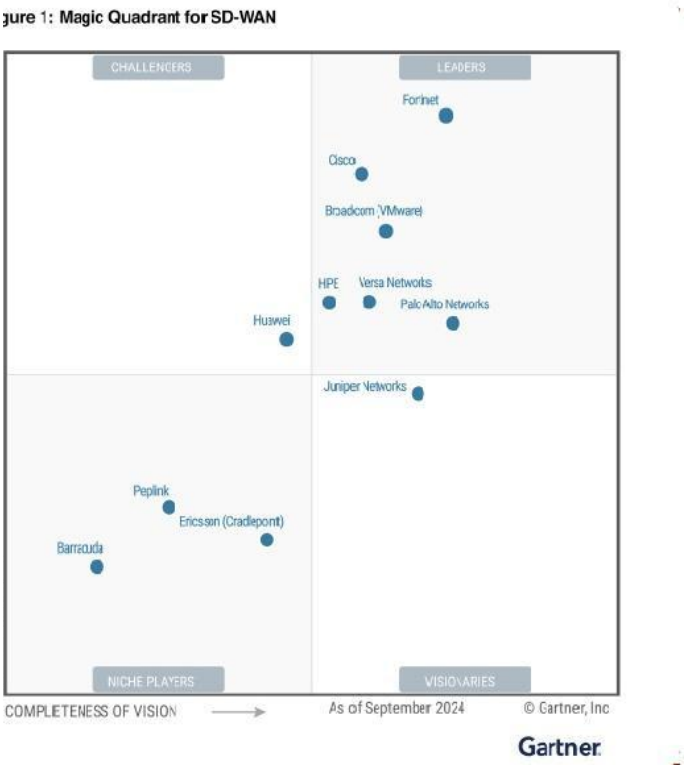
6.16. **Análise e comparação dos custos das soluções identificadas**

6.16.1. Para aferição e comparação dos custos associados às soluções identificadas, optamos por calcular o preço por MB mensal como forma de identificação daquela que possui menor custo. No entanto, deve ser observado que a solução 3, apesar de constar como valor inferior, possui requisitos técnicos superiores à solução 2.

	Valor Mensal
Solução 1: Link de Internet do tipo Banda Larga	Solução inviável
Solução 2: Link MPLS	R$ 18,41 por MB
Solução 3: Link MPLS + Internet + SD WAN Seguro	R$ 14,32 por MB

7. ANÁLISE DE PROJETOS SIMILARES

7.1. Segundo os mais recentes estudos do Gartner, o mercado global de infraestrutura de segurança de rede e conectividade utilizando tecnologia SD-WAN é amplamente dominado por soluções baseadas em equipamentos Fortinet, Palo Alto, Cisco Systems, entre outros. Os demais, segundo o Gartner, se encontram em posições de Visionários e Atores em Nichos de Mercado, como ilustrado na figura abaixo. Esta análise estabelece dois eixos de grandezas, quais sejam a Completude ou Integralidade da Solução e Habilidade de Executar, e divide o plano formado por estes eixos em quatro quadrantes.



7.2. **Contratações similares feitas pelo próprio Órgão/Entidade**

7.2.1. O PRODERJ realizou duas contratações similares, oriundas de adesões ao registro de preços N° 0001/2021, que foram os contratos Nº 004/2021 e Nº 005/2021. No entanto, apesar de serem objetos similares à presente licitação, possuem particularidades que diferem, como, por exemplo, uma rede de contingência a ser operada por prestadora distinta da que opera a rede principal, bem como acesso à Internet na modalidade satélite de baixa órbita.

7.3. **Contratações similares feitas por outros Órgãos/Entidade**

7.3.1. Diversos órgãos e secretarias do Governo do Estado realizaram contratações aderindo a mesma ata de registro de preços n° 0001/2021, porém as similaridades são as mesmas já apontadas.

7.3.2. Link Internet + SD-WAN Seguro

ÓRGÃO	CERTAME	OBJETO	ANÁLISE DE SIMILARIDADE
TRT 16ª REGIÃO	Proc. Adm 7885/2022	Contratação de links de comunicação de dados	Objeto semelhante ao projeto em questão. Inclusive trata-se de uma expansão do ambiente conforme a necessidade do Proderj.
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS	SEI 2023/000014246-00	Contratação de links de comunicação de dados	Objeto semelhante ao projeto em questão.

TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO	Proad nº 1.356/2023	Fornecimento de links de dados dedicados e com disponibilidade de conexão de 24 horas e 7 dias por semana.	Objeto semelhante ao projeto em questão.
TRIBUNAL REGIONAL DO TRABALHO - 24ª REGIÃO	Proad nº 24.695/2022	Contratação de serviços continuados de links de dados ponto a ponto, com concentração do tráfego na sede do TRT e controles centralizados de tráfego e segurança,	Objeto semelhante ao projeto em questão.

1. **Link de Internet sem SD-WAN**

ÓRGÃO	**CERTAME**	**OBJETO**	**ANÁLISE DE SIMILARIDADE**
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO	Proc. Adm. 23270.001276/2020-50	Contratação de links de comunicação de dados para acesso à internet.	Objeto semelhante ao projeto em questão. Inclusive trata-se de uma expansão do ambiente conforme a necessidade do Proderj.
PREFEITURA MUNICIPAL DE PRIMAVERA - PARÁ	PE Nº 09/20230028	Contratação de links de comunicação de dados para acesso à internet.	Objeto semelhante ao projeto em questão.

FUNDAÇÃO MUNICIPAL DE SAÚDE DE NITERÓI	PE MS Nº 29/2021	Fornecimento de links de dados dedicados e com disponibilidade de conexão de 24 horas e 7 dias por semana.	Objeto semelhante ao projeto em questão.
PREFEITURA MUNICIPAL DE PORTEL - PARÁ	CP No 20221019002	Contratação de serviços continuados de links de dados na internet.	Objeto semelhante ao projeto em questão.

1. **Redes Satelitais e Móveis**

ÓRGÃO	**CERTAME**	**OBJETO**	**ANÁLISE DE SIMILARIDADE**
PREFEITURA MUNICIPAL DE PORTEL - PARÁ	CP No 20221019002	Contratação de link de comunicação de dados via satélite Acesso à internet.	Objeto semelhante ao projeto em questão. Inclusive trata-se de uma expansão do ambiente conforme a necessidade do Proderj.
TRIBUNAL DE JUSTIÇA DO MARANHÃO	Proc. Adm. nº 47.810/2023	Contratação de link de comunicação de dados via satélite Acesso à internet.	Objeto semelhante ao projeto em questão.
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS	SEI 2023/000014246-00	Contratação de link de comunicação de dados via satélite Acesso à internet.	Objeto semelhante ao projeto em questão.

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ	PREGÃO ELETRÔNICO 013/2024	Contratação de link de comunicação de dados via satélite Acesso à internet.	Objeto semelhante ao projeto em questão.

8. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

8.1. O Estado do Rio de Janeiro tem como uma de suas metas maximizar a eficiência de seus serviços por meio da redução de custos e tempo envolvidos na realização de suas atividades.

8.2. Concomitantemente, busca o aumento de sua eficácia através da melhoria contínua da interação com seus órgãos e parceiros, necessitando de instrumentos de comunicação eficientes e tecnologicamente modernos, capazes de atender prontamente às suas demandas com a qualidade e disponibilidade necessária.

8.3. Com a crescente adoção de aplicativos hospedados em provedores de SaaS, Datacenters e serviços em Nuvem, bem como a necessidade de garantir alta disponibilidade do acesso sem sacrificar o desempenho, foi realizada uma análise comparativa entre três soluções de conectividade: banda larga, MPLS e links de Internet IP Simétricos gerenciados por SD-WAN.

8.4. Diante desse cenário, a solução que melhor atende aos requisitos técnicos e de negócio da demanda é a implementação de links de Internet IP Simétricos gerenciados por SD-WAN, que agrega todas as vantagens das alternativas anteriores e supera suas limitações. O SD-WAN possibilita um gerenciamento inteligente da conectividade, oferecendo benefícios como:

a) Redução de Custos: Flexibiliza os meios de acesso possíveis, sem comprometer a qualidade e aumentando o leque de opções disponíveis para as operadoras que poderão fazer melhor uso dos provedores locais.

b) Alta Disponibilidade e Redundância: O SD-WAN permite a utilização simultânea de múltiplos links, garantindo a continuidade operacional em caso de falhas.

c) Desempenho Otimizado: A tecnologia prioriza automaticamente o tráfego de aplicações críticas, assegurando melhor experiência para serviços essenciais como voz, vídeo e acesso remoto.

d) Maior Flexibilidade e Escalabilidade: Facilita a expansão da rede para novos sites sem depender da infraestrutura de um único provedor.

f) Segurança Aprimorada: Implementação de criptografia de ponta a ponta, segmentação de tráfego e integração com soluções avançadas de segurança, reduzindo vulnerabilidades inerentes ao uso da Internet pública.

g) Melhor Experiência para Aplicações em Nuvem: Permite roteamento otimizado diretamente para serviços SaaS e Cloud, reduzindo latência e melhorando o desempenho.

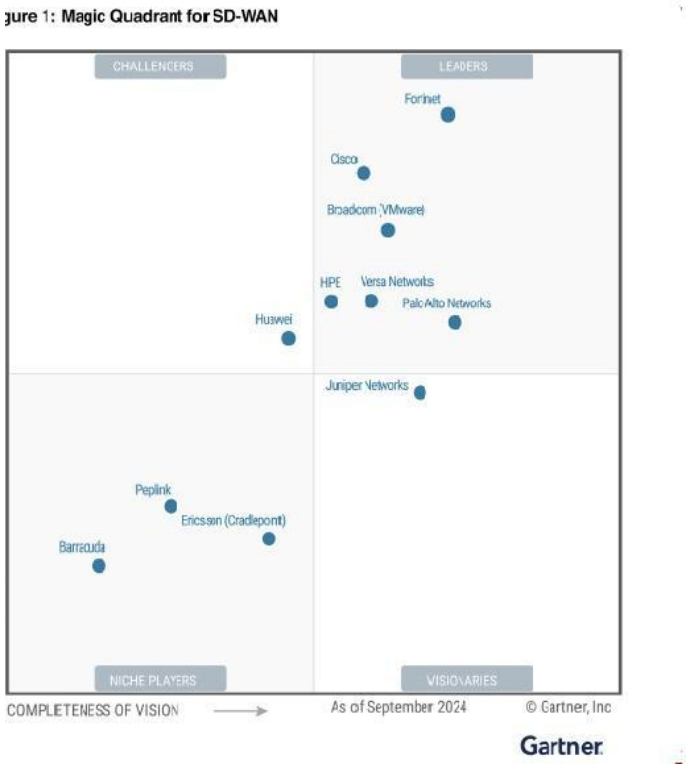
8.5. **Solução escolhida**

8.5.1. A solução 1 não atende pois, embora tenha custo reduzido, não atende aos requisitos de desempenho e segurança necessários para a operação dos serviços críticos da Administração Pública. Além disso, não oferece garantias de qualidade (SLA), estabilidade de conexão nem suporte adequado para aplicações de missão crítica. Em resumo, apresenta baixa qualidade e não contempla os requisitos essenciais para uma rede corporativa. Esta solução traz grande risco à segurança cibernética da infraestrutura computacional da Rede Governo.

8.5.2. A Solução 2 não atende, pois apesar de ser o serviço atualmente em uso para interconectar as Secretarias de Órgãos da Administração, oferecendo certo grau de confiabilidade e garantia de qualidade, a tecnologia MPLS não vem suprindo a alta demanda por largura de banda, impõe altos custos operacionais e limita a flexibilidade da rede. A expansão da infraestrutura MPLS exige contratos de longo prazo e depende da disponibilidade da rede do provedor, dificultando a escalabilidade e tornando-se menos competitiva em um cenário de crescente digitalização e demanda por acessos diretos à nuvem.

8.5.3. A Solução 3 é uma junção da 1 e 2, contendo uma conexão MPLS e uma conexão de Link de Internet interligadas e gerenciadas através da tecnologia SD-WAN, que vai na direção das necessidades atuais de expandir e melhorar a conectividade dos sites principais e remotos e a disponibilidade da

internet, através do equipamento SD-WAN que vai direcionar o tráfego do link em falha para o link que ainda estiver operacional, na questão de performance principalmente durante transmissões e vídeo conferências, quando vai gerenciar o tráfego de maneira a este ser encaminhado para internet através do Link local (prioritariamente) tendo regras de segurança da informação aplicadas localmente, sem necessitar passar pelo Data Center do PRODERJ, fazendo com que a Solução 3 seja a única que atende a completude dos requisitos. A solução contemplará alta resiliência, fazendo da Rede Conect@.RJ, uma rede totalmente contingente, com links sendo fornecidos por meios físicos de transmissão distintos, garantindo alta disponibilidade e mitigação de pontos de falha.



9. DEFESA DE MARCA

9.0.1. Não se aplica ao escopo da contratação.

10. MÉTRICA PARA MENSURAÇÃO E SERVIÇOS

10.1. Não se aplica ao escopo da contratação.

10.2. **ESTIMATIVA DAS QUANTIDADES**

10.2.1. Considerando que o objetivo é realizar uma contratação para abranger todo o Estado do Rio de Janeiro, as quantidades abaixo serão consolidadas com as demandas apresentadas na IRP (Intenção de Registro de Preços).

10.2.2. A presente contratação será conduzida sob o regime de registro de preços, com fornecimento sob demanda. Para tanto, a estimativa de quantidades para o PRODERJ foi estruturada com base em três eixos metodológicos complementares:

- Histórico de Contratações:

Foram utilizados como base os dados de utilização dos contratos nº 004/2021 e nº 005/2021, que atendem atualmente à espinha dorsal da Rede IP Governo. A análise considerou o número de circuitos ativos, suas capacidades médias e a evolução de demandas ao longo do período contratual.

-Projeção de Expansão da Rede e Demandas Estratégicas:

Consideraram-se os planos de transformação digital da Administração Pública Estadual, notadamente os

documentos estratégicos do PRODERJ (PEDTIC 2024) e o Plano de Contratações Anual. Foram incluídas, de forma preventiva, quantidades voltadas a localidades de difícil acesso, estruturas móveis (como veículos institucionais) e órgãos que deverão ser in

10.2.3. As quantidades registradas refletem uma estimativa referencial do consumo potencial durante a vigência da ata, respeitando os princípios da razoabilidade, economicidade e proporcionalidade. Ressalta-se que a execução contratual se dará exclusivamente conforme as necessidades efetivas, não configurando obrigação de consumo mínimo.

10.2.4. **Em síntese, as estimativas mínimas do PRODERJ permitem a manutenção da atual topologia da Rede Conect@.RJ nos moldes em que se encontra**, com significativo upgrade de velocidades, acessos das sedes atuais da autarquia (Centro e UERJ). Alguns itens não há demanda do PRODERJ, porém considerando a planta atual de circuitos em operação, trata-se de itens de necessidade de diversos Órgãos e Secretarias da Administração Pública.

Lote I - Rede SD-WAN Principal						
Item	ID SIGA	ID PCA	**Descrição**	**Métrica**	**Forma de Fornecimento**	**Quantidade estimada**
1	193830	*	Link de dados principal dedicado 10 mbps + equipamento sd-wan	Mensal	Sob demanda	0
2	193831	*	Link de dados principal dedicado 30 mbps + equipamento sd-wan	Mensal	Sob demanda	0
3	193832	*	Link de dados principal dedicado 50 mbps + equipamento sd-wan	Mensal	Sob demanda	0
4	193833	24424	Link de dados principal dedicado 100 mbps + equipamento sd-wan	Mensal	Sob demanda	2
5	193834	24413	Link de dados principal dedicado 200 mbps + equipamento sd-wan	Mensal	Sob demanda	2
6	193835	24426	Link de dados principal dedicado 500 mbps + equipamento sd-wan	Mensal	Sob demanda	4
7	193836	24426	Link de dados principal dedicado 1 gbps + equipamento sd-wan	Mensal	Sob demanda	2
8	193837	24418	Link de dados principal dedicado 2 gbps + equipamento sd-wan	Mensal	Sob demanda	4
9	193838	24414	Link de dados principal dedicado 4 gbps + equipamento sd-wan	Mensal	Sob demanda	4
10	193839	24419	Link de dados principal dedicado 10 gbps + equipamento sd-wan	Mensal	Sob demanda	4
11	193840	24410	Link de Dados - Acesso Lan-To-Lan 1 Gbps	Mensal	Sob demanda	2
12	193841	24427	Link de Dados - Acesso Lan-To-Lan 2 Gbps	Mensal	Sob demanda	2
13	193842	24415	Link de Dados - Acesso Lan-To-Lan 4 Gbps	Mensal	Sob demanda	2
14	193843	24428	Link de Dados - Acesso Lan-To-Lan 10 Gbps	Mensal	Sob demanda	2

Lote II - Rede SD-WAN Redundante						
Item	ID SIGA	ID PCA	**Descrição**	**Métrica**	**Forma de Fornecimento**	**Quantidade estimada**
1	193844	*	Link de Dados Redundante - Acesso Multimeio 10 Mbps	Mensal	Sob demanda	0
2	193845	*	Link de Dados Redundante - Acesso Multimeio 30 Mbps	Mensal	Sob demanda	0
3	193846	*	Link de Dados Redundante - Acesso Multimeio 50 Mbps	Mensal	Sob demanda	0
4	193847	24429	Link de Dados Redundante - Acesso Multimeio 100 Mbps	Mensal	Sob demanda	2
5	193848	24420	Link de Dados Redundante - Acesso Multimeio 200 Mbps	Mensal	Sob demanda	2
6	193849	24421	Link de Dados Redundante - Acesso Multimeio 500 Mbps	Mensal	Sob demanda	4
7	193850	24430	Link de Dados Redundante - Acesso Multimeio 1 Gbps	Mensal	Sob demanda	2
8	193851	24422	Link de Dados Redundante - Acesso Multimeio 2 Gbps	Mensal	Sob demanda	4
9	193852	24423	Link de Dados Redundante - Acesso Multimeio 4 Gbps	Mensal	Sob demanda	4
10	193853	24431	Link de Dados Redundante - Acesso Multimeio 10 Gbps	Mensal	Sob demanda	4
11	193854	24416	Link de Dados Rede Lan-To-Lan 1 Gbps	Mensal	Sob demanda	2
12	193855	24411	Link de Dados Rede Lan-To-Lan 2 Gbps	Mensal	Sob demanda	2
13	193856	24432	Link de Dados Rede Lan-To-Lan 4 Gbps	Mensal	Sob demanda	2
14	193857	24412	Link de Dados Rede Lan-To-Lan 10 Gbps	Mensal	Sob demanda	2
15	193858	24433	Link de Dados Rede IP Móvel de Baixa Órbita Fixa	Mensal	Sob demanda	2
16	193859	24417	Link de Dados Rede IP Móvel de Baixa Órbita Móvel	Mensal	Sob demanda	2
17	193860	24412	Link de Dados Rede IP Móvel 4G/5G (FWA)	Mensal	Sob demanda	10

* Itens sem demanda do PRODERJ.

11. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

11.1. A tabela abaixo consolida um levantamento de mercado contemplando custos unitários de itens semelhantes ofertados em diferentes Editais Públicos, ao qual servirá de base para a estimativa preliminar do valor da contratação do PRODERJ.

Lote I - Rede SD-WAN Principal							
			PRODERJ **ARP nº 01/2021**	**TRT - 18º Região** **PE nº 074003/2022**	**TRT - 3ª Região** **PE nº 06/2023**	**TRT 24 ª Região** **PROAD N° 24.695/2022**	**ANTT**
Item	**Descrição**	**Unid.**	**Preço Unitário (Sem ICMS)**	**Preço Unitário**	**Preço Unitário**	**Preço Unitário**	**Preço Unitário**
1	Link de Dados Principal - Acesso SD-WAN Dedicado 10 Mbps	mês	R$ 1.027,96		R$ 1.090,12		
2	Link de Dados Principal - Acesso SD-WAN Dedicado 30 Mbps	mês	R$ 2.826,08		R$ 1.426,10		
3	Link de Dados Principal - Acesso SD-WAN Dedicad 50 Mbps	mês	R$ 2.878,70	R$ 2.137,80	R$ 1.604,90	R$1.518,00	R$ 2.871,70

4	Link de Dados Principal - Acesso SD-WAN Dedicado 100 Mbps	mês	R$ 2.480,92				
5	Link de Dados Principal - Acesso SD-WAN Dedicado 200 Mbps	mês	R$ 3.663,77				
6	Link de Dados Principal -Acesso SD-WAN Dedicado 500 Mbps	mês	R$ 3.873,16				
7	Link de Dados Principal - Acesso SD-WAN Dedicado 1 Gbp	mês	R$ 4.082,47				
8	Link de Dados Principal - Acesso SD-WAN Dedicado 2 Gbps	mês	R$ 4.867,61				
9	Link de Dados Principal - Acesso SD-WAN Dedicado 4 Gbps	mês	R$ 5.652,71				
10	Link de Dados Principal - Acesso SD-WAN Dedicado 10 Gbp	mês	R$ 11.305,42				
11	Link de Dados - Acesso Lan-To-Lan 1 Gbps	mês	R$ 8.164,94				

12	Link de Dados - Acesso Lan-To-Lan 2 Gbps	mês	R$ 9.735,22				
13	Link de Dados - Acesso Lan-To-Lan 4 Gbps	mês	R$ 11.305,42				
14	Link de Dados - Acesso Lan-To-Lan 10 Gbps	mês	R$ 22.610,84				

Lote II - Rede SD-WAN Redundante							
			PRODERJ **ARP nº 01/2021**	**TRT - 18º Região** **PE nº 074003/2022**	**TRT - 3ª Região** **PE nº 06/2023**	**TRT 24 ª Região** **PROAD N° 24.695/2022**	**ANTT**
Item	**Descrição**	**Unid.**	**Preço Unitário (Sem ICMS)**	**Preço Unitário**	**Preço Unitário**	**Preço Unitário**	**Preço Unitário**
1	Link de Dados Redundante - Acesso Multimeio 10 Mbps	mês	R$ 1.027,96		R$ 1.090,12		
2	Link de Dados Redundante - Acesso Multimeio 30 Mbps	mês	R$ 2.826,08		R$ 1.426,10		
3	Link de Dados Redundante - Acesso Multimeio 50 Mbps	mês	R$ 2.878,70	R$ 2.137,80	R$ 1.604,90	R$1.518,00	R$ 2.871,70

4	Link de Dados Redundante - Acesso Multimeio 100 Mbps	mês	R$ 2.480,92				
5	Link de Dados Redundante - Acesso Multimeio 200 Mbps	mês	R$ 3.663,77				
6	Link de Dados Redundante - Acesso Multimeio 500 Mbps	mês	R$ 3.873,16				
7	Link de Dados Redundante - Acesso Multimeio 1 Gbps	mês	R$ 4.082,47				
8	Link de Dados Redundante - Acesso Multimeio 2 Gbps	mês	R$ 4.867,61				
9	Link de Dados Redundante - Acesso Multimeio 4 Gbps	mês	R$ 5.652,71				
10	Link de Dados Redundante - Acesso Multimeio 10 Gbps	mês	R$ 11.305,42				
11	Link de Dados Rede Lan-To-Lan 1 Gbps	mês	R$ 8.164,94				

12	Link de Dados Rede Lan-To-Lan 2 Gbps	mês	R$ 9.735,22				
13	Link de Dados Rede Lan-To-Lan 4 Gbps	mês	R$ 11.305,42				
14	Link de Dados Rede Lan-To-Lan 10 Gbps	mês	R$ 22.610,84				
			HUGHESNET	**STARLINK**	**MINISTÉRIO DA DEFESA** **PREGÃO ELETRONICO No 01/2024 160016**	**MARINHA DO BRASIL** **NAVIO PATRULHA BABITONGA** **CT Direta** **90010/2024**	**CLARO**
15	Link de Dados Rede IP Móvel de Baixa Órbita Fixa	mês			R$ 4.149,04		
16	Link de Dados Rede IP Móvel de Baixa Órbita Móvel	mês	R$ 209,00	R$ 450,00		R$ 800,00	
17	Link de Dados Rede IP Móvel 4G/5G (FWA)	mês					R$ 416,54

:e:

s://www.ofertahughesnet.com.br/?id_cidade=&nome_cidade=rio+de+janeiro
s://www.starlink.com/br/service-plans

s://www.claro.com.br/internet/movel/fwa-5g

11.2. Diante do levantamento realizado, foi aferida a estimativa da contratação mediante cálculo da média dos itens similares ao presente objeto. Para os links Lan-To-Lan, pelo fato de serem provisionados duas infra estruturas distintas em cada uma das pontas da conexão, estimamos para o custo associado o dobro do link de dados de mesma velocidade. Para o Lote II, cujos links de dados não possuem segurança embarcada, aplicamos redutor de 30% no valor que seria o equivalente estimado do equipamento SD-WAN seguro.

Rede Governo Principal					
Item	**Descrição**	**Métrica**	**Quantidade estimada**	**Custo Unitário Médio**	**Total Estimado**
1	Link de dados principal dedicado 10 mbps + equipamento sd-wan	Mensal	0	R$ 1.059,04	
2	Link de dados principal dedicado 30 mbps + equipamento sd-wan	Mensal	0	R$ 2.126,09	
3	Link de dados principal dedicado 50 mbps + equipamento sd-wan	Mensal	0	R$ 2.202,22	
4	Link de dados principal dedicado 100 mbps + equipamento sd-wan	Mensal	2	R$ 2.480,92	R$ 4.961,84
5	Link de dados principal dedicado 200 mbps + equipamento sd-wan	Mensal	2	R$ 3.663,77	R$ 7.327,54
6	Link de dados principal dedicado 500 mbps + equipamento sd-wan	Mensal	4	R$ 3.873,16	R$ 15.492,64
7	Link de dados principal dedicado 1 gbps + equipamento sd-wan	Mensal	2	R$ 4.082,47	R$ 8.164,94

8	Link de dados principal dedicado 2 gbps + equipamento sd-wan	Mensal	4	R$ 4.867,61	R$ 19.470,44
9	Link de dados principal dedicado 4 gbps + equipamento sd-wan	Mensal	4	R$ 5.652,71	R$ 22.610,84
10	Link de dados principal dedicado 10 gbps + equipamento sd-wan	Mensal	4	R$ 11.305,42	R$ 45.221,68
11	Link de Dados - Acesso Lan-To-Lan 1 Gbps	Mensal	2	R$ 8.164,94	R$ 16.329,88
12	Link de Dados - Acesso Lan-To-Lan 2 Gbps	Mensal	2	R$ 9.735,22	R$ 19.470,44
13	Link de Dados - Acesso Lan-To-Lan 4 Gbps	Mensal	2	R$ 11.305,42	R$ 22.610,84
14	Link de Dados - Acesso Lan-To-Lan 10 Gbps	Mensal	2	R$ 22.610,84	R$ 45.221,68
TOTAL ESTIMADO (60 MESES)					R$ 13.612.965,6

Rede Governo Redundante					
Item	**Descrição**	**Métrica**	**Quantidade estimada**	**Custo Unitário Médio**	**Total Estimado**
1	Link de Dados Redundante - Acesso Multimeio 10 Mbps	Mensal	0	R$ 1.059,04	
2	Link de Dados Redundante - Acesso Multimeio 30 Mbps	Mensal	0	R$ 2.126,09	

3	Link de Dados Redundante - Acesso Multimeio 50 Mbps	Mensal	0	R$ 2.202,22	
4	Link de Dados Redundante - Acesso Multimeio 100 Mbps	Mensal	2	R$ 2.480,92	R$ 4.961,84
5	Link de Dados Redundante - Acesso Multimeio 200 Mbps	Mensal	2	R$ 3.663,77	R$ 7.327,54
6	Link de Dados Redundante - Acesso Multimeio 500 Mbps	Mensal	4	R$ 3.873,16	R$ 15.492,64
7	Link de Dados Redundante - Acesso Multimeio 1 Gbps	Mensal	2	R$ 4.082,47	R$ 8.164,94
8	Link de Dados Redundante - Acesso Multimeio 2 Gbps	Mensal	4	R$ 4.867,61	R$ 19.470,44
9	Link de Dados Redundante - Acesso Multimeio 4 Gbps	Mensal	4	R$ 5.652,71	R$ 22.610,84
10	Link de Dados Redundante - Acesso Multimeio 10 Gbps	Mensal	4	R$ 11.305,42	R$ 45.221,68
11	Link de Dados Rede Lan-To-Lan 1 Gbps	Mensal	2	R$ 8.164,94	R$ 16.329,88
12	Link de Dados Rede Lan-To-Lan 2 Gbps	Mensal	2	R$ 9.735,22	R$ 19.470,44

13	Link de Dados Rede Lan-To-Lan 4 Gbps	Mensal	2	R$ 11.305,42	R$ 22.610,84
14	Link de Dados Rede Lan-To-Lan 10 Gbps	Mensal	2	R$ 22.610,84	R$ 45.221,68
15	Link de Dados Rede IP Móvel de Baixa Órbita Fixa	Mensal	2	R$ 4.149,04	R$ 8.298,08
16	Link de Dados Rede IP Móvel de Baixa Órbita Móvel	Mensal	2	R$ 486,33	R$ 972,66
17	Link de Dados Rede IP Móvel 4G/5G (FWA)	Mensal	10	R$ 416,54	R$ 4.165,40
TOTAL ESTIMADO (60 MESES)					R$ 14.419.134,00

12. DESCRIÇÃO DA SOLUÇÃO DE TI COMO UM TODO

12.1. Definição do objeto

12.1.1. Contratação de solução integrada de conectividade para rede corporativa privada principal e de redundância, bem como para acesso à Internet, com suporte à tecnologia SD-WAN e múltiplos meios de acesso, incluindo fibra óptica, banda larga, rádio, redes móveis (4G/5G) e satélite de baixa órbita, com gestão centralizada, alta disponibilidade, segurança embarcada para continuidade e modernização da Rede Conect@.RJ, contemplando o fornecimento de links de acesso, equipamentos, monitoramento, configuração e suporte técnico, para atendimento da administração pública, de acordo com as especificações, condições, quantidades e exigências a serem estabelecidas nos artefatos técnicos da contratação.

12.2. SNOC - Security and Network Operation Center

12.2.1. **Além do fornecimento dos links de acesso, contemplando todos os equipamentos e serviços de instalação, a CONTRATADA deverá estruturar um SNOC (Service and Network Operations Center), que é um centro de operações responsável pelo monitoramento, gerenciamento e suporte técnico de redes e serviços de telecomunicações. Ele combina as funções de um NOC (Network Operations Center), focado na infraestrutura de rede, e de um SOC (Security Operations Center), voltado para a segurança cibernética, garantindo assim um controle abrangente da operação. Essa abordagem integrada deverá ser disponibilizada exclusivamente no âmbito da prestação de serviços ao PRODERJ, que é o backbone da rede, e permitirá respostas rápidas a incidentes, ao mesmo tempo em que mantém o desempenho da infraestrutura de segurança da rede corporativa do estado. A infraestrutura de segurança da Rede Conect@.RJ deverá dispor de monitoramento pró-ativo com a utilização de ferramentas SIEM, WAF, DNS Filtering e ANTI-DDOS, sem custos adicionais ao PRODERJ, contemplando no mínimo as seguintes ações:**

12.3. Monitoramento em Tempo Real:

12.3.1. Supervisão contínua da performance da rede e dos serviços.

12.3.2. Detecção proativa de falhas e degradações de desempenho.

12.3.3. Coleta e análise de métricas, como latência, jitter, perda de pacotes e disponibilidade.

12.4. **Gerenciamento de Incidentes e Resolução de Problemas:**

12.4.1. Identificação e resposta rápida a falhas e vulnerabilidades.

12.4.2. Execução de protocolos de contingência para minimizar impactos.

12.4.3. Acompanhamento e resolução de chamados técnicos.

12.5. **Segurança da Informação:**

12.5.1. Monitoramento de ameaças e ataques cibernéticos.

12.5.2. Implementação de medidas de mitigação e resposta a incidentes de segurança.

12.5.3. Gerenciamento de políticas de acesso e conformidade com normas regulatórias.

12.6. **Gestão de Configuração e Mudanças:**

12.6.1. Administração de equipamentos de rede, firewalls, roteadores e SD-WAN.

12.6.2. Aplicação de atualizações, patches de segurança e ajustes na configuração.

12.6.3. Controle de mudanças para garantir a estabilidade dos serviços.

12.7. **Otimização de Recursos e Performance:**

12.7.1. Análise de tráfego e comportamento da rede para identificar melhorias.

12.7.2. Priorização de aplicações críticas e balanceamento de carga.

12.7.3. Gestão de capacidade para evitar gargalos e garantir crescimento sustentável.

12.8. **Relatórios e Auditoria:**

12.8.1. Geração de relatórios de disponibilidade, desempenho e segurança.

12.8.2. Registro de eventos e incidentes para auditoria e conformidade.

12.8.3. Análises preditivas para prevenção de problemas futuros.

12.8.4. O escopo e as especificações detalhadas do SNOC e demais itens do objeto estão descritas no Anexo I - Especificações Técnicas.

12.8.5. **Descrição pormenorizada, considerando todo o ciclo de vida do objeto a ser contratado, de forma precisa, suficiente e clara, por meio de especificações técnicas ou de desempenho do objeto usuais de mercado, vedando-se aquelas que, por excessivas, irrelevantes ou desnecessárias, limitem a competição**

12.8.6. O ciclo de vida dos links de dados refere-se ao processo desde a concepção até o descomissionamento de um link de comunicação utilizado para transmitir dados. Esse ciclo pode ser dividido em várias etapas principais:

12.9. **Planejamento e Projeto:**

12.9.1. Identificação das necessidades de comunicação.

12.9.2. Estudo de viabilidade técnica e econômica.

12.9.3. Definição dos requisitos de capacidade, cobertura e qualidade do serviço.

12.10. **Aquisição e Instalação:**

12.10.1. Seleção do fornecedor e contratação do serviço.

12.10.2. Aquisição de equipamentos necessários (cabos, switches, roteadores etc.).

12.10.3. Instalação física dos equipamentos e conexão dos cabos.

12.11. **Configuração e Testes:**

12.11.1. Configuração dos equipamentos para garantir compatibilidade e funcionalidade.○ Testes de desempenho e de segurança para verificar a qualidade da conexão.

12.11.2. Certificação dos padrões de qualidade e conformidade.

12.12. **Operação e Manutenção:**

12.12.1. Monitoramento contínuo da performance do link de dados.

12.12.2. Manutenção preventiva para evitar falhas e garantir a disponibilidade do serviço.○ Resolução de problemas e reparos emergenciais conforme necessário.

12.13. **Atualização e Expansão:**

12.13.1. Implementação de upgrades tecnológicos para melhorar a capacidade e eficiência.

12.13.2. Expansão da rede para atender novas demandas de dados.

12.13.3. Adaptação às mudanças nas tecnologias e nos requisitos de negócio.

12.14. **Descomissionamento:**

12.14.1. Avaliação da obsolescência e eficiência do link de dados.

12.14.2. Planejamento do desligamento da infraestrutura.

12.14.3. Retirada física dos equipamentos e cabos.

12.14.4. Descarte ou reciclagem dos componentes conforme políticas ambientais e regulamentações.

12.15. Cada uma dessas etapas é crucial para garantir a eficiência operacional e a qualidade do serviço ao longo da vida útil do link de dados. A gestão adequada de todas essas fases ajuda a maximizar o retorno sobre o investimento e a manter a infraestrutura de comunicação alinhada com as necessidades em constante evolução da Administração Pública.

13. NATUREZA DO OBJETO DA CONTRATAÇÃO

13.1. Trata-se o objeto de serviços de natureza comum, na forma do parágrafo único, do art. 6º, XIII, da Lei nº 14.133/2021, uma vez que os seus padrões de desempenho e qualidade estarão objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

13.2. O objeto constitui solução em TIC que agrega o serviço de natureza contínua.

14. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

14.1. Visando atender aos preceitos estabelecidos nas normativas vigentes, a solução deverá ser parcelada em 2 (dois) lotes, sendo que a vencedora do Lote I não poderá arrematar o Lote II, podendo participar da etapa de lances normalmente, tendo em vista que somente será inabilitada para o Lote II se efetivamente for considerada habilitada para o Lote I, abaixo os lotes propostos:

LOTE I - **Rede SD-WAN Principal**

LOTE II - **Rede SD-WAN Secundária**

14.2. Este parcelamento dos serviços técnicos a serem oferecidos visa essencialmente dar mais e melhores opções de conectividade para a administração, atendendo áreas mais remotas e carentes de infraestrutura de telecomunicações, bem como alcançar o máximo de economicidade possível dentro do objeto da contratação, sem prejuízos aos requisitos técnicos de funcionamento da rede.

14.3. Algumas tecnologias de acesso (Satelital de Baixa Órbita e FWA) foram incluídas apenas no Lote II, que é a parte do objeto referente aos links que servirão como redundância de acesso, para dar maior atratividade a este Lote apartado, mitigando riscos de resultar em deserto ou com baixa competitividade. Esta ação se mostra essencialmente importante, tendo em vista que na licitação anterior da Rede Conect@.RJ houve exatamente este tipo de cenário, em que um dos Lotes, com tecnologias de acessos distintas daquelas que são majoritaria no objeto (Ex. fibra ótica dedicada), resultou em deserto. Os links satelitais de baixa órbita e os do tipo FWA são importantes para atendimento a áreas remotas e com dificuldades para consolidação de estruturas físicas de telecomunicações, que podem ser atendidas por links satélitais ou tecnologias móveis de conectividade por meio de 4G/5G. Manter estas tecnologias aglutinadas em um único lote traz maior chance de obtenção de preços vantajosos à Administração Pública, diante de uma escala maior de itens no lote, além de promover maior disputa de preços que terá que necessariamente envolver também estes itens de tecnologia na composição dos preços do lote.

14.4. Entendemos que os lotes do presente certame não podem ser subdivididos ou parcelados, em vista dos seguintes fatores:

14.5. A divisão de qualquer lote, em qualquer outra composição, acarretaria a multiplicação da infraestrutura de backbone de dados para cada fornecedor contratado, aumentando assim os custos de gerência, energia elétrica, espaço físico, refrigeração e complexidade na interoperabilidade da rede, tornando o projeto inviável tecnicamente;

14.6. Aumento dos riscos ligados à indisponibilidade por conta de maiores dificuldades de análises técnicas em virtude do maior número de equipamentos necessários, tornando qualquer incidente mais difícil de identificar e solucionar;

14.7. Aumento dos riscos de segurança da informação, visto que mais fornecedores significam mais pontos de falha possíveis;

14.8. Aumento da complexidade e esforço técnico e administrativo (suporte, gestão, monitoramento, faturamento, etc.).

14.9. A divisão dos lotes em regiões geográficas pode implicar em que a competitividade se concentre nas capitais e regiões metropolitanas, deixando “desertos” outros lotes em regiões de interior,

comprometendo assim o atingimento do objetivo da contratação, que se trata da conectividade entre todos os órgãos da administração direta e indireta do Estado do Rio de Janeiro em uma rede governo segura.

