ANEXO I

TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS PARA A PRESTAÇÃO DO SERVIÇO DE COMUNICAÇÃO MULTIMÍDIA, DO SERVIÇO DE TRÂNSITO INTERNET DO SERVIÇO DE ACESSO À INTERNET BANDA LARGA E SERVIÇO DE SD-WAN, PARA O ACORDO DE NÍVEIS DE SERVIÇOS (SLA), PARA O GERENCIAMENTO, PARA O MONITORAMENTO E PARA O FORNECIMENTO DE INFORMAÇÕES RELATIVAS À PRESTAÇÃO DOS SERVIÇOS.

(PROCESSO PD-PRC-XXXXXX)

ÍNDICE

I. INTRODUÇÃO

1.1. As Especificações Técnicas que constam no presente documento constituem o Anexo I do Contrato e devem ser atendidas para sua execução pela CONTRATADA, pela PRODESP, referida como solicitante ou como Administradora da Rede e Serviços, pelos Órgãos/Entidades Signatários, denominados OES, que integram ou vierem a integrar a Rede Intragov, referidos como solicitantes, e pelas Unidades indicadas.

1.2. Os recursos utilizados para a prestação dos serviços em acordo com o objeto do Contrato fazem parte da Rede Intragov, rede de telecomunicações constituída para propiciar a integração entre os recursos de tecnologia de informação e comunicação das Unidades, bem como sua conectividade com a Internet e com outras redes privativas para navegação e acessibilidade ao conteúdo de bases de dados de interesse público.

1.2.1. A Rede Intragov deve apresentar condições técnicas para ser integrada a outras redes de telecomunicações ou a Serviços de Valor Adicionado (SVA) que venham a ser contratados para a prestação de outros serviços aos OES.

1.3. A PRODESP exerce as funções de interveniente contratante dos serviços e de administração da Rede Intragov, sendo neste caso referida como Administradora da Rede e Serviços, devendo ser representada por empregado indicado como Administrador da Rede, enquanto a CONTRATADA deve indicar um empregado para representá-la como Gestor da Rede, visando interagir com o Administrador da Rede no exercício de suas atribuições, conforme previsto neste Contrato e em seus anexos.

1.4. Os serviços a serem prestados são o Serviço de Comunicação Multimídia (SCM), o Serviço de Trânsito Internet (STI), o Serviço de Acesso à Internet Banda Larga Fixa (SAI-BL) e o Serviço de SD-WAN (SSDWAN).

1.4.1. O Serviço de Comunicação Multimídia deve ser prestado através de Rede IP Multisserviços.

1.4.2. O Serviço de Trânsito Internet deve ser prestado com a agregação de recursos à Rede IP Multisserviços.

1.4.3. O Serviço de Acesso à Internet Banda Larga deve ser prestado por meio de acesso à Internet em Banda Larga Fixa e de CPE.

1.4.4. O Serviço de Acesso à Internet Banda Larga Itinerante deve ser prestado por meio de acesso à Internet via Satélite e de Modem.

1.4.5. O Serviço de SSDWAN deve ser prestado em conformidade com as especificações técnicas e operacionais que constam do capítulo V – Descrição do Serviço de SD-WAN, deste documento.

1.5. Para a contratação do Serviço de Trânsito Internet (STI) é obrigatória a contratação prévia do Serviço de Comunicação Multimídia (SCM), exceto na seguinte situação:

1.5.1. No caso de contratação do Serviço de Trânsito Internet para qualquer um dos endereços de instalação dos PoP 1, 2 e 3 do AS GESP, desde que este esteja em Data Center do Governo de SP.

1.6. Para a contratação do Serviço de Acesso à Internet (SAI-BL) é obrigatório a contratação do SSDWAN.

1.6.1. Na hipótese do OES já contar com um serviço SD-WAN, este fica desobrigado a contratar o SSDWAN.

1.7. A CONTRATADA deve manter a tecnologia sempre atualizada para atender aos requisitos de disponibilidade, de confiabilidade, de integridade, de segurança e de qualidade definidos para a prestação dos serviços.

1.7.1. Eventuais substituições e/ou atualizações das RFC (*Request for Comments*) e de segurança constantes neste documento de especificação técnica devem ser observadas pela CONTRATADA visando a manutenção desses requisitos e a continuidade na prestação dos serviços.