14.10. A discussão sobre o não parcelamento do presente objeto já foi motivo de análise do TCE (PROCESSO Nº 108.185-6/19) que culminou em voto favorável ao PRODERJ manter a composição de lotes já definida, acatando as considerações técnicas e administrativas apresentadas.

14.11. Adicionalmente, subdivisões adicionais dos Lotes podem acarretar problemas de garantia e compatibilidade entre equipamentos de diferentes fornecedores, o que inviabiliza a aquisição por fornecedores distintos. Tendo em vista tratar-se de uma solução integrada, cada Lote definido deverá ser fornecido e implantado por único fornecedor e sobretudo, os produtos deverão ser ofertados do mesmo fabricante dos equipamentos e softwares, evitando assim incompatibilidades entre hardware, software, sistema de gerenciamento, implantação, suporte técnico e pós-venda. Fragmentações adicionais do objeto em vários, ocasionando diversas contratações, poderá comprometer o funcionamento do serviço que se vislumbra obter, revelando risco de impossibilidade de execução satisfatória do objeto.

14.12. Ainda sob a perspectiva técnica, consideramos a centralização da responsabilidade em uma única empresa contratada por Lote estabelecido, a qual entendemos ser a mais adequada não apenas em vista do acompanhamento de problemas e soluções, mas também em termos de facilitar a verificação das suas causas e atribuição de responsabilidade de modo a aumentar o controle sobre a execução do objeto licitado.

14.13. Assim, pretende-se com esta formação em dois Lotes, favorecer a Administração Pública com uma melhor prestação de serviço sem restringir a competitividade do certame, além dos melhores preços, a melhor tecnologia e também, do melhor gerenciamento dos contratos a serem firmados.

15. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

15.1. Os servidores serão devidamente indicados na fase de contratação, para desempenho de papéis como gestor do contrato, fiscal técnico, fiscal da área requisitante e fiscal administrativo, bem como os respectivos suplentes.

Necessidades de adequações no ambiente. A instalação de um link de dados requer um ambiente adequado para garantir a sua eficiência, segurança e durabilidade, tais como:

15.2. **Espaço físico adequado:**

15.2.1. O local deve ter espaço suficiente para a instalação dos equipamentos necessários, como racks, switches, roteadores, servidores, entre outros.

15.3. **Segurança física:**

15.3.1. O ambiente deve ser seguro contra acesso não autorizado. Isso pode incluir o uso de portas com fechaduras, câmeras de vigilância e outras medidas de segurança física para proteger os equipamentos de rede.

15.4. **Proteção contra interferências eletromagnéticas:**

15.4.1. Evitar a proximidade com fontes de interferência eletromagnética que possam prejudicar o desempenho do link de dados. Isso inclui equipamentos elétricos potentes, linhas de alta tensão, entre outros.

15.5. **Ventilação adequada:**

15.5.1. Os equipamentos de rede geram calor, portanto, é importante garantir uma boa ventilação no local de instalação para evitar o superaquecimento e garantir o funcionamento adequado dos dispositivos.

15.6. **Infraestrutura elétrica:**

15.6.1. Assegurar que haja energia elétrica confiável e suficiente para alimentar todos os equipamentos de rede, além de considerar a instalação de sistemas de energia alternativa ou de backup, como geradores, para evitar interrupções.

15.7. Considerando esses pontos, é possível garantir que o ambiente de instalação do link de dados seja seguro, eficiente e capaz de suportar as demandas operacionais necessárias.

16. REQUISITOS DE QUALIFICAÇÃO TÉCNICA

16.1. Comprovação de aptidão para a prestação de serviços, de acordo com as características,

quantidades e prazos compatíveis com o objeto, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, na forma do artigo 67 da Lei Federal nº 14.133/2021.

16.2. As certidões ou atestados, deverão demonstrar capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior, bem como documentos comprobatórios emitidos na forma do § 3º do art. 88 da Lei Federal nº 14.133/2021, atendendo no mínimo aos seguintes requisitos técnicos:

16.3. Para os Lotes I e II, comprovação de fornecimento de, no mínimo, 50% do somatório dos links de dados referentes aos itens 4 a 10, que são aqueles de maior relevância em cada lote, podendo o atestado referenciar a prestação de serviços em apenas um ou alguns dos itens;

16.4. Comprovação de prestação de serviços de Rede Corporativa IP gerenciada por SD-WAN;

16.5. Comprovação de prestação de serviços de Segurança Gerenciada (MSS);

16.6. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

16.7. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, resultando na comprovação de capacidade técnico-operacional de uma única contratação.

16.8. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foram prestados os serviços.

16.9. A motivação para os itens necessários à comprovação de aptidão técnica se dá em virtude de se tratar de contratação para atendimento em larga escala, que demanda a necessidade de prestador com capacidade de atendimento compatível com a criticidade do projeto, mitigando riscos à disponibilidade dos serviços do Governo, bem como diante da importância do objeto a ser contratado. A porcentagem mínima não se mostra viável ser associada a um único item ou a uma fração dos itens do lote, tendo em vista que não há, cada lote, itens de maior relevância técnica, todos são links de comunicação de dados, diferindo basicamente apenas as velocidades máximas. Mesmo os itens com maior quantidade ou aqueles que terão o maior valor estimado não podem se considerados como de maior relevância para fins de delimitação das comprovações de requisitos de qualificação técnica, pois na prática essa definição traria risco altíssimo de restrição a ampla competitividade ao certame, pois poderia uma empresa ser capaz de comprovar prestação de serviços para todas as demais velocidades, exceto aquela definida como mais relevante, deixando a mesma de forma da disputa, mesmo aquela empresa sendo plenamente capaz de executar o objeto.

16.10. A documentação a ser apresentada se mostra necessária por se tratar de contratação para atendimento em larga escala e visa garantir que a empresa vencedora do certame possui capacidade plena para atendimento ao objeto, sem risco de incapacidade técnica para prestação dos serviços nos níveis exigidos na documentação técnica, o que na prática representaria parada completa no funcionamento da máquina pública em nível generalizado, que hoje depende da rede de telecomunicações em pleno funcionamento por conta dos sistemas corporativos e acesso à Internet, no caso de uma prestadora que se mostre incapaz de entregar o objeto na quantidade e qualidade exigidas.

17. AMOSTRA, EXAME DE CONFORMIDADE E PROVA DE CONCEITO

17.1. Não se aplica ao escopo da contratação.

18. OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

18.1. Obrigações da Contratante

18.1.1. A CONTRATANTE fica obrigada a conservar todos os equipamentos e materiais disponibilizados na forma de comodato, não podendo utilizá-los senão de acordo com o contrato ou a natureza dele, sob pena de responder por perdas e danos perante a CONTRATADA.

18.2. Obrigações da Contratada

18.2.1. A CONTRATADA deverá executar o objeto com observância das especificações técnicas e regulamentação aplicável ao caso, com esmero e correção, refazendo tudo quanto for impugnado pela fiscalização, se necessário;

18.2.2. A CONTRATADA não poderá cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional;

18.2.3. A CONTRATADA deverá fornecer ao CONTRATANTE acesso irrestrito e em tempo real ao sistema de gerenciamento de manutenções, com possibilidade de abertura de chamados e acompanhamento de todos os dados lançados no sistema, realização de consultas em toda a base de dados e geração de relatórios;

18.2.4. Quando necessária a substituição de materiais, a CONTRATADA deverá instalar equipamentos atualizados tecnologicamente em sua última versão, não podendo estar em situação de End-of-Life ou End-of-Sale, estarem sendo suportados e recebendo atualizações de segurança do fabricante, e que atendam integralmente os requisitos técnicos, sem ônus ao CONTRATANTE;

18.2.5. Na ocorrência de furto, roubo ou dano decorrente de vandalismo praticado contra os equipamentos ou infraestrutura instalados, a CONTRATADA deverá efetuar a sua substituição, sem ônus ao CONTRATANTE, desde que não seja constatado o mau uso da solução ou desconformidades de instalação anteriormente reportadas pela CONTRATADA;

18.2.6. A CONTRATADA deverá comunicar ao Gestor/Fiscal do Contrato todas as ocorrências nos equipamentos instalados, que possam comprometer ou não os serviços;

18.2.7. Os custos da Manutenção Técnica Preventiva e Corretiva ocorrerão totalmente às custas da CONTRATADA, sem ônus ao CONTRATANTE;

18.2.8. A CONTRATADA deverá manter a mais absoluta confidencialidade sobre materiais, imagens, dados e informações disponibilizados ou conhecidos em decorrência da presente contratação, na forma da lei.

19. POSSIBILIDADE DE SUBCONTRATAÇÃO

19.1. Não se aplica a subcontratação em razão da composição do objeto distribuído em lotes compostos por itens de natureza indivisível.

20. PARTICIPAÇÃO DE MICROEMPRESAS, PEQUENAS EMPRESAS E EMPRESÁRIOS INDIVIDUAIS

20.1. Não se aplica, tendo em vista que o objeto desta licitação é indivisível, ou seja, não pode ser adquirido separadamente, sem prejuízo do resultado ou da qualidade do serviço.

21. PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

21.1. **Consórcios**

21.1.1. Será permitida a participação de pessoas jurídicas reunidas em consórcio, com o intuito de ampliar a competição, tendo em vista a grande abrangência territorial a ser coberta pela CONTRATADA, que demanda considerável estrutura logística para atendimento a CONTRATANTES que possuam unidades espalhadas em todo o território estadual, como, por exemplo, Polícias Militar e Civil, Bombeiros, etc., observadas as seguintes regras:

21.1.2. As empresas consorciadas apresentarão compromisso público ou particular de constituição do consórcio, subscrito por todas, onde deverá estar indicada a empresa líder como responsável principal perante o órgão licitante pelos atos praticados pelo consórcio, devendo constar expressamente do instrumento os poderes específicos para requerer, assumir compromissos, transigir, discordar, desistir, renunciar, receber e dar quitação, como também receber citação em Juízo;

21.1.3. Impedimento de a empresa consorciada participar, na mesma licitação, de mais de um consórcio ou de forma isolada;

21.1.4. O consórcio vencedor, quando for o caso, ficará obrigado a promover a sua constituição e registro antes da celebração do Contrato, nos termos do compromisso firmado conforme item 21.1.2;

21.1.5. As empresas consorciadas responderão solidariamente pelos atos praticados em consórcio, tanto na fase da licitação quanto na da execução do Contrato;

21.1.6. A substituição de consorciado deverá ser expressamente autorizada pelo órgão ou entidade contratante e condicionada à comprovação de que a nova empresa do consórcio possui, no mínimo, os mesmos quantitativos para efeito de habilitação técnica e os mesmos valores para efeito de qualificação econômico-financeira apresentados pela empresa substituída para fins de habilitação do consórcio no processo licitatório que originou o contrato.

21.1.7. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno

porte e forem exigidos no Edital requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% para o consórcio em relação ao valor exigido para os licitantes individuais.

21.2. **Cooperativas**

21.2.1. Não se aplica a participação de cooperativas neste certame, tendo em vista a especificidade do objeto, que compreende serviços de instalação de circuitos de comunicação de dados com o fornecimento de equipamentos, materiais e dispositivos necessários a sua execução, bem como observado o mercado, o qual é composto por empresas de organização tradicional aptas a fornecer a integralidade do objeto. Ademais, os serviços previstos no objeto demandam subordinação. Tais premissas em nada prejudicam a ampla concorrência na licitação.

22. PRAZO DO CONTRATO E POSSIBILIDADE DE PRORROGAÇÃO

22.1. **Vigência contratual**

22.1.1. O prazo de vigência dos contratos para os lotes será de 60 (sessenta) meses, prorrogáveis em sucessivos períodos de 12 (meses), até o limite de 120 (cento e vinte) meses, contados a partir da data da divulgação no Portal Nacional de Contratações Públicas, conforme preveem os art. 106 e 107 da Lei nº 14.133/2021.

22.1.2. A vigência estendida se justifica pela natureza dos serviços, que envolvem suporte técnico contínuo à solução, demandando uma estrutura operacional capaz de atender à diversidade de localidades dos pontos de instalação. A complexidade logística associada ao atendimento distribuído implica custos significativos, e um prazo contratual estendido permitirá ao mercado ofertar condições mais vantajosas. Além disso, trata-se de um projeto de longo prazo e sem previsão de descontinuidade, o que otimiza aspectos administrativos e contratuais.

22.1.3. O prazo contratual estendido permitirá maior participação do mercado no certame, tendo em vista que garante uma maior previsibilidade das margens de lucro diante dos custos da operação como um todo, que envolvem equipamentos, recursos humanos e logística de instalação e manutenção. O princípio da competitividade é a essência da licitação. Em suma, o princípio da competitividade, de um lado, exige que se verifique a possibilidade de se ter um número ampliado de interessados que possam atender e fornecer o que a Administração Pública necessita. Portanto, a competição é exatamente a razão determinante do procedimento. Com um número maior de licitantes participando do evento licitatório, mais fácil será à Administração Pública encontrar a melhor oferta. É verdade que muitas vezes temos dificuldades para julgar a satisfação desse item editalício, porque a interpretação literal da legislação nos distancia do interesse público. Tais problemas de ordem prática deverão ser resolvidos com a aplicação do princípio da competitividade como o busca do com o alongamento da vigência do contrato.

22.1.4. Diante do exposto, um prazo de vigência maior tornaria a contratação mais atrativa, estaria inserida na lógica de mercado da duração de contratos para esse tipo de serviço e contribuiria para mitigar os riscos de uma eventual necessidade da realização de uma nova contratação do serviço em tela e atenderia os princípios da economicidade, razoabilidade, competitividade e interesse público.

22.1.5. O prazo de vigência do Contrato poderá ser prorrogado, sucessivamente, por períodos de 12 (doze) meses, até o máximo de 10 (dez) anos, na forma dos arts. 106 e 107 da Lei n° 14.133/2021, desde que observadas as condições previstas no Contrato, e mediante a celebração de termo aditivo.

23. LOCAL DE ENTREGA DOS BENS OU DA PRESTAÇÃO DO SERVIÇO

23.1. A entrega do objeto desta contratação ocorrerá nos locais informados pelo CONTRATANTE, através da ordem de serviço emitida.

24. PRAZOS E CONDIÇÕES DE ENTREGA DOS BENS E SERVIÇOS

24.1. **Prazos de entrega**

24.1.1. O prazo de entrega completa da solução será de até 180 (cento e oitenta) dias corridos após emissão da ordem de serviço, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Contratações Públicas.

24.2. **CRONOGRAMA DOS EVENTOS**

24.2.1. Além de outros prazos previstos neste documento, a CONTRATADA deverá cumprir os eventos básicos descritos nas tabelas a seguir, respeitando os prazos máximos estabelecidos:

a) **Contratos PRODERJ e outros cujo Projeto Executivo estabeleça a criação de backbone/concentrador próprio:**

LOTE I

MARCOS	PRAZOS (DIAS)	EVENTO	RESPONSÁVEL
D	0 (zero)	Assinatura do contrato entre o CONTRATANTE e a empresa Licitante vencedora.	CONTRATANTE e CONTRATADA
D1	D+30	Entrega do Projeto Executivo e Planos de Implantação.	CONTRATADA
D2	D1+15	Aprovação do Projeto Executivo e dos Planos de Implantação.	CONTRATANTE
D3	D2+60	Instalação e configuração dos equipamentos concentradores, solução de segurança, enlaces de backbone principais e SD-WAN.	CONTRATADA
D4	D3+60	Instalação e configuração dos enlaces remotos principais contratados da Rede Conect@.RJ	CONTRATADA
D5	D4+15	Recebimento definitivo, autorização para emissão de faturamento e início do período de execução dos	CONTRATANTE e CONTRATADA

LOTE II

MARCOS	PRAZOS (DIAS)	EVENTO	RESPONSÁVEL
D	0 (zero)	Assinatura do contrato entre o CONTRATANTE e a empresa Licitante vencedora.	CONTRATANTE e CONTRATADA
D1	D+30	Entrega do Projeto Executivo e Planos de Implantação.	CONTRATADA

D2	**D1+15**	**Aprovação do Projeto Executivo e dos Planos de Implantação.**	**CONTRATANTE**
D3	**D2+60**	**Instalação e configuração dos equipamentos concentradores e enlaces de backbone principais.**	**CONTRATADA**
D4	**D3+60**	**Instalação e configuração dos enlaces remotos de contingência contratados da Rede Conect@.RJ**	**CONTRATADA**
D5	**D4+15**	**Recebimento definitivo, autorização para emissão de faturamento e início do período de execução dos serviços.**	**CONTRATANTE e CONTRATADA**

b) **Contratos cujo Projeto Executivo não demande a criação de backbone/concentrador próprio:**

LOTE I

MARCOS	PRAZOS (DIAS)	EVENTO	RESPONSÁVEL
D	**0 (zero)**	**Assinatura do contrato entre o CONTRATANTE e a empresa Licitante vencedora.**	**CONTRATANTE e CONTRATADA**
D1	**D+30**	**Entrega do Projeto Executivo e Planos de Implantação.**	**CONTRATADA**
D2	**D1+15**	**Aprovação do Projeto Executivo e dos Planos de Implantação.**	**CONTRATANTE**
D3	**D2+60**	**Instalação e configuração dos enlaces remotos SD-WAN principais contratados da Rede Conect@.RJ**	**CONTRATADA**
D4	**D3+15**	**Recebimento definitivo, autorização para emissão de faturamento e início do período de execução dos serviços.**	**CONTRATANTE e CONTRATADA**

LOTE II

MARCOS	PRAZOS (DIAS)	EVENTO	RESPONSÁVEL
D	**0 (zero)**	**Assinatura do contrato entre o CONTRATANTE e a empresa Licitante vencedora.**	**CONTRATANTE e CONTRATADA**
D1	**D+30**	**Entrega do Projeto Executivo e Planos de Implantação.**	**CONTRATADA**
D2	**D1+15**	**Aprovação do Projeto Executivo e dos Planos de Implantação.**	**CONTRATANTE**
D3	**D2+60**	**Instalação e configuração dos enlaces remotos de contingência contratados da Rede Conect@.RJ**	**CONTRATADA**
D4	**D3+15**	**Recebimento definitivo, autorização para emissão de faturamento e início do período de execução dos serviços.**	**CONTRATANTE e CONTRATADA**

24.2.2. Os tempos considerados na tabela deverão ser contados em dias corridos.

24.2.3. Os prazos considerados na tabela foram dimensionados de modo a garantir a manutenção da conectividade da rede e resguardar o impacto causado por eventuais indisponibilidades na troca de Operadoras de telecomunicações.

24.2.4. A autorização para o pagamento mensal de cada circuito será efetuada somente após o recebimento do serviço referente ao circuito em questão de modo definitivo.

24.2.5. Não será concedido sob nenhuma hipótese ou alegação reajuste retroativo à data em que a CONTRATADA legalmente faria jus, se o respectivo pedido de reajuste não for solicitado dentro do primeiro mês de aniversário do Contrato.

24.3. **Condições da entrega**

24.3.1. O fornecimento dos equipamentos que farão parte da infraestrutura de rede e conectividade, abrange o transporte do material desde o endereço de origem da firma CONTRATADA até o local de recebimento, sem ônus para a CONTRATANTE, devendo ser realizado em veículo adequado, acondicionado em embalagens protetoras lacradas e devidamente identificadas para facilitar o recebimento.

24.3.2. Todos os equipamentos deverão ser entregues de forma completa, ou seja, com todos os insumos necessários a sua correta instalação e operação, tais como cabos de força, manuais e acessórios e etc.

25. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E ACEITE DO OBJETO EXECUTADO

25.1. Mensalmente a CONTRATADA deverá encaminhar, para a apreciação da Fiscalização da

PRODERJ e do órgão aderente (CONTRATANTE), os documentos comprobatórios das atividades realizadas no último período de medição. A CONTRATADA poderá consolidar esses documentos em um único relatório que deverá conter as seguintes informações, abaixo elencadas:

25.1.1. Resumo descritivo da operação dos serviços no período em questão;

25.1.2. Ações de melhorias implantadas no mês;

25.1.3. Análise das ocorrências de acionamento fora do horário administrativo e ações tomadas ou sugeridas, quando não forem da competência da CONTRATADA, para evitar a recorrência;

25.1.4. Identificação de todas as violações, bem como as justificativas para cada violação;

25.1.5. O PRODERJ poderá, exclusivamente a seu critério, dispensar a CONTRATADA da apresentação de parte dos documentos ou indicadores mencionados. Tal dispensa será formalizada por e-mail do fiscal ou do gerente de contrato.

25.1.6. Em reunião de início de prestação dos serviços será informado o período de referência para aferição dos indicadores e após o fechamento do período de apuração a CONTRATADA disporá de 3 (três) dias úteis para apresentar os documentos comprobatórios de prestação de serviço;

25.1.7. O nível de qualidade e eficácia dos serviços prestados será monitorado conjuntamente pelo PRODERJ e pela CONTRATADA;

25.2. **Os relatórios e indicadores usaram como fonte de informação:**

25.2.1. Informações dos CONSOLES dos produtos;

25.2.1.1. SIEM;

25.2.1.2. a Solução de Gestão de chamados e atendimentos, através de pesquisa de satisfação sistemática para cada solicitação atendida;

25.2.1.3. Sistema de administração de redes e de monitoração de disponibilidade da infraestrutura da CONTRATANTE;

25.2.1.4. Sistemas de informações próprios ou licenciados da CONTRATANTE;

25.2.1.5. Observações da Fiscalização da CONTRATANTE.

25.3. Os serviços serão acompanhados mensalmente a partir dos seguintes relatórios:

25.3.1. Políticas de segurança revistas e/ou criadas para melhoria do ambiente;

25.3.2. Solução de Incidentes de segurança associados ao Suporte assistido de gerência de rede e segurança;

25.3.3. Número de políticas implementadas de detecção e resposta automática a incidentes de segurança da informação;

25.3.4. Números de instruções técnicas associadas à solução de problemas cadastrados na base de conhecimento;

25.3.5. Reincidência do mesmo problema de segurança da informação;

25.4. Outras formas definidas pelo CONTRATANTE em comum acordo com a CONTRATADA. A medição dos serviços será baseada nos seguintes indicadores e metas:

25.5. **Índice de Disponibilidade Mensal do Enlace**

25.6. Percentual de tempo, durante o mês de operação em que um enlace, incluído o CPE, venha a permanecer em condições normais de funcionamento.

25.6.1. IDM = [(To – Ti)/To]*100

25.6.2. Onde:

25.6.3. IDM: Índice de Disponibilidade Mensal do Enlace. ● To: período de operação em um mês.

25.6.4. Ti: somatório dos tempos de inoperância durante o período de operação em um mês em minutos.

25.6.5. A CONTRATADA realizará, por meio da solução de gerenciamento, a coleta e o armazenamento de informações a respeito dos enlaces contemplando um histórico de 12 (doze) meses.

25.6.6. Os tempos de inoperância serão os tempos em que os enlaces apresentarem problemas e serão obtidos dos registros de eventos no sistema de gerenciamento da CONTRATADA, confrontados com as informações do sistema de monitoramento da CONTRATANTE.

25.6.7. Somente serão desconsiderados para efeito de desconto os tempos de inoperância causados

por manutenções programadas com a prévia anuência da CONTRATANTE, bem como casos fortuitos de força maior, devidamente comprovados.

25.7. **Taxa de Erro de Bit - TxErr**

25.7.1. Relação entre a quantidade de bits corretamente transmitidos para cada bit transmitido com erro em um determinado enlace pertencente à rede de acesso. A Taxa de Erro de Bit deverá ser medida por solicitação da CONTRATANTE. Bit de

25.7.2. TxErr: Taxa de Erro de Bit

25.7.3. BErr: número de bits com erro no período da medição.

25.7.4. BTot: número total de bits no período de medição.

25.7.5. A CONTRATADA deverá disponibilizar, quando solicitado pela CONTRATANTE relatório com os valores medidos da taxa de erro de determinado enlace, quando os enlaces apresentarem problemas físicos de transmissão na rede de acesso ou quando necessária auditoria específica em relação a este nível de serviço em determinado enlace.

25.8. **Taxa de Perda de Pacotes - TPP**

25.8.1. Representa a quantidade de pacotes perdidos fim a fim. É a medida em percentual tomado como referência o volume total de pacotes que alcançaram o destino, dentro do volume total de pacotes transmitidos.

25.8.2. É medida em percentual tomado como referência o volume total de pacotes que alcançaram o destino (medido na interface WAN do CPE do terminal de destino) dentre o volume total de pacotes transmitidos (medido na interface WAN do CPE do terminal de origem).

25.8.3. TPP = (NPP / NPT) * 100%

25.8.4. Onde:

25.8.5. TPP: Taxa de Perda de Pacotes.

25.8.6. NPP: número de pacotes perdidos.

25.8.7. NPT: número total de pacotes transmitidos.

25.8.8. A CONTRATANTE poderá solicitar medições em horários específicos, conforme acordado com a CONTRATADA.

25.8.9. A CONTRATADA disponibilizará, quando solicitado pela CONTRATANTE, relatórios com os valores das medições solicitadas, referentes ao percentual de perda de pacotes.

25.8.10. Um enlace será considerado indisponível sempre que a perda de pacotes for superior a 5%, e o enlace não esteja operando acima de sua capacidade durante um período superior a 10 (dez) minutos.

25.8.11. A CONTRATADA realizará, por meio da solução de gerenciamento, a coleta e o armazenamento de informações a respeito da perda de pacotes, mesmo que de forma independente do modelo descrito acima.

25.9. **Tempo de Retardo - RTT**

25.9.1. Tempo gasto entre a transmissão do primeiro bit de um pacote até a recepção do último bit do mesmo pacote, em apenas um dos sentidos da transmissão.

25.9.2. A apuração do retardo na Rede Governo será efetuada com o envio de pacotes ICMP de tamanho fixo de 32 (trinta e dois) octetos de dados, entre terminais de origem e destino localizados em sítios da rede dentro do mesmo backbone e retornando à origem onde será realizada a medição do tempo de resposta destes pacotes. Como o tempo de resposta corresponde ao tempo de ida e volta do pacote, o tempo de retardo será considerado como o tempo de resposta dividido por dois.

25.9.3. O tempo de resposta limite a ser aguardado para cada pacote deverá ser de 5 (cinco) segundos. Valores superiores a este tempo serão considerados “timeout”.

25.9.4. Cada medida deverá ser realizada através do envio de uma série de 4 (quatro) pacotes ICMP por vez. O valor instantâneo do retardo referente a uma medida será igual à média aritmética dos quatro valores dos tempos de resposta referentes à série de pacotes.

25.9.5. ICMP enviados, dividida por dois, pois será considerado o retardo apenas em um dos sentidos da comunicação.

25.9.6. RTT = média do retardo de 4 pacotes ICMP.

25.9.7. Um enlace será considerado indisponível sempre que o tempo de retardo da rede for superior a 1000 (mil) ms para enlaces terrestres e 2000 (dois mil) ms para enlaces satélites durante um período superior a 10 (dez) minutos.

25.9.8. Medições sobre demanda a CONTRATADA pelo CONTRATANTE, permitindo a auditoria do valor deste indicador.

25.9.9. A CONTRATADA deverá disponibilizar ao CONTRATANTE, quando demandada, um relatório com os diversos valores apurados. Os relatórios deverão fornecer os valores medidos nos intervalos de tempo solicitados e as médias de retardo para cada par de sítios escolhido, que espelhem todas as condições/medidas/resultados da fórmula do cálculo.

25.9.10. A CONTRATADA realizará, por meio da solução de gerenciamento, a coleta e o armazenamento de informações a respeito da latência dos circuitos de forma, mesmo que de forma independente do modelo descrito acima.

25.10. **Prazo de Reparo – PR**

25.10.1. Prazo limite para reparo e o restabelecimento de um enlace com 100% de operabilidade, na ocorrência de inoperância ou falha.

25.10.2. Apuração do tempo de restabelecimento de um enlace, a partir de consulta na solução de gerenciamento da CONTRATADA, devidamente confrontada com o sistema de monitoramento da CONTRATANTE e subsequente comparação com o valor descrito no limiar de Qualidade deste indicador.

25.10.3. O CONTRATANTE, quando devidamente comprovada sua responsabilidade no fato gerador de eventual atraso no restabelecimento do enlace, deverá autorizar a CONTRATADA a atualizar tal fato em seus registros, excluindo-se então o período informado do cálculo de indisponibilidade do enlace.

25.10.4. A CONTRATADA deverá disponibilizar mensalmente ao CONTRATANTE relatório com os valores apurados, por enlace, inclusive contabilizando os valores a serem descontados dos enlaces pela perda deste indicador.

25.10.5. PR = Tr - Ti

25.11. Onde:

25.11.1. PR: prazo de reparo

25.11.2. Tr: instante de restabelecimento de um enlace

25.11.3. Ti: instante de indisponibilidade de um enlace

25.11.4. A CONTRATADA deverá confirmar junto à CONTRATANTE o retorno operacional de um enlace para o fechamento do reparo.

25.11.5. Prazo para Alteração de Configuração - PAC

25.11.6. Prazo, em horas, para a CONTRATADA alterar a configuração do serviço solicitado pelo CONTRATANTE.

25.11.7. A alteração de configuração solicitada deverá ser possível de ser realizada remotamente, sem que seja necessário qualquer estudo prévio ou elaboração de projeto lógico específico para a sua execução.

25.11.8. Dependendo do volume de solicitações a solicitação será tratada como projeto, independentemente do tipo de solicitação.

25.11.9. PAC = Tsa - Taa

25.12. Onde:

25.12.1. PAC: prazo de alteração da configuração do serviço.

25.12.2. Tsa: instante de solicitação da alteração.

25.12.3. Taa: instante de atendimento da solicitação da alteração

25.12.4. O CONTRATANTE deverá validar o atendimento da solicitação de alteração de configuração executada.

25.12.5. Face ao exposto anteriormente são definidos três níveis de atendimento às solicitações:

25.12.5.1. Alteração de Configuração de Baixa Complexidade.

25.12.5.2. Alteração de Configuração de Média Complexidade.

25.12.5.3. Alteração de Configuração de Alta Complexidade.

25.12.6. As solicitações de alteração de configuração que necessitem de agendamento em conjunto com a CONTRATANTE e prazos acordados entre ambas as partes, sendo que os prazos não sejam cumpridos por culpa exclusiva da CONTRATADA estão sujeitas às mesmas penalidades previstas para este indicador.

25.12.7. A CONTRATADA deverá disponibilizar para o CONTRATANTE, mensalmente relatórios contemplando as solicitações de alteração de configuração informando os prazos de atendimento.

25.13. **Prazo para Alteração da Taxa de Transmissão de um Enlace - PAT**

25.13.1. Prazo máximo para alteração de taxa de transmissão de um enlace já instalado em um determinado endereço.

25.13.1.1. PAT = Tsat - Taat

25.13.2. Onde:

25.13.2.1. PAT: prazo de Alteração de Taxa de Transmissão de um Enlace

25.13.2.2. Tsat: instante de solicitação da alteração de taxa de transmissão.

25.13.2.3. Taat: instante de atendimento da solicitação da taxa de transmissão.

25.13.3. Mensalmente, para cada sítio, deverão ser fornecidos os tempos para alteração da taxa de transmissão pela CONTRATADA a partir da base de dados da CONTRATADA e comparados com os registros da CONTRATANTE.

25.13.4. Independente de já existir um enlace instalado no endereço, a CONTRATADA deverá apresentar um estudo de viabilidade técnica em até 10 dias úteis ou 15 (quinze) dias corridos da solicitação de atendimento.

25.13.5. A CONTRATADA deverá disponibilizar relatório mensal com os prazos auferidos.

25.14. **Prazo de Atendimento a Novos Endereços - PAN.**

25.14.1. Prazo máximo de atendimento de solicitações de implantação de circuitos em novos endereços.

25.14.2. O prazo de atendimento também deverá incluir a atualização das informações dos enlaces na solução de gerência da CONTRATADA.

25.14.3. Independente do caso, a CONTRATADA deverá apresentar um estudo de viabilidade técnica em até 10 (dez) dias úteis ou 15 (quinze) dias corridos da solicitação de atendimento.

25.14.3.1. PAN = Tsan - Taan

25.14.4. Onde:

25.14.4.1. PAN: prazo de Atendimento a Novos Endereços.

25.14.4.2. Tsan: instante de solicitação de atendimento

25.14.4.3. Taan: instante de atendimento da solicitação.

25.14.5. A CONTRATADA deverá disponibilizar relatório mensal com os prazos apurados.

25.15. **Das Penalidades**

25.15.1. O atraso injustificado no prazo de entrega do Projeto Executivo de 30 (trinta) dias corridos da data de assinatura do contrato, poderá acarretar multa no valor de 0,2% (dois décimos por cento) sobre o somatório mensal dos links constantes no Projeto Executivo, por dia de atraso, limitado a 9% (nove por cento), quando poderão ser tomadas ações administrativas com vistas à rescisão do contrato, por descumprimento total da obrigação. Caso o Projeto Executivo seja rejeitado pelo CONTRATANTE na hipótese prevista neste Estudo Técnico e Anexos, a CONTRATADA terá 5 dias corridos para readequar, após este prazo incidirá a multa prevista na presente cláusula.

25.15.2. Os atrasos injustificados no prazo de instalação e configuração dos enlaces aprovados no projeto executivo, excluindo-se as apresentações de relatórios, poderá causar multa no valor de 0,2 (dois décimos por cento) sobre o valor mensal de cada link em atraso limitados a 18%. Em função da quantidade dos links fora do prazo poderão ser tomadas ações administrativas com vistas à rescisão do contrato, por descumprimento total da obrigação.

25.15.3. Os atrasos injustificados nos prazos previstos no item 24.2 - CRONOGRAMA DE EVENTOS por

período superior a 180 (cento e oitenta) dias para os contratos cujo Projeto Executivo demande a criação de backbone, e superior a 120 (cento e vinte dias) para os contratos sem previsão de criação de backbone/concentrador, caracteriza o descumprimento total da obrigação, punível com as sanções previstas neste documento.

25.15.4. Nos casos de não atendimento dos indicadores de qualidade de serviços, conforme estabelecido neste Estudo Técnico e Anexos, que acarrete indisponibilidade dos serviços, serão efetuados descontos proporcionais automáticos pelos serviços não prestados.

25.15.5. O descumprimento dos Níveis Mínimos de Serviço (NMS) caso não sejam observados os prazos máximos para o retorno da disponibilidade regular dos serviços, sem prejuízo dos descontos sobre a fatura mensal, segundo os seguintes critérios:

25.15.6. Para o indicador "Índice de Disponibilidade Mensal do Enlace (IDM)", cada 0,1% (um décimo por cento) abaixo da métrica correspondente de cada tipo de enlace, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

25.15.7. Para o indicador "Taxa de Erro de Bit (TrErr)", sempre que houver aferição e este se encontrar em desacordo com o nível de serviço contratado, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

25.15.8. Para o indicador "Taxa de Perda de Pacotes (TPP)", sempre que houver aferição e este se encontrar em desacordo com o nível de serviço contratado, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

25.15.9. Para o indicador "Retardo da Rede (Retardo)", sempre que houver aferição e este se encontrar em desacordo com o nível de serviço contratado, será aplicado desconto correspondente a 3,0% (três por cento), calculado sobre o valor mensal do circuito afetado.

25.15.10. Para o indicador "Prazo para Reparo / Restabelecimento de um Enlace (PR)", cada 1 (uma) hora acima da métrica estabelecida no nível de serviço contratado, será aplicado desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado.

25.15.11. Para o indicador "Prazo para Alteração de Configuração de Roteadores (PAC)", para cada 1% do prazo estipulado em atraso, para o nível de serviço contratado, será aplicado desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado.

25.15.12. Para o indicador "Prazo para Alteração de Taxa de Transmissão de um Enlace (PAT)", cada 1 (um) dia acima da métrica estabelecida no nível de serviço contratado, será aplicado desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado.

25.15.13. Para o indicador "Prazo para Alteração a Novos Endereços (PAN)", a cada 1 (um) dia acima da métrica estabelecida no nível de serviço contratado, será aplicado desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado.

25.15.14. Descontos sobre a fatura mensal cumulativos em cada circuito serão limitadas ao valor mensal do circuito contratado.

25.15.15. Descontos sobre a fatura mensal serão cumulativos dentro de cada mês e não excederão a 30% (trinta por cento) do valor mensal do contrato.

25.15.16. Atingido esse limite, poderão ser tomadas ações administrativas com vistas à rescisão do contrato, por descumprimento da obrigação contratual, sem prejuízo das demais sanções previstas no contrato.

25.15.17. Essas sanções Estes descontos sobre a fatura mensal poderão ser aplicadas cumulativamente com as demais sanções previstas no contrato, não terão caráter compensatório e sua cobrança não isentará a CONTRATADA da obrigação de indenizar eventuais perdas e danos.

25.15.18. A sanção aplicada à CONTRATADA e os prejuízos por ela causados à CONTRATANTE poderão ser deduzidos de qualquer crédito a ela devido, cobrados direta ou judicialmente.

25.15.19. O valor da multa poderá ser descontado do pagamento a ser efetuado à CONTRATADA:

- Se o valor a ser pago à CONTRATADA não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.
- Se os valores do pagamento e da garantia forem insuficientes, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial.

a) Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA à CONTRATANTE, este será encaminhado para inscrição em dívida ativa.

b) Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser

complementada no prazo de até 10 (dias) dias úteis, contado da solicitação da CONTRATANTE, a partir do qual se observará o disposto nos itens da Cláusula Garantia deste contrato.

26. CRITÉRIOS DE MEDIÇÃO, DE PAGAMENTO E FORMA DE REAJUSTAMENTO DO CONTRATO

26.1. Os pagamentos serão realizados pelo ÓRGÃO GERENCIADOR, ÓRGÃOS PARTICIPANTES e ÓRGÃOS ADERENTES, de acordo com as contratações realizadas por cada um deles.

26.2. A CONTRATANTE deverá pagar 60 (sessenta) parcelas, sendo efetuadas mensal e diretamente na conta corrente de titularidade da CONTRATADA a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro.

26.3. No caso de a CONTRATADA estar estabelecida em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pelo CONTRATANTE a impossibilidade da CONTRATADA, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pela CONTRATADA.

26.4. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do objeto ou de cada parcela, mediante atestação, que não poderá ser realizada pelo ordenador de despesas, conforme disposto no Edital e/ou no Termo de Referência, bem ainda no artigo 140, II, alínea “b”, da Lei Federal nº 14.133/2021 e arts. 20 e 22, XXIII, do Decreto Estadual nº 48.817/2023.

26.5. Quando houver glosa parcial do objeto, o CONTRATANTE deverá comunicar à CONTRATADA para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

26.6. A CONTRATADA deverá encaminhar a Nota Fiscal ou Fatura para pagamento ao CONTRATANTE, para o endereço eletrônico a ser indicado.

26.7. O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal ou Fatura.

26.8. Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

26.9. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

26.10. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

26.11. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele Regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar nº 123/2006.

26.12. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível à CONTRATADA, sofrerão a incidência de atualização monetária e juros de mora pelo IPCA-E, calculado pro rata die, e aqueles pagos em prazo inferior ao estabelecido no instrumento convocatório serão feitos mediante desconto de 0,5% (um meio por cento) ao mês, calculado pro rata die.

26.13. A CONTRATADA deverá emitir a Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS nº 42/2009, com a redação conferida pelo Protocolo ICMS nº 85/2010, e caso seu estabelecimento esteja localizado no Estado do Rio de Janeiro, deverá observar a forma prescrita nas alíneas a, b, c, d e e, do §1º, do art. 2º da Resolução SEFAZ nº 971/2016.

26.14. Caso a CONTRATADA não esteja aplicando o regime de cotas na forma da Lei Estadual nº 7.258, de 12 de abril de 2016, do edital e do contrato, suspender-se-á o pagamento devido, até que seja sanada a irregularidade apontada pelo Órgão de fiscalização do Contrato.

26.15. Reajuste de Preços

26.15.1. Os preços contratados serão reajustados após o interregno de 1 (um) ano, mediante solicitação da CONTRATADA.

26.15.2. O intervalo mínimo de 1 (um) ano para o primeiro reajuste será contado da data do orçamento estimado.

26.15.3. Nos reajustes subsequentes ao primeiro, o intervalo mínimo de um ano será contado a partir do fato gerador que deu ensejo ao último reajuste.

26.15.4. Os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, exclusivamente para as obrigações que se iniciem após a anualidade.

26.15.5. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

26.15.6. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer, sendo adotado na aferição final o índice definitivo.

26.15.7. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

26.15.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

26.15.9. O pedido de reajuste deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação contratual, sob pena de preclusão.

26.15.10. Os efeitos financeiros do pedido de reajuste serão contados:

26.15.10.1. Da data-base prevista no contrato, desde que requerido o reajuste no prazo de 60 (sessenta) dias da data de publicação do índice ajustado contratualmente;

26.15.10.2. A partir da data do requerimento da CONTRATADA, caso o pedido seja formulado após o prazo fixado na alínea a, acima, o que não acarretará a alteração do marco para cômputo da anualidade do reajustamento, já adotado no edital e no contrato.

26.15.11. Caso, na data de eventual prorrogação contratual, ainda não tenha sido divulgado o índice de reajuste, deverá, a requerimento da CONTRATADA, ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro da CONTRATADA, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

26.15.12. A extinção do contrato não configura óbice para o deferimento do reajuste solicitado tempestivamente, hipótese em que será concedido por meio de termo indenizatório.

26.15.13. O reajuste será realizado por apostilamento, se esta for a única alteração contratual a ser realizada.

26.15.14. O reajuste de preços não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea “d”, da Lei n.º 14.133/2021.

27. REGRAS PARA RECEBIMENTO DO OBJETO

27.1. O objeto do contrato será recebido em tantas parcelas quantas forem ao do pagamento, na seguinte forma:

27.1.1. provisoriamente, pelos fiscais dos contratos, mediante termo, no prazo de 15 (quinze) dias corridos após a entrega dos serviços, quando verificado o cumprimento das exigências de caráter técnico;

27.1.2. definitivamente, pelos fiscais ou comissão de fiscalização, após decorrido o prazo de 30 (trinta) dias corridos do recebimento provisório, mediante termo detalhado que comprove o atendimento das exigências contratuais.

27.2. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato ou termo de referência, podendo ser fixado pelo fiscal do contrato um prazo para a substituição do bem, ou o refazimento do serviço, às custas da CONTRATADA, sem prejuízo da aplicação das penalidades, sendo sempre necessário a motivação da recusa.

27.3. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela legislação pertinente e pelo contrato.

27.4. Salvo disposição em contrário constante do edital, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta da CONTRATADA.

27.5. A Comissão de Fiscalização, sob pena de responsabilidade administrativa, anotará em registro próprio as ocorrências relativas à execução do contrato, determinando o que for necessário à

regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 10 (dez) dias, para ratificação.

27.6. A CONTRATADA declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a lhes fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem julgados necessários ao desempenho de suas atividades.

27.7. A instituição e a atuação da fiscalização do serviço objeto do contrato, não exclui ou atenua a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

27.8. A CONTRATADA se compromete a realizar de forma remota (por videoconferência) ou nas dependências da CONTRATANTE, antes do início da implantação da solução dos lotes I e II, uma reunião inicial de projeto em conjunto com as áreas de Segurança da Informação e Infraestrutura da CONTRATANTE, para definir o Plano de Trabalho de instalação e configuração da solução. A reunião deverá ocorrer durante o prazo previsto para instalação e configuração da solução.

27.9. Após a reunião inicial de projeto, será produzida uma ata assinada por todos os participantes da CONTRATANTE e da CONTRATADA, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da equipe do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários.

28. CONDIÇÕES DE GARANTIA CONTRATUAL

28.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei Federal nº 14.133/2021, correspondente a 5% (cinco por cento) de seu valor anual.

28.2. O referido percentual, resguardada a discricionariedade prevista no acima citado art. 96, caput e o teto estabelecido no caput do art. 98 do mesmo diploma legal, considera a natureza do objeto (serviços), enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do Órgão CONTRATANTE em razão do volume de recursos financeiros envolvidos no certame, visando impedir a inexecução, mesmo que parcial do objeto e danos ao erário.

28.3. A CONTRATADA poderá optar pelas seguintes modalidades de garantia:

28.3.1. caução em dinheiro ou em títulos da dívida pública;

28.3.2. seguro-garantia;

28.3.3. fiança bancária; e

28.3.4. título de capitalização custeado por pagamento único, com resgate pelo valor total.

28.4. Qualquer que seja a modalidade escolhida pela CONTRATADA, a garantia assegurará o pagamento de:

28.4.1. prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações neste previstas;

28.4.2. multas moratórias, compensatórias e administrativas aplicadas pela Administração à CONTRATADA; e

28.4.3. obrigações trabalhistas e previdenciárias de qualquer natureza, assim como as obrigações de regularidade perante o FGTS, não adimplidas pela CONTRATADA, quando couber.

28.5. A garantia, qualquer que seja a modalidade escolhida, terá validade durante a vigência do Contrato e por mais 90 (noventa) dias após o término deste prazo de vigência.

28.6. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, a CONTRATADA ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

28.7. Ressalvada a hipótese de seguro-garantia, em que deverá ser observado o prazo regular, a CONTRATADA apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contado da assinatura do Contrato.

28.8. Caso oferecida a modalidade de seguro-garantia, sua apresentação deve ocorrer em 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, e observar-se-ão as seguintes condições:

28.8.1. a apólice permanecerá em vigor mesmo que a CONTRATADA não pague o prêmio nas datas convencionadas;

28.8.2. a apólice deverá acompanhar as modificações referentes à vigência do Contrato principal, mediante a emissão do respectivo endosso pela seguradora;

28.8.3. será permitida a substituição da apólice na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto;

28.8.4. a apólice somente será aceita se contemplar todos os eventos, observada a legislação que rege a matéria.

28.9. Em caso de oferecimento de títulos da dívida pública, estes devem ser emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

28.10. Caso a opção seja por fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

28.11. Caso a opção seja por garantia em dinheiro, deverá ser efetuada em favor da CONTRATANTE, na conta corrente da instituição financeira contratada pelo Estado, cujo valor será corrigido monetariamente e restituído à CONTRATADA, na forma do item 18.17.

28.12. A CONTRATADA obriga-se a fazer a reposição, a suplementação ou a renovação da garantia, no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificado, no caso desta ser executada, total ou parcialmente, ou o Contrato for prorrogado ou tiver o seu valor alterado, assim como em qualquer outra situação que exija a manutenção da condição de garantia contratual.

28.13. A inobservância do prazo fixado para apresentação, reposição, suplementação ou renovação da garantia acarretará a aplicação de multa e/ou outras penalidades, na forma disposta no contrato.

28.14. O atraso superior a 25 (vinte e cinco) dias autoriza o CONTRATANTE a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, com a aplicação das sanções cabíveis.

28.15. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

28.16. O emitente da garantia ofertada pela CONTRATADA deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

28.17. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

28.18. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

28.19. Extinguir-se-á a garantia com a restituição da apólice, carta fiança, título da dívida pública ou autorização para a liberação da caução em dinheiro, atualizada monetariamente, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

28.20. A garantia somente será liberada ou restituída, após a fiel execução do Contrato ou pela sua extinção, por culpa exclusiva da Administração, ou quando assim convencionado, em se tratando de extinção consensual da contratação.

28.21. A CONTRATADA autoriza a CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no Edital e no Contrato.

29. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

29.1. Os estudos preliminares evidenciaram que a contratação da solução descrita se mostra tecnicamente viável e absolutamente necessária por ser tratar de um serviço essencial ao Estado. Adicionalmente, o serviço de Internet Satelital de Baixa Órbita e Geoestacionária, bem como soluções do tipo FWA já se encontram estabelecidos no mercado corporativo brasileiro, e por esta razão verificamos totalmente viável a sua inclusão no presente certame.

29.2. Restrito aos aspectos técnicos, declaramos a contratação pretendida como viável, uma vez que existem fornecedores no mercado ofertando regularmente os serviços necessários para alcançar os resultados pretendidos pela Administração.

30. ANEXOS

30.1. Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este documento principal do qual correspondem a parte integrante e indissociável:

30.2. Especificações Técnicas do Objeto (117848748)

30.3. Mapa de Riscos (117849155)

31. EQUIPE RESPONSÁVEL

Daniel Luzente de Lima Diretor / DIRIT ID: 4349885-0	**Luís Cláudio Marinho Coelho** Gerente / GERRT ID: 5140902-0	**Charles Monteiro Guimarães** Diretor de Patrimônio e Logística ID: 4432892-3	**Marco Antônio de Andrade UCP** ID: 4284601-3

Rio de Janeiro, na data da assinaura eletrônica.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 13/11/2025, às 11:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 13/11/2025, às 11:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 13/11/2025, às 11:57, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 13/11/2025, às 16:38, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117848252** e o código CRC **3DEDB637**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO I - ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. CONCEITOS

1.1. Rede SD-WAN:

1.1.1. Entende- se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou desempenho e utilização de túneis VPN para comunicação entre os sites remotos;

1.1.2. Total independência da tecnologia de transporte, permitindo a utilização de tecnologias como:

a) MPLS;

b) Rede Wireless (Rádio, 3G/4G/5G, e outras tecnologias);

c) Internet;

d) Satélite;

e) Links Ponto a Ponto.

Fonte Wikipedia (https://en.wikipedia.org/wiki/SD-WAN)

1.2. Rede IP Satelital de Baixa Órbita

1.2.1. Um serviço de satélite de baixa órbita (LEO) oferece acesso à internet banda larga e outros serviços por meio de uma constelação de satélites que orbitam a Terra a altitudes entre 160 e 2.000 km. Essa órbita baixa, comparada aos satélites tradicionais em órbitas geoestacionárias mais altas, proporciona diversas vantagens, como:

a) Baixa latência: A menor distância entre os satélites LEO e a Terra resulta em tempos de resposta (latência) significativamente menores, tornando-os ideais para aplicações que exigem comunicação em tempo real, como videoconferências, jogos online e transmissões ao vivo.

b) Alta capacidade: A constelação de satélites LEO oferece uma grande quantidade de largura de banda disponível, possibilitando downloads e uploads rápidos, além de suporte para vários usuários simultâneos. Ampla cobertura: Os satélites LEO podem fornecer cobertura de internet para áreas remotas e subatendidas, onde a infraestrutura terrestre é limitada ou inexistente, como regiões rurais, montanhas e oceanos. Flexibilidade: Os serviços LEO são escaláveis e podem ser facilmente adaptados às necessidades de diferentes usuários, desde residências individuais até grandes empresas e

instituições governamentais.

c) Um exemplo de serviço LEO é a Starlink, um dos serviços de satélite LEO mais conhecidos, operado pela SpaceX. A constelação Starlink já conta com milhares de satélites em órbita e oferece internet de alta velocidade para usuários em diversos países ao redor do mundo.

d) Internet de alta velocidade: Os serviços LEO podem oferecer velocidades de download e upload comparáveis às conexões de fibra óptica, com ping baixo e alta confiabilidade.

e) Ampla cobertura: Os satélites LEO podem fornecer internet para áreas onde outras opções, como cabo ou DSL, não estão disponíveis.

f) Fácil instalação: Os terminais LEO geralmente são pequenos e fáceis de instalar, permitindo que os usuários configurem seu serviço de internet rapidamente.

g) Portabilidade: Os terminais LEO podem ser transportados para diferentes locais, tornando-os ideais para uso em viagens ou áreas remotas.

1.2.2. Desvantagens dos serviços LEO:

a) Custo: Os serviços LEO podem ser mais caros do que as opções de internet tradicionais, especialmente durante os primeiros anos de operação.

b) Impacto ambiental: A grande quantidade de satélites LEO em órbita pode causar preocupações com a poluição luminosa e potencial interferência em observações astronômicas.

c) Dependência do clima: O mau tempo, como chuva forte ou neve, pode afetar o sinal do satélite LEO.

1.2.3. No geral, os serviços de satélite LEO oferecem uma alternativa promissora para o acesso à internet em áreas onde as opções tradicionais são limitadas ou inexistentes. Com a constante evolução da tecnologia e a redução dos custos, os serviços LEO se tornaram mais acessíveis e populares, principalmente no segmento corporativo.

1.2.4. Para recepção dos sinais A CONTRATADA deverá fornecer uma antena receptora e os demais equipamentos para fornecimento do serviço de conectividade a internet.

1.2.5. Cada satélite deverá se comunicar com estações terrestres e outros satélites na constelação, reduzindo a latência, ou seja, o tempo de resposta para a transmissão de dados.

1.2.6. Nas localidades com sistema satelital de baixa órbita, a CONTRATADA deve garantir que, uma vez atingido o limite da franquia mensal de dados estabelecido no contrato, os serviços de conexão com a internet permaneçam ativos para os usuários, sem interrupções, porém sem acesso prioritário.

1.2.7. Ao final do CONTRATO todos os equipamentos deverão ser desinstalados e recolhidos pela CONTRATADA em um prazo de até 30 dias, a contar da data de término da vigência.

1.2.8. O Governo do Estado do RJ possui necessidades específicas que poderiam ser atendidas por este serviço, como ações administrativas, sociais ou fiscalizatórias itinerantes, onde seria possível transportar e montar a solução em diferentes endereços. Outra opção seria instalação em viaturas oficiais do Governo, como, por exemplo das Polícias Militar e Civil, onde está sendo adotado o item de

câmera corporal e o acesso à Internet nessa modalidade permitiria acesso em tempo real às imagens, não necessitando a espera do policial ao local de descarga das imagens para depois ter acesso às mesmas.

1.2.9. No contexto da mobilidade, os serviços LEO móveis se dividem em dois modelos principais de operação:

a) **Móvel Desmontável (Transportável):** Esse modelo consiste em um kit de antena e terminal de usuário que pode ser rapidamente montado e desmontado em diferentes localidades. Ideal para operações temporárias ou missões específicas, o equipamento pode ser transportado em veículos, helicópteros ou embarcações e posicionado em campo para garantir conectividade em pontos remotos ou fora da cobertura terrestre. Após a chegada ao local, o equipamento pode ser montado em poucos minutos, possibilitando o acesso à internet de alta velocidade com baixa latência. Esse modelo é especialmente útil em situações como desastres naturais, operações de saúde pública, eventos cívicos itinerantes e bases móveis temporárias.

b) **Móvel em Movimento (On-the-Move):** Esse modelo envolve antenas específicas para operação contínua durante o deslocamento de viaturas, embarcações ou aeronaves. Utilizando tecnologia de rastreamento dinâmico e correção automática de posicionamento, esses terminais permitem a manutenção da conexão com a constelação de satélites LEO mesmo em movimento a altas velocidades, como em rodovias, patrulhamento marítimo ou áreas rurais extensas. É ideal para veículos de emergência, policiamento ostensivo, viaturas de monitoramento ambiental e qualquer outro uso que exija conectividade contínua e em tempo real sem necessidade de parada para conexão. O serviço garante qualidade de transmissão adequada para dados críticos, incluindo vídeo em tempo real, comunicação VoIP e sistemas embarcados.

1.2.10. Ambas as modalidades aumentam significativamente a capacidade operacional do Estado, permitindo que órgãos públicos atuem com maior autonomia, conectividade e segurança em regiões de difícil acesso, áreas sem infraestrutura de telecomunicações ou em operações com necessidade de mobilidade constante.

1.3. Rede IP Móvel 4G/5G (FWA)

1.3.1. O serviço de acesso à Internet via **Fixed Wireless Access (FWA)** baseia-se na utilização de redes móveis celulares (como 4G LTE ou 5G NR) para prover conectividade de banda larga fixa a um ponto determinado, por meio de equipamentos dedicados (CPEs) instalados nas instalações do contratante. Diferente do acesso móvel tradicional, o FWA oferece conexão estável, contínua e com garantias de desempenho compatíveis com aplicações corporativas, mesmo utilizando a infraestrutura de redes móveis.

1.3.2. Com a evolução das tecnologias móveis, especialmente o 5G, o FWA tornou-se uma alternativa viável e de alto desempenho à conexão fixa com fio, especialmente em localidades onde a infraestrutura de fibra óptica ou cabo metálico é inexistente, limitada ou economicamente inviável. A arquitetura do FWA utiliza equipamentos com capacidade de comunicação direta com a estação rádio-base da operadora, mantendo um canal fixo de dados com alta largura de banda, baixa latência e confiabilidade para aplicações críticas.

1.3.3. Assim, o serviço aqui descrito deve garantir a entrega de banda larga de qualidade, com parâmetros técnicos que atendam tanto às demandas de usuários

finais quanto aos requisitos técnicos e operacionais de redes corporativas e ambientes governamentais.

1.3.4. **Especificações Técnicas Mínimas**

1.3.4.1. **Tipo de Serviço**

a) Acesso fixo à Internet do tipo Fixed Wireless Access (FWA), com meio de transmissão via redes móveis 4G LTE ou 5G NR.

1.3.4.2. **Velocidade e Desempenho**

a) Velocidade mínima de download: 100 Mbps.

b) Garantia de banda mínima: 80% da velocidade contratada em 95% do tempo (média mensal).

c) Latência média: inferior a 50 ms.

d) Jitter: inferior a 20 ms.

1.3.4.3. **Meio de Acesso e Equipamentos**

a) Acesso por rede móvel com uso de CPE (Customer Premises Equipment) fornecido em regime de comodato.

b) O CPE deverá ter:

I - Suporte a MIMO 2x2 ou superior.

II - Porta Ethernet RJ-45 Gigabit.

III - Gestão remota via TR-069, SNMP ou similar.

IV - Suporte a IPv4 e IPv6.

V - Capacidade de fallback automático de 5G para 4G, caso necessário.

VI - Chip SIM (M2M ou similar) embutido ou inserido para autenticação.

2. LOTE I - REDE GOVERNO PRINCIPAL

2.1. Conceito

2.1.1. Trata-se de solução para viabilizar a interligação principal das redes locais das Secretarias e Órgãos Estaduais em todos os Municípios do Estado do Rio de Janeiro, e a Representação do Governo em Brasília, de forma a prover transmissão de dados, voz e imagem entre essas redes geograficamente dispersas, com utilização da tecnologia SD-WAN. A tecnologia permite a configuração de parâmetros de QoS (Qualidade do Serviço), priorização de tipos pré-definidos de tráfego e segurança na transferência de informações, de forma que os serviços e sistemas disponibilizados no Datacenter da Rede IP Governo, mantido e gerenciado pelo PRODERJ, (correio eletrônico, sistemas, Portal do Governo do Estado, videoconferência, dentre outros) estejam acessíveis em tempo real e integral pelas unidades regionais fixas e temporárias.

2.1.2. Os meios de acessos para conexão dos links principais, última milha, deverão ser preferencialmente através de fibra ótica, par metálico ou Wireless para as pontas remotas da rede SD-WAN e obrigatoriamente através de fibra ótica para as localidades onde se encontram os Datacenters do PRODERJ.

2.1.3. A infraestrutura de rede da CONTRATADA deverá ser capaz de suportar serviços adicionais que possam ser solicitados pela CONTRATANTE, como expansão

ou redução de banda mínima de acesso garantida, ou alteração do endereço de um novo sítio, ou mesmo adição de um novo sítio não contemplado na relação de sítios. Em todos os casos, a CONTRATADA deve manter os níveis de serviços de desempenho especificados.

2.1.4. O limite de atuação da CONTRATADA deverá ser a porta de rede local do roteador CPE.

2.1.5. A assessoria de TIC de cada Secretaria ou Órgão será responsável pelo fornecimento de cabo(s) de rede local certificado(s) no padrão RJ-45 para interligação do(s) roteador CPE com o switch(es)/firewall(s) de sua propriedade, os quais serão responsáveis pelo encaminhamento de pacotes e conexões aos ativos finais de comunicação. Os links oferecidos devem ser capazes de fornecer acesso ao ambiente público da internet, através do PRODERJ, mediante enlace seguro via SD-WAN.

2.1.6. Os links oferecidos devem ser capazes de fornecer acesso ao ambiente público da internet, através do link local do CONTRATANTE, ou através do PRODERJ no caso de circuito MPLS, mediante enlace seguro via SD-WAN..

2.1.7. Os links a serem contratados deverão respeitar o plano de endereçamento das Redes Locais atuais, permitindo o roteamento entre as redes conectadas através do backbone PRODERJ. Os detalhes de endereçamento deverão ser definidos em conjunto com CONTRATADA.

2.1.8. A tecnologia SD-WAN deve isolar logicamente o link da rede de terceiros, inclusive da internet.

2.1.9. A CONTRATADA deverá elaborar o Projeto Físico e Lógico, que deverá ser submetido a CONTRATANTE para aprovação quando da implantação dos circuitos solicitados.

2.1.10. O link para um sítio será considerado recebido provisoriamente se os testes de funcionamento e comutação com link redundante, caso exista, forem aprovados pela CONTRATANTE.

2.1.11. A CONTRATANTE será responsável pela configuração dos elementos de sua rede interna de forma que projeto aprovado possa ser implantado.

2.1.12. A contratação contempla também a instalação, configuração de equipamentos e enlaces de comunicação, e o gerenciamento proativo contra falhas e incidentes de segurança cibernética para os links de dados com segurança embarcada;

2.1.13. A tecnologia SD-WAN fornecida pela CONTRATADA deverá prover infraestrutura capaz de suportar ao menos 1 (um) link adicional de igual capacidade do Lote II para comutação para fins de contingência, no mínimo em modo ativo x passivo;

2.1.14. Nesse documento, utiliza- se o termo **sítio** como referência as unidades descentralizadas e a sede do Datacenter da Rede IP Governo, a serem contempladas na rede SD-WAN.

2.2. ESPECIFICAÇÕES TÉCNICAS DA REDE PRINCIPAL - SD-WAN

2.2.1. A Rede SD-WAN deverá permitir a criação de múltiplas redes virtuais (VRFs) ou túneis criptográficos/VPN; ;

2.2.2. O provedor que atenderá a demanda de formação da Rede IP Governo (Lote I) poderá subcontratar os meios de acesso à última milha, sem que isso

implique a transferência de responsabilidade, que será exclusiva da CONTRATADA vencedora do certame;

2.2.3. A CONTRATANTE poderá solicitar a interconexão via SD-WAN de Unidades Descentralizadas Temporárias (Containers de Eventos, Unidades Móveis, Posto de Policiamento etc.). Para estas solicitações, além dos appliances SD-WAN, a CONTRATADA deverá fornecer o acesso à internet através de tecnologias Wireless (Rádio ou 3G/4G/5G).

2.2.4. Para efeitos de dimensionamento e precificação, as solicitações de ativação de unidades temporárias serão categorizadas como Ativação de SD-WAN Unidades Descentralizadas Temporárias.

2.2.5. Os Órgãos e Secretarias de governo poderão constituir cada um sua própria VRF, contudo a interligação destas redes com o Backbone da Rede IP Governo deverá seguir as orientações e estrutura estipulada pelo PRODERJ descritas neste documento, tendo como premissas a segurança e padronização da Rede IP Governo;

2.2.6. Quando o link instalado no sítio for de internet, permitir que os sites remotos possam fazer acesso à Internet diretamente, sem a necessidade de encaminhamento deste tráfego ao Datacenters

2.2.7. Os roteadores CPE (Customer Premises Equipment) deverão ser fornecidos pela CONTRATADA de acordo com os requisitos previstos neste documento e adequados as especificações e velocidades dos circuitos a serem contratados;

2.2.8. Os CPEs das Unidades Especiais e dos Sítios (Fixos e Temporários) devem conter solução embarcada (Roteamento + SD-WAN Seguro) e deverá atender a todos os requisitos especificados no Termo de Referência e este Encarte Técnico.

2.2.9. Os CPEs Concentradores dos Datacenter da PRODERJ deverão ser distintos para realizarem as funções de Roteamento de internet da Rede IP Governo e SD-WAN Seguro.

2.2.10. A infraestrutura de rede da CONTRATADA deverá ser passível de ser redimensionada e ser capaz de suportar serviços adicionais que possam ser solicitados pelo PRODERJ, como expansão ou redução de banda mínima de acesso garantida, ou alteração do endereço de um novo sítio, ou mesmo adição de um novo sítio não contemplado na relação de sítios. Em todos os casos, a CONTRATADA deve manter os níveis de serviços de desempenho especificados;

2.2.11. O limite de atuação da CONTRATADA deverá ser a porta de rede local do roteador CPE;

2.2.12. A assessoria de TIC de cada Secretaria ou Órgão será responsável pelo fornecimento de cabo(s) de rede local certificado(s) no padrão RJ-45 para interligação do(s) roteador CPE com o switch (es) /firewall(s) de sua propriedade, os quais serão responsáveis pelo encaminhamento de pacotes e conexões aos ativos finais de comunicação;

2.2.13. A rede oferecida deve ser logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da internet;

2.2.14. A rede deverá ser flexível e escalável, permitindo acomodação instantânea do tráfego dos sítios em todo momento durante o período de vigência do contrato, permitindo a adaptação tempestiva a eventuais aumentos ou diminuição de demanda por tráfego, ou necessidade de provimento de novos serviços;

2.2.15. A Rede IP Governo de contingência (Lote 2) contratada deverá respeitar o plano de endereçamento das Redes Locais atuais, permitindo o roteamento entre as redes conectadas. Os detalhes de endereçamento deverão ser definidos em conjunto com CONTRATADA;

2.2.16. O uso da tecnologia SD-WAN deverá permitir que a rede se beneficie das vantagens da adoção desse padrão, tais como: configuração de recursos de qualidade de serviço (QoS), flexibilidade na definição de topologia lógica, simplificação de roteamento, menor custo, implantação de parâmetros de segurança da informação, entre outros;

2.2.17. Rede IP Governo a ser entregue deverá atender também aos seguintes requisitos:

a) Ser de alta qualidade, disponibilidade e atualização tecnológica;

b) Possibilitar o suporte à implantação de soluções de contingência e redundância;

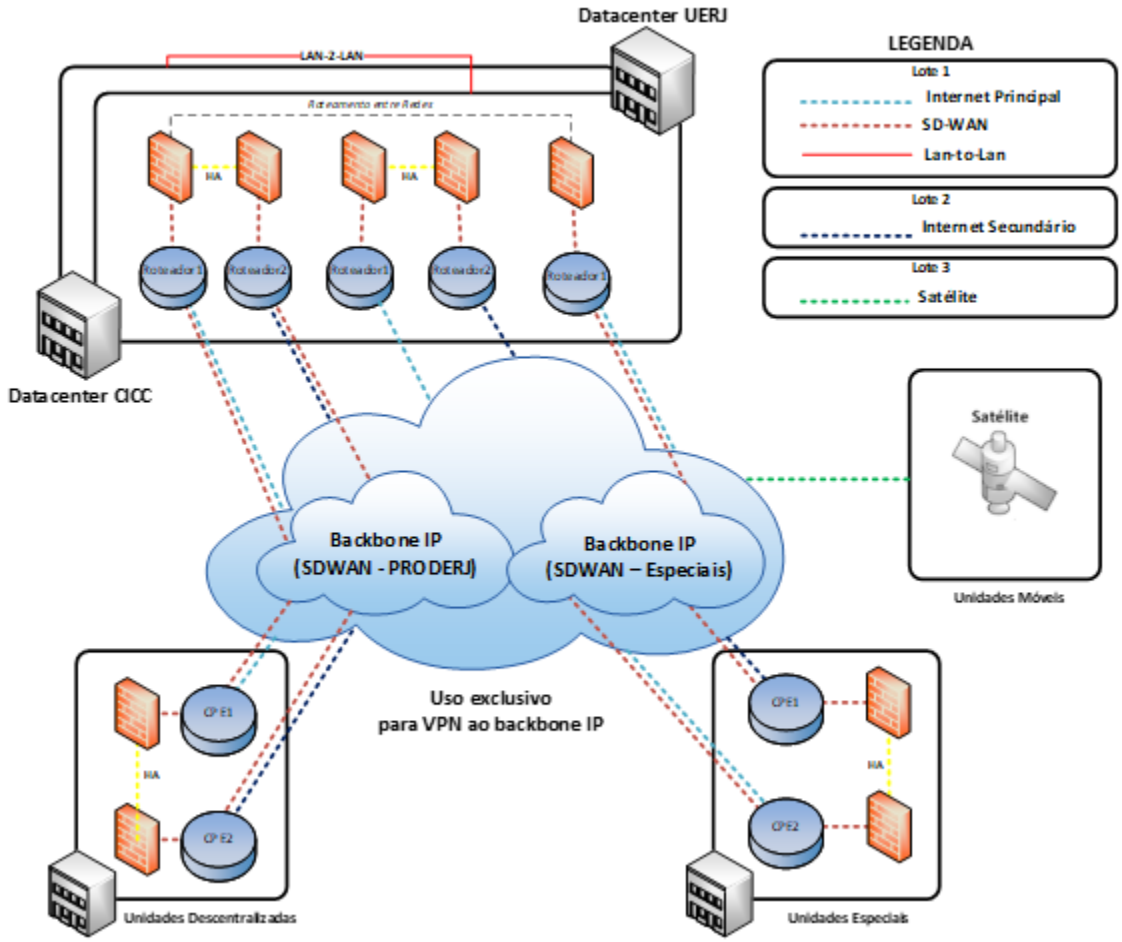
c) Suportar Qualidade de Serviço fim a fim, permitindo a priorização do tráfego de voz e videoconferência;

d) Possuir Backbone IP com de tolerância a falhas em suas conexões, com baixos tempos de convergência em caso de falha de enlaces ou equipamentos;

e) Para os links de dados com segurança, possuir solução embarcada no CPE ou em appliances próprios, desde que atendam aos requisitos do Termo de Referência e este Encarte Técnico;

f) Seguir as melhores práticas de projeto e suporte e operação de redes.

2.2.18. A solução deverá ser ofertada prevendo o atendimento de várias VRFs independentes utilizando a tecnologia SD-WAN, sendo que o Core da Rede deverá atender as condições de contingência entre sites distintos, considerando como exemplo a topologia da rede conforme figura abaixo:



2.2.19. A topologia definida será implementada sob demanda da CONTRATANTE, podendo ter suas características de velocidades, localidades e componentes físicos e lógicos alterados a qualquer tempo.

2.2.20. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 100ms.

2.3. DOS LOCAIS DE IMPLANTAÇÃO

2.3.1. Os endereços de instalação dos circuitos constantes foram levantados no momento da elaboração do Estudo Técnico, e pode haver alterações até a finalização do procedimento licitatório. Durante a implantação de cada circuito, a CONTRATADA deverá validar os endereços junto aos Órgãos e Secretarias do Governo com a anuência do PRODERJ;

2.3.2. Durante o decorrer da vigência do contrato de prestação poderá eventualmente haver mudança de endereços dos sites relacionados;

2.3.3. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios (unidades descentralizadas) e unidades especiais localizados no Estado do Rio de Janeiro e Brasília, durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão ou redução de bandas de comunicação, respeitados os limites legais e técnicos, bem como os prazos estipulados;

2.3.4. A CONTRATANTE poderá solicitar a desativação do serviço prestado de qualquer sítio ou, bem como mudança de local de prestação dos serviços ou mesmo

adição de um novo sítio não contemplado na relação de sítios indicados, sem que isso enseje qualquer tipo de ônus a mesma. A CONTRATANTE deverá comunicar essas alterações em tempo hábil antes do início da prestação do serviço;

2.3.5. Eventuais mudanças de local de prestação dos serviços poderão ser solicitadas, durante a vigência do contrato. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da mesma localidade;

2.4. PROJETO EXECUTIVO DA REDE SD-WAN

2.4.1. O Projeto Executivo deverá contemplar os seguintes itens:

a) Definição de topologias físicas e lógicas da rede;

b) Cronograma da implantação dos serviços;

c) Os Esquemas de redundância para os enlaces necessários;

d) O Plano de Roteamento;

e) Os parâmetros de qualidade de serviço;

f) Dimensionamento de enlaces e interfaces de comunicação;

g) Plano de endereçamento compatível com a atual rede corporativa do Governo do Estado do Rio de Janeiro, associando endereços IPs privados de modo a torná-los únicos dentro da nuvem SD-WAN; Cronograma de execução de obras civis de responsabilidade da CONTRATADA, caso seja necessário;

h) Definição do QoS e dos perfis de banda por Classe de Serviço.

2.5. ESPECIFICAÇÃO DOS EQUIPAMENTOS CONCENTRADORES E DA SOLUÇÃO DE SEGURANÇA DO DATACENTER DO PRODERJ, UNIDADES ESPECIAIS E SITIOS

2.5.1. Para cada Backbone, deverão ser fornecidos pela CONTRATADA, sob demanda do PRODERJ, 2 (Dois) pares de roteadores novos e de primeiro uso para serem os concentradores dos Datacenters do PRODERJ em endereços a serem definidos no momento da contratação, considerando inicialmente CICC e UERJ. Estes equipamentos formarão os perímetros interno e externo da Rede IP Governo, nas duas localidades, cada qual com seus dois pares de equipamentos..

2.5.2. Estes equipamentos serão utilizados exclusivamente para o Núcleo da Rede IP Governo, situados nos Datacenters do PRODERJ.

2.5.3. Com o objetivo de permitir o controle das conexões dos distintos Órgãos e Unidades às aplicações sitiadas no PRODERJ, a CONTRATADA deverá prover solução de Firewall/IPS ao backbone PRODERJ, que poderá ser a mesma solução que fará a função de Roteador SD-WAN, unidades especiais e dos sítios, com as especificações a seguir:

a) TIPO I: circuitos com velocidades de até 100 Mbps.

b) TIPO II: circuitos com velocidade de até 1 Gbps.

c) TIPO III: circuitos com velocidade de até 4 Gbps.

d) TIPO IV: circuitos com velocidade de até 10Gbps.

2.5.4. **CAPACIDADES DOS EQUIPAMENTOS CONCENTRADORES**

a) Throughput de, no mínimo, 35 (trinta e cinco) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, antibot e prevenção de ameaças avançadas de dia zero;

b) Suporte a, no mínimo, 30M (trinta milhões) de conexões simultâneas;

c) Suporte a, no mínimo, 750.000 (setecentos e cinquenta mil) novas conexões por segundo;

d) Throughput de, no mínimo, 75 (setenta e cinco) Gbps para conexões VPN;

e) Deve suportar a performance considerando as funcionalidades de Next-Generation Firewall de 88 (oitenta e oito) Gbps, com as funcionalidades de controle de aplicação, prevenção de intrusão e firewall habilitadas;

f) Suportar e estar licenciado para acesso remoto client-to-site ilimitado ou com a licença de maior capacidade;

g) Throughput de, no mínimo, 125 (cento e vinte e cinco) Gbps de IPS;

h) No mínimo, 08 (oito) interfaces de rede 10Gbps SFP+;

i) Deve ser fornecido e configurado com, no mínimo, (2) duas QSFP+; (40 Gb);

j) Deve ser fornecido e configurado com, no mínimo, (2) duas QSFP28; (100Gb)

k) Possuir 2 (duas) interfaces de rede dedicadas para sincronismo;

l) Possuir 2 (duas) interfaces de rede dedicadas ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

m) Possuir 1 (uma) interface do tipo console ou similar;

n) Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento. Caso o equipamento não possua essa interface física/dedicada, deverá ser composto com outro equipamento de terceiro que faça esta função, desde que não seja solução de software livre.

o) Possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes;

p) Possuir 2 (dois) discos Solid State Drive (SSD), cada um com no mínimo 960 GB de capacidade de armazenamento para o Sistema Operacional.

q) Deve suportar a inspeção de tráfego encriptado TLS, com throughput de no mínimo 10 (dez) Gbps com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, antibot e prevenção de ameaças avançadas de dia zero, medido com perfil de tráfego web, simulando aplicações comumente

utilizadas por usuários da internet.

r) Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

s) Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.

t) A solução deve suportar dual stack IPv4/IPv6 e NAT64.

u) Suportar configurar IPv6 em Dual Stack em uma interface Bond/Agregação, essa configuração também pode ser configurada em uma sub-interface de Bond/Agregação;

v) Deve suportar NAT64 e NAT46;

w) Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

x) Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras.