1.8. A prestação dos serviços pode vir a ser objeto de avaliação visando garantir a manutenção dos requisitos e a continuidade na prestação dos serviços, em consonância com os critérios e condições descritas a seguir:

1.8.1. A avaliação será feita pela Administradora da Rede e Serviços em conjunto com a CONTRATADA, a qualquer tempo, de forma remota ou nas dependências da CONTRATADA, por iniciativa da Administradora da Rede e Serviços ou de qualquer OES que a solicite.

1.8.2. A decisão de efetuar a avaliação deve ser comunicada à CONTRATADA, via correspondência oficial, com antecedência de 5 (cinco) dias corridos, na qual devem constar o motivo e o objeto da avaliação.

1.8.3. A CONTRATADA deve disponibilizar todas as informações e os meios necessários, bem como cooperar para o bom andamento das atividades inerentes a esta avaliação.

1.8.4. No decorrer da avaliação, serão realizados diagnósticos e estabelecidas ações com prazos para a solução das questões levantadas.

1.8.5. A divulgação dos resultados deve ser feita através de relatório validado pelos avaliadores, pelo Administrador da Rede e pelo Gestor da Rede.

1.9. Os serviços devem ser prestados em todos os municípios do território do Estado de São Paulo e em Brasília-DF.

1.10. O SCM e o STI devem ser prestados em conformidade com as especificações técnicas e operacionais que constam dos capítulos II – Descrição do Serviço de Comunicação Multimídia, e III – Descrição do Serviço de Trânsito Internet, deste documento.

1.11. O SAI-BL e o SAI-BLI devem ser prestados em conformidade com as especificações técnicas e operacionais que constam do capítulo IV– Descrição do Serviço de Acesso à Internet Banda Larga, deste documento.

1.12. O SSDWAN deve ser prestado em conformidade com as especificações técnicas e operacionais que constam do capítulo V – Descrição do Serviço de SD-WAN, deste documento.

1.13. Os serviços devem ser prestados em conformidade com indicadores de desempenho técnico-operacional que constam do capítulo VI- Acordo de Níveis de Serviços (SLA), deste documento.

1.14. As redes, os serviços e os recursos a eles agregados devem ser gerenciados em conformidade com as especificações técnicas e operacionais que constam do capítulo VII – Gerenciamento, deste documento.

1.15. As redes, os serviços e os recursos a eles agregados são objeto de monitoramento, por parte da Administradora da Rede e Serviços, em conformidade com as especificações técnicas e operacionais que constam do capítulo VIII – Monitoramento, deste documento.

1.16. A CONTRATADA deve fornecer as informações relativas à prestação dos serviços especificados neste documento, em conformidade com as especificações técnicas e operacionais que constam do capítulo IX – Fornecimento de Informações, deste documento.

1.17. O Acordo Operacional, firmado entre a CONTRATADA e a PRODESP nos termos do capítulo correspondente no Contrato, estabelece os procedimentos operacionais e administrativos associados à prestação dos serviços a serem observados pela CONTRATADA, pela PRODESP, pelos OES e pelas Unidades indicadas, com o suporte do Sistema de Apoio Operacional e Gestão (SAOG) da PRODESP.

1.17.1. A CONTRATADA deve adicionalmente atender solicitações sobre incidente na prestação dos serviços, conforme disposto no Acordo Operacional, através de telefone com número 0800, disponível durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

Definição dos Lotes

1.18. Está indicado na tabela a seguir a descrição do lote e os respectivos serviços.

Lote	Serviços
Lote 1	SCM e STI
Lote 2	SAI-BL e SAI-BLI
Lote 3	SSDWAN

1.19. Este termo de referência é comum a todos os lotes, cujos serviços e seus requisitos encontram-se respectivamente discriminados de acordo com o título de cada seção do documento.

1.20. Quando não houver indicação do lote no título da seção, o requisito deverá ser considerado comum a todos os lotes.

1.21. Devido a interdependência e a necessidade de integração técnica e operacional entre todos os serviços especificados no presente termo de referência, recomenda-se a leitura e o conhecimento integral de todo seu conteúdo, ainda que a responsabilidade da CONTRATADA seja delimitada pelo respectivo serviço que vier a prestar à PRODESP e aos órgãos partícipes da Rede INTRAGOV.

Parcelamento da solução de TIC

1.22. A estratégia de divisão da contratação dos serviços para a Rede INTRAGOV em lotes para este projeto foi precedida por uma análise equilibrada entre os benefícios esperados e os desafios potenciais que surgem desse modelo de licitação.