2.5.4.1. **CAPACIDADES DO CPE TIPO I**

a) Throughput de, no mínimo, 1.800 (mil e oitocentos) Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, antibot e prevenção de ameaças avançadas de dia zero;

b) Suporte a, no mínimo, 2M (dois milhões) de conexões simultâneas;

c) Suporte a, no mínimo, 64.000 (sessenta e quatro mil) novas conexões por segundo;

d) Throughput de, no mínimo, 3.500 (três mil e quinhentos) Mbps para conexões VPN;

e) Deve suportar a performance considerando as funcionalidades de Next-Generation Firewall de 4.500 (quatro mil e quinhentos) Mbps, com as funcionalidades de controle de aplicação, prevenção de intrusão e firewall habilitadas;

f) Suportar e estar licenciado para acesso remoto client-to-site para 500 (quinhentos) usuários;

g) Throughput de, no mínimo, 5.000 (cinco mil) Mbps de IPS;

h) No mínimo, 1 (uma) interface de rede 1 Gbps SFP base-F;

i) No mínimo, 17 (dezessete) interfaces de rede 10/100/1000 base-T;

j) No mínimo, 1 (uma) interface de rede 10 Gbps base-T;

k) No mínimo, 2 (duas) interfaces de rede 2,5 Gbps base-T;

l) Possuir 1 (uma) interface do tipo console ou similar.

2.5.4.2. **CAPACIDADES DO CPE TIPO II**

a) Throughput de, no mínimo, 2.000 (dois mil) Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, antibot e prevenção de ameaças avançadas de dia zero;

b) Suporte a, no mínimo, 2,2M (dois milhões e duzentas mil) conexões simultâneas;

c) Suporte a, no mínimo, 65.000 (sessenta e cinco mil) novas conexões por segundo;

d) Throughput de, no mínimo, 3.800 (três mil e oitocentos) Mbps para conexões VPN;

e) Deve suportar a performance considerando as funcionalidades de Next-Generation Firewall de 4.800 (quatro mil e oitocentos) Mbps, com as funcionalidades de controle de aplicação, prevenção de intrusão e firewall habilitadas;

f) Suportar e estar licenciado para acesso remoto client-to-site para 500 (quinhentos) usuários;

g) Throughput de, no mínimo, 5.300 (cinco mil e trezentos) Mbps de IPS;

h) No mínimo, 1 (uma) interface de rede 1 Gbps SFP base-F;

i) No mínimo, 17 (dezessete) interfaces de rede 10/100/1000 base-T;

j) No mínimo, 1 (uma) interface de rede 10 Gbps base-T;

k) No mínimo, 2 (duas) interfaces de rede 2,5 Gbps base-T;

l) Possuir 1 (uma) interface do tipo console ou similar.

2.5.4.3. **CAPACIDADES DO CPE TIPO III**

a) Throughput de, no mínimo, 7 (sete) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, antibot e prevenção de ameaças avançadas de dia zero;

b) Suporte a, no mínimo, 7M (sete milhões) de conexões simultâneas;

c) Suporte a, no mínimo, 190.000 (cento e noventa mil) novas conexões por segundo;

d) Throughput de, no mínimo, 21 (vinte e um) Gbps para conexões VPN;

e) Deve suportar a performance considerando as funcionalidades de Next-Generation Firewall de 20 (vinte) Gbps, com as funcionalidades de controle de aplicação, prevenção de intrusão e firewall habilitadas;

f) Suportar e estar licenciado para acesso remoto client-to-site ilimitado ou com a licença de maior capacidade;

g) Throughput de, no mínimo, 28 (vinte e oito) Gbps de IPS;

h) No mínimo, 8 (oito) interfaces de rede de 1Gbps SFP;

i) No mínimo, 2 (duas) interfaces de rede de 2,5 Gbps base-T;

j) No mínimo, 18 (dezoito) interfaces de rede 10/100/1000 base-T;

k) No mínimo, 4 (quatro) interfaces de rede de 10 Gbps SFP+;

l) Possuir 1 (uma) interface do tipo console ou similar.

2.5.4.4. **CAPACIDADES DO CPE TIPO IV**

a) Throughput de, no mínimo, 20 (vinte) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL,

antivírus, antibot e prevenção de ameaças avançadas de dia zero;

b) Suporte a, no mínimo, 25M (vinte e cinco milhões) de conexões simultâneas;

c) Suporte a, no mínimo, 530.000 (quinhentas e trinta mil) novas conexões por segundo;

d) Throughput de, no mínimo, 70 (setenta) Gbps para conexões VPN;

e) Deve suportar a performance considerando as funcionalidades de Next-Generation Firewall de 57 (cinquenta e sete) Gbps, com as funcionalidades de controle de aplicação, prevenção de intrusão e firewall habilitadas;

f) Suportar e estar licenciado para acesso remoto client-to-site ilimitado ou com a licença de maior capacidade;

g) Throughput de, no mínimo, 73 (setenta e três) Gbps de IPS;

h) No mínimo, 12 (doze) interfaces de rede de 10 Gbps base-F SFP+;

i) No mínimo, 6 (seis) interfaces de rede 10/100/1000 base-T;

j) No mínimo, 4 (quatro) interfaces de rede de 25 Gbps base-F SFP28;

k) Possuir 1 (uma) interface do tipo console ou similar;

l) Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento. Caso o equipamento não possua essa interface física/dedicada, deverá ser composto com outro equipamento de terceiro que faça esta função, desde que não seja solução de software livre.

m) Possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes;

n) Possuir 2 (dois) discos Solid State Drive (SSD), cada um com no mínimo 960 GB de capacidade de armazenamento para o Sistema Operacional.

o) Deve suportar a inspeção de tráfego encriptado TLS, com throughput de no mínimo 5,5 (cinco e meio) Gbps com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, antibot e prevenção de ameaças avançadas de dia zero, medido com perfil de tráfego web, simulando aplicações comumente utilizadas por usuários da internet.

p) Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

q) Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.

r) A solução deve suportar dual stack IPv4/IPv6 e NAT64.

s) Suportar configurar IPv6 em Dual Stack em uma interface Bond/Agregação, essa configuração também pode ser configurada em uma sub-interface de Bond/Agregação;

t) Deve suportar NAT64 e NAT46;

u) Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

v) Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras.

2.5.5. FUNCIONALIDADES COMUNS AOS CONCENTRADORES E AOS CPEs TIPOS I, II, III e IV:

2.5.5.1. FUNCIONALIDADES GERAIS

a) As capacidades de throughput e interfaces solicitadas deverão ser comprovadas através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

b) Os valores de capacidade são considerados para cada equipamento, não sendo permitida a soma dos valores dos membros do cluster;

c) Todos as medições constantes no datasheet deverão ser realizadas de modo que o tráfego seja completamente inspecionado antes de ser encaminhado, para que se privilegie a segurança frente a capacidade de encaminhamento;

d) O modo de inspeção de pacotes configurado nos concentradores, para todas as medições constantes no datasheet, deve ser de tal maneira que o payload seja montado no concentrador e seu conteúdo analisado, antes de qualquer encaminhamento de pacotes para o equipamento de destino. Dessa forma, o encaminhamento deve ser feito após análise e garantia de que não existe nenhum código malicioso no payload;

e) A medição do tráfego não deve empregar técnicas de análise parcial de pacotes IP. Isso inclui, por exemplo, a verificação apenas do cabeçalho ou apenas dos primeiros bytes.

f) A comprovação do throughput do tráfego, com a inspeção completa dos pacotes IP, deve ser realizada através de documentações públicas do fabricante.

g) As interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, as interfaces devem ser fornecidas com os transceivers/transceptores necessários para a plena utilização;

h) A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;

i) É permitido a composição da solução ofertada entre diversos fabricantes, desde que não inclua solução de software livre;

j) A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

k) Na data da proposta, nenhum dos modelos ofertados poderá constar em listas de end- of-life, end-of-support e/ou end-of-sale do fabricante;

l) Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela CONTRATADA, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

m) Os gateways de segurança, bem como a gerência centralizada,

deverão suportar monitoramento através de SNMP v2 e v3;

n) Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

o) Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

p) A solução deve consistir em appliance de proteção de rede com funcionalidades de proteção de próxima geração;

q) As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

r) O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

s) A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

t) Realizar upgrade via SCP, SFTP e https via interface WEB

u) Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

v) Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

w) Deve suportar os seguintes tipos de NAT:

x) Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

y) Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

z) Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.

aa) Enviar logs para sistemas de monitoração externos, simultaneamente;

ab) Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

ac) Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall, não sendo obrigatório para os CPEs Tipo I e II.

ad) Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2), não sendo obrigatório para os CPEs Tipo I e II;

ae) Suportar OSPF graceful restart, não sendo obrigatório para os CPEs Tipo I e II;

af) Autenticação integrada via Kerberos.

ag) Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

ah) A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

ai) A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

aj) Deve possuir mecanismo de ativação de validada da regra com período customizado;

ak) Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet.

al) Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

am) Deve permitir a configuração do tempo de checagem para cada um dos links.

an) As RFCs sinalizadas nas especificações dos equipamentos concentradores e CPEs são referências às funcionalidades solicitadas, sendo aceitas implementações do IETF mais atualizadas.

2.5.5.2. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB**

a) Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

b) Controle de políticas por usuários, grupos de usuários, IPs e redes;

c) Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

d) Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

e) Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

f) Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

g) Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

h) Reconhecer pelo menos 5.700 (cinco mil e setecentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

i) A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

j) Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

k) Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

l) Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

m) Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

n) A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 120 categorias de aplicações WEB pré-definidas pelo fabricante;

o) Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

p) Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as subcategorias do Facebook, como Facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

q) A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

r) Atualizar a base de assinaturas de aplicações automaticamente;

s) Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

t) Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

u) Deve suportar múltiplos métodos de identificação e classificação das aplicações, por, pelo menos, checagem de assinaturas, decodificação de protocolos ou análise heurística;

v) Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

w) Deve possibilitar que o controle de portas seja aplicado para todas

as aplicações;

x) A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

y) Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

z) Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

aa) Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

ab) Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

ac) Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

ad) Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

ae) Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

af) Suportar a criação de categorias de URLs customizadas;

ag) Suportar a exclusão de URLs do bloqueio, por categoria;

ah) Permitir a customização de página de bloqueio;

ai) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

aj) Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API’s ou Syslog, para a identificação de endereços IP e usuários;

ak) Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

2.5.5.3. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇA

a) Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Antimalware integrados no próprio equipamento de firewall;

b) Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

c) Deve sincronizar as assinaturas de IPS, Antivírus, Antimalware quando implementado em alta disponibilidade ativo/passivo;

d) Deve suportar granularidade nas políticas de Antivírus e Antimalware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

e) A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, baseado em threshold de CPU

f) Deverá possuir os seguintes mecanismos de inspeção de IPS:

g) Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

h) Detectar e bloquear a origem de portscans;

i) Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

j) Possuir assinaturas para bloqueio de ataques de buffer overflow;

k) Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

l) Suportar bloqueio de arquivos por tipo;

m) Identificar e bloquear comunicação com botnets;

n) Deve suportar referência cruzada com CVE;

o) Em cada proteção de segurança, deve estar incluso informações como:

p) Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

q) Severidade;

r) Tipo de ação a ser executada.

s) O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

t) O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

u) O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

v) O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

w) Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

x) O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

y) Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

z) A solução de IPS deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas em modo de detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

aa) O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

ab) A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

ac) A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

ad) Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

ae) Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

af) O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

ag) A solução de IPS deve determinar, de forma automática, se qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitando qualquer tipo de alteração na base de assinatura atual;

ah) A solução de antimalware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

ai) A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

aj) Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

ak) A solução deve permitir a criação de allowlist baseado no MD5 do arquivo;

al) Os eventos devem identificar o país de onde partiu a ameaça;

am) A funcionalidade de IPS e antibot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

an) Suportar rastreamento de vírus em arquivos pdf;

ao) Deve suportar a inspeção em arquivos comprimidos (zip, gzip, etc.);

ap) Possuir a capacidade de prevenção de ameaças não conhecidas;

aq) Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada

ar) A solução de Antivírus e Antimalware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

as) A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

at) Suportar a criação de políticas por Geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;

au) Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

av) A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorith) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

aw) A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

ax) Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

ay) A solução de Antimalware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

az) A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (Command & Control);

2.5.5.4. **FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO E SD-WAN**

I - Suportar a criação de políticas de QoS por:

a) Endereço de origem, endereço de destino e por porta;

b) O QoS deve possibilitar a definição de classes por:

c) Banda garantida, banda máxima e fila de prioridade;

d) Disponibilizar estatísticas em tempo real para classes de QoS;

e) A solução deverá oferecer orquestração centralizada de políticas e gerenciamento para SD-WAN, permitindo a configuração e o controle de políticas de rede a partir de um único ponto, garantindo desempenho otimizado, segurança aprimorada e fácil administração em toda a rede.

f) A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser

tomado para uma aplicação;

g) A solução deverá permitir a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote ou todos ao mesmo tempo

h) A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por mínimo icmp e http;

i) O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

j) Deve possibilitar a definição do link de saída para uma aplicação específica;

k) A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

l) Deve possibilitar a agregação de túneis IPSec, realizando balanceamento por conexão entre os túneis; com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Facebook etc.), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de criar políticas de controle de banda, além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em IPs de origem e destino, usuários e portas;

m) A solução de SD-WAN deve prover estatísticas em tempo real a respeito da performance do health check (perda de pacotes, jitter e latência);

n) Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

o) A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

p) Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

q) A solução deverá permitir que o orquestrador esteja na nuvem do fabricante, ou seja, instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual.

2.5.5.5. **FUNCIONALIDADES DE VPN**

a) Suportar VPN Site-to-Site e Client-To-Site;

b) Suportar IPSec VPN;

c) A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

d) Suportar SSL VPN ou IPSec;

e) A VPN IPSec deve suportar: 3DES, Autenticação MD5, SHA-1, SHA-384, AES-XCBC, Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

f) A VPN SSL deve suportar:

g) Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento;

h) As funcionalidades de VPN SSL ou IPSec devem ser atendidas com ou sem o uso de agente;

i) Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário, não sendo obrigatório para os CPEs Tipo I e II;

j) Atribuição de endereço IP nos clientes remotos de VPN;

k) Atribuição de DNS nos clientes remotos de VPN;

l) Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL ou IPSec;

m) Suportar autenticação via AD/LDAP, certificado e base de usuários local;

n) Suportar leitura e verificação de CRL (certificate revocation list);'

o) A tecnologia de VPN Client-to-Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

p) O agente de VPN SSL ou IPSec deve ser compatível com pelo menos: Windows 10 e superiores, MacOS X e superiores, distribuições GNU/Linux;

2.6. **SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY**

2.6.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

2.6.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.

2.6.3. Não será aceito soluções que dependa da estrutura de hipervisor do contratante para a análise de ameaças de dia zero, como VMWare ESXi, Microsoft Hyper-V, entre outros;

2.6.4. Prevenir, através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo de comunicação Web (HTTP e HTTPS) ou FTP, após análise completa do arquivo no ambiente sandbox, sem que este seja entregue parcialmente ao cliente.

2.6.5. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

2.6.6. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

2.6.7. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

2.6.8. O conteúdo enviado para a solução de Sandboxing deverá ser feito

automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

2.6.9. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

2.6.10. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

2.6.11. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

2.6.12. Toda análise deverá ser realizada em nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

2.6.13. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

2.6.14. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

2.6.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar ou class);

2.6.16. A solução deve suportar inspeção para o protocolo SMBv3;

2.6.17. O relatório das emulações deve conter captura de tela dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

2.6.18. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema.

2.6.19. As atualizações deverão ser providas pelo fabricante;

2.6.20. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede e endereço IP;

2.6.21. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, doc, docx, dot, docm, dotx, dotm;

2.6.22. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

2.6.23. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL’s, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

2.6.24. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

2.6.25. A solução deve possuir mecanismo de inteligência artificial para

identificar e prevenir sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

2.6.26. Caso seja identificado como um site de phishing a solução deverá bloquear o acesso do usuário ao tentar fazer o envio de suas credenciais.

2.6.27. O mecanismo de classificação antiphishing deve atuar sem a necessidade de instalação de agente na máquina do usuário;

2.6.28. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

a) Número de arquivos emulados;

b) Número de arquivos com malware.

2.6.29. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

2.6.30. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

a) O tamanho máximo do arquivo emulado seja excedido;

b) O tempo máximo de emulação seja excedido.

2.7. SOLUÇÃO DE GERENCIAMENTO DE SEGURANÇA

2.7.1. A solução de gerência deverá ser separada dos gateways de segurança, que gerenciará políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

2.7.2. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

2.7.3. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

2.7.4. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

2.7.5. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

2.7.6. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

2.7.7. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

2.7.8. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

2.7.9. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

2.7.10. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

2.7.11. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

2.7.12. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

2.7.13. Suportar backup das configurações e rollback de configuração para a última configuração salva;

2.7.14. Suportar validação de regras antes da aplicação;

2.7.15. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

2.7.16. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

2.7.17. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

2.7.18. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

2.7.19. Permitir a criação de certificados digitais para autenticação de usuários;

2.7.20. O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos gateways de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Antimalware e Sandboxing);

2.7.21. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

2.7.22. A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0;

2.7.23. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

2.7.24. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

2.7.25. A solução deverá enviar a solicitação de aprovação de políticas de segurança por, pelo menos, uma das seguintes formas, Email, Requisição WEB ou Scripts.

2.7.26. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

2.7.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

2.7.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Antimalware), e URLs que passaram pela solução;

2.7.29. Deve ser possível exportar os logs em CSV ou TXT;

2.7.30. A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

2.7.31. A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

2.7.32. A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

2.7.33. O visualizador de log deve ter um recurso de pesquisa de texto livre;

2.7.34. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

2.7.35. Possibilitar rotação do log;

2.7.36. Suportar geração de relatórios.

2.7.37. No mínimo os seguintes relatórios devem ser gerados:

a) Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Antimalware), de rede vinculadas a este tráfego;

b) Deve permitir a criação de relatórios personalizados;

c) O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6;

d) Possuir capacidade de integração com soluções de terceiros via API e suportar configurações através de RestAPI.

e) A solução deverá ser capaz de automatizar a contenção de ataques, impedindo que eles se espalhem pela rede através da execução de ações preventivas coordenadas e imediatas.

f) A solução deverá alertar automaticamente as equipes de segurança assim que uma ameaça for detectada, minimizando o tempo de resposta e permitindo ações corretivas rápidas e eficazes.

g) A solução deverá ser capaz de integrar-se com sistemas de gerenciamento de fluxo de trabalho existentes, como pelo menos os seguintes serviços, ServiceNow, Jira e Microsoft Teams, para facilitar a coordenação e o gerenciamento de respostas a incidentes.

h) A solução deverá fornecer a capacidade personalizar playbooks de automação, permitindo que as organizações ajustem as respostas automáticas.

2.7.38. O modulo de automação deverá permitir pelos menos as seguintes automações:

a) Bloquear ataques de scanners identificados pelo IPS;

b) Notificar quando um super usuário fizer login via CLI nos equipamentos;

c) Notificar quando for executar script quando;

d) Quarentenar endereços IPs;

e) Deve consolidar logs e relatórios de todos os dispositivos administrados;

f) Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

g) Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

h) Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

2.7.39. A gerência centralizada deve possuir módulo para validação de conformidade com ao menos as seguintes normas de mercado:

a) ISO 27001;

b) PCI-DSS;

c) GDPR (base da norma LGPD);

2.7.40. A solução para validação de conformidade, deve ser contemplada para o primeiro ano de projeto para adequação as novas normas de mercado que a instituição seguirá. Não sendo permitido licenciamento mensalizado “trial”, ou seja, deve ser considerado uma licença de uso anual, podendo ela ser renovada por um período maior.

2.7.41. Caso a solução não possua tal módulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas “Software Livre”.

2.7.42. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;

2.7.43. Permitir a customização do padrão regulatório da própria instituição;

2.7.44. Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

2.7.45. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;

2.7.46. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual;

2.7.47. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;

2.7.48. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

2.7.49. Possuir alertas de políticas informando as potenciais violações de conformidade;

2.7.50. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;

2.7.51. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

2.7.52. Permitir que os relatórios possam ser salvos, enviados e impressos;

2.7.53. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino etc.;

2.7.54. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

a) Visualizar quantidade de tráfego utilizado de aplicações e navegação;

b) Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

c) A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

d) A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

e) Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando, para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

f) Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

g) Criar certificados digitais para acesso dos usuários VPN;

h) Criar certificados digitais para VPNs Site-to-Site;

i) Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

j) Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

k) Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição altera.

l) A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como, por exemplo pesquisar logs de antivírus e navegação web simultaneamente na mesma query de pesquisa.

m) O relatório das emulações (sandboxing) deve conter captura de tela dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

n) A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino dos logs na mesma tela de pesquisa.

o) Possuir mecanismo para que logs antigos sejam removidos automaticamente;

p) Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

q) Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

r) Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso

de CPU;

s) A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

t) A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

u) A solução deve ser capaz de personalizar e criar regras de correlação;

v) A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

w) A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

2.8. DOS CIRCUITOS DE ACESSO DA REDE IP GOVERNO

2.8.1. CIRCUITOS DE ACESSO DO DATACENTER DO PRODERJ

2.8.1.1. Os circuitos de acessos principais do Backbone da Rede IP Governo conectados ao Datacenter do PRODERJ deverão atender aos seguintes requisitos.

a) Todos os circuitos deverão ser atendidos obrigatoriamente através de Fibra Ótica;

b) A redundância com enlaces de comunicação (Lote II) e os equipamentos SD-WAN seguros (Lote I) deverá ser implementada de forma que cada enlace do Lote II seja fisicamente conectado a um equipamento SD-WAN do Lote I, sendo obrigatória a utilização de operadoras distintas para cada enlace. Os circuitos fornecidos deverão ser capazes de assumir integralmente o tráfego em caso de falha do enlace principal.

c) Cada enlace de comunicação contratado no Lote II, tanto o principal quanto o de contingência, deverá ser entregue conectado a um equipamento PE (Provider Edge) físico pertencente a operadora distinta e integrado ao backbone da respectiva CONTRATADA, garantindo diversidade física e lógica na infraestrutura de acesso.

2.8.1.2. As CONTRATADAS deverão elaborar o Projeto Físico e Lógico de Redundância, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados.

2.8.2. CIRCUITOS DE ACESSO DAS UNIDADES ESPECIAIS

2.8.2.1. Todos os circuitos deverão ser atendidos preferencialmente por Fibra Ótica;

2.8.2.2. Na hipótese da entrega ocorrer por meio de outra tecnologia, a CONTRATANTE deverá ser previamente comunicada, cabendo a ela a responsabilidade pelo aceite do circuito;

2.8.2.3. A CONTRATADA deverá elaborar o Projeto Físico e Lógico, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados;

2.8.2.4. Casos de exceções para atendimento as Redes dos Órgãos e Unidades do Governo deverão ser tratadas com Órgãos com a anuência da Gerência de Redes e Telecomunicações do PRODERJ, durante validação do Projeto Executivo com os

envolvidos;

2.8.2.5. A solução completa deverá ser testada pela CONTRATADA periodicamente ao longo da execução do contrato.

2.8.2.6. A periodicidade deverá ser semestral e o horário da realização dos testes será definido em comum acordo com o PRODERJ que deverá ser notificado para acompanhar os testes;

2.8.2.7. A CONTRATADA deverá disponibilizar relatório com os resultados dos testes de contingência;

2.8.2.8. O PRODERJ poderá solicitar a realização extraordinária dos testes com antecedência mínima de sete dias úteis.

2.9. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA A REDE IP GOVERNO PRINCIPAL

2.9.1. Os sítios de interesse da CONTRATANTE para a Rede IP Governo são classificados conforme os seguintes tipos:

a) Sede da Rede IP Governo;

b) Unidades especiais: Palácio Guanabara e Palácio das Laranjeiras;

c) Demais unidades: Secretarias e Órgãos do Governo Estadual e outras unidades descentralizadas Fixas e Móveis.

d) Cada endereço receberá uma única classificação, e a CONTRATADA deverá ter condições de atender a possível mudança quando solicitado pelo CONTRATANTE durante a vigência contratual;

e) Uma série de indicadores deverá ser a calculada pela CONTRATADA periodicamente como condição para pagamento dos serviços. A CONTRATADA deverá disponibilizar mensalmente ao PRODERJ, relatórios digitais com o cálculo dos indicadores, totalizados e apresentados mensalmente por enlace;

f) Essas métricas servirão como limiar de qualidade do serviço, compondo o que será denominado de Níveis Mínimos de Serviço (NMS);

g) No Termo de Referência encontram-se a definição básica destes indicadores e sua fórmula de cálculo.

2.9.2. Índice Disponibilidade Mensal do Enlace (IDM)

2.9.2.1. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede WAN estará operacional em um determinado período de tempo, para cada sítio da rede corporativa do Governo do Estado do Rio de Janeiro. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês;

2.9.2.2. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente;

2.9.2.3. Para cada sítio conectado, deverá ser garantida o Índice de

Disponibilidade Mensal do Enlace (IDM) conforme os níveis a seguir:

2.9.3. **Nível IDM Sítios**

≥ 99,80%

N1 ou Core de Rede IP Governo e Unidades Especiais 1h 27m 7s / mês

≥ 99,30%

N2 ou Demais Unidades pertencentes à Região Metropolitana do Estado 5hs 4m 55s / mês

≥ 99,03%

N3 ou Demais Unidades pertencentes à Região Interior do Estado 7hs 2m 31s / mês

2.9.4. **Taxa de Erro de Bit (TxErr)**

2.9.4.1. Para Rede IP Governo a TxErr será medida da Taxa de Erro da conexão de acesso ao Backbone IP MPLS da CONTRATADA.

Nível	TxErr	Tipo de Acesso
N1	≤ 10-7	Fibra Ótica e Rádio Terrestre
N2	≤ 10-6	Par metálico e Acesso Satélite

2.9.5. **Taxa de Erro de Bit (TxErr)**

2.9.5.1. **Taxa de Perda de Pacotes (TPP)**

- Para Rede IP Governo a Taxa de Perda de Pacotes deverá ser menor ou igual a 2% para qualquer tipo de acesso.
- A perda de pacote do Backbone IP do Núcleo do Backbone IP da CONTRATADA deverá ser menor que 1%.

2.9.5.2. **Tempo de Retardo (RTT)**

- Para Rede IP Governo a Taxa o Tempo de Retardo deverá atender para os limiares abaixo conforme o tipo de acesso.

Nível	RTT	Sítios
N1	≤ 100ms	Fibra Ótica, Rádio Terrestre e Par Metálico

N2	≤ 1000ms	Acesso Satélite

2.9.6. **Tempo de Retardo (RTT)**

2.9.6.1. **Prazo de Reparo (PR)**

- Para Rede IP Governo de contingência o Prazo de Reparo deverá atender para os limiares abaixo.

Nível	PR	Sítios
N1	≤ 2 horas	Core de Rede IP Governo e Unidades Especiais
N2	≤ 5 horas	Demais Unidades pertencentes à Região Metropolitana do Estado
N3	≤ 7 horas	Demais Unidades pertencentes à Região Interior do Estado

2.9.6.2. **Prazo de Reparo (PR)**

- **Prazo de Alteração de Configuração dos Serviços (PAC)**

- Para Rede IP Governo de contingência o prazo de Alteração de Configuração dos Serviços deverá atender para os limiares conforme abaixo.

Nível	PAC	Complexidade
N1	≤ 72 horas	Baixa
N2	≤ 10 dias	Média
N3	≤ 60 dias	Alta

2.9.7. **Prazo de Alteração de Configuração dos Serviços (PAC)**

2.9.7.1. **Prazo de Alteração da Taxa de Transmissão de um Enlace (PAT)**

- Para Rede IP Governo de contingência o prazo de Alteração de Taxa de Transmissão de um Enlace.

Nível	PAT	Sítios

N1	≤ 30 dias	Core de Rede IP Governo e Unidades Especiais
N2	≤ 60 dias	Demais Unidades pertencentes à Região Metropolitana e Interior do Estado

2.9.8. **Prazo de Alteração de Transmissão (PAT)**

2.9.8.1. **Prazo de Atendimento a Novos Endereços (PAN)**

- Para Rede IP Governo de contingência o prazo de Atendimento a Novos Endereços será de 60 dias;
- As métricas apresentadas neste item servirão de base para avaliação e verificação da qualidade dos serviços prestados pela CONTRATADA.

2.10. TECNOLOGIAS ALTERNATIVAS DE ACESSO

2.10.1. Será permitida a utilização de links de tecnologias alternativas, como, por exemplo, radiofrequência, satélite, ADSL, Wireless (3G/4G/5G). Desde que sejam devidamente integrados à Rede IP Governo Principal, preservando todos os requisitos de desempenho, disponibilidade e segurança definidos no Termo de Referência e este Encarte Técnico;

2.10.2. Com exceção do atendimento às Unidades Descentralizadas Temporárias, a utilização da tecnologia 4G ou 5G será permitida exclusivamente para fins de cumprimento de prazo de instalação, sendo obrigatória a sua substituição por outra tecnologia alternativa em um prazo máximo de 90 (noventa) dias, a contar da data de ativação do circuito, considerando ainda o limite estabelecido para implantação definido no item específico;

2.10.3. Os links em tecnologias alternativas deverão ser controlados e gerenciados por tecnologia de integração tipo SD-WAN, conforme especificações constantes no Termo de Referência e Encartes Técnicos;

2.10.4. Os acessos que utilizarem tecnologias alternativas dentro da região metropolitana serão exclusivamente para circuitos fora do backbone do PRODERJ, com velocidades de no máximo 100 Mbps e somente serão instalados mediante autorização expressa da CONTRATANTE;

2.10.5. A configuração da Região Metropolitana a ser considerada pela CONTRATADA tem como base legal a Lei Complementar n° 184/2018;

2.10.6. Cabe ressaltar que, a critério da CONTRATANTE, novas localidades poderão ser conectadas à Rede de Tecnologias Alternativas, assim como solicitadas atualizações das velocidades inicialmente definidas, respeitando os requisitos do Termo de Referência e Encartes Técnicos.

2.11. ESPECIFICAÇÃO TÉCNICA DO ACESSO VIA SATÉLITE

2.11.1. O Serviço VPN através de acessos satélite tem por objetivo ser uma alternativa para atendimento de localidades, onde não existam facilidades de acesso terrestre convencionais.

2.11.2. Neste item são descritos requisitos para prestação do serviço VPN

através de acessos satélites VSAT.

2.11.3. Os satélites para acesso VSAT (Very Small Aperture Terminal) estão em órbita geoestacionária e fazem o intermédio da transmissão dos dados entre as pequenas estações terrestres remotas (terminais VSAT) e a estação de terrestre mestre ou "HUB";

2.11.4. O serviço deverá ser prestado através da tecnologia VSAT com antenas remotas parabólicas terminais entre 75 cm e 1,2m de diâmetro;

2.11.5. A CONTRATADA deverá disponibilizar:

2.11.5.1. **Características básicas do serviço a ser prestado:**

a) IP MPLS com acesso satélite, qualidade de serviço e perfil de tráfego;

b) Três perfis de tráfego: D (dados), DV (dados e voz), DVV (dados, voz e/ou vídeo);

c) Antenas de 1.2m;

d) Cobertura Nacional;

e) Operação em Banda Ku;

f) Utilização da tecnologia VSAT (TDMA) banda larga bidirecional.

2.11.5.2. **Definições:**

a) Taxa Nominal de Download: corresponde à velocidade de pico que poderá ser alcançada pelo usuário no sentido download da rede para o cliente. A velocidade de pico não é garantida e depende da carga de tráfego da rede;

b) Velocidade Típica de Download: é a taxa tipicamente garantida no sentido de download;

c) Taxa Nominal de Upload: corresponde à velocidade de pico que poderá ser alcançada pelo usuário no sentido upload do cliente para rede. A velocidade de pico não é garantida e depende da carga de tráfego da rede;

d) Velocidade Típica de Upload: é a taxa tipicamente garantida no sentido de upload.

e) O serviço ofertado pela CONTRATADA deverá atender aos seguintes Perfis de Tráfego.

f) Perfil D: 100% de tráfego de dados;

g) Perfil DV: 70% de tráfego de dados e 30% de tráfego de voz. Podendo através ser disponibilizados até 2 canais de voz;

h) Perfil DVV: 70% de tráfego de dados, 30% de tráfego de voz e/ou vídeo;

i) Neste perfil a velocidade deverá ser no mínimo de 10 Mbps, podendo ser disponibilizados até 5 canais de voz de 28Kbps ou um canal de voz e um de vídeo de 128Kbps.

j) A CONTRATADA deverá fornecer antena VSAT e receptor satélite IDU (Indoor Unit), conjuntamente com os serviços de instalação e manutenção dos acessos VSAT;

k) A CONTRATADA também deverá fornecer o roteador adequado à

prestação do serviço SD-WAN com acesso satélite;

l) Os Órgãos CONTRATANTES serão responsáveis por disponibilizar local, energia e aterramento e climatização adequada para instalação dos equipamentos, com deverá possuir sistema de para-raios em suas instalações, caso necessário para disponibilização dos serviços.

2.12. ESPECIFICAÇÃO TÉCNICA DO ACESSO VIA RADIOFREQUÊNCIA

2.12.1. O Serviço de acesso através de RADIOFREQUÊNCIA tem por objetivo ser uma alternativa para atendimento de localidades, onde não existam facilidades de acesso convencionais.

2.12.2. Neste item são descritos requisitos para prestação do serviço de acesso através de RADIOFREQUÊNCIA.

2.12.3. Os enlaces deverão ser dedicados ponto-a-ponto interligando a localidade ao backbone da CONTRATADA, e consequentemente à rede privada da Rede IP Governo;

2.12.4. Os circuitos de dados deverão ter características de transparência de protocolos de comunicação, ou seja, deverão permitir o tráfego de dados independentemente do tipo de protocolo de comunicação utilizado no âmbito da rede Rede IP Governo;

2.12.5. Os enlaces deverão operar baseados em protocolo IP e com encapsulamento Ethernet em todo o trecho;

2.12.6. Os enlaces deverão utilizar espectros de frequências administrados pela ANATEL, conforme descrição do art. 4º, inciso XXI, da Resolução ANTEL nº 259, de 19 de abril de 2001;

2.12.7. Deverão ser utilizadas faixas de frequência licenciadas junto à ANATEL de 6, 8, 11, 18, e 23 GHz, com modulação mínima de 256 QAM no que se refere aos cálculos de capacidade e performance dos radioenlaces;

2.12.8. Não serão aceitos circuitos que utilizem enlaces de rádio com espectros de frequência não administrados pela ANATEL e não licenciáveis, por exemplo, 2,4 e 5,8 GHz;

2.12.9. Utilizar rádio digital que apresente certificado ANATEL, dentro da validade, e registro como tipo de produto “Transceptor Digital”;

2.12.10. Utilizar antena que apresente certificado ANATEL, dentro da validade, e registro como tipo de produto “Antena Direcional – Categoria II”;

2.12.11. A CONTRATADA é responsável por executar todas as providências necessárias à manutenção do registro regular das radiofrequências durante a vigência do contrato;

2.13. ESPECIFICAÇÃO TÉCNICA DO ACESSO PONTO-A-PONTO (LAN-TO-LAN)

2.13.1. Considera-se um enlace ponto-a-ponto, dois circuitos distintos implantados nas duas localidades interligadas. Desta forma, admite-se a cobrança dos dois circuitos que formam o enlace ponto-a-ponto nos valores estipulados na ata de registro de preços estabelecida para a velocidade demandada.

2.13.2. O circuito ponto-a-ponto deverá ser utilizado única e exclusivamente

para conexão entre dois pontos, pois não contempla a conectividade com a Rede Governo somente por ela;

2.13.3. Os circuitos do tipo ponto-a-ponto deverão manter latência máxima de até 20ms;

2.13.4. Deverá suportar o trânsito de múltiplas VLANs (modo trunk) simultaneamente;

2.13.5. Deverá suportar agregação de portas (etherchannel, port-channel).

2.13.6. Deverá estar monitorado pelo Serviço de Gerência de Rede ofertado pela CONTRATADA.

2.14. **REQUISITOS DA TECNOLOGIA SD-WAN**

2.14.1. Entende- se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

2.14.2. A solução deve ser composta com uma console central que será responsável por fazer a configuração e upgrade de sistema operacional dos CPEs instalados nos Datacenters da CONTRATANTE e nas localidades remotas;

2.14.3. A solução deve permitir a comunicação dos Datacenters com os diversos sites remotos através dos túneis VPN;

2.14.4. A solução poderá ser instalada de maneira que ela passe a ser o Default Gateway da localidade, para que todo o tráfego que entrará ou sairá da localidade passe pela solução;

2.14.5. Deverá possuir separação total do plano de controle do plano de dados, permitindo a continuidade do funcionamento da rede mesmo que haja perda de comunicação entre os CPEs (central e remotos) e os elementos de controle da rede;

2.14.6. Deverá suportar autenticação centralizada para os elementos de rede (plano de controle, plano de dados e ferramenta de gerenciamento);

2.14.7. Permitir que os sites remotos possam fazer acesso à Internet diretamente, sem a necessidade de encaminhamento deste tráfego ao Datacenters;

2.14.8. O sistema deve ser capaz de suportar que aplicações SaaS / IaaS / PaaS possam ser encaminhados diretamente para os seus respectivos provedores de serviços (nuvem), permitindo obter latências necessárias para funcionamento adequados destes serviços;

2.14.9. Funções de Planejamento e Instalação da Solução:

a) A Solução deve permitir ao administrador informar quais são as suas redes WAN. Exemplo: MPLS1, MPLS2, Internet, Satélite, dentre outras.

b) Deverá ser possível informar qual rede local de cada site será divulgado em cada WAN;

c) Deve ser possível informar quais as Subnets e VLANs fazem parte da rede local dessa localidade;

d) Deve ser possível informar quais são os links disponíveis nessa localidade e como cada link se conecta com cada uma das WANs;

e) Caso a rede do cliente não possua o serviço de DHCP, a solução deverá permitir a configuração manual dos parâmetros mínimos para que encontre o Sistema Central;

2.14.10. Classificação de Aplicações:

a) A classificação de aplicações é um requisito fundamental dessa solução, pois várias funções solicitadas nessa especificação utilizarão as aplicações para poder tomar decisão sobre o que fazer o com tráfego;

b) Seleciona o destino do tráfego de uma aplicação forma dinâmica, com base em informações de camada 3 (rede), 4 (transporte) e 7 (aplicação);

2.14.11. Classificação de Aplicações Padrões de Mercado:

2.14.11.1. A Solução deve possuir uma base de assinatura para as aplicações padrões de mercado, e usar essas assinaturas para poder classificar o tráfego. Pelo menos as seguintes aplicações devem fazer parte da base de assinaturas:

a) Facebook, Apple FaceTime, Apple iTunes, Apple Update, Apple iCloud, Apple Filing Protocol; Apple App Store; Apple Update; Twitter, Instagram, Linkedin, Google Plus, Google Photos, Google Earth, Google Play, Google Services, Microsoft Remote Procedure Call, Microsoft Office365, Microsoft Multimedia Streaming, Salesforce, SAP, Rhapsody, Hulu, Netflix, YouTube, Spotify, RTSP, FTPS, Windows File Sharing (SMB/CIFS), SkyDrive, TFTP, Bittorrent, FTP, FTP DATA, Dropbox, Skype, Outlook Web Service, Yahoo!Mail, Yahoo Messenger , Yahoo Messenger Video, SMTP, POP3, Gmail, WhatsApp, Wikipedia, Evernote, Lotus-Notes, Lync, RTP, SIP, Citrix, Lync, GoToMeeting, WebEx, NetBIOS, Syslog, SSL, Network Time Protocol (NTP), SNMP, MySQL Protocol, PostgreSQL, Sybase, LDAP; Adobe Connect; Border Gateway Protocol (BGP); Bitcoin client; DHCP; DTLS; OSPF; Routing Information Protocol (RIP); Secure Socket Layer (SSL); Syslog; TACACS+; Telnet; TFTP; VMware vMotion; VMware vSphere; e Windows Update

2.14.12. Funções de Encaminhamento de Tráfego pela WAN:

2.14.12.1. A Solução deverá ser capaz de estabelecer túneis VPN de maneira automática sobre a rede WAN existente entre os equipamentos que fazem parte da solução;

2.14.12.2. Deverá permitir a criação de diferentes topologias de VPN, diferenciadas por aplicação, dentro de uma mesma rede;

2.14.12.3. Deve ser possível estabelecer a VPN entre os sites nas seguintes topologias:

a) Hub-and-Spoke,

b) Parcial-Mesh

c) A solução deve ser capaz de criar VPN “Hub-and-Spoke”, onde um determinado site só fechará a VPN para o site determinado pelo administrador;

2.14.12.4. A solução deve ser capaz de medir a qualidade dos túneis VPN considerando os seguintes parâmetros de qualidade:

a) Jitter;

b) Latência;

c) Perda de Pacotes;

d) A solução deve permitir ao administrador definir políticas de encaminhamento de tráfego que levem em consideração a disponibilidade da VPN, e em caso de falha do link, o tráfego deve ser desviado para outra VPN ativa;

e) A solução deve permitir ao administrador definir políticas de engenharia de tráfego que levem em consideração as métricas de Jitter, Latência e Perda de Pacotes para selecionar qual caminho uma aplicação utilizará.

2.15. REQUISITOS DA INTERLIGAÇÃO DE CONTINGÊNCIA

2.15.1. Os circuitos para interligação entre os dois Datacenters do PRODERJ, localizados na UERJ e no CICC, ou em outros locais conforme previsto no edital, deverão necessariamente ser do tipo ponto-a-ponto (layer 2);

2.15.2. Poderá ser utilizada a tecnologia L2VPN, ou similar, desde que atenda aos requisitos do Termo de Referência e este Encarte Técnico;

2.15.3. Esta interligação deverá possuir baixa latência, tipicamente abaixo de 20ms, possibilitando a implementação de sistemas de replicação de bases de dados entre os dois Datacenter e soluções de Disaster Recovery;

2.15.4. A conectividade entre os Datacenters deverá ser no mínimo na velocidade de 1Gbps e máximo de 10Gbps, através de solução de transporte PTN, Metro Ethernet ou DWDM;

2.15.5. A conectividade desta interligação deverá ser realizada com os Roteadores Concentradores do Núcleo da Rede IP Governo;

2.15.6. A CONTRATADA deverá confeccionar, quando solicitado, o projeto lógico envolvendo esta interligação, que deverá ser aprovado pelo PRODERJ antes da sua implantação;

2.15.7. O PRODERJ será responsável pela configuração dos elementos de sua rede interna de forma que projeto aprovado possa ser implantado.

2.16. CARACTERÍSTICAS BÁSICAS DO ACESSO À INTERNET

2.16.1. Em ambos os Lotes, deverá ser provisionado no backbone da Rede Governo no PRODERJ o acesso dedicado à Internet para os órgãos e secretarias da Administração Pública.

2.16.2. O objetivo principal aqui é o fornecimento do serviço de acesso à internet para a Rede IP Governo, com objetivo de centralizar a conexão com a Internet para as unidades descentralizadas abrangidas pela Rede IP Governo, bem como prover o acesso da grande rede aos serviços hospedados no PRODERJ.

2.16.3. A CONTRATADA deverá garantir o nível de disponibilidade especificado neste documento;

2.16.4. A contratação contempla a instalação e configuração dos equipamentos e enlaces de comunicação, e o gerenciamento proativo do serviço, visando à melhoria do processo de recuperação do serviço em caso de falha.

2.16.5. O acesso à INTERNET compreende o fornecimento de banda INTERNET

dedicada e exclusiva. Neste serviço consta ainda o fornecimento de endereçamento IPs públicos conforme necessidade da CONTRATANTE. A banda contratada prevê a criação de uma interface L3 exclusiva para o acesso Internet.

2.16.6. Deverá ser fornecido, no mínimo, um bloco de endereçamento IP público com 254 endereços utilizáveis (bloco /24), de forma fixa, roteável e globalmente acessível, para atender os Data Center do PRODERJ e grandes sítios, conforme necessidade;

2.16.7. Os demais sítios, devem receber, no mínimo, um bloco de endereçamento IP público com 16 endereços utilizáveis (bloco /28), de forma fixa, roteável e globalmente acessível, nos demais sítios, conforme necessidade;

2.16.8. As especificações técnicas descritas nesse documento englobam definições do projeto detalhado da rede, premissas de topologia de rede, tecnologias de acesso aplicáveis, capacidades de enlaces de comunicação, aspectos de interconexão e de roteamento, requisitos de qualidade de serviço, definições de gerência de rede e aspectos de segurança da informação;

2.16.9. A topologia a ser implantada deverá ser efetuada mediante ativação de circuito de comunicação de dados, instalação de equipamentos e prestação de serviços de instalação, configuração, suporte técnico e gerenciamento proativo de falhas, conforme especificações técnicas constantes nesse documento;

2.16.10. A CONTRATADA deverá se encarregar de prover o meio físico de interligação entre a sua rede e a Rede IP Governo, atendendo aos parâmetros definidos nesta especificação, ficando este serviço sob sua inteira responsabilidade;

2.16.11. A solução adotada pela CONTRATADA deverá atender a todas as normas técnicas exigidas pelos órgãos públicos competentes e responsáveis pela regulamentação;

2.16.12. A CONTRATADA poderá subcontratar os meios de acesso à última milha, no termos no Termo de Referência, sem que isso implique e transferência de responsabilidade, que será exclusiva da CONTRATADA vencedora do certame;

2.17. **ESPECIFICAÇÕES TÉCNICAS**

2.17.1. Cada um dos acessos e respectivos circuitos de comunicação de dados devem apresentar, no mínimo, as seguintes especificações técnicas gerais: Ter capacidade de expansão até a velocidade máxima de operação da interface utilizada, quando solicitado pela CONTRATANTE;

2.17.2. Prover conexão à Rede Corporativa da Rede IP Governo por meio de, pelo menos, uma interface do tipo Giga Ethernet Full Duplex;

2.17.3. O acesso deve ser dedicado e o serviço deverá possuir a banda garantida de acordo com a velocidade do acesso contratado;

2.17.4. O Serviço fornecido deverá suportar o protocolo IPV6, caso solicitado pela CONTRATANTE;

2.17.5. A prestação do serviço compreende a disponibilização, instalação, ativação e configuração do(s) equipamento(s) que compõem o acesso, e outros que possibilitem a utilização do serviço objeto da presente contratação;

2.17.6. A CONTRATADA deverá disponibilizar toda a infraestrutura de telecomunicações (equipamentos e insumos) necessária ao pleno funcionamento dos serviços contratados, sem custo adicional a CONTRATANTE;

2.17.7. A CONTRATADA deverá possuir Backbone IP próprio, com conexão

própria a outros Provedores de Acesso à Internet Nacionais e Internacionais;

2.17.8. O Backbone da CONTRATADA deverá possuir conexão a mais de dois AS (Autonomous System), independentes e distintos;

2.17.9. A CONTRATADA deverá possuir pelo menos um POP (ponto de presença) próprio no exterior para a troca de tráfego internacional;

2.17.10. O serviço IP dedicado deverá suportar aplicações TCP/IP (Transmission Control Protocol / Internet Protocol), tais como:

a) HTTP, HTTPS

b) FTP (File Transfer Protocol)

c) TELNET (TERminal NETwork)

d) SSH (Secure Shell)

e) SMTP (Simple Mail Transfer Protocol)

f) SMTPS (Simple Mail Transfer Protocol Secure)

g) POP3 (Post Office Protocol version 3)

h) LDAP (Lightweight Directory Access Protocol)

i) VPN, e tráfego de vídeo e voz sobre IP (VoIP), no sentido para a Internet e vice-versa.

2.17.11. O Provedor deverá dispor de recursos de gerência e supervisão para o circuito;

2.17.12. Para os Links concentradores A CONTRATADA deverá disponibilizar faixa de endereço IP válido, com no mínimo 256 (quinhentos e doze) endereços IP válidos;

2.17.13. A CONTRATADA também deverá disponibilizar quando adequadamente justificado pela CONTRATANTE faixa de endereçamento IP válidos adicionais, com o objetivo de atender as necessidades operacionais da CONTRATANTE.

2.17.14. A CONTRATADA deverá disponibilizar servidores de DNS secundário na função “recursivo”, ou seja, ao receberem uma solicitação de qualquer usuário na qual o mesmo não tenha a informação em cache ou não sendo o seu próprio domínio, ele se encarrega em buscar essa informação em outro servidor de DNS;

2.17.15. Caso os servidores de DNS da CONTRATADA sejam utilizados como secundário, a CONTRATADA deverá gerenciar a transferência dos registros de zona com o seu servidor de DNS primário da CONTRATANTE. A CONTRATADA também deverá fornecer as informações relativas à compatibilidade entre os seus servidores de DNS primários e os servidores secundários;

2.17.16. Servidor NTP (Network Time Protocol) ou acesso a servidores NTP públicos nacionais para sincronismo de horário dos servidores e ativos de rede da CONTRATANTE;

2.17.17. Os servidores de DNS da CONTRATADA deverão dar suporte à tecnologia DNSSEC (Domain Name System Security Extensions) ou DNS over SSL (Security Socket Layer);

2.17.18. Os canais de comunicação deverão ser configurados com velocidades simétricas (upstream = downstream);

2.17.19. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 100ms.

2.18. **PERSPECTIVA DE CRESCIMENTO DOS NÚMEROS DE SÍTIOS E DA ALTERAÇÃO DA BANDA DE ACESSO**

2.19. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão de bandas de comunicação, respeitados os limites legais e técnicos, bem como as condições estipuladas nos níveis de serviços;

2.20. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços ou mesmo a adição de um novo sítio, sem que isso enseje custos de qualquer natureza ao solicitante.

2.21. **SERVIÇO DE ANTI-DDOS**

2.21.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (DoS – Denial of Service) e DDOS Distributed Denial of Service);

2.21.2. A análise deverá ser passiva sem utilização de elementos probes para coleta dos dados a serem analisados;

2.21.3. A Solução deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não;

2.21.4. O ataque deve ser mitigado na estrutura da CONTRATADA, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelos Órgãos do Governo do estado do Rio continuem disponíveis aos seus usuários;

2.21.5. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

2.21.6. A solução deverá possuir interface de gerência e operação via WEB em cima de SSL, a interação entre os elementos de limpeza e detecção será feita através desta interface, assim como as configurações de limpeza, análise e os alertas de ataques;

2.21.7. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

2.21.8. Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada;

2.21.9. A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico; Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE;

2.21.10. Para a mitigação dos ataques não deverá ser encaminhado o tráfego para limpeza fora do território brasileiro;

2.21.11. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantida em operação ininterrupta durante as 24 (vinte e

quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

2.21.12. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

2.21.13. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATANTE.;

2.21.14. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP;

2.21.15. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

a) Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP.

b) Ataques a pilha TCP, incluindo mau uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.

c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

d) Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing).

2.21.16. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.

2.21.17. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole.;

2.21.18. Realizar a comunicação da ocorrência do ataque ao órgão do Governo CONTRATANTE imediatamente após a detecção;

2.21.19. Disponibilizar relatórios mensais de mitigação de ataques;

2.21.20. Disponibilizar um Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

2.21.21. A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra ataques DDOS (Distributed Denial of Service);

2.21.22. A proteção deverá operar sem exigir o desligamento de qualquer outro circuito de acesso do Órgão, independente de quantos ou quais sejam os demais fornecedores;

2.21.23. A solução ofertada não poderá afetar a visibilidade do endereço de origem das requisições, mantendo o tráfego legítimo livre de qualquer modificação; A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;

2.21.24. A CONTRATADA deverá disponibilizar acesso a sistema de monitoramento que permita a visualização do tráfego, emissão de relatórios, visualização de alertas e informações da conta associada aos serviços de proteção;

2.21.25. O serviço deve ter a capacidade de mitigar ataques no perímetro Internacional, em pelo menos dois pontos distintos e na borda Nacional;

2.21.26. Uma vez que o ataque é detectado pela solução, o equipamento instalado no backbone da operadora, responsável pela mitigação do trafego de ataque, deverá ser alertado e então todo o trafego do cliente deverá ser direcionado imediatamente, sem impactos e/ou interrupção do serviço;

2.21.27. O Serviço de Backbone (Anti-DDOS), deverá possuir o seguinte SLA (Service Level Agremment):

a) Prazo para entrega de relatórios mensais: até 5 (cinco) dias úteis.

b) Prazo para entrega de relatórios de incidente (após mitigação do ataque): até 5 (cinco) dias úteis.

c) Atendimento às solicitações em regime 24 x 7 x todos os dias do ano:

I - Prioridade 1: Requisição de adição/retirada de rede monitorada, modificação na lista de contatos autorizados do cliente, relatórios de dados do tráfego do cliente monitorado em um período especifico. Prazo máximo de 2 horas

II - Prioridade 2: Requisição da lista de redes monitoradas, alertas e mitigações, informações sobre ataques recebidos, lista de contatos autorizados pelo cliente. Prazo máximo de 8 horas.

III - SLA de Mitigação de Ocorrência de Incidentes:

a) Item Ocorrências Prazo

b) Início do Ataque

c) Detecção do Ataque

d) Tempo de Detecção Até 15 minutos

2.21.28. Contato com PRODERJ

2.21.28.1. A CONTRATADA deverá entrar em contato com o PRODERJ e solicitar autorização para dar início à mitigação do tráfego;

2.21.28.2. **Caso a CONTRATADA por qualquer razão não consiga contato com o responsável pela área de TIC do PRODERJ, esta poderá implementar as ações de mitigação do ataque que julgar necessárias, comunicando assim que possível a CONTRATANTE.**

2.22. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA OS ACESSOS À INTERNET

2.22.1. Uma série de indicadores deverá ser a calculada pela CONTRATADA periodicamente como condição para pagamento dos serviços. A CONTRATADA deverá disponibilizar mensalmente ao CONTRATANTE, relatórios digitais com o cálculo dos indicadores, totalizados e apresentados mensalmente por enlace.

2.22.2. Essas métricas servirão como limiar de qualidade do serviço, compondo o que será denominado de Níveis Mínimos de Serviço (NMS). No Termo de Referência encontram-se a definição básica destes indicadores e sua fórmula de

cálculo.

2.22.3. Classificam-se cada sítio como básico ou crítico, sendo o primeiro com atendimento 8x5 e dias comerciais, e o segundo 24x7x365;

2.22.4. Cada endereço constante no Anexo II receberá uma única classificação, e a CONTRATADA deverá ter condições de atender a possível mudança quando solicitado pelo CONTRATANTE durante a vigência contratual;

2.22.5. **Índice Disponibilidade Mensal do Enlace (IDM)**

2.22.5.1. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede WAN estará operacional em um determinado período de tempo, para cada sítio da rede corporativa do Governo do Estado do Rio de Janeiro. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês.

2.22.5.2. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

2.22.6. **Nível IDM Serviços**

1. ≥ 99,80%

    1. N1 ou Serviços de Acesso à Internet do Datacenter PRODERJ 1h 27m 7s / mês

2. ≥ 99,30%

    1. N2 ou Serviços de Acesso à Internet demais órgãos e secretarias – região metropolitana 5hs 4m 55s / mês

3. ≥ 99,03%

    1. N3 ou Serviços de Acesso à Internet demais órgãos e secretarias – região não metropolitana 7hs 2m 31s / mês

2.22.7. **Taxa de Erro de Bit (TxErr)**

2.22.7.1. Para o Serviço de Acesso à Internet a TxErr será medida da Taxa de Erro da conexão do acesso ao Backbone IP da CONTRATADA.

2.22.7.2. Nível TxErr Acessos

N1 ≤ 10-7 Conexões dos Acessos à Internet

2.22.8. **Taxa de Perda de Pacotes (TPP)**

2.22.8.1. Para o Serviço de Acesso à Internet a Taxa de Perda de Pacotes deverá se ser menor ou igual a 2%.

2.22.8.2. A perda de pacote do Backbone IP do Núcleo do Backbone IP da

CONTRATADA deverá ser menor que 1%.

2.22.9. **Tempo de Retardo (RTT)**

2.22.9.1. Para os Serviços de Acessos à Internet o Tempo de Retardo deverá atender aos limiares abaixo, considerando a medição ao primeiro elemento de roteamento do Backbone IP da CONTRATADA.

Nível	RTT	Sítios
N1	≤ 100ms	Fibra Ótica, Rádio Terrestre e Par Metálico
N2	≤ 1000ms	Acesso Satélite

2.22.10. **Tempo de Retardo**

2.22.10.1. **Prazo de Reparo (PR)**

Para os Serviços de Acesso à Internet o Prazo de Reparo deverá atender o limiar abaixo.

Nível	PR	Sítios
N1	≤ 2 horas	Core de Rede IP Governo e Unidades Especiais
N2	≤ 5 horas	Demais Unidades pertencentes à Região Metropolitana do Estado
N3	≤ 7 horas	Demais Unidades pertencentes à Região Interior do Estado

2.22.11. **Prazo de Reparo (PR)**

2.22.11.1. **Prazo de Alteração de Transmissão de um Enlace (PAT)**

Para os Serviços de Acesso à Internet o Prazo de Alteração de Transmissão de um Enlace deverá atender ao limiar abaixo

Nível	PAT	Sítios
N1	≤ 30 dias	Core de Rede IP Governo e Unidades Especiais
N2	≤ 60 dias	Demais Unidades pertencentes à Região Metropolitana e Interior do Estado

2.22.12. **Prazo de Alteração de Transmissão (PAT)**

2.22.12.1. **Prazo de Atendimento a Novos Endereços (PAN)**

- Para os Serviços de Acesso à Internet, o Atendimento a Novos Endereços deverá ser de 60 dias.
- **As métricas apresentadas nesse subitem e nos Níveis Mínimos de Serviço (NMS) deverão ser avaliadas como fins de verificação da qualidade dos serviços prestados pela CONTRATADA.**

2.23. **REQUISITOS GERAIS DOS CPE**

2.23.1. Os roteadores e equipamentos o que neste documento chamaremos de CPE (Customer Premises Equipment), de propriedade da CONTRATADA, a serem disponibilizados em cada um dos endereços deverão satisfazer os seguintes requisitos:

2.23.2. Atenderem totalmente aos recursos solicitados, apresentando total compatibilidade e interoperabilidade, evitando-se problemas futuros na Rede do Governo;

2.23.3. Serem fornecidos com todos os componentes, módulos e acessórios necessários ao seu funcionamento atendendo aos requisitos deste documento;

2.23.4. Todos os roteadores CPE do Backbone PRODERJ, unidades especiais e dos sítios especificados deverão ser dimensionados, fornecidos, instalados, configurados, mantidos, gerenciados e operados de modo a garantir o desempenho e os níveis de serviços contratados;

2.23.5. Todos os roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), devem ser dimensionados de forma que tenham capacidade de encaminhamento de pacotes IPV4/IPV6, em pacotes por segundo, compatíveis com as velocidades dos enlaces WAN conectados;

2.23.6. Deverá ser possível acessar o equipamento e aplicar configurações durante momentos em que o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;

2.23.7. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para o Governo do Estado;

2.23.8. Todas as atualizações e correções (patches) de softwares, necessárias para o cumprimento dos requisitos exigidos neste documento técnico, deverão ser monitoradas e realizadas pela CONTRATADA sem ônus adicionais para o Governo do Estado, e comunicadas previamente, quando estas exigirem reinicialização de Equipamentos;

2.23.9. A CONTRATADA deverá aplicar atualização em prazo máximo de 10 dias após formalização pelo CONTRATANTE, considerando que deverá ser feito agendamento prévio em virtude da necessidade de janela de manutenção;

2.23.10. A CONTRATADA deverá garantir todos os roteadores atualizados desde o primeiro dia da vigência contratual, procedendo com no mínimo mais quatro atualizações em intervalo de 6 meses;

2.23.11. A CONTRATADA deverá habilitar nos roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), o protocolo SNMP, disponibilizando nestes uma comunidade SNMP com acesso de leitura e permitir a solicitação de configuração de traps específicos pelo PRODERJ;

2.23.12. A configuração lógica dos roteadores CPE, para cada nível de serviço, será definida pela CONTRATADA com a aprovação do PRODERJ, e apresentada no Projeto Executivo;

2.23.13. Todos os equipamentos fornecidos pela CONTRATADA deverão suportar os protocolos IPV4 e IPV6;

2.23.14. Os roteadores fornecidos deverão contemplar todas as interfaces necessárias para o fornecimento dos circuitos por parte da CONTRATADA e com as especificações adequadas;

2.23.15. Todos os roteadores deverão possuir no mínimo uma interface LAN de 1G padrão Ethernet para a conexão da Rede Local dos endereços, sendo que devem satisfazer também as necessidades específicas em termos de desempenho e interfaces, como, por exemplo: no caso da necessidade de balanceamento de dois circuitos em um mesmo roteador;

2.23.16. Os CPEs das Unidades Especiais e dos Sítios (Fixos e Temporários) devem conter solução embarcada (Roteamento + SD-WAN Seguro) e deverá atender a todos os requisitos especificados no Termo de Referência e este Encarte Técnico.

2.23.17. Os CPEs Concentradores dos Datacenter da PRODERJ deverão ser distintos para realizarem as funções de Roteamento de internet da Rede IP Governo e SD-WAN.

2.23.18. Os circuitos de dados referentes ao **LOTE I – Rede Principal** deverão ser entregues acompanhados de CPEs com funcionalidade nativa de **SD-WAN Seguro**, integrando as capacidades de roteamento e orquestração lógica de múltiplos enlaces de comunicação, conforme definido no presente documento técnico. Esses CPEs deverão dispor de, pelo menos, uma interface física dedicada exclusivamente para conexão direta com o circuito de dados do **LOTE II – Rede de Redundância**, de forma que a gestão da comutação, balanceamento ou encaminhamento inteligente do tráfego entre os dois enlaces seja realizada integralmente pelo equipamento do LOTE I. O CPE fornecido neste lote deverá ser capaz de aplicar políticas de SD-WAN, incluindo priorização de tráfego, detecção de degradação de performance, failover automático, criptografia fim a fim e controle de qualidade de serviço (QoS), assegurando conectividade contínua e segura, conforme os níveis de serviço contratados.

2.23.19. **Os circuitos de dados do LOTE II – Rede de Contingência não deverão ser acompanhados de CPEs com função de SD-WAN. A CONTRATADA deverá entregar apenas o circuito físico, devidamente instalado, testado e ativado, com interface padronizada e compatível com os CPEs do LOTE I, que farão o gerenciamento lógico e a comutação entre os enlaces. O circuito do LOTE II será conectado diretamente ao CPE já instalado com o circuito principal do LOTE I, devendo operar como canal de contingência sob gerenciamento completo do equipamento com função de SD-WAN. Essa abordagem garante redução de complexidade operacional e compatibilidade total entre os enlaces, além de otimizar a continuidade dos serviços em caso de falha ou degradação do enlace principal.**

2.24. DOS REQUISITOS DE ROTEAMENTO

2.24.1. O Plano de Roteamento deverá ser proposto pela prestadora vencedora em seu Projeto Executivo. Serão definidas as características dos protocolos de roteamento que serão instalados em cada um dos sítios, de forma a garantir a interconexão entre eles;

2.24.2. A CONTRATADA deverá prestar os serviços de comunicação de dados, conforme os seguintes padrões: RFC 1163 (BGP - Border Gateway Protocol), RFC 2283 (Multiprotocol Extensions for BGP-4) e RFC 2547 (BGP/MPLS/VPNs);

2.24.3. As premissas para a criação do Plano de Roteamento da rede são:

a) Ser escalável;

b) Realizar agregação de rotas para endereços contíguos;

c) Manter o plano de roteamento atual das redes internas da Rede IP Governo principal;

d) Permitir o acesso de qualquer ponto da rede às aplicações compartilhadas.

2.24.4. Devido ao porte da rede corporativa, a configuração do roteamento através de rotas estáticas pode não ser muito atrativa, pois a tarefa de gerenciamento de rotas principais e alternativas, para o caso de falhas, se torna uma tarefa muito trabalhosa e suscetível a erros;

2.24.5. Ficará a cargo da CONTRATADA a definição do protocolo de roteamento a ser utilizado entre os roteadores PE e CPE. Porém, recomenda-se o uso de um protocolo com baixo tempo de convergência, como o BGP em sua última versão. Nesse sentido, a solução de roteamento deverá permitir a convergência da rede em um tempo menor que 20 (vinte) segundos para o caso de mudança topológica da rede causada por falha(s) em enlace(s) ou equipamento(s);

2.24.6. A solução de roteamento deverá ser projetada e implantada de forma escalável permitindo a evolução e o crescimento da rede.

2.25. ESPECIFICAÇÕES DE QOS DA REDE IP GOVERNO PRINCIPAL

2.25.1. A Rede IP Governo deverá suportar Qualidade de Serviço (QoS), de acordo com condições estabelecidas nesse item, inclusive considerando a arquitetura DiffServ;

2.25.2. Deverá permitir a obtenção de escalabilidade e eficácia na diferenciação dos serviços através da implementação de mecanismos de classificação e condicionamento somente nos elementos de borda da rede e aplicação “per-hop behaviors” aos agregados de tráfego que forem marcados usando se o campo DS nos campos apropriados dos cabeçalhos de pacotes MPLS;

2.25.3. No escopo da conexão de cada cliente, há a necessidade de diferenciação de serviços, incluindo a alocação de banda e priorização de pacotes para redução de atrasos de certas classes de tráfego;

2.25.4. A CONTRATADA deverá implementar e fornecer, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de, pelo menos, 5 (cinco) classes de serviços:

a) Supervisão de Rede: aplicações de monitoramento e controle da

rede, que deverão ser priorizadas acima de todas as outras a fim de garantir a disponibilidade de recursos para as intervenções preventivas ou corretivas que se façam necessárias ao seu correto funcionamento, tais como, por exemplo: Telnet, SSH, SNMP, NTP, syslog e Radius, Esta classe de serviço deverá ser utilizada exclusivamente pela empresa prestadora do serviço para o gerenciamento da Rede;

b) Tempo Real – aplicações de Voz e Vídeo sensíveis que são sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem priorização de pacotes limitadas a 50% da Banda;

c) Deverá a CONTRATADA disponibilizar duas classes de serviços distintas de Tempo Real, uma para Voz e outra para Vídeo;

d) Dados Críticos: aplicações críticas que exigem a entrega garantida e tratamento prioritário, tais como acesso HTTP e HTTPS a portais corporativos internos; Dados Prioritários: aplicações que sejam menos críticas, mas que também necessitem de tratamento prioritário na rede da CONTRATADA;

e) Melhor Esforço – Best Effort: todo tráfego não explicitamente atribuído às classes Supervisão da Rede, Tempo Real, Dados Prioritários deverá ser alocado nesta classe. Sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como tráfegos importantes; Essa classe deverá permitir o fluxo de tráfego, se houver recursos disponíveis na rede, impedindo que esse tráfego afete negativamente as demais classes;

2.25.5. As classes de serviço serão aquelas específicas de uma Rede MPLS nativo ou de uma Rede SD-WAN;

2.25.6. A definição das classes e percentuais de reserva de banda deverá discutida com a equipe técnica do PRODERJ para definição no Projeto Executivo da solução. A equipe de engenharia de tráfego da CONTRATADA deverá, sempre que possível, auxiliar acerca de tais aspectos de modo a otimizar a operação da rede. Ademais, o PRODERJ poderá solicitar a qualquer momento a modificação nas configurações das classes de serviço, de modo a adaptar à evolução de tráfego de suas aplicações.

2.26. DOS REQUISITOS DE SEGURANÇA

2.26.1. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados;

2.26.2. A CONTRATADA deverá implementar quaisquer controles de segurança (bloqueios, cancelamentos de links, etc), quando solicitado pelo CONTRATANTE, caso se identifique riscos de disponibilidade ou de cometimento de crimes através da rede corporativa;

2.26.3. A ação descrita no subitem anterior possui o intuito de prevenção de incidentes de segurança de forma a garantir níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do Governo do Estado do Rio de Janeiro, não eximindo a CONTRATADA das responsabilidades previstas no Termo de Referência e este Encarte Técnico;

2.26.4. Em relação aos aspectos técnicos de segurança da informação, a CONTRATADA deverá atender aos seguintes requisitos:

a) Prover uma rede logicamente independente e isolada de qualquer rede de terceiros, inclusive da internet.

b) O isolamento deverá ser realizado em nível lógico do MPLS e em nível 2 (do modelo OSI) para o acesso.

c) Esta garantia deverá ser implantada fim-a-fim e também se aplica às soluções de contingência;

d) Caso seja solicitado pelo PRODERJ, a CONTRATADA deverá aplicar nos roteadores CPEs fornecidos e em outros equipamentos, exclusivos para prestação de serviços, implementações de segurança tais como: autenticação do roteador CPE, controle de acesso aos dispositivos, listas de acesso e logging e outras configurações necessárias à segurança da Rede IP Governo;

e) Caso necessário deverá ser empregado esquema de autenticação no nível de protocolo de roteamento, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da Rede IP Governo;

f) Será responsabilidade da CONTRATADA, manter em seus quadros técnicos especialistas em segurança e prover serviços específicos de prevenção e reação aos incidentes de segurança em tecnologia da informação;

2.26.5. A CONTRATADA deverá configurar de maneira apropriada os elementos de rede para habilitar o registro dos eventos da Rede IP Governo de contingência, tais como conexões externas e registro de utilização de serviços (por exemplo, arquivos transferidos através de FTP e tentativas de login não autorizados). Os registros devem estar com o horário sincronizado via protocolo NTP e possuir detalhes suficientes para identificação do evento, seu autor, seu alvo/objeto e momento de ocorrência;

2.26.6. A CONTRATADA deverá possuir um sistema dedicado à coleta e ao armazenamento dos registros gerados pelos dispositivos da Rede IP Governo de contingência;

2.26.7. A CONTRATADA deverá aplicar e manter atualizados patches de segurança nos seus roteadores, incluindo os CPE dos sítios ou em outros equipamentos de suas redes, exclusivos para prestação de serviços ao Governo do Estado;

2.26.8. **A CONTRATADA deverá informar ao PRODERJ os patches de segurança necessários para a atualização dos roteadores CPEs do backbone do PRODERJ, unidades especiais e dos sítios, exclusivos para prestação de serviços a Rede do Governo.**

2.27. SERVIÇO DE SEGURANÇA GERENCIADA (MSS)

2.27.1. O Serviço de Segurança Gerenciada tem por objetivo ofertar uma camada de segurança adicional para a Rede IP Governo, devendo estar presente no Datacenter do PRODERJ com abrangência de monitoramento global da Rede IP Governo Principal e de Redundância, e de acordo com as especificações do Termo de Referência e este Encarte Técnico.

2.27.2. A solução de segurança deverá ser baseada em hardware do tipo appliance, com recursos de Next Generation Firewall (NGFW), além de console de gerenciamento e monitoração;

2.27.3. A camada de serviço fará análise, monitoramento, detecção e prevenção de ameaças e ataques no escopo do tráfego de rede, incluindo tráfegos considerados suspeitos e maliciosos, tentativas de intrusão ou ataques virtuais;

2.27.4. O monitoramento do ambiente do CONTRATANTE será contínuo e ininterrupto com objetivo de oferecer observabilidade e respostas imediatas a potenciais ameaças e ataques cibernéticos;

2.27.5. Fornecer serviço de conectividade unificada e segura, protegendo usuários, dispositivos, e ambientes corporativos, otimizando o desempenho e baixa latência;

2.27.6. Os dados gerados pela solução de segurança deverão ser exportáveis para formato compatível com as soluções de gestão mantidas pelo PRODERJ (OTRS, OCOMON, OSSIM) ou entregues sob a forma de relatórios;

2.27.7. A solução de segurança poderá fazer parte da solução de SD-WAN, desde que atenda integralmente os requisitos técnicos especificados neste encarte técnico;

2.27.8. A solução de segurança deverá ser capaz de inspecionar integramente o tráfego máximo do link de dados associado, com todas as funcionalidades de firewall, IPS e filtro de conteúdo web habilitadas;

2.27.9. Deverá ser realizado o gerenciamento da solução de Firewall para proteção dos circuitos da Rede IP Governo, administrando e configurando-o de forma a minimizar os incidentes de Segurança;

2.27.10. A monitoração deve ocorrer 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante os 365 (trezentos e sessenta e cinco) dias do ano;

2.27.11. Periodicamente sugerir alterações nas regras dos equipamentos de segurança, visando melhorar a proteção da rede, evitando o uso de equipamentos que estejam em End of Sale e End of Life;

2.27.12. Implementar novas regras nos equipamentos de segurança, em conformidade com o solicitado pela CONTRATANTE;

2.27.13. A solução ofertada pela CONTRATADA deverá contemplar:

a) A Análise e supervisão dos eventos de segurança;

b) A Detecção de alertas de segurança;

c) A Gestão e a resposta a incidentes de segurança;

d) Possibilidade de criação, alteração e manutenção de 50 (cinquenta) regras mensais na política de Segurança original. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;

2.27.14. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

2.27.15. A CONTRATANTE deverá ter acesso irrestrito os appliances da solução de segurança de forma a realizar a correta fiscalização técnica dos serviços;

2.27.16. O gerenciamento deve contemplar:

a) Criação e administração de políticas de firewall; Criação e administração de políticas de IPS/IDS;

b) Monitoração de logs.

c) Atuar pro ativamente para solucionar possíveis problemas e incidentes de segurança;

d) Os logs devem ser armazenados por um período mínimo de 12 (doze) meses;

e) A solução de segurança ofertada deverá ser capaz de gerenciar firewall (UTM ou NGFW) e IPS, com todos os recursos implementados; A solução de gerência deverá disponibilizar para Relatórios Mensais de Segurança;

f) Os alertas deverão ser direcionados para o CONTRATANTE titular de cada circuito;

2.27.17. A solução de segurança ofertada pela CONTRATADA deverá atender aos seguintes Níveis de Serviços:

Prioridade 1: Indisponibilidade de componentes críticos do serviço, criação e alteração de regras: no máximo em até 2 horas; Prioridade 2: Indisponibilidade parcial módulos ou componentes críticos do serviço: no máximo em até 8 horas;

Prioridade 3: Indisponibilidade de componentes não críticos do serviço: no máximo em até 24 horas;

Prioridade 4: Indisponibilidade parcial módulos ou componentes não críticos do Serviço: no máximo em até 4 dias (96 horas);

Prioridade 5: Requisições de logs, relatórios ou alteração de configurações e mudanças que não impactam na disponibilidade do ambiente: no máximo em até 7 dias (168 horas);

2.28. SERVIÇO DE GERÊNCIA DE REDE INTEGRADA

2.28.1. A CONTRATADA deverá disponibilizar o Serviço de Gerência Integrada da Rede IP Governo Principal e de Redundância, contemplando todos os links contratados, em conformidade com os seguintes requisitos:

2.28.2. A CONTRATADA deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, relatórios, tickets e de nível de serviço para todos os lotes contratados;

2.28.3. A CONTRATADA deverá integrar física e logicamente os serviços dos Lotes I e II de forma que se permita realizar a gestão integrada dos serviços, processos e infraestruturas disponibilizadas;

2.28.4. A Solução de Gerência da Rede não deverá demandar ao CONTRATANTE quaisquer custos de licenciamento para o seu funcionamento pleno;

2.28.5. A Solução de Gerência da Rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

2.28.6. A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma

proativa, antecipando- se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano;

2.28.7. A abertura do chamado deverá ser realizada pela equipe do Serviço de Gerência de Rede da CONTRATADA, imediatamente após a constatação de defeito ou falha em qualquer circuito ou serviço que esteja em funcionamento e seja da responsabilidade da Operadora correspondente. Após a abertura do chamado, em um prazo máximo de 20 (vinte) minutos, o atendente responsável pela abertura de chamado deverá entrar em contato com técnico do CONTRATANTE, informando as providências já tomadas e a estimativa para solução do problema;

2.28.8. A solução de Gerência da Rede da CONTRATADA deverá enviar os alertas de incidentes no mínimo via e-mail, opcionalmente via SMS de forma adicional;

2.28.9. A solução fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

2.28.10. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto, não serão aceitas soluções que possuem acessos segmentados aos módulos;

2.28.11. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

2.28.12. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc;

2.28.13. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente;

2.28.14. A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

2.28.15. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clients específicos, portanto, não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plug-ins nos desktops dos colaboradores da CONTRATANTE;

2.28.16. O acesso deverá ser via web padrão HTTP e suportar a HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português;

2.28.17. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets, portanto não serão aceitas soluções que não possuam essa compatibilidade;

2.28.18. A Solução de Gerência da Rede deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única;

2.28.19. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari;

2.28.20. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

2.28.21. A Solução de Gerência da Rede deverá fornecer, através do portal, visualização de informações on- line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos

elementos monitorados:

a) Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações;

b) Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados;

c) Consumo de banda dos enlaces (entrada e saída) separados por dia e mês;

d) Consumo de banda por classe de serviço, separados por dia e mês;

e) Ocupação de memória e CPU dos roteadores CPE;

f) Retardo dos enlaces separados por dia e mês;

g) Perda de pacotes (descarte) no sentido IN e OUT em %;

h) Taxa de pacotes com erros em erros por segundo;

i) Latência em milissegundos;

2.28.22. A Solução de Gerência da Rede deverá permitir a apresentação de indicadores que reflitam o nível de SLA (Service Level Agreement) e SLM (Service Level Management) dos serviços contratados;

2.28.23. Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:

a) Enlace: designação, tecnologia e nível de serviço;

b) Roteador CPE: fabricante e modelo e configuração física (interfaces, memória, slots, dentre outros);

c) Endereçamento lógico: endereços IPs e máscaras.