1.23. Segmentar a contratação em lotes é uma estratégia que visa estimular a ampla participação de empresas de diferentes portes e especialidades, atuantes no setor de tecnologia da informação e comunicação, resultando em propostas mais competitivas e, possivelmente, em preços de serviços mais vantajosos para a administração pública estadual.

1.24. Está estratégia exclui a dependência de uma única empresa, possibilitando uma gestão de riscos mais eficaz. Caso surjam problemas com o fornecedor de um lote específico, as demais partes do projeto podem prosseguir com menores impactos em comparação com um único fornecedor, garantindo a continuidade e a conclusão bem-sucedida do projeto.

1.25. Essa abordagem também favorece a inovação, pois permite que empresas especializadas concentrem seus esforços em áreas específicas do projeto, resultando em soluções inovadoras e mais eficientes. A competição entre fornecedores especializados estimula a busca por práticas e tecnologias de ponta, beneficiando o desenvolvimento do projeto como um todo.

1.26. Outro aspecto relevante para a decisão de se repartir a contratação em lotes é a possibilidade de adaptar-se melhor à dinâmica do mercado. Isso permite ajustar a estrutura da licitação conforme as características e capacidades dos fornecedores disponíveis, contribuindo para uma seleção mais alinhada às necessidades do projeto. No contexto atual, onde existe uma concentração no mercado de telecomunicações (conforme dados da Anatel de setembro de 2023, mais de 60% dos acessos Banda Larga no Estado de São Paulo são providos por duas das maiores empresas Operadoras de Telecom no Brasil), a licitação em um único lote restringiria a competitividade, o que não é salutar em um processo licitatório.

1.27. Em uma análise isenta, é crucial reconhecer que tal abordagem não está livre de desafios. Um dos principais desafios enfrentados ao dividir a contratação em lotes surge na necessidade de uma coordenação técnica e operacional eficiente entre todos as empresas contratadas para a prestação dos serviços. A integração harmoniosa dos diferentes escopos de cada lote é complexa, exigindo uma gestão diligente para assegurar a prestação coesa do serviço de forma global, traduzindo-se numa prestação de serviços públicos aos cidadãos com maior eficiência e com custos otimizados.

1.28. Outro desafio considerado foi a possibilidade de haver uma redundância de esforços administrativos, uma vez que cada lote implica em contratos e acordos operacionais individuais, gestão e monitoramento separado. Este aumento na complexidade administrativa pode resultar em custos indiretos adicionais, contrapondo, em parte, a economia de custo alcançada pela divisão em lotes.

1.29. A aglutinação dos objetos em um único lote, sem a devida justificativa técnica, evidência de sua vantajosidade e garantia de um ambiente em que ocorra uma ampla concorrência contraria o posicionamento do Tribunal de Contas do Estado de São Paulo, conforme podemos observar do texto extraído do Manual básico (Licitações e contratos Principais aspectos da fase preparatória) do TCE e de uma decisão do próprio TCE que ratifica esse posicionamento.

> ***"TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO***
>
> ***MANUAL BÁSICO***
>
> ***Licitações e contratos Principais aspectos da fase preparatória***
>
> ***Problema da aglutinação: impede-se a participação, na licitação, de empresas capazes de atender a um dos objetos pretendidos, talvez com preços bastante competitivos. Em relação à divisão do objeto em lotes, tratando-se de produtos díspares, de naturezas diversas e comercializados por empresas que atuam em diferentes segmentos de mercado, este E. Tribunal tem determinado a segregação destes produtos em lotes distintos para que seja ampliado o espectro de possíveis fornecedores em potencial e, consequentemente, elevadas as perspectivas de obtenção da proposta mais vantajosa ao interesse público, com melhor atenção ao princípio da isonomia."***
>
> ***"TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO***
>
> ***Processo: TC-019319.989.23-2.***
>
> ***"Início pela questão considerada procedente pela unanimidade dos órgãos desta Corte, qual seja, a indevida aglutinação do objeto em um único lote, uma vez que, embora guardem relação de pertinência entre si, as atividades pertencem a ramos distintos de mercado, situação agravada pela vedação de participação de empresas reunidas em consórcio e de subcontratação, evidenciando um afunilamento do universo competitivo."***

1.30. Portanto, a estratégia da repartição em lotes, precedida por uma análise equilibrada entre os benefícios esperados e os desafios potenciais, surgiu como uma estratégia flexível e eficaz, ao mesmo tempo em que há o reconhecimento que uma gestão eficaz desses desafios é crucial para assegurar o sucesso do projeto, maximizando os ganhos decorrentes da competição, inovação e adaptação ao mercado, ao mesmo tempo em que minimiza os riscos associados à abordagem da realização do certame por lotes, de forma a garantir uma contratação mais eficiente e alinhada aos objetivos do Governo do Estado de São Paulo.

Estratégia da licitação em lotes

1.31. Com o intuito de afastar o risco mencionado no item 1.24 do presente termo de referência a licitação será dividida em três lotes, conforme tabela apresentada no item 1.18, facultando-se aos licitantes participarem em qualquer um dos lotes, porém, um licitante poderá vencer somente um lote.

1.32. Os lotes serão licitados individualmente, o vencedor do primeiro lote não participará dos pregões subsequentes e assim sucessivamente (vencedor do lote 2 não poderá participar do lote 3). Essa medida tem como objetivo evitar imbróglio com o processo licitatório, mediante o fornecimento de lances por parte de licitante que não poderá vencer o pregão.

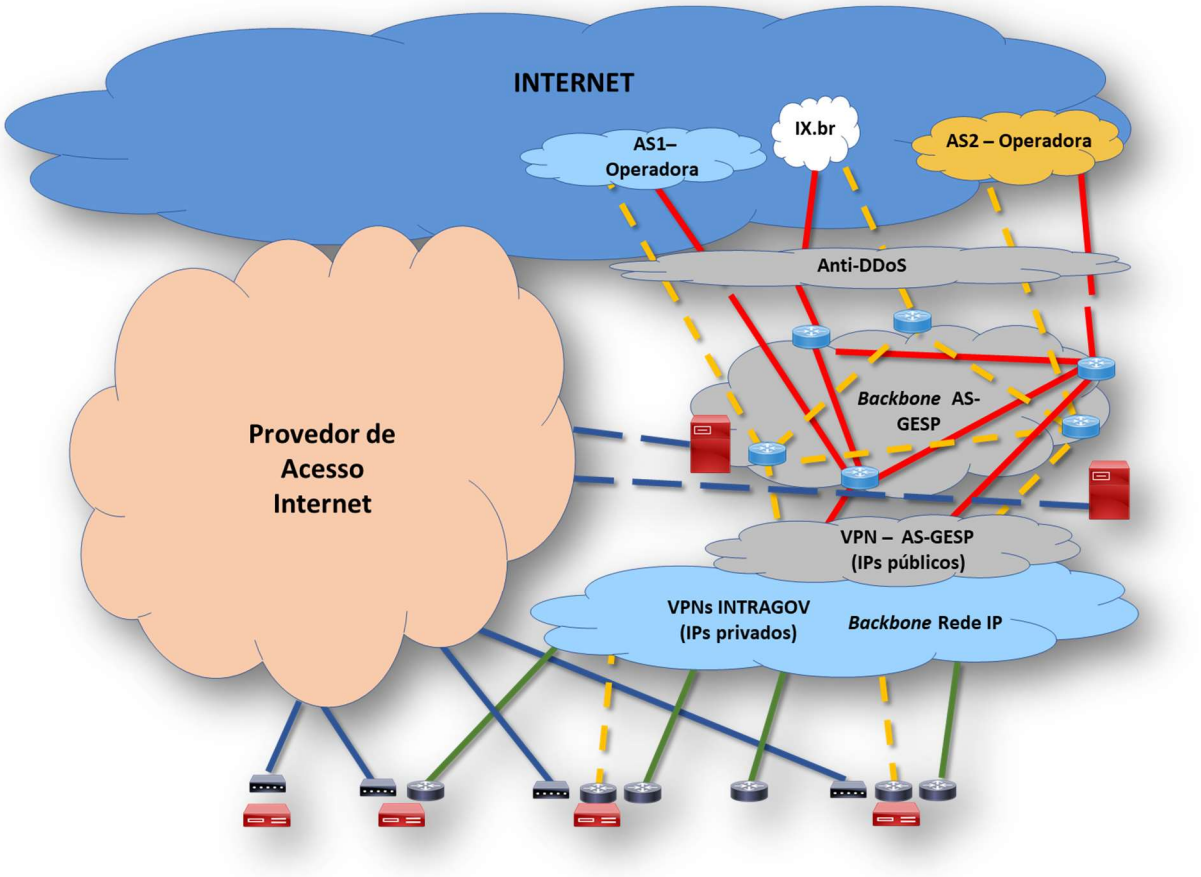
1.33. Para evitar que o licitante vencedor do pregão do lote 1 e que porventura seja desclassificado na fase de habilitação, não participe das licitações dos lotes 2 e 3, o pregão dos lote subsequente somente ocorrerá após a fase de habilitação do pregão anterior.