2.28.24. A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados. A Solução de Gerência da Rede deverá permitir a criação de Relatórios:

a) Permitir ser exportados conforme os principais métodos como: pdf, csv, pacote office;

b) Relatórios de desempenho sumarizados por períodos específicos;

c) Relatórios de desempenho classificados em uma visão TOP N;

d) Top Roteadores % de utilização de CPU

e) Top N Interfaces % de utilização

f) Top N Interfaces com descartes

g) Top N Interfaces com eventos de Latência

h) Relatórios de disponibilidade com períodos específicos;

i) Dashboards relacionando falhas, desempenho e disponibilidade;

j) Dashboards executivos com visão sumarizada de indicadores operacionais (Pro atividade, Taxa de Reincidência, Reparos no Prazo e Taxa de Falha).

2.28.25. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados;

2.28.26. Os dados gerados pela solução de Gerência de Rede deverão ser exportáveis para formato compatível com as soluções de gestão mantidas pelo PRODERJ (Zabbix, OTRS, OCOMON, OSSIM) ou entregues sob a forma de relatórios;

2.28.27. A Solução de Gerência da Rede deverá armazenar os dados por um período de 12 (doze) meses;

2.29. DOS REQUISITOS DE INFRAESTRUTURA

2.29.1. Os equipamentos fornecidos pela contratada deverão ser capazes de operar com a alimentação elétrica de 110V ou 220V e frequência de 60Hz;

2.29.2. A CONTRATADA será responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os Equipamentos/recursos que forem necessários (roteadores, modems, estações de gerenciamento, meios de transmissão, cabeamento WAN, acessórios necessários, dentre outros) para o provimento dos serviços.

2.29.3. Os Equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos;

2.29.4. A infraestrutura interna da rede da CONTRATADA (backbones, POPs, Equipamentos internos, dentre outros) deverá ser atendida por solução de alimentação e proteção elétrica de modo a manter todos os Equipamentos em operação por tempo indeterminado no caso de falta de energia;

2.29.5. A CONTRATADA será responsável pela interligação da rede entre o Distribuidor Geral (DG) de telefonia do prédio em cada um dos sítios e o local físico onde será instalado o roteador CPE para os acessos por rede cabeada;

2.29.6. Os circuitos deverão ser atendidos através de acessos terrestres: fibra, par metálico ou enlaces de rádio de frequência licenciada;

2.29.7. Os circuitos via Satélite serão permitidos exclusivamente para fins de atendimento de Unidades Descentralizadas Temporárias e para o cumprimento de prazo de instalação, sendo que para o último caso será obrigatória a sua substituição por outra tecnologia alternativa em um prazo máximo de 90 (noventa) dias, a contar da data de ativação do circuito, considerando ainda o limite estabelecido para implantação definido no Termo de Referência e Encartes Técnicos para os links constantes em anexo específico;

2.29.8. Os acessos que utilizarem Satélite dentro da região metropolitana serão exclusivamente para endereços fora do backbone do PRODERJ e poderão usar tecnologia VSAT com banda assimétrica;

2.29.9. Para o caso de atendimento do sítio por meio de rede não-cabeada, por exemplo, enlace de rádio frequência terrestre em frequência licenciada ou satélite, quando a implantação implique a necessidade de execução de obras civis, estas ficarão a cargo da CONTRATANTE, e deverão constar do cron ograma que faz parte do Projeto Executivo. Nestes casos, a CONTRATADA apresentará relatório de visita contendo as adequações e providências necessárias para a conclusão da instalação dos circuitos.

2.30. REQUISITOS DE IMPLANTAÇÃO DOS SERVIÇOS

2.30.1. Para cada um dos acessos contratados deverão ser prestados serviços de ativação dos circuitos de comunicação de dados, bem como instalação e configuração dos equipamentos;

2.30.2. Para cada instalação de conectividade SDWAN, deverão ser utilizados equipamentos atualizados tecnologicamente em sua última versão, não podendo estar em situação de End- of- Life ou End-of-Sale, estarem sendo suportados e recebendo atualizações de segurança do fabricante, e que atendam integralmente os requisitos técnicos estabelecidos no Termo de Referência e este Encarte Técnico, bem como realizar a substituição de qualquer componente sempre que solicitado pela CONTRATANTE, com a devida justificativa técnica;

2.30.3. Os serviços de ativação e instalação dos circuitos e equipamentos deverão ser prestados no ambiente computacional da Rede IP Governo – Unidades Especiais e Unidades Descentralizadas atendidas pela Rede IP Governo conforme os Locais de Prestação dos Serviços;

2.30.4. A CONTRATADA deverá em, no máximo, de 30 (trinta) dias corridos, contados a partir da assinatura do Contrato, apresentar Projeto Executivo contendo o Plano de Implantação dos Serviços para cada uma das localidades contratadas;

2.30.5. Os planos de implantação contidos no projeto executivo deverão ser aprovados pelo CONTRATANTE em até 15 (quinze) dias corridos após sua apresentação. Os planos de implantação deverão prever a disponibilidade do serviço de internet da Rede IP Governo, garantindo a migração sem a interrupção dos serviços existentes;

2.30.6. Após a validação dos Planos de Implantação contidos no Projeto Executivo, a CONTRATADA deverá entregar a solução totalmente operacional, com os níveis de serviços exigidos, incluindo equipamentos e circuitos de comunicação, quando se iniciará os trabalhos de atestação e conformidade;

2.30.7. A ativação dos enlaces referentes ao backbone da Rede IP Simétrica deverá ser feita numa única fase, que terá duração máxima de até 30 (trinta) dias, incluindo instalação e ativação dos circuitos, a contar da data de aprovação do Projeto Executivo;

2.30.8. Poderá ser solicitado uma dilação do prazo de entrega, para caso de aprovação do projeto de acesso juntamente com a Prefeitura do Rio de Janeiro.

2.30.9. Caso o Projeto Executivo não seja aprovado pelo CONTRATANTE, a CONTRATADA deverá corrigi-lo e reapresentá-lo em no máximo 5 (cinco) dias corridos após a comunicação da sua rejeição;

2.30.10. O início da implantação dar-se-á somente após a aprovação pelo CONTRATANTE do Projeto Executivo e dos testes realizados no ambiente de testes;

2.30.11. O atraso na entrega do Projeto Executivo poderá causar sanções à CONTRATADA conforme condições elencadas na Cláusula Das Sanções do Termo de Referência;

2.30.12. A CONTRATADA deverá apresentar durante a implantação, semanalmente, relatórios de acompanhamento das atividades, nos quais deverão constar as atividades realizadas e a duração de cada atividade;

2.30.13. A CONTRATADA deverá documentar, em forma de relatório, o estado da infraestrutura física antes e depois das instalações realizadas, inclusive com fotografias do ambiente que sofreu alterações, antes e depois das instalações

realizadas;

2.30.14. Todo o processo de instalação e implantação da solução será acompanhado e supervisionado pela Gerência de Redes e Telecomunicações da Diretoria de Infraestrutura Tecnológica do PRODERJ, à qual a licitante vencedora deverá se reportar antes de qualquer ação e decisão referente à implantação da solução em tela;

2.30.15. A não aceitação pelo CONTRATANTE das soluções adotadas, devido a não conformidade com as solicitações deste Estudo Técnico, poderá resultar em rescisão total ou parcial do contrato de prestação de serviços;

2.30.16. Os equipamentos instalados deverão vir com a última versão de firmware disponibilizada pelo fabricante, de modo a minimizar a probabilidade de atualização de versões assim que a solução estiver totalmente operacional;

2.30.17. Os trabalhos de migração e instalação de equipamentos poderão ocorrer fora do período de expediente do CONTRATANTE, a saber: de 19h às 23h, nos finais de semana e feriados de modo que o impacto seja o mínimo possível ao ambiente computacional;

2.30.18. A CONTRATADA ficará obrigada a manter sigilo sobre todas as informações referentes à solução implantada, bem como acerca das instalações da Rede IP Governo, sendo vedada qualquer divulgação destas informações sem prévia autorização, por escrito, do órgão, cabendo penalizações administrativas e sanções legais cabíveis, em caso de descumprimento;

2.30.19. Os custos externos ao ambiente da CONTRATANTE com realização de canalização, entradas, tubulações, entre outros, serão realizados pela licitante sem ônus adicional ao CONTRATANTE;

2.30.20. A passagem doa cabos para prestação dos Serviços serão de responsabilidade da CONTRATADA, sendo recomendada vistoria para verificação das condições de infraestrutura predial do Backbone da Rede IP Governo;

2.30.21. O CONTRATANTE deverá prover as condições de infraestrutura física em seu ambiente, como tubulações, energia elétrica e climatização adequada para que o serviço possa ser prestado pela CONTRATADA;

2.30.22. A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do CONTRATANTE ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da instalação e configuração da solução, na área de prestação dos serviços, mesmo que fora do exercício;

2.30.23. Os roteadores destinados ao funcionamento da Rede IP Governo, alocados em ambiente da CONTRATANTE, deverão ser acessíveis a partir de plataformas de gerenciamento SNMP, localizadas na rede interna do PRODERJ;

2.30.24. Uma vez instalados, os equipamentos deverão ser cadastrados em software de gerenciamento SNMP disponível no PRODERJ, que contará com o apoio da CONTRATADA, se necessário;

2.30.25. Os agentes SNMP instalados nos equipamentos deverão suportar mensagens nas versões v1, v2c e v3, para realização de consultas de objetos da MIB II (RFC 1213) e da host-resources-MIB (RFC 1514);

2.30.26. Após a assinatura do contrato, o PRODERJ informará à CONTRATADA os endereços IP dos seus sistemas de gerenciamento da rede (NMS) que deverão estar autorizados a realizar consultas SNMP (get) nos equipamentos da rede, receber traps SNMP e o nome da comunidade (community string) que deverá ser configurado;

2.30.27. Todos os roteadores destinados ao funcionamento da rede, alocados em ambiente da CONTRATADA, deverão ser capazes de encaminhar mensagens SYSLOG para plataformas de armazenamento de logs, localizadas na rede interna do PRODERJ;

2.30.28. Após a assinatura do contrato, o PRODERJ informará à CONTRATADA os endereços IP dos seus sistemas de armazenamento que deverão receber as mensagens syslog;

2.30.29. Deverá ser disponibilizada a geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, dos níveis de serviço contratados;

2.30.30. O serviço de gerenciamento deve atuar de forma proativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço estabelecida nos Níveis Mínimos de Serviços, realizando abertura, acompanhamento e fechamento de chamados técnicos relacionados com indisponibilidade e desempenho no serviço de Rede IP Governo, operando em regime 24 horas por dia, 7 (sete) dias por semana, para enlaces classificados como críticos, e 8x5 para enlaces classificados com básicos, durante toda a vigência do contrato;

2.30.31. A indisponibilidade dos dados de gerência (coleta não realizada, dados não acessíveis) será contabilizada como indisponibilidade do(s) serviço(s) associado(s), passível de desconto, no período em que os dados não forem coletados ou ficarem inacessíveis, caso isto implique a perda de dados de gerenciamento.

2.30.32. A CONTRATADA deverá finalizar a instalação de todos os links constantes em anexo específico contendo os endereços em até 180 dias.

2.31. PROJETO EXECUTIVO

2.31.1. O Projeto Executivo deve conter, no mínimo, as seguintes informações:

a) Projeto técnico de implantação dos serviços denominado Plano de Implantação para cada um dos enlaces contratados.

b) Procedimentos de instalação do ponto de acesso.

c) Descrição de equipamentos e circuitos de comunicação de dados.

d) Adaptações necessárias ao ambiente computacional.

e) Cronograma de implantação dos serviços.

f) Parâmetros de qualidade de serviço.

g) Descrição dos níveis de serviço acordados.

h) Topologia final de rede.

i) Processo de abertura de chamados de suporte técnico e responsáveis pelo atendimento.

2.31.2. Uma vez apresentado, o projeto executivo será submetido à aprovação da equipe técnica do CONTRATANTE, que detectará os ajustes, se necessários. A CONTRATADA deverá corrigi-lo e reapresentá-lo em no máximo 5 (cinco) dias corridos.

2.32. REQUISITOS DO SERVIÇO DE SUPORTE TÉCNICO

2.32.1. A CONTRATADA deverá disponibilizar um número único nacional não tarifado (0800) para abertura de chamados de suporte técnico, como também o Serviço de Gerência fornecido pela CONTRATADA deverá ser capaz de gerenciar os níveis de serviços acordados;

2.32.2. A assistência técnica on-site deverá ser prestada nas instalações do CONTRATANTE, sítios e unidades especiais conforme os prazos estipulados nos Níveis Mínimos de Serviço (NMS);

2.32.3. No momento de abertura do chamado deverá ser fornecido ao CONTRATANTE um número único de identificação do chamado;

2.32.4. Os chamados somente poderão ser abertos e fechados após autorização do CONTRATANTE;

2.32.5. Os serviços de suporte técnico deverão incluir serviços de atualização dos Equipamentos componentes da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de software de Equipamentos;

2.32.6. A CONTRATADA deverá disponibilizar, ainda, um número de telefone ao CONTRATANTE para contato com a área de 2º nível para solução de problemas urgentes que necessitem a atuação imediata, tais como: reinício de interfaces de roteadores, conferência de aplicação de políticas nos roteadores, lista de acesso, ativação de modo debug de forma temporário para diagnóstico, verificação de logs, configuração de velocidade e modo de operação de interfaces, elaboração de listas de acesso temporárias e reinício de equipamentos;

2.32.7. O CONTRATANTE reserva-se o direito de promover, a qualquer tempo, alterações nas políticas de utilização do serviço de acesso à Internet, ficando a CONTRATADA, neste caso, será obrigada a prestar o suporte técnico necessário à implementação dessas diretrizes nos equipamentos por ela empregados na prestação os serviços, inclusive nos roteadores locados, sem prejuízo das condições de funcionamento previstas no edital;

2.32.8. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo CONTRATANTE;

2.32.9. Em caso de reiterado inadimplemento do SLA, o CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato;

2.32.10. Durante a vigência do contrato, a CONTRATADA deverá manter preposto aceito pela Administração do CONTRATANTE para representá-la administrativamente sempre que houver necessidade.

2.33. REQUISITOS PARA ACEITAÇÃO DOS SERVIÇOS

2.33.1. A implantação da Rede IP Governo Principal, dar-se-á por implantação de enlaces em cada sítio. Os sítios e enlaces a serem contratados serão definidos durante a assinatura do contrato;

2.33.2. Os serviços de implantação de cada enlace serão verificados individualmente, e estarão sujeitos a dois tipos de aceitação: denominados: Termo de Aceitação Provisória e Termo de Aceitação Definitiva.

2.33.3. **Critérios para Aceitação Provisória dos serviços de implantação**

2.33.4. A aceitação da implantação do enlace deverá atender os seguintes requisitos:

a) A Aceitação Provisória dar-se-á em até 30 (trinta) dias úteis após a entrega do serviço do sítio, com a observação do CONTRATANTE, de normalidade no provimento dos serviços para este enlace;

b) Para os sítios que fizerem parte do ambiente de teste, o prazo para a aceitação provisória contará a partir da data do início dos testes;

c) Caso haja rejeição na aceitação do serviço do sítio, o CONTRATANTE poderá solicitar a suspensão da implantação até que possíveis problemas sejam sanados, sem que isso gere direito à CONTRATADA de protelar a implantação dos demais sítios dentro dos prazos definidos;

d) Os testes de aceitação provisória dos serviços de rede serão compostos, no mínimo, por testes de conectividade/funcionais e testes de contingência; A aceitação ocorrerá caso os resultados dos testes estejam conforme os requisitos do projeto;

e) Um enlace da rede será considerado aceito nos testes de conectividade/funcionais, se:

f) O tempo de retardo da conexão e o desempenho do roteador CPE estiverem dentro dos limites estabelecidos no Nível Mínimo de Serviços (NMS) por um período de 2 (dois) dias úteis;

g) A taxa de erro de bit estiver dentro dos limites estabelecidos no mesmo no Nível Mínimo de Serviços (NMS), quando solicitado pelo CONTRATANTE;

h) A transação padrão de um sistema corporativo definido pelo CONTRATANTE puder ser completada com sucesso, dentro das características da aplicação;

i) Os Equipamentos CPEs puderem ser visualizados, consultados e terem seus dados de monitoramento coletados por ferramentas apropriadas do CONTRATANTE;

j) A solução de contingência para um sítio será considerada recebida provisoriamente se os testes de funcionamento e comutação forem aprovados pelo CONTRATANTE;

k) Após a execução dos testes, e verificado que o enlace implantado atende os requisitos conforme descrito nos itens anteriores, a Comissão de Recebimento do CONTRATANTE emitirá o Termo de Recebimento Provisório (TRP) do enlace contratado.

2.33.5. **Critérios para Aceitação Definitiva dos serviços de implantação**

a) A aceitação final se dará após o término do Período de Funcionamento Experimental (PFE), que se inicia com a emissão do TRP e se encerra após o decurso de um período completo de 10 (dez) dias corridos sem nenhuma ocorrência de erros no enlace contratado. A este período sem ocorrência de falhas, denominaremos “Período no-failures”;

b) Período no-failures: quando todas as pendências forem retiradas, será marcado o início de um período que se estenderá por 10 (dez)

dias, no qual a solução não deverá apresentar falhas de projeto/especificação. Este período será reiniciado sucessivamente todas as vezes que for detectada alguma falha, adiando assim a conclusão do PFE;

c) Ao final do PFE, concluído com sucesso, será emitido o Termo de Recebimento Definitivo (TRD), pela Comissão de Recebimento do CONTRATANTE, autorizando, a partir de então o recebimento das faturas de serviço relativas a esse enlace;

d) **A emissão do TRD não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas, estendendo-se a necessidade de teste destas facilidades ao longo do período de garantia.**

2.34. REQUISITOS DE GERENCIAMENTO DOS SERVIÇOS

2.34.1. Mensalmente, a CONTRATADA deverá encaminhar ao CONTRATANTE relatório com todos os chamados de suporte técnicos abertos / fechados, com a identificação do chamado, data e hora de abertura, nome da pessoa que abriu e do técnico alocado, bem como as atividades executadas, data e hora de fechamento do chamado e resolução aplicada;

2.34.2. O relatório deverá ser enviado juntamente com a fatura de prestação dos serviços e deverá apresentar informações acerca da aferição dos níveis de serviço contratados, como descrição dos períodos de indisponibilidade, para cada um dos acessos contratados;

2.34.3. Os relatórios deverão ser detalhados dia, período e causas de eventuais indisponibilidades de serviço ocorridas, bem como o somatório total de minutos de todas as ocorrências e o cálculo do Índice de Disponibilidade Mensal (D) correspondente ao período de faturamento;

2.34.4. A entrega dos relatórios mensais é condição necessária à atestação dos serviços, pelo CONTRATANTE, para fins de pagamento;

2.34.5. Caso o Índice de Disponibilidade Mensal, seja inferior ao especificado neste Termo de Referência, a CONTRATADA deverá encaminhar relatório com o cálculo do total de desconto a ser aplicado no valor da fatura, de acordo com a seguinte fórmula:

VD = CM * [(100 - D) / 100],

Onde:

VD é o valor do desconto;

CM é o custo mensal dos serviços prestados;

D é o índice de disponibilidade mensal dos serviços, calculado pelas fórmulas especificadas nos Níveis Mínimos de Serviço (NMS)

2.34.6. O CONTRATANTE reserva-se o direito de promover, a qualquer tempo, alterações nas políticas de utilização da Rede IP Governo, ficando a CONTRATADA,

neste caso, obrigada a prestar o suporte técnico necessário à implementação dessas diretrizes nos equipamentos por ela empregados na prestação os serviços, inclusive nos roteadores locados, sem prejuízo das condições de funcionamento previstas no edital;

2.34.7. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo PRODERJ;

2.34.8. Em caso de reiterado inadimplemento do SLA, o CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato;

2.34.9. Durante a vigência do contrato, a CONTRATADA deverá manter preposto aceito pela Administração do CONTRATANTE para representá-la administrativamente sempre que houver necessidade.

2.35. MODELO DE PRESTAÇÃO DOS SERVIÇOS

2.35.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

2.35.2. O modelo de prestação de serviços conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo CONTRATANTE, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas pró-ativamente pela CONTRATADA, por meio do serviço de gerência da rede. A prestação dos serviços englobará prazos e condições da entrega da solução, incluindo requisitos de implantação e migração da solução.

2.35.3. Os níveis mínimos de serviço contratados, apresentados nos Níveis Mínimos de Serviços (NMS) serão registrados e monitorados pela CONTRATADA e o CONTRATANTE, e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade. Essa condição será fundamento para efetuar os pagamentos previstos, durante toda a vigência do contrato.

2.35.4. Os pagamentos serão efetuados, mensalmente, em moeda corrente nacional e em até 15 (quinze) dias úteis após apresentação das notas fiscais. Os critérios detalhados para o pagamento mensal estão definidos no Termo de Referência.

3. LOTE II - REDE GOVERNO REDUNDANTE

3.1. Conceito

3.1.1. Trata-se de solução para viabilizar a **interligação redundante** das redes locais das Secretarias e Órgãos Estaduais em todos os Municípios do Estado do Rio de Janeiro, bem como a Representação do Governo em Brasília, com a finalidade de assegurar a continuidade dos serviços de transmissão de dados, voz e imagem entre essas redes geograficamente dispersas. A conectividade será estabelecida por meio de enlaces dedicados, permitindo a comunicação com o

Datacenter da Rede IP Governo, mantido e gerenciado pelo PRODERJ, onde estão hospedados os serviços institucionais (correio eletrônico, sistemas, Portal do Governo do Estado, videoconferência, dentre outros), garantindo sua acessibilidade em tempo integral pelas unidades regionais fixas e temporárias, mesmo em cenários de falha na conexão principal.

3.1.2. Os meios de acesso para os enlaces redundantes, na última milha, deverão ser preferencialmente por fibra ótica, podendo ser utilizados outros meios, como par metálico ou soluções Wireless, quando justificado tecnicamente. Para as localidades onde se encontram os Datacenters do PRODERJ, o acesso deverá ser obrigatoriamente por fibra ótica.

3.1.3. A infraestrutura de rede da CONTRATADA deverá ser capaz de suportar ampliações ou alterações nos serviços contratados, como aumento ou redução da largura de banda garantida, mudanças de endereço ou inclusão de novos sítios, devendo, em todos os casos, manter os níveis de desempenho pactuados.

3.1.4. O limite de atuação da CONTRATADA será a porta de rede local do roteador CPE fornecido.

3.1.5. Os links oferecidos devem ser capazes de fornecer acesso ao ambiente público da internet, através do link local do CONTRATANTE, ou através do PRODERJ no caso de circuito MPLS, mediante enlace seguro via SD-WAN. Os enlaces contratados devem permitir, durante a vigência do contrato, adaptações ágeis a mudanças de demanda por tráfego ou à necessidade de disponibilização de novos serviços.

3.1.6. A assessoria de TIC de cada Secretaria ou Órgão será responsável pelo fornecimento de cabo(s) de rede local certificado(s) no padrão RJ-45 para interligação do(s) roteador(es) CPE com o(s) switch(es)/firewall(s) de sua propriedade, que deverão encaminhar os pacotes e conexões aos ativos finais de rede.

3.1.7. Os links fornecidos deverão possibilitar acesso ao ambiente público da internet, por meio da infraestrutura do PRODERJ, utilizando conexões seguras baseadas em mecanismos tradicionais de roteamento e filtragem de tráfego.

3.1.8. Os enlaces contratados devem permitir, durante a vigência do contrato, adaptações ágeis a mudanças de demanda por tráfego ou à necessidade de disponibilização de novos serviços.

3.1.9. Os enlaces deverão respeitar o plano de endereçamento das redes locais atualmente em operação, permitindo o roteamento entre os diversos sítios conectados via backbone do PRODERJ, conforme diretrizes técnicas a serem definidas conjuntamente entre as partes.

3.1.10. O tráfego deverá ser logicamente isolado de redes de terceiros, inclusive da internet, por meio de configurações no roteamento e nos dispositivos de segurança sob responsabilidade do PRODERJ.

3.1.11. A CONTRATADA deverá elaborar Projeto Físico e Lógico da solução, o qual deverá ser submetido à aprovação da CONTRATANTE previamente à implantação dos enlaces.

3.1.12. O link redundante será considerado aceito provisoriamente mediante aprovação nos testes de funcionamento e de comutação com o link principal, quando aplicável.

3.1.13. A configuração dos elementos internos da rede da CONTRATANTE será de responsabilidade desta, devendo seguir os parâmetros definidos no projeto aprovado.

3.1.14. A contratação inclui a instalação e configuração dos equipamentos necessários, bem como dos enlaces de comunicação, ficando o gerenciamento proativo contra falhas e incidentes de segurança cibernética a cargo da operadora da Rede IP Governo Principal.

3.1.15. Neste documento, utiliza-se o termo *sítio* para designar as unidades descentralizadas e a sede do Datacenter da Rede IP Governo contempladas na rede de comunicação redundante.

3.2. ESPECIFICAÇÕES TÉCNICAS DA REDE GOVERNO REDUNDANTE

3.2.1. A Rede de contingência (Lote II) será composta exclusivamente por enlaces de comunicação de dados, sem fornecimento de roteadores ou CPEs, sendo os circuitos fisicamente conectados aos equipamentos instalados no âmbito do Lote I, que realizará as funções de roteamento, segurança e controle de tráfego.

3.2.2. O provedor responsável pela entrega dos enlaces de comunicação do Lote II poderá subcontratar os meios de acesso à última milha, desde que mantenha a responsabilidade integral sobre o cumprimento de todos os requisitos técnicos e operacionais previstos neste documento.

3.2.3. A CONTRATANTE poderá solicitar a ativação de enlaces temporários para atendimento a Unidades Descentralizadas Temporárias (como containers de eventos, unidades móveis, postos de policiamento etc.). Para estas solicitações, a CONTRATADA deverá prover o enlace de comunicação até o ponto de interligação com o equipamento do Lote I, bem como o acesso à internet por meio de tecnologias Wireless ou Satélite, quando necessário.

3.2.4. Para fins de planejamento e precificação, essas ativações temporárias serão tratadas como Enlaces de Comunicação para Unidades Descentralizadas Temporárias.

3.2.5. A segmentação lógica das redes continuará sob responsabilidade do PRODERJ, utilizando os recursos dos equipamentos do Lote I. A entrega dos enlaces do Lote II deverá atender ao plano de endereçamento definido pela CONTRATANTE e ser compatível com a integração à estrutura lógica vigente.

3.2.6. Os meios de acesso à última milha para os enlaces do Lote II deverão ser preferencialmente por fibra ótica, sendo também admitidas soluções por par metálico, satélites ou tecnologias wireless, desde que observados os critérios de desempenho exigidos.

3.2.7. Não haverá fornecimento de equipamentos de borda (roteadores/CPEs) no Lote II. Os enlaces contratados deverão ser entregues com terminação física compatível para conexão direta aos equipamentos fornecidos no Lote I.

3.2.8. Os equipamentos de rede e segurança embarcados necessários à operação serão de responsabilidade do Lote I. Os enlaces do Lote II terão função exclusivamente de transporte de dados até os pontos de interconexão definidos pela CONTRATANTE.

3.2.9. Nos Datacenters do PRODERJ, os enlaces do Lote II deverão ser entregues em pontos de conexão compatíveis com os equipamentos concentradores já existentes, respeitando a separação lógica entre as funções de roteamento e os serviços públicos de internet.

3.2.10. A infraestrutura do Lote II deverá ser flexível e escalável, permitindo modificações futuras, como alteração de endereço, aumento ou redução de banda, ou inclusão de novos pontos de acesso, mantendo os níveis mínimos de desempenho acordados.

3.2.11. O ponto de entrega dos enlaces do Lote II será a interface física de rede

indicada pela CONTRATANTE nos equipamentos do Lote I. Não haverá responsabilidade da CONTRATADA quanto à configuração ou operação desses equipamentos.

3.2.12. A infraestrutura interna de rede local nas Secretarias e Órgãos permanecerá sob responsabilidade da própria unidade, incluindo cabeamento e integração com os ativos de rede existentes.

3.2.13. A rede de enlaces do Lote II deverá ser logicamente e fisicamente independente de outras redes da CONTRATADA, incluindo a internet pública, e compatível com os requisitos de segurança da informação definidos pela CONTRATANTE.

3.2.14. Os enlaces do Lote II deverão respeitar o plano de endereçamento da Rede IP Governo vigente, possibilitando o roteamento entre os sítios conectados por meio da infraestrutura e dos equipamentos do Lote I, conforme diretrizes do PRODERJ.

3.2.15. A Rede de contingência a ser entregue no Lote II deverá atender aos seguintes requisitos:

3.2.16. Ter alta qualidade, disponibilidade e compatibilidade tecnológica com a estrutura da Rede IP Governo;

3.2.17. Viabilizar a implementação de estratégias de contingência e redundância conforme diretrizes da CONTRATANTE;

3.2.18. Suportar recursos de Qualidade de Serviço fim a fim (QoS), priorizando tráfego sensível (voz, vídeo) conforme definição no Lote I; a rede de transporte deve ter tolerância a falhas e rápida recuperação;

3.2.19. Garantir transporte seguro de dados, sendo a criptografia e demais mecanismos de proteção tratados nos equipamentos do Lote I; a rede deverá seguir as melhores práticas de projeto e operação de redes.

3.2.20. A topologia da rede de enlaces do Lote II será definida conforme demanda da CONTRATANTE, podendo sofrer alterações em seus parâmetros físicos e lógicos (velocidades, localidades, meios de acesso) durante a vigência contratual.

3.2.21. A latência máxima entre o ponto de acesso do enlace e o backbone da CONTRATADA não deverá exceder 100 ms

3.3. DOS LOCAIS DE IMPLANTAÇÃO DA REDE GOVERNO REDUNDANTE

3.3.1. Os endereços de instalação dos circuitos constantes foram levantados no momento da elaboração do Estudo Técnico, e pode haver alterações até a finalização do procedimento licitatório. Durante a implantação de cada circuito, a CONTRATADA deverá validar os endereços junto aos Órgãos e Secretarias do Governo com a anuência do PRODERJ;

3.3.2. Durante o decorrer da vigência do contrato de prestação poderá eventualmente haver mudança de endereços dos sites relacionados;

3.3.3. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios (unidades descentralizadas) e unidades especiais localizados no Estado do Rio de Janeiro e Brasília, durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão ou redução de bandas de comunicação, respeitados os limites legais e técnicos, bem como os prazos estipulados;

3.3.4. A CONTRATANTE poderá solicitar a desativação do serviço prestado de

qualquer sítio ou, bem como mudança de local de prestação dos serviços ou mesmo adição de um novo sítio não contemplado na relação de sítios indicados, sem que isso enseje qualquer tipo de ônus a mesma. A CONTRATANTE deverá comunicar essas alterações em tempo hábil antes do início da prestação do serviço;

3.3.5. Eventuais mudanças de local de prestação dos serviços poderão ser solicitadas, durante a vigência do contrato. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da mesma localidade;

3.4. PROJETO EXECUTIVO DA REDE REDUNDANTE

3.4.1. O Projeto Executivo deverá contemplar os seguintes itens:

a) Definição de topologias físicas e lógicas da rede;

b) Cronograma da implantação dos serviços;

c) Adequações ao Plano de Roteamento da Rede Governo Principal;

d) Os parâmetros de qualidade de serviço;

e) Dimensionamento de enlaces e interfaces de comunicação;

f) Plano de endereçamento compatível com a atual rede principal, associando endereços IPs privados de modo a torná-los únicos dentro da nuvem;

g) Cronograma de execução de obras civis de responsabilidade da CONTRATADA, caso seja necessário;

h) Definição do QoS e dos perfis de banda por Classe de Serviço.

3.5. ESPECIFICAÇÃO DOS LINKS CONCENTRADORES REDUNDANTES DO DATACENTER DO PRODERJ

3.5.1. Para cada Backbone, deverão ser fornecidos pela CONTRATADA, sob demanda do PRODERJ, dois links de acesso para serem os concentradores de tráfego nos Datacenters do PRODERJ em endereços a serem definidos no momento da contratação, considerando inicialmente CICC e UERJ. Estes links formarão os perímetros interno e externo da Rede IP Governo Redundante, nas duas localidades, cada qual com seus dois pares de links.

3.5.2. Estes links serão utilizados exclusivamente para o Núcleo da Rede IP Governo, situados nos Datacenters do PRODERJ.

3.6. DOS CIRCUITOS DE ACESSO DA REDE IP GOVERNO

3.7. CIRCUITOS DE ACESSO DO DATACENTER DO PRODERJ

3.7.1. Os circuitos de acessos principais do Backbone da Rede IP Governo conectados ao Datacenter do PRODERJ deverão atender aos seguintes requisitos.

3.7.2. Todos os circuitos deverão ser atendidos obrigatoriamente através de Fibra Ótica;

3.7.3. A CONTRATADA deverá elaborar o Projeto Físico e Lógico de

Redundância, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados.

3.8. CIRCUITOS DE ACESSO DAS UNIDADES ESPECIAIS

3.8.1. Todos os circuitos deverão ser atendidos preferencialmente por Fibra Ótica;

3.8.2. O circuito ponto-a-ponto deverá ser utilizado único e exclusivamente para conexão entre dois pontos, pois não contempla a conectividade com a Rede Governo somente por ela;

3.8.3. Na hipótese da entrega ocorrer por meio de outra tecnologia, a CONTRATANTE deverá ser previamente comunicada, cabendo a ela a responsabilidade pelo aceite do circuito;

3.8.4. A CONTRATADA deverá elaborar o Projeto Físico e Lógico, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados;

3.8.5. Casos de exceções para atendimento as Redes dos Órgãos e Unidades do Governo deverão ser tratadas com Órgãos com a anuência da Gerência de Redes e Telecomunicações do PRODERJ, durante validação do Projeto Executivo com os envolvidos;

3.8.6. A solução completa deverá ser testada pela CONTRATADA periodicamente ao longo da execução do contrato.

3.8.7. A periodicidade deverá ser semestral e o horário da realização dos testes será definido em comum acordo com o PRODERJ que deverá ser notificado para acompanhar os testes;

3.8.8. A CONTRATADA deverá disponibilizar relatório com os resultados dos testes de redundância;

3.8.9. O PRODERJ poderá solicitar a realização extraordinária dos testes com antecedência mínima de sete dias úteis.

3.9. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA A REDE IP GOVERNO REDUNDANTE

3.9.1. Os sítios de interesse da CONTRATANTE para a Rede IP Governo Redundante são classificados conforme os seguintes tipos:

a) Sede da Rede IP Governo;

b) Unidades especiais: Palácio Guanabara e Palácio das Laranjeiras;

c) Demais unidades: Secretarias e Órgãos do Governo Estadual e outras unidades descentralizadas Fixas e Móveis.

3.9.2. Cada endereço receberá uma única classificação, e a CONTRATADA deverá ter condições de atender a possível mudança quando solicitado pelo CONTRATANTE durante a vigência contratual;

3.9.3. Uma série de indicadores deverá ser a calculada pela CONTRATADA periodicamente como condição para pagamento dos serviços. A CONTRATADA deverá disponibilizar mensalmente ao PRODERJ, relatórios digitais com o cálculo dos indicadores, totalizados e apresentados mensalmente por enlace;

3.9.4. Essas métricas servirão como limiar de qualidade do serviço, compondo o que será denominado de Níveis Mínimos de Serviço (NMS);

3.9.5. No Termo de Referência encontram-se a definição básica destes indicadores e sua fórmula de cálculo.

3.10. **Índice Disponibilidade Mensal do Enlace (IDM)**

3.11. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede WAN estará operacional em um determinado período de tempo, para cada sítio da rede corporativa do Governo do Estado do Rio de Janeiro. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês;

3.12. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente;

3.13. Para cada sítio conectado, deverá ser garantida o Índice de Disponibilidade Mensal do Enlace (IDM) conforme os níveis a seguir:

3.14. **Nível IDM Sítios**

≥ 99,80%

N1 ou Core de Rede IP Governo e Unidades Especiais 1h 27m 7s / mês

≥ 99,30%

N2 ou Demais Unidades pertencentes à Região Metropolitana do Estado 5hs 4m 55s / mês

≥ 99,03%

N3 ou Demais Unidades pertencentes à Região Interior do Estado 7hs 2m 31s / mês

3.15. **Taxa de Erro de Bit (TxErr)**

3.15.1. Para Rede IP Governo a TxErr será medida da Taxa de Erro da conexão de acesso ao Backbone IP MPLS da CONTRATADA.

Nível	TxErr	Tipo de Acesso
N1	≤ 10-7	Fibra Ótica e Rádio Terrestre
N2	≤ 10-6	Par metálico e Acesso Satélite

3.16. **Taxa de Erro de Bit (TxErr)**

3.17. **Taxa de Perda de Pacotes (TPP)**

3.17.1. Para Rede IP Governo a Taxa de Perda de Pacotes deverá ser menor ou igual a 2% para qualquer tipo de acesso.

3.17.2. A perda de pacote do Backbone IP do Núcleo do Backbone IP da CONTRATADA deverá ser menor que 1%.

3.18. **Tempo de Retardo (RTT)**

3.18.1. Para Rede IP Governo a Taxa o Tempo de Retardo deverá atender para os limiares abaixo conforme o tipo de acesso.

Nível	RTT	Sítios
N1	≤ 100ms	Fibra Ótica, Rádio Terrestre e Par Metálico
N2	≤ 1000ms	Acesso Satélite

3.19. **Tempo de Retardo (RTT)**

3.20. **Prazo de Reparo (PR)**

3.20.1. Para Rede IP Governo de Redundância o Prazo de Reparo deverá atender para os limiares abaixo.

Nível	PR	Sítios
N1	≤ 2 horas	Core de Rede IP Governo e Unidades Especiais
N2	≤ 5 horas	Demais Unidades pertencentes à Região Metropolitana do Estado
N3	≤ 7 horas	Demais Unidades pertencentes à Região Interior do Estado

3.21. **Prazo de Reparo (PR)**

3.22. **Prazo de Alteração de Configuração dos Serviços (PAC)**

3.22.1. Para Rede IP Governo de Redundância o prazo de Alteração de Configuração dos Serviços deverá atender para os limiares conforme abaixo.