1.34. Para efeitos de participação nesse processo licitatório, no que concerne as regras estabelecidas no item, 1.31 e 1.32, serão consideradas a mesma pessoa jurídica empresas pertencentes ao mesmo grupo econômico ou empresarial.

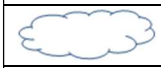
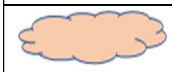
1.34.1. São consideradas empresas pertencentes ao mesmo grupo econômico ou empresarial, aquelas empresas controladas ou controladoras da licitante, filiais ou subsidiárias, ou que tenha pelo menos uma pessoa física ou jurídica que seja sócia ou possua vínculo com a licitante.

1.35. A figura abaixo representa a topologia das comunicações entre as unidades cliente e provedoras, considerando as infraestruturas a serem providas para a prestação dos serviços: SCM, STI, SAI-BL e SSDWAN.

1.36. A solução SD-WAN a ser proposta deve se integrar à diferentes Provedores de Acesso à Internet Banda Larga (representados pela nuvem de nome “Provedor de Acesso Internet”) e às VPNs IP/MPLS Intragov (representadas pela nuvem de nome “VPNs INTRAGOV” na figura abaixo).



	Acesso principal: AS GESP: 200 Gbps por enlace
	Acesso Internet dedicado simétrico
	Acesso redundante: mesmas capacidades dos enlaces primários
	Acessos SCM
	Acessos SAI-BL
	Ambiente da Operadora

	Ambiente de Governo
	Contingência de Operadora para a Internet
	Ponto de troca de tráfego metropolitano
	Provedor de Acesso Internet Banda Larga
	CPE do SCM
	CPE do SAI-BL
	Roteadores de borda
	Dispositivo SD-WAN Central (PoP 1 e PoP 2)
	Dispositivo SD-WAN Remoto

1.37. Os dispositivos SD-WAN devem ser instalados nas unidades cliente (UC) e nas unidades provedoras (UP) interconectando-se aos equipamentos de borda dos prestadores de serviço de Internet Banda Larga e das VPNs MPLS, conforme ilustrado na parte mais inferior da figura.

1.37.1. Entende-se por Unidade o ambiente de rede local (LAN), única ou segmentada, com recursos de tecnologia de informação e comunicação.

1.37.2. Entende-se por Unidade Provedora (UP) a Unidade em que prevalece o interesse de oferecer informação para a Rede Intragov ou para terceiros.

1.37.3. Entende-se por Unidade Cliente (UC) a Unidade em que prevalece o interesse de buscar informação na Rede Intragov ou fora dela.

1.38. Os dispositivos SD-WAN devem ser dimensionados para comunicação com pelo menos dois enlaces de comunicação (sendo um de Internet banda larga e um MPLS).

1.39. A solução SD-WAN deve ser escalável para permitir a inclusão de novas unidades, conforme a necessidade.

1.40. Para cada OES, considerando as unidades provedoras e clientes, a solução SD-WAN deve permitir a configuração de diferentes topologias como *hub-and-spoke*, *partial-mesh* e *full-mesh*.

1.41. A solução SD-WAN deve dar suporte aos modelos *overlay* de conectividade *full-mesh, partial-mesh* e *hub-and-spoke*.

1.41.1. Entende-se por *full-mesh* o modelo do tipo multiponto-multiponto em que qualquer Unidade (UP ou UC) associada a um grupo de unidades tem conectividade com qualquer outra Unidade (UP ou UC) do mesmo grupo.

1.41.2. Entende-se por *partial-mesh* o modelo do tipo multiponto-multiponto em que determinadas Unidades (UP ou UC) associadas a um grupo de unidades possuem conectividade com determinadas Unidades (UP ou UC) do mesmo grupo.

1.41.3. Entende-se por *hub-and-spoke* o modelo do tipo multiponto-ponto em que qualquer UC associada a um grupo de unidades só possui conectividade com a UP do mesmo grupo.

1.42. O modelo de conectividade *full-mesh* pode ser utilizado para a prestação da rede *overlay* SD-WAN nas modalidades *multicast, anycast* ou *unicast*, e o modelo *hub-and-spoke* somente para a prestação da rede na modalidade *unicast*.

1.43. A solução deve permitir a comunicação indireta entre unidades de uma mesma instância através de uma topologia *hub-and-spoke*.

1.44. A topologia de cada órgão será definida em fase de projeto, após a assinatura do contrato, conforme o interesse de tráfego de cada instituição.

1.45. Os dispositivos SD-WAN alocados nas UPs (Centrais) serão interligados entre si em *full-mesh* conforme definição da Administradora da Rede e Serviços.

1.46. A solução deve prever a funcionalidade de concentrador para roteamento, disponibilizando a comunicação entre as Unidades totalmente migradas para o SD-WAN, parcialmente migradas para o SD-WAN e não migradas para o SD-WAN conforme item 5.1.32.

1.47. A solução deve ser escalável para permitir a agregação de enlaces de banda larga disponibilizados pelo OES, sendo permitida a alteração da prestação do serviço, caso seja necessário um dispositivo SD-WAN com capacidade superior ou que suporte um maior número de interfaces WAN.

1.48. Para a execução dos procedimentos operacionais e administrativos associados à prestação dos serviços, a CONTRATADA, a Administradora da Rede e Serviços e os OES devem utilizar o Sistema de Apoio Operacional e Gestão (SAOG), ferramenta desenvolvida pela PRODESP.

1.49. Deve ser atribuído a cada serviço contratado e a recursos utilizados na prestação do serviço, um código de identificação (ID) a ser utilizado como referência nos procedimentos de relacionamento entre a CONTRATADA, OES e Administradora da Rede e Serviços, e estabelecidos no Acordo Operacional.

1.50. O SAOG será utilizado para suporte, no mínimo, aos seguintes processos:

1.50.1. Atendimento a Solicitações de Serviços.

1.50.2. Registro e acompanhamento de Incidentes.

1.50.3. Gestão do SLA.

1.50.4. Gestão de Conectividade na Rede.

1.50.5. Monitoramento da Rede.

1.50.6. Desempenho dos ID.

1.51. Cabe à Administradora da Rede e Serviços a apuração dos indicadores de SLA previstos no Contrato, com base nas informações registradas no SAOG e fornecidas pela CONTRATADA.

1.52. A CONTRATADA deve fazer uso do SAOG como usuária em interface web disponibilizada pela PRODESP e/ou por meio de troca eletrônica de informações via API.

1.53. Caso seja adotada a troca eletrônica de informações entre a PRODESP e a CONTRATADA, a CONTRATADA deve prover e manter toda a infraestrutura dedicada para enviar e receber informações relativas à prestação dos serviços de/para o SAOG.

1.53.1. Uma das terminações do circuito de comunicação deve ser instalada e mantida na PRODESP em Taboão da Serra – SP.

1.53.2. Eventuais falhas nessa comunicação não eximem a CONTRATADA do cumprimento dos indicadores de SLA pertinentes, dado que o SAOG é a ferramenta oficial para o processo de Gestão do SLA, sendo a CONTRATADA usuária compulsória desse sistema.

1.53.3. O SAOG disponibiliza informações relativas à prestação dos serviços para a CONTRATADA de forma automática, não havendo responsabilidade por parte da PRODESP pela validação e sincronização dessas informações com as bases de dados da CONTRATADA.

1.53.4. A troca de mensagens entre o SAOG e os sistemas da CONTRATADA deve se basear em API do SAOG, utilizando o protocolo de rede HTTP (*Hypertext Transfer Protocol*).

II. DESCRIÇÃO DO SERVIÇO DE COMUNICAÇÃO MULTIMÍDIA (Lote 1)

Prestação do Serviço de Comunicação Multimídia

2.1. O Serviço de Comunicação Multimídia (SCM) consiste na oferta de capacidade de transmissão, emissão e recepção, de modo simétrico, de informações multimídia, na forma de pacotes IP, na modalidade *unicast*, na modalidade *multicast* e na modalidade *anycast*, atendendo os requisitos das classes de serviço, entre as Unidades, tanto Cliente (UC) quanto Provedora (UP), participantes da Rede Intragov, ou entre essas Unidades e a Internet, por meio do Serviço de Trânsito Internet (STI).