Nível	PAC	Complexidade
N1	≤ 72 horas	Baixa
N2	≤ 10 dias	Média
N3	≤ 60 dias	Alta

3.23. **Prazo de Alteração de Configuração dos Serviços (PAC)**

3.24. **Prazo de Alteração da Taxa de Transmissão de um Enlace (PAT)**

3.24.1. Para Rede IP Governo de Redundância o prazo de Alteração de Taxa de Transmissão de um Enlace.

Nível	PAT	Sítios
N1	≤ 30 dias	Core de Rede IP Governo e Unidades Especiais
N2	≤ 60 dias	Demais Unidades pertencentes à Região Metropolitana e Interior do Estado

3.25. **Prazo de Alteração de Transmissão (PAT)**

3.26. **Prazo de Atendimento a Novos Endereços (PAN)**

3.26.1. Para Rede IP Governo de Redundância o prazo de Atendimento a Novos Endereços será de 60 dias;

3.26.2. As métricas apresentadas neste item servirão de base para avaliação e verificação da qualidade dos serviços prestados pela CONTRATADA.

3.27. **TECNOLOGIAS ALTERNATIVAS DE ACESSO**

3.27.1. Será permitida a utilização de links de tecnologias alternativas, como, por exemplo, radiofrequência, satélite, ADSL, Wireless (3G/4G/5G). Desde que sejam devidamente integrados à Rede IP Governo Principal, preservando todos os requisitos de desempenho, disponibilidade e segurança definidos no Termo de Referência e este Encarte Técnico;

3.27.2. Com exceção do atendimento às Unidades Descentralizadas Temporárias, a utilização da tecnologia 4G ou 5G será permitida exclusivamente para fins de cumprimento de prazo de instalação, sendo obrigatória a sua substituição por outra tecnologia alternativa em um prazo máximo de 90 (noventa) dias, a contar da data de ativação do circuito, considerando ainda o limite estabelecido para implantação definido no item específico;

3.27.3. Os links em tecnologias alternativas deverão ser controlados e gerenciados por tecnologia de integração tipo SD-WAN, conforme especificações constantes no Termo de Referência e Encartes Técnicos;

3.27.4. Os acessos que utilizarem tecnologias alternativas dentro da região metropolitana serão exclusivamente para circuitos fora do backbone do PRODERJ, com velocidades de no máximo 100 Mbps e somente serão instalados mediante autorização expressa da CONTRATANTE;

3.27.5. A configuração da Região Metropolitana a ser considerada pela CONTRATADA tem como base legal a Lei Complementar n° 184/2018;

3.27.6. Cabe ressaltar que, a critério da CONTRATANTE, novas localidades poderão ser conectadas à Rede de Tecnologias Alternativas, assim como solicitadas atualizações das velocidades inicialmente definidas, respeitando os requisitos do Termo de Referência e Encartes Técnicos.

3.28. **ESPECIFICAÇÃO TÉCNICA DO ACESSO VIA SATÉLITE**

3.28.1. O Serviço VPN através de acessos satélite tem por objetivo ser uma alternativa para atendimento de localidades, onde não existam facilidades de acesso terrestre convencionais.

3.28.2. Neste item são descritos requisitos para prestação do serviço VPN através de acessos satélites VSAT.

3.28.3. Os satélites para acesso VSAT (Very Small Aperture Terminal) estão em órbita geoestacionária e fazem o intermédio da transmissão dos dados entre as pequenas estações terrestres remotas (terminais VSAT) e a estação de terrestre mestre ou "HUB";

3.28.4. O serviço deverá ser prestado através da tecnologia VSAT com antenas remotas parabólicas terminais entre 75 cm e 1,2m de diâmetro;

3.28.5. A CONTRATADA deverá disponibilizar:

3.28.5.1. Características básicas do serviço a ser prestado:

a) IP MPLS com acesso satélite, qualidade de serviço e perfil de tráfego;

b) Três perfis de tráfego: D (dados), DV (dados e voz), DVV (dados, voz e/ou vídeo);

c) Antenas de 1.2m;

d) Cobertura Nacional;

e) Operação em Banda Ku;

f) Utilização da tecnologia VSAT (TDMA) banda larga bidirecional.

3.28.5.2. Definições:

a) Taxa Nominal de Download: corresponde à velocidade de pico que poderá ser alcançada pelo usuário no sentido download da rede para o cliente. A velocidade de pico não é garantida e depende da carga de tráfego da rede;

b) Velocidade Típica de Download: é a taxa tipicamente garantida no sentido de download;

c) Taxa Nominal de Upload: corresponde à velocidade de pico que poderá ser alcançada pelo usuário no sentido upload do cliente para rede. A velocidade de pico não é garantida e depende da carga de tráfego da rede;

d) Velocidade Típica de Upload: é a taxa tipicamente garantida no sentido de upload.

3.28.5.3. O serviço ofertado pela CONTRATADA deverá atender aos seguintes Perfis de Tráfego:

a) Perfil D: 100% de tráfego de dados;

b) Perfil DV: 70% de tráfego de dados e 30% de tráfego de voz. Podendo através ser disponibilizados até 2 canais de voz;

c) Perfil DVV: 70% de tráfego de dados, 30% de tráfego de voz e/ou vídeo;

3.28.5.4. Neste perfil a velocidade deverá ser no mínimo de 10 Mbps, podendo ser disponibilizados até 5 canais de voz de 28Kbps ou um canal de voz e um de

vídeo de 128Kbps.

3.28.5.5. A CONTRATADA deverá fornecer antena VSAT e receptor satélite IDU (Indoor Unit), conjuntamente com os serviços de instalação e manutenção dos acessos VSAT;

3.28.5.6. A CONTRATADA também deverá fornecer o roteador adequado à prestação do serviço SD-WAN com acesso satélite;

3.28.5.7. Os Órgãos CONTRATANTES serão responsáveis por disponibilizar local, energia e aterramento e climatização adequada para instalação dos equipamentos, com deverá possuir sistema de para-raios em suas instalações, caso necessário para disponibilização dos serviços.

3.29. ESPECIFICAÇÃO TÉCNICA DO ACESSO VIA RADIOFREQUÊNCIA

3.29.1. O Serviço de acesso através de RADIOFREQUÊNCIA tem por objetivo ser uma alternativa para atendimento de localidades, onde não existam facilidades de acesso convencionais.

3.29.2. Neste item são descritos requisitos para prestação do serviço de acesso através de RADIOFREQUÊNCIA.

3.29.3. Os enlaces deverão ser dedicados ponto-a-ponto interligando a localidade ao backbone da CONTRATADA, e consequentemente à rede privada da Rede IP Governo;

3.29.4. Os circuitos de dados deverão ter características de transparência de protocolos de comunicação, ou seja, deverão permitir o tráfego de dados independentemente do tipo de protocolo de comunicação utilizado no âmbito da rede Rede IP Governo;

3.29.5. Os enlaces deverão operar baseados em protocolo IP e com encapsulamento Ethernet em todo o trecho;

3.29.6. Os enlaces deverão utilizar espectros de frequências administrados pela ANATEL, conforme descrição do art. 4º, inciso XXI, da Resolução ANTEL nº 259, de 19 de abril de 2001;

3.29.7. Deverão ser utilizadas faixas de frequência licenciadas junto à ANATEL de 6, 8, 11, 18, e 23 GHz, com modulação mínima de 256 QAM no que se refere aos cálculos de capacidade e performance dos radioenlaces;

3.29.8. Não serão aceitos circuitos que utilizem enlaces de rádio com espectros de frequência não administrados pela ANATEL e não licenciáveis, por exemplo, 2,4 e 5,8 GHz;

3.29.9. Utilizar rádio digital que apresente certificado ANATEL, dentro da validade, e registro como tipo de produto “Transceptor Digital”;

3.29.10. Utilizar antena que apresente certificado ANATEL, dentro da validade, e registro como tipo de produto “Antena Direcional – Categoria II”;

3.29.11. A CONTRATADA é responsável por executar todas as providências necessárias à manutenção do registro regular das radiofrequências durante a vigência do contrato;

3.30. ESPECIFICAÇÃO TÉCNICA DO ACESSO PONTO-A-PONTO (LAN-TO-LAN)

3.30.1. Considera-se um enlace ponto-a-ponto, dois circuitos distintos implantados nas duas localidades interligadas. Desta forma, admite-se a cobrança dos dois circuitos que formam o enlace ponto-a-ponto nos valores estipulados na ata de registro de preços estabelecida para a velocidade demandada.

3.30.2. O circuito ponto-a-ponto deverá ser utilizado única e exclusivamente para conexão entre dois pontos, pois não contempla a conectividade com a Rede Governo somente por ela;

3.30.3. Os circuitos do tipo ponto-a-ponto deverão manter latência máxima de até 20ms;

3.30.4. Deverá suportar o trânsito de múltiplas VLANs (modo trunk) simultaneamente;

3.30.5. Deverá suportar agregação de portas (etherchannel, port-channel).

3.30.6. Deverá estar monitorado pelo Serviço de Gerência de Rede ofertado pela CONTRATADA.

3.31. REQUISITOS DA INTERLIGAÇÃO DE CONTINGÊNCIA

3.31.1. Os circuitos para interligação entre os dois Datacenters do PRODERJ, localizados na UERJ e no CICC, ou em outros locais conforme previsto no edital, deverão necessariamente ser do tipo ponto-a-ponto (layer 2);

3.31.2. Poderá ser utilizada a tecnologia L2VPN, ou similar, desde que atenda aos requisitos do Termo de Referência e este Encarte Técnico;

3.31.3. Esta interligação deverá possuir baixa latência, tipicamente abaixo de 20ms, possibilitando a implementação de sistemas de replicação de bases de dados entre os dois Datacenter e soluções de Disaster Recovery;

3.31.4. A conectividade entre os Datacenters deverá ser no mínimo na velocidade de 1Gbps e máximo de 10Gbps, através de solução de transporte PTN, Metro Ethernet ou DWDM;

3.31.5. A conectividade desta interligação deverá ser realizada com os Roteadores Concentradores do Núcleo da Rede IP Governo;

3.31.6. A CONTRATADA deverá confeccionar, quando solicitado, o projeto lógico envolvendo esta interligação, que deverá ser aprovado pelo PRODERJ antes da sua implantação;

3.31.7. O PRODERJ será responsável pela configuração dos elementos de sua rede interna de forma que projeto aprovado possa ser implantado.

3.32. CARACTERÍSTICAS BÁSICAS DO ACESSO À INTERNET

3.32.1. Em ambos os Lotes, deverá ser provisionado no backbone da Rede Governo no PRODERJ o acesso dedicado à Internet para os órgãos e secretarias da Administração Pública.

3.32.2. O objetivo principal aqui é o fornecimento do serviço de acesso à internet para a Rede IP Governo, com objetivo de centralizar a conexão com a

Internet para as unidades descentralizadas abrangidas pela Rede IP Governo, bem como prover o acesso da grande rede aos serviços hospedados no PRODERJ.

3.32.3. A CONTRATADA deverá garantir o nível de disponibilidade especificado neste documento;

3.32.4. A contratação contempla a instalação e configuração dos equipamentos e enlaces de comunicação, e o gerenciamento proativo do serviço, visando à melhoria do processo de recuperação do serviço em caso de falha.

3.32.5. O acesso à INTERNET compreende o fornecimento de banda INTERNET dedicada e exclusiva. Neste serviço consta ainda o fornecimento de endereçamento IPs públicos conforme necessidade da CONTRATANTE. A banda contratada prevê a criação de uma interface L3 exclusiva para o acesso Internet.

3.32.6. Deverá ser fornecido, no mínimo, um bloco de endereçamento IP público com 254 endereços utilizáveis (bloco /24), de forma fixa, roteável e globalmente acessível, para atender os Data Center do PRODERJ e grandes sítios, conforme necessidade;

3.32.7. Os demais sítios, devem receber, no mínimo, um bloco de endereçamento IP público com 16 endereços utilizáveis (bloco /28), de forma fixa, roteável e globalmente acessível, nos demais sítios, conforme necessidade;

3.32.8. As especificações técnicas descritas nesse documento englobam definições do projeto detalhado da rede, premissas de topologia de rede, tecnologias de acesso aplicáveis, capacidades de enlaces de comunicação, aspectos de interconexão e de roteamento, requisitos de qualidade de serviço, definições de gerência de rede e aspectos de segurança da informação;

3.32.9. A topologia a ser implantada deverá ser efetuada mediante ativação de circuito de comunicação de dados, instalação de equipamentos e prestação de serviços de instalação, configuração, suporte técnico e gerenciamento proativo de falhas, conforme especificações técnicas constantes nesse documento;

3.32.10. A CONTRATADA deverá se encarregar de prover o meio físico de interligação entre a sua rede e a Rede IP Governo, atendendo aos parâmetros definidos nesta especificação, ficando este serviço sob sua inteira responsabilidade;

3.32.11. A solução adotada pela CONTRATADA deverá atender a todas as normas técnicas exigidas pelos órgãos públicos competentes e responsáveis pela regulamentação;

3.32.12. A CONTRATADA poderá subcontratar os meios de acesso à última milha, no termos no Termo de Referência, sem que isso implique e transferência de responsabilidade, que será exclusiva da CONTRATADA vencedora do certame;

3.33. **ESPECIFICAÇÕES TÉCNICAS**

3.33.1. Cada um dos acessos e respectivos circuitos de comunicação de dados devem apresentar, no mínimo, as seguintes especificações técnicas gerais: Ter capacidade de expansão até a velocidade máxima de operação da interface utilizada, quando solicitado pela CONTRATANTE;

3.33.2. Prover conexão à Rede Corporativa da Rede IP Governo por meio de, pelo menos, uma interface do tipo Giga Ethernet Full Duplex;

3.33.3. O acesso deve ser dedicado e o serviço deverá possuir a banda garantida de acordo com a velocidade do acesso contratado;

3.33.4. O Serviço fornecido deverá suportar o protocolo IPV6, caso solicitado pela CONTRATANTE;

3.33.5. A prestação do serviço compreende a disponibilização, instalação, ativação e configuração do(s) equipamento(s) que compõem o acesso, e outros que possibilitem a utilização do serviço objeto da presente contratação;

3.33.6. A CONTRATADA deverá disponibilizar toda a infraestrutura de telecomunicações (equipamentos e insumos) necessária ao pleno funcionamento dos serviços contratados, sem custo adicional a CONTRATANTE;

3.33.7. A CONTRATADA deverá possuir Backbone IP próprio, com conexão própria a outros Provedores de Acesso à Internet Nacionais e Internacionais;

3.33.8. O Backbone da CONTRATADA deverá possuir conexão a mais de dois AS (Autonomous System), independentes e distintos;

3.33.9. A CONTRATADA deverá possuir pelo menos um POP (ponto de presença) próprio no exterior para a troca de tráfego internacional;

3.33.10. Realizar, manter e prover meios de acessos, com no mínimo 10 Gbps, entre o enlace principal instalado no Datacenter do PRODERJ e o Ponto de Troca de Tráfego (PTT). A realização desta ligação deve estar no projeto de implementação do enlace principal do PRODERJ, que atenderá à Rede IP Governo, garantindo a continuidade dos serviços providos e sem tarifação de tráfego;

3.33.11. Deverá fornecer a interligação ao Ponto de Troca de Tráfego (PTT), garantindo no mínimo duas saídas nacionais geograficamente distintas, sendo uma conexão com o PTT-RJ e outra com o PTT-SP. As conexões deverão contemplar, sempre que disponíveis, a participação dos principais provedores de conteúdo, tais como: Amazon, Google, Oracle, Microsoft, Cisco Umbrella, Akamai, Cloudflare, Meta, entre outros.

3.33.12. O somatório das bandas de saída nacional e internacional entre os AS de, pelo menos, 100 Gbps;

3.33.13. O serviço IP dedicado deverá suportar aplicações TCP/IP (Transmission Control Protocol / Internet Protocol), tais como:

a) HTTP, HTTPS

b) FTP (File Transfer Protocol)

c) TELNET (TERminal NETwork)

d) SSH (Secure Shell)

e) SMTP (Simple Mail Transfer Protocol)

f) SMTPS (Simple Mail Transfer Protocol Secure)

g) POP3 (Post Office Protocol version 3)

h) LDAP (Lightweight Directory Access Protocol)

i) VPN, e tráfego de vídeo e voz sobre IP (VoIP), no sentido para a Internet e vice-versa.

3.33.14. O Provedor deverá dispor de recursos de gerência e supervisão para o circuito;

3.33.15. Para os Links concentradores a CONTRATADA deverá disponibilizar faixa de endereço IP válido, com no mínimo 254 (duzentos e cinquenta e quatro) endereços IP válidos;

3.33.16. Para os Links das demais localidades a CONTRATADA deverá

disponibilizar faixa de endereço IP válido, com no mínimo 16 (dezesseis) endereços IP válidos

3.33.17. A CONTRATADA também deverá disponibilizar quando adequadamente justificado pela CONTRATANTE faixa de endereçamento IP válidos adicionais, com o objetivo de atender as necessidades operacionais da CONTRATANTE.

3.33.18. A CONTRATADA deverá disponibilizar servidores de DNS secundário na função “recursivo”, ou seja, ao receberem uma solicitação de qualquer usuário na qual o mesmo não tenha a informação em cache ou não sendo o seu próprio domínio, ele se encarrega em buscar essa informação em outro servidor de DNS;

3.33.19. Caso os servidores de DNS da CONTRATADA sejam utilizados como secundário, a CONTRATADA deverá gerenciar a transferência dos registros de zona com o seu servidor de DNS primário da CONTRATANTE. A CONTRATADA também deverá fornecer as informações relativas à compatibilidade entre os seus servidores de DNS primários e os servidores secundários;

3.33.20. Servidor NTP (Network Time Protocol) ou acesso a servidores NTP públicos nacionais para sincronismo de horário dos servidores e ativos de rede da CONTRATANTE;

3.33.21. Os servidores de DNS da CONTRATADA deverão dar suporte à tecnologia DNSSEC (Domain Name System Security Extensions) ou DNS over SSL (Security Socket Layer);

3.33.22. Os canais de comunicação deverão ser configurados com velocidades simétricas (upstream = downstream);

3.33.23. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 100ms.

3.34. PERSPECTIVA DE CRESCIMENTO DOS NÚMEROS DE SÍTIOS E DA ALTERAÇÃO DA BANDA DE ACESSO

3.34.1. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão de bandas de comunicação, respeitados os limites legais e técnicos, bem como as condições estipuladas nos níveis de serviços;

3.34.2. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços ou mesmo a adição de um novo sítio, sem que isso enseje custos de qualquer natureza ao solicitante.

3.35. SERVIÇO DE ANTI-DDOS

3.35.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS (DoS – Denial of Service) e DDOS Distributed Denial of Service);

3.35.2. A análise deverá ser passiva sem utilização de elementos probes para coleta dos dados a serem analisados;

3.35.3. A Solução deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não;

3.35.4. O ataque deve ser mitigado na estrutura da CONTRATADA, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelos Órgãos do Governo do estado do Rio continuem disponíveis aos seus usuários;

3.35.5. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

3.35.6. A solução deverá possuir interface de gerência e operação via WEB em cima de SSL, a interação entre os elementos de limpeza e detecção será feita através desta interface, assim como as configurações de limpeza, análise e os alertas de ataques;

3.35.7. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;

3.35.8. Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada;

3.35.9. A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico; Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE;

3.35.10. Para a mitigação dos ataques não deverá ser encaminhado o tráfego para limpeza fora do território brasileiro;

3.35.11. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantida em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

3.35.12. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

3.35.13. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATANTE.;

3.35.14. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP;

3.35.15. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

a) Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP.

b) Ataques a pilha TCP, incluindo mau uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.

c) Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

d) Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing).

3.35.16. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.

3.35.17. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole.;

3.35.18. Realizar a comunicação da ocorrência do ataque ao órgão do Governo CONTRATANTE imediatamente após a detecção;

3.35.19. Disponibilizar relatórios mensais de mitigação de ataques;

3.35.20. Disponibilizar um Centro Operacional de Segurança no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

3.35.21. A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra ataques DDOS (Distributed Denial of Service);

3.35.22. A proteção deverá operar sem exigir o desligamento de qualquer outro circuito de acesso do Órgão, independente de quantos ou quais sejam os demais fornecedores;

3.35.23. A solução ofertada não poderá afetar a visibilidade do endereço de origem das requisições, mantendo o tráfego legítimo livre de qualquer modificação; A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;

3.35.24. A CONTRATADA deverá disponibilizar acesso a sistema de monitoramento que permita a visualização do tráfego, emissão de relatórios, visualização de alertas e informações da conta associada aos serviços de proteção;

3.35.25. O serviço deve ter a capacidade de mitigar ataques no perímetro Internacional em, pelo menos,dois pontos distintos e na borda Nacional;

3.35.26. Uma vez que o ataque é detectado pela solução, o equipamento instalado no backbone da operadora, responsável pela mitigação do trafego de ataque, deverá ser alertado e então todo o trafego do cliente deverá ser direcionado imediatamente, sem impactos e/ou interrupção do serviço;

3.35.27. O Serviço de Backbone (Anti-DDOS), deverá possuir o seguinte SLA (Service Level Agreement):

a) Prazo para entrega de relatórios mensais: até 5 (cinco) dias úteis.

b) Prazo para entrega de relatórios de incidente (após mitigação do ataque): até 5 (cinco) dias úteis.

c) Atendimento às solicitações em regime 24 x 7 x todos os dias do ano:

Prioridade 1: Requisição de adição/retirada de rede monitorada, modificação na lista de contatos autorizados do cliente, relatórios de dados do tráfego do cliente

monitorado em um período especifico. Prazo máximo de 2 horas

Prioridade 2: Requisição da lista de redes monitoradas, alertas e mitigações, informações sobre ataques recebidos, lista de contatos autorizados pelo cliente. Prazo máximo de 8 horas.

3.36. **SLA de Mitigação de Ocorrência de Incidentes:**

3.36.1. Item Ocorrências Prazo

3.36.2. Início do Ataque

3.36.3. Detecção do Ataque

3.36.4. Tempo de Detecção Até 15 minutos

3.37. **Contato com PRODERJ**

3.37.1. A CONTRATADA deverá entrar em contato com o PRODERJ e solicitar autorização para dar início à mitigação do tráfego;

3.37.2. **Caso a CONTRATADA por qualquer razão não consiga contato com o responsável pela área de TIC do PRODERJ, esta poderá implementar as ações de mitigação do ataque que julgar necessárias, comunicando assim que possível a CONTRATANTE.**

3.38. **NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA OS ACESSOS À INTERNET**

3.38.1. Uma série de indicadores deverá ser a calculada pela CONTRATADA periodicamente como condição para pagamento dos serviços. A CONTRATADA deverá disponibilizar mensalmente ao CONTRATANTE, relatórios digitais com o cálculo dos indicadores, totalizados e apresentados mensalmente por enlace.

3.38.2. Essas métricas servirão como limiar de qualidade do serviço, compondo o que será denominado de Níveis Mínimos de Serviço (NMS). No Termo de Referência encontram-se a definição básica destes indicadores e sua fórmula de cálculo.

3.38.3. Classificam-se cada sítio como básico ou crítico, sendo o primeiro com atendimento 8x5 e dias comerciais, e o segundo 24x7x365;

3.38.4. Cada endereço constante no Anexo II receberá uma única classificação, e a CONTRATADA deverá ter condições de atender a possível mudança quando solicitado pelo CONTRATANTE durante a vigência contratual;

3.39. **Índice Disponibilidade Mensal do Enlace (IDM)**

3.39.1. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede WAN estará operacional em um determinado período de tempo, para cada sítio da rede corporativa do Governo do Estado do Rio de Janeiro. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês.

3.39.2. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a

disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

3.40. **Nível IDM Serviços**

≥ 99,80%

N1 ou Serviços de Acesso à Internet do Datacenter PRODERJ 1h 27m 7s / mês

≥ 99,30%

N2 ou Serviços de Acesso à Internet demais órgãos e secretarias – região metropolitana 5hs 4m 55s / mês

≥ 99,03%

N3 ou Serviços de Acesso à Internet demais órgãos e secretarias – região não metropolitana 7hs 2m 31s / mês

3.41. **Taxa de Erro de Bit (TxErr)**

3.41.1. Para o Serviço de Acesso à Internet a TxErr será medida da Taxa de Erro da conexão do acesso ao Backbone IP da CONTRATADA.

3.41.2. Nível TxErr Acessos

3.41.3. N1 ≤ 10-7 Conexões dos Acessos à Internet

3.42. **Taxa de Perda de Pacotes (TPP)**

3.42.1. Para o Serviço de Acesso à Internet a Taxa de Perda de Pacotes deverá se ser menor ou igual a 2%.

3.42.2. A perda de pacote do Backbone IP do Núcleo do Backbone IP da CONTRATADA deverá ser menor que 1%.

3.43. **Tempo de Retardo (RTT)**

3.43.1. Para os Serviços de Acessos à Internet o Tempo de Retardo deverá atender aos limiares abaixo, considerando a medição ao primeiro elemento de roteamento do Backbone IP da CONTRATADA.

Nível	RTT	Sítios
N1	≤ 100ms	Fibra Ótica, Rádio Terrestre e Par Metálico
N2	≤ 1000ms	Acesso Satélite

3.44. **Tempo de Retardo**

3.45. **Prazo de Reparo (PR)**

3.45.1. Para os Serviços de Acesso à Internet o Prazo de Reparo deverá atender o limiar abaixo.

Nível	PR	Sítios
N1	≤ 2 horas	Core de Rede IP Governo e Unidades Especiais
N2	≤ 5 horas	Demais Unidades pertencentes à Região Metropolitana do Estado
N3	≤ 7 horas	Demais Unidades pertencentes à Região Interior do Estado

3.46. **Prazo de Reparo (PR)**

3.47. **Prazo de Alteração de Transmissão de um Enlace (PAT)**

3.47.1. Para os Serviços de Acesso à Internet o Prazo de Alteração de Transmissão de um Enlace deverá atender ao limiar abaixo

Nível	PAT	Sítios
N1	≤ 30 dias	Core de Rede IP Governo e Unidades Especiais
N2	≤ 60 dias	Demais Unidades pertencentes à Região Metropolitana e Interior do Estado

3.48. **Prazo de Alteração de Transmissão (PAT)**

3.49. **Prazo de Atendimento a Novos Endereços (PAN)**

3.49.1. Para os Serviços de Acesso à Internet, o Atendimento a Novos Endereços deverá ser de 60 dias.

3.49.2. As métricas apresentadas nesse subitem e nos Níveis Mínimos de Serviço (NMS) deverão ser avaliadas como fins de verificação da qualidade dos serviços prestados pela CONTRATADA.

3.50. **DOS REQUISITOS DE ROTEAMENTO**

3.50.1. A solução de rede de dados redundante, a ser contratada no âmbito do Lote II, deverá estar tecnicamente apta a operar de forma complementar e subordinada à rede de dados principal, contratada no Lote I.

3.50.2. O plano de roteamento IP da Rede IP Governo será definido, gerenciado e atualizado exclusivamente pela CONTRATADA do Lote I, responsável pela solução de rede principal, com SD-WAN embarcada e serviços de gerenciamento de rede centralizado.

3.50.3. A rede redundante deverá permitir o roteamento de pacotes IP conforme as mesmas rotas, políticas e tabelas de encaminhamento definidas para a rede principal, assumindo automaticamente ou sob supervisão da CONTRATANTE o tráfego de dados em caso de falha, degradação ou indisponibilidade dos enlaces principais.

3.50.4. A CONTRATADA do Lote II deverá garantir compatibilidade total com os protocolos de roteamento, prefixos IP e planos de endereçamento definidos no escopo da rede principal, não sendo admitida a utilização de sistemas ou arquiteturas que exijam reconfiguração manual ou lógica da estrutura principal.

3.50.5. As conexões físicas da rede redundante deverão ser entregues de forma transparente até os pontos de interconexão com os equipamentos da solução de roteamento principal (appliances SD-WAN ou roteadores CPE do Lote I), cabendo à CONTRATADA do Lote I a administração das rotas e a comutação entre enlaces.

3.50.6. A troca de informações de rede entre as CONTRATADAS deverá observar padrões técnicos abertos e compatíveis com os protocolos adotados pela CONTRATANTE (tais como BGP, OSPF, VRRP, entre outros), conforme estabelecido no projeto executivo aprovado.

3.50.7. A atuação da CONTRATADA do Lote II limitar-se-á à disponibilização dos enlaces redundantes em conformidade com os parâmetros físicos, lógicos e operacionais previamente definidos, ficando vedado qualquer tipo de gestão autônoma de rotas, tunelamento, NAT ou qualquer outra forma de encapsulamento que impacte o comportamento da rede principal.

3.51. ESPECIFICAÇÕES DE QOS DA REDE IP GOVERNO REDUNDANTE

3.51.1. A Rede IP Governo de Redundante deverá suportar Qualidade de Serviço (QoS), de acordo com condições estabelecidas nesse item, inclusive considerando a arquitetura DiffServ;

3.51.2. Deverá permitir a obtenção de escalabilidade e eficácia na diferenciação dos serviços através da implementação de mecanismos de classificação e condicionamento somente nos elementos de borda da rede e aplicação “per-hop behaviors” aos agregados de tráfego que forem marcados usando se o campo DS nos campos apropriados dos cabeçalhos de pacotes MPLS;

3.51.3. No escopo da conexão de cada cliente, há a necessidade de diferenciação de serviços, incluindo a alocação de banda e priorização de pacotes para redução de atrasos de certas classes de tráfego;

3.51.4. A CONTRATADA deverá garantir as configurações implementadas no equipamento de SD-WAN fornecido no Lote I de forma a garantir, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de, pelo menos, 5 (cinco) classes de serviços:

a) Supervisão de Rede: aplicações de monitoramento e controle da rede, que deverão ser priorizadas acima de todas as outras a fim de garantir a disponibilidade de recursos para as intervenções preventivas ou corretivas que se façam necessárias ao seu correto funcionamento, tais como, por exemplo: Telnet, SSH, SNMP, NTP, syslog e Radius, Esta classe de serviço deverá ser utilizada exclusivamente pela empresa prestadora do serviço para o gerenciamento da Rede;

b) Tempo Real – aplicações de Voz e Vídeo sensíveis que são sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem

priorização de pacotes limitadas a 50% da Banda;

3.52. Deverá a CONTRATADA garantir a continuidade da disponibilização de duas classes de serviços distintas de Tempo Real, uma para Voz e outra para Vídeo;

3.53. Dados Críticos: aplicações críticas que exigem a entrega garantida e tratamento prioritário, tais como acesso HTTP e HTTPS a portais corporativos internos; Dados Prioritários: aplicações que sejam menos críticas, mas que também necessitem de tratamento prioritário na rede da CONTRATANTE;

3.54. Melhor Esforço – Best Effort: todo tráfego não explicitamente atribuído às classes Supervisão da Rede, Tempo Real, Dados Prioritários deverá ser alocado nesta classe. Sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como tráfegos importantes; Essa classe deverá permitir o fluxo de tráfego, se houver recursos disponíveis na rede, impedindo que esse tráfego afete negativamente as demais classes;

3.55. As classes de serviço serão aquelas específicas de uma Rede MPLS nativo ou de uma Rede SD-WAN;

3.56. A definição das classes e percentuais de reserva de banda deverá discutida com a equipe técnica do PRODERJ para definição no Projeto Executivo da solução. A equipe de engenharia de tráfego da CONTRATADA deverá, sempre que possível, auxiliar acerca de tais aspectos de modo a otimizar a operação da rede. Ademais, o PRODERJ poderá solicitar a qualquer momento a modificação nas configurações das classes de serviço, de modo a adaptar à evolução de tráfego de suas aplicações.

3.57. DOS REQUISITOS DE SEGURANÇA

3.57.1. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados;

3.57.2. A CONTRATADA deverá implementar quaisquer controles de segurança (bloqueios, cancelamentos de links, etc), quando solicitado pelo CONTRATANTE, caso se identifique riscos de disponibilidade ou de cometimento de crimes através da rede corporativa, dentro dos limites possíveis de atuação da mesma, tendo em vista que o objeto do Lote II se resume ao enlace de comunicação, sem contemplar equipamentos de roteamento e segurança;

3.57.3. A ação descrita no subitem anterior possui o intuito de prevenção de incidentes de segurança de forma a garantir níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do Governo do Estado do Rio de Janeiro, não eximindo a CONTRATADA das responsabilidades previstas no Termo de Referência e este Encarte Técnico;

3.57.4. Em relação aos aspectos técnicos de segurança da informação, a CONTRATADA deverá atender aos seguintes requisitos:

a) Prover uma rede logicamente independente e isolada de qualquer rede de terceiros, inclusive da internet.

b) O isolamento deverá ser realizado em nível lógico do MPLS e em nível 2 (do modelo OSI) para o acesso.

3.57.5. Esta garantia deverá ser implantada fim-a-fim e também se aplica às soluções de contingência;

3.57.6. Caso seja solicitado pelo PRODERJ, o link de redundância deverá suportar as implementações de segurança aplicados ao equipamento SD-WAN fornecido no Lote I, tais como: autenticação do roteador CPE, controle de acesso aos dispositivos, listas de acesso e logging e outras configurações necessárias à segurança da Rede IP Governo;

3.57.7. Caso necessário deverá suportar o esquema de autenticação no nível de protocolo de roteamento, aplicável ao equipamento de SD-WAN fornecido no Lote I, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da Rede IP Governo;

3.57.8. A CONTRATADA deverá garantir a continuidade das configurações dos elementos de rede aplicáveis ao equipamento SD-WAN fornecido no Lote I, que habilitam o registro dos eventos da Rede IP Governo de contingência, tais como conexões externas e registro de utilização de serviços (por exemplo, arquivos transferidos através de FTP e tentativas de login não autorizados). Os registros devem estar com o horário sincronizado via protocolo NTP e possuir detalhes suficientes para identificação do evento, seu autor, seu alvo/objeto e momento de ocorrência;

3.57.9. A CONTRATADA deverá garantir a continuidade do sistema dedicado à coleta e ao armazenamento dos registros gerados pelos dispositivos da Rede IP Governo de contingência, aplicável ao equipamento de SD-WAN fornecido no Lote I;

3.57.10. A CONTRATADA deverá garantir acesso aos patches de segurança do equipamento de SD-WAN fornecido no Lote I;

3.58. SERVIÇO DE GERÊNCIA INTEGRADA DA REDE IP GOVERNO REDUNDANTE

3.58.1. A Rede IP Governo Redundante deverá contar com o serviço de Gerência de Rede Integrada contratada junto a operadora do Lote I, com o objetivo de assegurar a supervisão contínua e unificada de todos os enlaces contratados para a Rede IP Governo.

3.58.2. A responsabilidade pelo, monitoramento proativo da Rede IP Governo Redundante é atribuição da CONTRATADA do Lote I, responsável pelo fornecimento dos enlaces principais com solução de SD-WAN embarcada.

3.58.3. A responsabilidade pelo diagnóstico de falhas, gestão de eventos e coordenação de ações corretivas da Rede IP Governo Redundante é atribuição da CONTRATADA do Lote II, responsável pelo fornecimento dos enlaces principais com solução de SD-WAN embarcada.

3.58.4. A CONTRATADA do Lote I deverá, obrigatoriamente, implementar mecanismos de monitoramento dos enlaces redundantes contratados no Lote II, devendo manter registro e supervisão dos eventos de indisponibilidade ou degradação de desempenho desses enlaces.

3.58.5. Constatada a falha, interrupção ou qualquer anormalidade nos enlaces redundantes do Lote II, a CONTRATADA do Lote I deverá notificar formalmente, de forma imediata e automatizada, a CONTRATADA do Lote II para que sejam adotadas as providências corretivas cabíveis, conforme os prazos de resposta e solução definidos contratualmente.

3.58.6. A CONTRATADA do Lote I deverá manter canal de comunicação direto e documentado com a CONTRATADA do Lote II, incluindo mecanismos para abertura e acompanhamento de chamados técnicos relacionados aos enlaces redundantes.

3.58.7. A CONTRATADA do Lote II deverá disponibilizar à CONTRATANTE ferramenta de gerenciamento centralizado (painel único) que permita visualizar todos os enlaces redundantes, bem como o histórico de incidentes e intervenções.

3.58.8. A CONTRATADA do Lote II deverá assegurar, por sua vez, a plena integração técnica e operacional com a infraestrutura de monitoramento e gestão da CONTRATADA do Lote I, permitindo a coleta de métricas, envio de traps SNMP, logs e quaisquer outros dados necessários à gerência unificada da rede.

3.58.9. A Solução de Gerência da Rede não deverá demandar ao CONTRATANTE quaisquer custos de licenciamento para o seu funcionamento pleno;

3.58.10. Em caso de incidentes massivos, a CONTRATADA deverá informar uma lista de links afetados em até 2 horas a partir do início do problema via portal ou e-mail.

3.58.11. A solução de Gerência da Rede da CONTRATADA deverá enviar os alertas de incidentes no mínimo via e-mail, opcionalmente via SMS de forma adicional;

3.58.12. A solução fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

3.58.13. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto não serão aceitas soluções que possuem acessos segmentados aos módulos;

3.58.14. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

3.58.15. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc;

3.58.16. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente; A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

3.58.17. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clients específicos, portanto não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plug-ins nos desktops dos colaboradores da CONTRATANTE;

3.58.18. O acesso deverá ser via web padrão HTTP e suportar a HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português;

3.58.19. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets, portanto não serão aceitas soluções que não possuam essa compatibilidade;

3.58.20. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari;

3.58.21. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

3.58.22. A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados.

3.58.23. A Solução de Gerência da Rede deverá permitir a criação de Relatórios:

3.58.24. Permitir ser exportados conforme os principais métodos como: pdf, csv,

pacote office;

3.58.25. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados;

3.58.26. A Solução de Gerência da Rede deverá armazenar os dados por um período de 12 (doze) meses;

3.59. DOS REQUISITOS DE INFRAESTRUTURA

3.59.1. Se necessário, os equipamentos fornecidos pela contratada deverão ser capazes de operar com a alimentação elétrica de 110V ou 220V e frequência de 60Hz;

3.59.2. Excetuando-se os equipamentos de roteamento e segurança que fazem parte do escopo da solução do Lote I – Rede Governo Principal, a CONTRATADA será responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os Equipamentos/recursos que forem necessários (modems, estações de gerenciamento, meios de transmissão, cabeamento WAN, acessórios necessários, dentre outros) para o provimento dos serviços. Os Equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos;

3.59.3. A infraestrutura interna da rede da CONTRATADA (Backbones, POPs, Equipamentos internos, dentre outros) deverá ser atendida por solução de alimentação e proteção elétrica de modo a manter todos os Equipamentos em operação por tempo indeterminado no caso de falta de energia;

3.59.4. A CONTRATADA será responsável pela interligação da rede entre o Distribuidor Geral (DG) de telefonia do prédio em cada um dos sítios e o local físico onde se encontra instalado o CPE da Rede Governo Principal, que receberá os acessos por rede cabeada redundante;

3.59.5. Para o caso de atendimento do sítio por meio de rede não-cabeada, por exemplo, enlace de rádio frequência terrestre, satélite ou wireless, quando a implantação implique a necessidade de execução de obras civis, estas ficarão a cargo da CONTRATANTE, e deverão constar do cro nograma que faz parte do Projeto Executivo. Nestes casos, a CONTRATADA apresentará relatório de visita contendo as adequações e providências necessárias para a conclusão da instalação dos circuitos.