2.2. O SCM deve ser prestado em conformidade com a regulamentação aplicável, aprovada pela ANATEL, e o previsto no Contrato, em especial atendendo às metas de qualidade da prestação dos serviços relacionadas aos indicadores de desempenho técnico-operacional do Acordo de Níveis de Serviços (SLA).

2.3. A prestação do SCM deve ser feita em protocolo IP desde a porta LAN, inclusive, do CPE da unidade de origem até a porta LAN, inclusive, do CPE da unidade de destino do tráfego, na modalidade fim a fim entre Unidades, tanto UP quanto UC, através da Rede IP Multisserviços.

2.4. O SCM deve ser prestado com isolamento de tráfego IP entre as redes locais das Unidades (UP ou UC) de forma segura, com uso da técnica de tunelamento, através da configuração de múltiplas VPN (Rede Virtual Privada) sobre a plataforma IP-MPLS do *backbone* da Rede IP Multisserviços.

2.4.1. A Rede IP Multisserviços deve dar suporte a quantidade ilimitada de VPN.

2.5. A prestação do SCM na modalidade *unicast* consiste na transmissão de pacotes IP por uma unidade de origem (UP ou UC) e em sua recepção pela unidade de destino (UP ou UC).

2.6. A prestação do SCM nas modalidades *unicast* e *multicast* deve permitir tráfego baseado no *Internet Protocol*, tanto na versão 4 (IPv4) quanto na versão 6 (IPv6) *Dual Stack*.

2.6.1. A prestação do SCM na modalidade *anycast* deve permitir o tráfego baseado no *Internet Protocol* versão 6 (IPv6).

2.7. O SCM deve dar suporte ao encaminhamento de tráfego *unicast* destinado a uma UP principal para a sua respectiva UP redundante, no modelo de *site backup*, visando atender às necessidades de alta disponibilidade.

2.7.1. No *backbone* da Rede IP Multisserviços devem ser definidas prioridades nas divulgações das rotas IPv4 de modo que a prioridade maior seja da UP principal e a menor da UP redundante.

2.7.2. Na eventual indisponibilidade do SCM da UP principal, o tráfego destinado a ela deve ser comutado automaticamente ou manualmente, a critério do OES, para o SCM da UP redundante, devendo retornar para o SCM da UP principal, também de forma automática ou manualmente, a critério do OES, quando do seu restabelecimento.

2.7.3. No caso do IPv6, o *backbone* da Rede IP Multisserviços deve suportar o recurso *anycast* para o modelo de *site backup*.

2.7.4. Cabe à Administradora da Rede e Serviços definir as UP que devem ser configuradas como principal e como redundante, conforme disposto no Acordo Operacional.

2.8. A prestação do SCM na modalidade *multicast* consiste na transmissão de pacotes IP por uma Unidade (UP ou UC) geradora, decorrente de uma requisição feita por uma Unidade (UP ou UC) receptora, e na multiplicação e distribuição dos pacotes IP pela Rede IP Multisserviços para todas as Unidades (UP ou UC) receptoras, pertencentes a uma mesma VPN.

2.9. A prestação do SCM na modalidade *multicast* deve ser feita de modo que qualquer host *multicast* possa estabelecer uma sessão *multicast* com qualquer outro host *multicast*, cujas Unidades participam da mesma VPN.

2.9.1. Entende-se por host *multicast* a estação de geração ou recepção instalada na rede local da Unidade (UP ou UC), a qual está habilitada a estabelecer, controlar e a encerrar uma sessão *multicast*.

2.9.2. Entende-se por sessão *multicast* a conexão lógica entre *hosts multicast* estabelecida na Rede IP Multisserviços.

2.10. A prestação do SCM na modalidade *multicast* deve permitir a alternância da função de geração entre os *hosts multicast* participantes de uma mesma sessão *multicast*.

2.11. A prestação do SCM na modalidade *multicast* deve permitir que distintos *hosts multicast* instalados em uma Unidade (UP ou UC) possam estabelecer diferentes sessões *multicast* simultaneamente.

2.12. A prestação do SCM na modalidade *anycast* consiste na transmissão de pacotes IPv6 por uma Unidade de origem (UP ou UC) e em sua recepção por uma única UP de destino participante de um grupo de potenciais UP receptoras, as quais são identificadas pelo mesmo endereço IPv6 de destino, sendo, neste caso, Unidades de origem e destino pertencentes a uma mesma VPN.

2.13. O SCM deve dar suporte ao modelo de conectividade *full-mesh* e ao modelo de conectividade *hub-and-spoke*.

2.14. O modelo de conectividade *full-mesh* pode ser utilizado para a prestação do SCM nas modalidades *multicast, anycast* ou *unicast*, e o modelo *hub-and-spoke* somente para a prestação do SCM na modalidade *unicast*.

2.15. Quando solicitado pela Administradora da Rede e Serviços, a CONTRATADA deve habilitar a troca de tabela de rotas entre CPE e PE, por meio de protocolos de roteamento dinâmico.

2.16. O SCM deve ser prestado em conformidade com 5 (cinco) classes de serviço (CoS), cujas características são apresentadas na tabela a seguir:

CLASSES DE SERVIÇO (CoS)	CARACTERÍSTICAS
TEMPO REAL – VOZ	Tráfego de aplicação de voz interativa, sensível a retardo (*delay*), a variações de retardo da rede (*jitter*) e a perda de pacotes que requer priorização de pacotes e reserva de banda.
TEMPO REAL - VÍDEO	Tráfego de aplicação de vídeo interativo e videomonitoramento, sensível a retardo (*delay*), a variações de retardo da rede (*jitter*) e a perda de pacotes, que requer priorização de pacotes e reserva de banda.
MISSÃO CRÍTICA	Tráfego de aplicações interativas, de caráter crítico para o negócio, e de sinalização de voz e vídeo, sensível a retardo (*delay*) e perda de pacotes e que requer priorização de pacotes e reserva de banda.
SUPORTE À NEGÓCIO	Tráfego de aplicações não interativas, importante para o atendimento ao negócio, que requer entrega garantida, priorização de pacotes e reserva de banda.
PADRÃO	Tráfego de aplicações diversas com menor garantia de entrega, que não requer priorização de pacotes nem reserva de banda.

2.17. A prestação do SCM deve ser feita atendendo aos parâmetros de Qualidade de Serviço (QoS) correspondentes a cada classe de serviço que constam na tabela a seguir:

CLASSES DE SERVIÇO (CoS)	PARÂMETROS DE QoS
TEMPO REAL - VOZ	Latência < = 140 ms (terrestre) Latência < = 700 ms (satélite) *Jitter* < = 30 ms (terrestre) *Jitter* < = 30 ms (satélite) Perda de pacotes < = 0,1 % (terrestre) Perda de pacotes < = 1,0 % (satélite)
TEMPO REAL – VÍDEO	Latência < = 160 ms Latência < = 700 ms (somente para interações não interativas por satélite) *Jitter* < = 30 ms Perda de pacotes < = 0,1 %
MISSÃO CRÍTICA	Latência < = 200 ms Latência < = 750 ms (somente para sinalização de voz por satélite) Perda de pacotes < = 0,5 %
SUPORTE À NEGÓCIO	Latência < = 200 ms Perda de pacotes < = 1,0 %
PADRÃO	Latência < = 300 ms (terrestre) Latência < = 850 ms (satélite) Perda de pacotes < = 2,0 %

2.17.1. Entende-se por latência o período total de tempo, expresso em milissegundos, para transportar um pacote IP de um CPE de origem até um CPE de destino na Rede IP Multisserviços e transportar o respectivo pacote de resposta até o CPE de origem.

2.17.2. Entende-se por *jitter* ou variação do atraso, expresso em milissegundos, a variação máxima de retardo entre pacotes IP sucessivos de um fluxo de pacotes transportados pela Rede IP Multisserviços entre o CPE de origem e o CPE de destino.

2.17.3. Entende-se por perda de pacotes, expresso em percentagem, a quantidade de pacotes IP não recebidos no CPE de destino em relação ao total de pacotes enviados pelo CPE de origem.

2.17.4. A critério do OES, o SCM com capacidade nominal igual ou inferior a 256 kbps pode ser provido em classe de serviço única e com latência de até 800 ms.

2.18. Para fins de aceite da implantação da solução a CONTRATADA deve realizar testes de integração entre o SCM, STI, SAI-BL e SSDWAN.

Configuração das Redes Virtuais Privadas (VPN)

2.19. Cada VPN configurada no *backbone* da Rede IP Multisserviços se constitui no elemento de conectividade de um conjunto de UC e, normalmente, uma UP ou, excepcionalmente, mais de uma UP.

2.20. Uma Unidade (UP ou UC) pode estar associada a apenas uma VPN para cada SCM.

Requisitos Operacionais e