3.60. REQUISITOS DE IMPLANTAÇÃO

3.60.1. Para cada um dos acessos contratados deverão ser prestados serviços de ativação dos circuitos de comunicação de dados, bem como integração física aos equipamentos de SD-WAN fornecidos no Lote I, que somente poderá ser efetivada após evidenciada a condição de conectividade básica do enlace de comunicação;

3.60.2. Os serviços de ativação e instalação dos circuitos e equipamentos deverão ser prestados no ambiente computacional da Rede IP Governo – Unidades Especiais e Unidades Descentralizadas atendidas pela Rede IP Governo conforme os Locais de Prestação dos Serviços;

3.60.3. Caso o Projeto Executivo não seja aprovado pelo CONTRATANTE, a CONTRATADA deverá corrigi-lo e reapresentá-lo em no máximo 5 (cinco) dias

corridos após a comunicação da sua rejeição;

3.60.4. O atraso na entrega do Projeto Executivo poderá causar sanções à CONTRATADA conforme condições elencadas no TERMO DE REFERÊNCIA;

3.60.5. A não aceitação pelo CONTRATANTE das soluções adotadas, devido a não conformidade com as solicitações deste documento, poderá resultar em rescisão total ou parcial do contrato de prestação de serviços;

3.60.6. A CONTRATADA deverá apresentar, semanalmente, relatórios de acompanhamento das atividades, nos quais deverão constar as atividades realizadas e a duração de cada atividade;

3.60.7. A CONTRATADA deverá apresentar, semanalmente, relatórios de acompanhamento das atividades, nos quais deverão constar as atividades realizadas e a duração de cada atividade durante a execução do Projeto Executivo;

3.60.8. A CONTRATADA ficará obrigada a manter sigilo sobre todas as informações referentes à solução implantada, bem como acerca das instalações da Rede IP Governo, sendo vedada qualquer divulgação destas informações sem prévia autorização, por escrito, do órgão, cabendo penalizações administrativas e sanções legais cabíveis, em caso de descumprimento;

3.60.9. A CONTRATADA assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do Governo do Estado do Rio de Janeiro ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando da instalação e configuração da solução, na área de prestação dos serviços, mesmo que fora do exercício;

3.60.10. Deverá ser disponibilizada a geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, dos níveis de serviço contratados e validação das faturas;

3.60.11. O serviço de gerenciamento deve atuar de forma proativa, dentro dos limites de atuação aplicáveis, antecipando-se aos problemas na rede e garantindo a qualidade do serviço estabelecida nos Níveis Mínimos de Serviços, realizando abertura, acompanhamento e fechamento de chamados técnicos relacionados com indisponibilidade e desempenho no serviço de Rede IP Governo, operando em regime 24 horas por dia, 7 (sete) dias por semana, durante toda a vigência do contrato;

3.60.12. A CONTRATADA deverá finalizar a instalação de todos os links constantes no Anexo I - Local de Prestação dos Serviços da Rede IP Governo em até 180 dias.

3.61. PROJETO EXECUTIVO

3.61.1. O Projeto Executivo deverá contemplar os seguintes itens:

a) Definição de topologias físicas e lógicas da rede;

b) Cronograma da implantação dos serviços;

c) Os Esquemas de redundância para os enlaces necessários;

d) O Plano de Roteamento;

e) Os parâmetros de qualidade de serviço;

f) Dimensionamento de enlaces e interfaces de comunicação;

g) Plano de endereçamento compatível com a atual rede corporativa do Governo do Estado do Rio de Janeiro, associando endereços IPs privados de modo a torná-los únicos dentro da nuvem SD-WAN; Cronograma de execução de obras civis de responsabilidade da CONTRATADA, caso seja necessário;

h) Definição do QoS e dos perfis de banda por Classe de Serviço.

3.62. REQUISITOS DO SERVIÇO DE SUPORTE TÉCNICO

3.62.1. A CONTRATADA deverá disponibilizar um número único nacional não tarifado (0800) para abertura de chamados de suporte técnico, como também o Serviço de Gerência fornecido pela CONTRATADA deverá ser capaz de gerenciar os níveis de serviços acordados;

3.62.2. A assistência técnica on-site deverá ser prestada nas instalações do CONTRATANTE conforme os prazos estipulados nos Níveis Mínimos de Serviço (NMS);

3.62.3. No momento de abertura do chamado deverá ser fornecido ao CONTRATANTE um número único de identificação do chamado;

3.62.4. Os chamados somente poderão ser abertos e fechados após autorização do CONTRATANTE;

3.62.5. Os serviços de suporte técnico deverão incluir serviços de atualização dos Equipamentos componentes da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de software de Equipamentos;

3.62.6. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo CONTRATANTE;

3.62.7. Em caso de reiterado inadimplemento do SLA, o CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato;

3.62.8. Durante a vigência do contrato, a CONTRATADA deverá manter preposto aceito pela Administração do CONTRATANTE para representá-la administrativamente sempre que houver necessidade.

3.63. REQUISITOS DE GERENCIAMENTO DOS SERVIÇOS

3.63.1. Mensalmente, a CONTRATADA deverá encaminhar ao CONTRATANTE relatório com todos os chamados de suporte técnicos abertos / fechados, com a identificação do chamado, data e hora de abertura, nome da pessoa que abriu e do técnico alocado, bem como as atividades executadas, data e hora de fechamento do chamado e resolução aplicada;

3.63.2. O relatório deverá ser enviado juntamente com a fatura de prestação dos serviços e deverá apresentar informações acerca da aferição dos níveis de serviço contratados, como descrição dos períodos de indisponibilidade, para cada um dos acessos contratados;

3.63.3. Os relatórios deverão ser detalhados dia, período e causas de eventuais indisponibilidades de serviço ocorridas, bem como o somatório total de minutos de

todas as ocorrências e o cálculo do Índice de Disponibilidade Mensal (D) correspondente ao período de faturamento;

3.63.4. A entrega dos relatórios mensais é condição necessária à atestação dos serviços, pelo CONTRATANTE, para fins de pagamento;

3.63.5. Caso o Índice de Disponibilidade Mensal, seja inferior ao especificado neste Termo de Referência, a CONTRATADA deverá encaminhar relatório com o cálculo do total de desconto a ser aplicado no valor da fatura, de acordo com a seguinte fórmula:

VD = CM * [(100 - D) / 100],

Onde:

VD é o valor do desconto;

CM é o custo mensal dos serviços prestados;

D é o índice de disponibilidade mensal dos serviços, calculado pelas fórmulas especificadas nos Níveis Mínimos de Serviço (NMS)

3.63.6. O CONTRATANTE reserva-se o direito de promover, a qualquer tempo, alterações nas políticas de utilização da Rede IP Governo, ficando a CONTRATADA, neste caso, obrigada a prestar o suporte técnico necessário à implementação dessas diretrizes nos equipamentos por ela empregados na prestação os serviços, sem prejuízo das condições de funcionamento previstas no edital;

3.63.7. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo PRODERJ;

3.63.8. Em caso de reiterado inadimplemento do SLA, o CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato;

3.63.9. Durante a vigência do contrato, a CONTRATADA deverá manter preposto aceito pela Administração do CONTRATANTE para representá-la administrativamente sempre que houver necessidade.

3.64. REQUISITOS PARA ACEITAÇÃO DOS SERVIÇOS

3.64.1. A implantação da Rede IP Governo Redundante, dar-se-á por implantação de enlaces em cada sítio. Os sítios e enlaces a serem contratados serão definidos durante a assinatura do contrato;

3.64.2. Os serviços de implantação de cada enlace serão verificados individualmente, e estarão sujeitos a dois tipos de aceitação: denominados: Termo de Aceitação Provisória e Termo de Aceitação Definitiva.

3.65. Critérios para Aceitação Provisória dos serviços de implantação

3.65.1. A aceitação da implantação do enlace deverá atender os seguintes

requisitos:

3.65.1.1. A aceitação Provisória dar-se-á em até 30 (trinta) dias úteis após a entrega do serviço do sítio, com a observação do CONTRATANTE, de normalidade no provimento dos serviços para este enlace;

3.65.1.2. Para os sítios que fizerem parte do ambiente de teste, o prazo para a aceitação provisória contará a partir da data do início dos testes;

3.65.1.3. Caso haja rejeição na aceitação do serviço do sítio, o CONTRATANTE poderá solicitar a suspensão da implantação até que possíveis problemas sejam sanados, sem que isso gere direito à CONTRATADA de protelar a implantação dos demais sítios dentro dos prazos definidos;

3.65.1.4. Os testes de aceitação provisória dos serviços de rede serão compostos, no mínimo, por testes de conectividade/funcionais e testes de contingência; A aceitação ocorrerá caso os resultados dos testes estejam conforme os requisitos do projeto;

3.65.1.5. Um enlace da rede será considerado aceito nos testes de conectividade/funcionais, se:

a) O tempo de retardo da conexão estiver dentro dos limites estabelecidos no Nível Mínimo de Serviços (NMS) por um período de 2 (dois) dias úteis;

b) A taxa de erro de bit estiver dentro dos limites estabelecidos no mesmo no Nível Mínimo de Serviços (NMS), quando solicitado pelo CONTRATANTE; A transação padrão de um sistema corporativo definido pelo CONTRATANTE puder ser completada com sucesso, dentro das características da aplicação;

3.65.2. A solução de redundância para um sítio será considerada recebida provisoriamente se os testes de funcionamento e comutação forem aprovados pelo CONTRATANTE;

3.65.3. Após a execução dos testes, e verificado que o enlace implantado atende os requisitos conforme descrito nos itens anteriores, a Comissão de Recebimento do CONTRATANTE emitirá o Termo de Recebimento Provisório (TRP) do enlace contratado.

3.65.4. **Critérios para Aceitação Definitiva dos serviços de implantação**

3.65.4.1. A aceitação final se dará após o término do Período de Funcionamento Experimental (PFE), que se inicia com a emissão do TRP e se encerra após o decurso de um período completo de 10 (dez) dias corridos sem nenhuma ocorrência de erros no enlace contratado. A este período sem ocorrência de falhas, denominaremos “Período no-failures”;

3.65.4.2. Período no-failures: quando todas as pendências forem retiradas, será marcado o início de um período que se estenderá por 10 (dez) dias, no qual a solução não deverá apresentar falhas de projeto/especificação. Este período será reiniciado sucessivamente todas as vezes que for detectada alguma falha, adiando assim a conclusão do PFE;

3.65.4.3. Ao final do PFE, concluído com sucesso, será emitido o Termo de Recebimento Definitivo (TRD), pela Comissão de Recebimento do CONTRATANTE, autorizando, a partir de então o recebimento das faturas de serviço relativas a esse enlace;

3.65.4.4. A emissão do TRD não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas,

estendendo-se a necessidade de teste destas facilidades ao longo do período de garantia.

3.66. MODELO DE PRESTAÇÃO DOS SERVIÇOS

3.66.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

3.66.2. O modelo de prestação de serviços conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo CONTRATANTE, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas pró-ativamente pela CONTRATADA, por meio do serviço de gerência da rede. A prestação dos serviços englobará prazos e condições da entrega da solução, incluindo requisitos de implantação e migração da solução.

3.66.3. Os níveis mínimos de serviço contratados, apresentados nos Níveis Mínimos de Serviços (NMS) serão registrados e monitorados pela CONTRATADA e o CONTRATANTE, e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade. Essa condição será fundamento para efetuar os pagamentos previstos, durante toda a vigência do contrato.

3.66.4. **Os pagamentos serão efetuados, mensalmente, em moeda corrente nacional e em até 15 (quinze) dias úteis após apresentação das notas fiscais. Os critérios detalhados para o pagamento mensal estão definidos no Termo de Referência.**

3.67. REDE IP MÓVEL

3.67.1. LINK IP MÓVEL DE BAIXA ÓRBITA

3.67.1.1. Os links da Rede IP Móvel de Baixa Órbita poderão fazer parte da Rede IP Governo Redundante, integrando-se no equipamento SD-WAN fornecido pelo link do Lote I, ou funcionar como link de acesso normal para fins de atendimento a áreas com poucas facilidades de infraestrutura.

3.67.2. Móvel Desmontável (Transportável):

3.67.2.1. Trata-se de serviço de enlace de dados para acesso à Internet através de uso de Rede Satelital de Baixa Órbita, que deverá ter a capacidade de funcionamento na modalidade itinerante, ou seja, deverá ser desmontável e remontável em qualquer endereço do Estado do RJ, sem a necessidade de novas instalações físicas e/ou lógicas.

3.67.2.2. Se propõe a ser usado em ações fiscalizatórias, sociais, etc., que funcionem de maneira itinerante.

3.68. **ESPECIFICAÇÕES TÉCNICAS DA REDE**

3.68.1. O serviço deverá atender no mínimo às seguintes especificações técnicas:

3.68.1.1. Velocidade:

a) Download: de até 200 Mbps

b) Upload: de até 20 Mbps

3.68.1.2. Latência:

a) De até 200 ms

3.68.1.3. Cobertura:

a) Em todo o território do Estado do RJ, com foco em áreas remotas e subatendidas Acesso à Internet mesmo em velocidades de até 16km/h

3.68.1.4. Disponibilidade:

a) Acima de 97% por mês

3.68.1.5. Franquia de dados:

a) até 1 (um) Terabyte de dados, sem paralisação do serviço quando atingido o máximo da franquia, devendo a velocidade ser reduzida.

b) até 5 (cinco) Terabyte de dados, sem paralisação do serviço quando atingido o máximo da franquia, devendo a velocidade ser reduzida.

c) **até 50 (cinquenta) Terabyte de dados, sem paralisação do serviço quando atingido o máximo da franquia, devendo a velocidade ser reduzida.**

3.69. **ESPECIFICAÇÕES TÉCNICAS DO TERMINAL DE USUÁRIO**

3.69.1. O terminal a ser fornecido para uso da rede móvel transportável deverá atender, no mínimo, às seguintes especificações técnicas:

3.69.2. Antena satelital de uso fixo eventual (Starlink Standard), com as seguintes características:

a) Modelo compatível com o serviço Starlink Roam ou equivalente, com capacidade de operação em qualquer ponto com visada direta ao céu.

b) Antena do tipo motorizada (modelo circular) ou fixação manual ajustável (modelo retangular), com base de montagem removível, tipo pedestal ou tripé.

c) Capacidade de autoalinhamento com os satélites da constelação Starlink, com apontamento automático no modelo motorizado.

d) Cobertura em toda a área geográfica nacional onde houver sinal da constelação Starlink.

e) Grau de proteção ambiental IP54 ou superior.

f) Faixa de temperatura de operação entre -30 °C e +50 °C.

g) Peso máximo de 4,2 kg.

h) Consumo médio de energia de até 100W.

3.70. **Fonte e conectividade:**

3.70.1. Fonte de alimentação bivolt automática (100–240 V AC, 50/60 Hz).

3.70.2. Roteador Wi-Fi integrado compatível com padrão IEEE 802.11ac (Wi-Fi 5), com alcance de até 185 m² (modelo retangular) ou superior.

3.70.3. Cabo de alimentação e dados entre antena e fonte/roteador com comprimento mínimo de 15 metros.

3.71. **Operação e gerenciamento:**

3.71.1. Suporte a IPv6 nativamente.

3.71.2. Gerenciamento via aplicativo oficial da Starlink (iOS/Android) e interface web.

3.71.3. Possibilidade de visualizar velocidade de c**onexão, qualidade do sinal, reiniciar o terminal remotamente, realizar testes de conectividade e alterar nome/rede do Wi-Fi.**

3.72. **Instalação:**

3.72.1. O terminal deverá ser entregue com todos os acessórios de instalação: base de apoio, fonte de energia, roteador Wi-Fi, cabos e conectores.

3.72.2. A instalação poderá ser feita pelo próprio usuário sem necessidade de ferramentas especiais, devendo estar acompanhada de manual e/ou vídeo de instrução em português.

3.72.3. O conjunto deverá ser armazenável em caixa ou maleta de transporte resistente e de fácil deslocamento.

3.73. **Móvel em Movimento (On-the-Move):**

3.73.1. O serviço deverá atender no mínimo às seguintes especificações técnicas:

3.73.1.1. Velocidade:

a) Download: de até 220 Mbps

b) Upload: de até 25 Mbps

3.73.1.2. Latência:

a) De até 99 ms em condições ideais de visada e cobertura

3.73.1.3. Cobertura:

a) Em todo o território nacional, inclusive em áreas remotas, vias intermunicipais, rodovias, estradas vicinais e áreas com pouca ou nenhuma cobertura celular, com conectividade ativa durante o deslocamento em veículos terrestres, embarcações ou unidades móveis.

3.73.1.4. Disponibilidade:

a) Acima de 99% por mês, considerando operação contínua em movimento.

3.73.1.5. Franquia de dados prioritários:

a) Até 1 (um) Terabyte por mês de dados com priorização de tráfego, sem paralisação do serviço após o limite, com possível redução de

velocidade ou priorização.

b) Até 5 (cinco) Terabytes por mês de dados prioritários, conforme plano contratado.

c) Até 50 (cinquenta) Terabytes por mês de dados prioritários, conforme necessidade, podendo o serviço continuar ativo mediante políticas de controle de banda aplicadas pelo provedor.

3.74. **ESPECIFICAÇÕES TÉCNICAS DO TERMINAL DE USUÁRIO**

3.74.1. O equipamento terminal a ser fornecido para operação da rede móvel em movimento deverá atender, no mínimo, às seguintes características:

3.74.2. Antena de alto desempenho tipo plano, com as seguintes capacidades técnicas:

a) Capacidade de rastreamento dinâmico de satélites em movimento, suportando comunicação ativa enquanto o veículo estiver em deslocamento.

b) Instalação fixa sobre o teto ou estrutura de veículos, embarcações ou unidades móveis, sem necessidade de alinhamento manual.

c) Classificação de proteção ambiental mínima IP56.

d) Resistência a temperaturas de operação entre -30 °C e +50 °C.

3.75. **Interfaces e conectividade:**

3.75.1. Fonte de alimentação com entrada 100–240 V AC, bivolt automática, 50/60 Hz.

3.75.2. Compatibilidade com roteador Wi-Fi 5 ou superior, incluso no kit.

3.76. **Operação e gestão:**

3.76.1. Suporte nativo a IPv6.

3.76.2. Gerenciamento por aplicativo móvel (iOS e Android) e portal web.

3.76.3. Acesso a painéis com informações de conectividade, diagnóstico, reboot remoto e posicionamento geográfico.

3.77. **Homologação:**

3.77.1. O equipamento deverá possuir homologação válida pela ANATEL, nos termos da Resolução 242/2000.

3.78. **Instalação:**

3.78.1. A CONTRATADA deverá realizar a instalação física do terminal sobre o veículo ou estrutura designada, com os devidos suportes fixadores, cabos e fonte de alimentação.

3.78.2. A instalação deverá considerar operação ininterrupta, inclusive com fonte de energia veicular ou nobreak, conforme indicado pela CONTRATANTE.

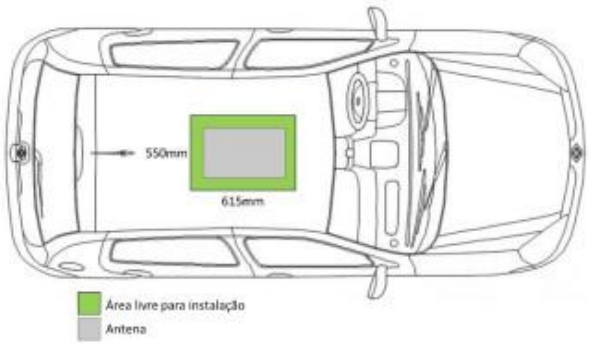
3.78.3. Considerando-se as dimensões e peso do equipamento (antena), a

instalação deverá seguir as normas previstas na Resolução Contran nº 955 de 28/03/2022 que dispõe sobre o transporte de cargas ou bicicletas nas partes externas dos veículos dos tipos automóvel, caminhonete, camioneta e utilitário.

3.78.4. A antena deverá ser fixada por parafusos em um suporte metálico compatível.

3.78.5. O suporte deve ser instalado sobre uma superfície estruturalmente sólida e horizontal, afastado de outros equipamentos.

3.78.6. O suporte deverá ser instalado de forma que a extremidade inferior esteja apontando para frente.



3.78.7. A área disponível no teto do veículo para instalação da antena será de, pelo menos, 615mm x 550mm conforme figura abaixo:

a) A fixação do suporte no teto do veículo deverá ser feita preferencialmente com super imãs magnéticos (do tipo neodímio).

b) A CONTRATADA deverá garantir que a instalação esteja devidamente ancorada de modo que não seja derrubada, lançada ou arrastada sobre a via.

c) Toda e qualquer perfuração na superfície do veículo para instalação do suporte deverá ser previamente autorizada pela CONTRATANTE.

d) Caso a perfuração da carroceria seja aprovada, a CONTRATADA deverá providenciar arruelas de vedação de borracha bem como o uso de selantes de silicone em todos os orifícios.

e) Os cabos de conexão entre a unidade externa (antena) e dos

equipamentos internos (roteador e fonte) deverão ser instalados preferencialmente sem a necessidade de quaisquer tipos de furos na carroceria do veículo.

f) Os cabos deverão estar devidamente ancorados.

3.79. DOS LOCAIS DE IMPLANTAÇÃO

3.79.1. O serviço deverá ter abrangência em todo o território do Estado RJ e Representação do Governo do Estado do RJ em Brasília.

3.79.2. Os locais de entrega e instalação serão informados pelo CONTRATANTE.

3.80. DOS REQUISITOS DE INFRAESTRUTURA

3.80.1. Os equipamentos fornecidos pela contratada deverão ser capazes de operar com a alimentação elétrica de 110V ou 220V e frequência de 60Hz;

3.80.2. A CONTRATADA será responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os Equipamentos/recursos que forem necessários (roteadores, antenas, modems, estações de gerenciamento, meios de transmissão, cabeamento WAN e LAN, acessórios necessários, dentre outros) para o provimento dos serviços. Os Equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos;

3.81. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) DA REDE IP BAIXA ÓRBITA

3.81.1. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede IP Satelital de Baixa Órbita Móvel estará operacional em um determinado período de tempo, para cada enlace contratado. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês;

3.81.2. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente;

3.81.3. Para cada sítio conectado, deverá ser garantida o Índice de Disponibilidade Mensal do Enlace (IDM) conforme abaixo:

IDM ≥ 97,00%

3.82. Prazo de Reparo (PR)

14. Nível	15. PR	16. Sítios
17. N1	18. ≤ 5 horas	19. Região Metropolitana do Estado

20. N2	21. ≤ 10 horas	22. Demais Unidades pertencentes à Região Interior do Estado

3.82.1. Para Rede IP Satelital de Baixa Órbita Móvel Itinerante o Prazo de Reparo deverá atender para os limiares abaixo.

3.83. **Prazo de Reparo (PR)**

3.84. **Prazo de Atendimento a Novos Endereços (PAN)**

3.84.1. Para Rede IP Satelital de Baixa Órbita Móvel Itinerante o prazo de Atendimento a Novos Endereços será de 75 dias;

3.84.2. As métricas apresentadas neste item servirão de base para avaliação e verificação da qualidade dos serviços prestados pela CONTRATADA.

3.85. **LINK DE DADOS Rede IP Móvel 4G/5G (FWA)**

3.85.1. Os links da Rede IP Móvel **4G/5G (FWA)** poderão fazer parte da Rede IP Governo Redundante, integrando-se no equipamento SD-WAN fornecido pelo link do Lote I, ou funcionar como link de acesso normal para fins de atendimento a áreas com poucas facilidades de infraestrutura, eventos itinerantes, etc.

3.86. **ESPECIFICAÇÕES TÉCNICAS DA REDE – LINK IP MÓVEL 4G/5G (FWA)**

3.86.1. O serviço deverá atender, no mínimo, às seguintes especificações técnicas:

3.86.1.1. Velocidade:

a) Download: de até 200 Mbps (em redes 5G) ou até 100 Mbps (em redes 4G LTE), conforme cobertura e capacidade local.

b) Upload: de até 50 Mbps (5G) ou até 20 Mbps (4G LTE), conforme cobertura.

3.86.1.2. Latência:

a) De até 100 ms em redes 5G e até 150 ms em redes 4G LTE, em condições normais de operação.

3.86.1.3. Cobertura:

a) Em todo o território do Estado do Rio de Janeiro, incluindo zonas urbanas, rurais e regiões com infraestrutura limitada de conectividade, desde que dentro da área de cobertura das operadoras móveis com tecnologia 4G ou 5G.

3.86.1.4. Disponibilidade:

a) Disponibilidade mensal mínima de 95%, considerando a natureza móvel do serviço e dependência da cobertura de rede das operadoras.

3.86.1.5. Franquia de dados:

a) Até 1 (um) Terabyte de dados por mês, sem bloqueio do serviço após atingido o limite, com redução de velocidade conforme política de gestão de tráfego da operadora.

b) Até 5 (cinco) Terabytes de dados por mês, mediante contratação

específica.

c) Até 50 (cinquenta) Terabytes de dados por mês, para planos empresariais ou governamentais de alta capacidade, conforme disponibilidade da operadora.

3.87. **ESPECIFICAÇÕES TÉCNICAS DO TERMINAL DE USUÁRIO – ROTEADOR 4G/5G (FWA)**

3.87.1. O equipamento terminal (CPE) fornecido para operação da solução FWA deverá atender, no mínimo, às seguintes especificações técnicas:

3.87.1.1. Interface de acesso à rede móvel:

a) Compatível com redes móveis 4G LTE (Cat 12 ou superior) e 5G NR Sub-6GHz (NSA ou SA), com fallback automático para 3G, quando aplicável.

b) Suporte a múltiplas bandas de frequência (multiband) usadas pelas operadoras nacionais.

c) Slot(s) para cartão SIM padrão (Nano ou Micro), com suporte a eSIM opcional.

d) Capacidade de seleção automática ou manual da operadora.

3.87.1.2. Conectividade com rede local (LAN):

a) **No mínimo 2 (duas) portas Ethernet Gigabit (RJ-45).**

b) **Interface Wi-Fi padrão IEEE 802.11ac (Wi-Fi 5) ou superior, com alcance interno mínimo de 100m².**

c) **Capacidade de criação de rede Wi-Fi isolada para convidados (Guest Network).**

3.87.1.3. Funcionalidades e recursos técnicos:

a) Função de roteamento IP nativo (NAT/DHCP) com firewall integrado.

b) Suporte a VPN pass-through (IPSec, L2TP, GRE).

c) Monitoramento de tráfego e estatísticas de uso.

d) Capacidade de fallback automático entre 5G/4G/3G sem necessidade de reinicialização.

3.87.1.4. Instalação e antenas:

a) Fornecido com antena(s) interna(s) de alto ganho e, adicionalmente, antena externa destacável ou fixa, com ganho mínimo de 5dBi para melhor recepção de sinal em áreas de cobertura crítica.

b) Cabo de extensão de antena com, no mínimo, 5 metros, quando aplicável.

c) Alimentação bivolt automática (100–240V, 50/60 Hz). Opcional: suporte a alimentação via 12V DC para operação em ambientes móveis.

3.87.1.5. Requisitos regulatórios e operacionais:

a) Equipamento homologado pela ANATEL, conforme Resolução nº 715/2019 (ou norma vigente).

b) Suporte técnico e manutenção pelo período mínimo de 60

(sessenta) meses.

c) Manual de operação em português e interface de gerenciamento acessível por navegador (GUI Web).

d) Possibilidade de bloqueio da faixa de frequência ou operadora para otimização da conectividade.

3.87.1.6. Recursos adicionais desejáveis:

a) Suporte a dual-SIM (ativo ou standby), para redundância de operadora.

b) Possibilidade de configuração remota (TR-069 ou similar).

c) Modo bridge transparente ou passthrough, se requerido pela topologia de rede.

Rio de Janeiro, na data da assinaura eletrônica.

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 13/11/2025, às 11:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 13/11/2025, às 11:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 13/11/2025, às 11:57, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 13/11/2025, às 16:38, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117848748** e o código CRC **447B1A35**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

MAPA DE RISCOS

FASE DE ANÁLISE

(X) Planejamento da Contratação e Seleção do Fornecedor

( ) Gestão do Contrato

RISCO 1			
NÃO EXECUÇÃO DOS SERVIÇOS DE MIGRAÇÃO PARA A NOVA REDE NO PRAZO ESTIPULADO DE 90 DIAS			
Probabilidade:		( ) Baixa ( ) Média (X) Alta	
Impacto:		( ) Baixa ( ) Média (X) Alta	
Id		**Dano**	
1.	Indisponibilidade na prestação de serviços e interrupção da comunicação entre os órgãos do Governo do Estado com a indisponibilidade da rede governo.		
Id		**Ação Preventiva**	**Responsável**
1.	Estudar a possibilidade de aumento do prazo estipulado		Presidência do PRODERJ
Id		**Ação de Contingência**	**Responsável**

1.	Contratar de forma emergencial a prestadora atual, visando manter a prestação de serviços e a comunicação e conectividade da rede governo	Proderj

RISCO 2			
DIFICULDADE DE INTEGRAÇÃO ENTRE REDES, CASO FORNECEDOR DIFERENTE SEJA VENCEDOR DO CERTAME			
Probabilidade:	( ) Baixa (X) Média ( ) Alta		
Impacto:	( ) Baixa (X) Média ( ) Alta		
Id		**Dano**	
1.	Maior tempo de execução das atividades e subsequentemente atraso de entrega da nova rede		
Id		**Ação Preventiva**	**Responsável**
1.	Exigir estudo técnico da empresa vencedora contemplando o projeto de migração e suas fases.		Fornecedor
Id		**Ação de Contingência**	**Responsável**
1.	Estender o contrato com a atual fornecedora, gerando mais custo para o estado		Proderj

RISCO 3
PERDA DA CAPACIDADE DE PAGAMENTO AO FORNECEDOR DEVIDO À FALTA DE ORÇAMENTO

Probabilidade:		( ) Baixa ( ) Média (X) Alta	
Impacto:		( ) Baixa ( ) Média (X) Alta	
Id		**Dano**	
1.	Possibilidade de interrupção na prestação dos serviços		
Id		**Ação Preventiva**	**Responsável**
1.	Garantir junto ao governo os recursos necessários		Direção/presidência
Id		**Ação de Contingência**	**Responsável**
1.	Negociar com fornecedores a manutenção dos serviços críticos ao menos.		Direção/presidência

RISCO 4			
PROBLEMAS DE REFRIGERAÇÃO NO DATACENTER POR CONTA DA ADIÇÃO DE EQUIPAMENTOS DE OUTRO FORNECEDOR, CASO DE FORNECEDOR DIFERENTE DO ATUAL VENÇA O CERTAME.			
Probabilidade:		( ) Baixa (X) Média ( ) Alta	
Impacto:		( ) Baixa (X) Média ( ) Alta	
Id		**Dano**	
1.	Possibilidade de interrupção na prestação dos serviços por falhas nos equipamentos por excesso de temperatura		

Id		Ação Preventiva	Responsável
1.	Instalação de novos aparelhos de ar-condicionado já adquiridos, mas ainda não instalados.		PRODERJ
Id		**Ação de Contingência**	**Responsável**
1.	Negociar com SERPRO nova localização para instalação dos equipamentos como contingência		Direção/presidência

RISCO 5			
PROBLEMAS DE DESEMPENHO DE NOVAS TECNOLOGIAS EM UMA REDE SD-WAN			
Probabilidade:	( ) Baixa (X) Média ( ) Alta		
Impacto:	( ) Baixa (X) Média ( ) Alta		
Id		**Dano**	
1.	Possibilidade de problemas de desempenho de links cujo provimento se dá através de circuitos de tecnologias alternativas (4G, ADSL, Satélite, etc).		
Id		**Ação Preventiva**	**Responsável**
1.	Executar testes prévios com estas novas tecnologias a fim de homologá-las		FORNECEDOR
Id		**Ação de Contingência**	**Responsável**

1.	Penalidades conforme edital	FORNECEDOR/PRODERJ

RISCO 6			
DIFICULDADE NA VIABILIDADE DE INSTALAÇÃO DE LINKS			
Probabilidade:		(X) Baixa ( ) Média ( ) Alta	
Impacto:		( ) Baixa (X) Média ( ) Alta	
Id		**Dano**	
1.	Possibilidade de interrupção na prestação dos serviços para órgãos		
Id		**Ação Preventiva**	**Responsável**
1.	Garantir que as informações de localidades de instalação de links esteja clara no posterior Edital, garantindo que a vencedora do certame possua viabilidade técnica para a instalação		PRODERJ
Id		**Ação de Contingência**	**Responsável**
1.	Desclassificar a atual vencedora e chamar a próxima da lista		PRODERJ

RISCO 7	
ESPECIFICAÇÃO INCORRETA OU INCOMPLETA DA SOLUÇÃO DESEJADA	
Probabilidade:	(X) Baixa ( ) Média ( ) Alta

Impacto:		( ) Baixa ( ) Média (X) Alta	
Id		**Dano**	
1.	Não atingimento do objetivo em sua completude		
Id		**Ação Preventiva**	**Responsável**
1.	Garantir que os estudos técnicos preliminares foram realizados de forma adequada e englobando todo o escopo necessário ao atingimento dos objetivos.		PRODERJ
Id		**Ação de Contingência**	**Responsável**
1.	Negociação com a contratada para atender algum item que tenha ficado de fora da especificação.		PRODERJ

RISCO 8			
MOROSIDADE NA EXECUÇÃO DO PROCESSO DE CONTRATAÇÃO			
Probabilidade:		( ) Baixa (X) Média ( ) Alta	
Impacto:		( ) Baixa ( ) Média (X) Alta	
Id		**Dano**	
1.	Extensão do pagamento da antiga fornecedora com subsequente aumento do custo do projeto		
Id		**Ação Preventiva**	**Responsável**

1.	Garantir que os estudos técnicos preliminares gerem os prazos corretos e que sejam colocadas multas pesadas a serem aplicadas ao contratado para inibir esta morosidade.	PRODERJ
Id	**Ação de Contingência**	**Responsável**
1.	Aumento dos recursos das equipes relacionadas ao processo de contratação visando obter celeridade no mesmo.	PRODERJ

RISCO 9			
AUSÊNCIA DE INTERESSADOS NA LICITAÇÃO COMO UM TODO OU EM ALGUM LOTE			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória (x) Seleção do Fornecedor ( ) Gestão do Contrato		

Id	**Dano**	
1.	Licitação deserta ou fracassada Falta do fornecimento pretendido	
Id	**Ação Preventiva**	**Responsável**
1.	Realização de pesquisa de preços ampla	Equipe de planejamento
Id	**Ação de Contingência**	**Responsável**
1.	Repetição do certame ou contratação direta, na forma do artigo 75, III, da Lei nº 14.133/2021, se o certame, justificadamente, não puder ser repetido sem prejuízo para a Administração	VPA

( ) Planejamento da Contratação e Seleção do Fornecedor

(X) Gestão do Contrato

RISCO 10			
INTERRUPÇÃO DO SERVIÇO			
Probabilidade:	(X) Baixa ( ) Média ( ) Alta		
Impacto:	( ) Baixa ( ) Média (X) Alta		
Id		**Dano**	
1.	Interrupção da conectividade da rede governo, parada de sistemas e serviços prestados ao estado e aos cidadãos.		
Id		**Ação Preventiva**	**Responsável**
1.	Garantir que os estudos técnicos preliminares gerem os prazos e garantias corretas e que sejam colocadas multas pesadas a serem aplicadas ao contratado.		PRODERJ
Id		**Ação de Contingência**	**Responsável**
1.	Contratação de links de dados em outra operadora para reestabelecer a conectividade ao menos do BackBone da rede.		PRODERJ

RISCO 11	
PREJUÍZO À SEGURANÇA DA INFORMAÇÃO	
Probabilidade:	(X) Baixa ( ) Média ( ) Alta
Impacto:	( ) Baixa ( ) Média (X) Alta

Id		Dano	
1.	Vazamento ou perda/comprometimento de dados sigilosos do Governo.		
Id		**Ação Preventiva**	**Responsável**
1.	Garantir que os estudos técnicos preliminares gerem os prazos e garantias corretas e que sejam colocadas multas pesadas a serem aplicadas ao contratado em caso de vazamento de informações sigilosas.		PRODERJ
Id		**Ação de Contingência**	**Responsável**
1.	Segregação do segmento de rede afetado e tratamento do incidente.		PRODERJ

RISCO 12			
BAIXA QUALIDADE NO SERVIÇO PRESTADO			
Probabilidade:	(X) Baixa ( ) Média ( ) Alta		
Impacto:	( ) Baixa (X) Média ( ) Alta		
Id		**Dano**	
1.	Má qualidade nos links de dados, falhas nas comunicações entre a Rede Governo.		
Id		**Ação Preventiva**	**Responsável**

1.	Garantir que os estudos técnicos preliminares gerem os requisitos e garantias corretas e que sejam colocadas multas a serem aplicadas ao contratado em caso não cumprimento contratual.	PRODERJ
Id	**Ação de Contingência**	**Responsável**
1.	Aplicação das multas previstas em contrato.	PRODERJ

Documento assinado eletronicamente por **Luís Cláudio Marinho Coelho**, **Gerente**, em 13/11/2025, às 11:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 13/11/2025, às 11:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 13/11/2025, às 11:57, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 13/11/2025, às 16:38, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117849155** e o código CRC **988256CB**.

Referência: Processo nº SEI-430002/000539/2025 SEI nº 117849155

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone: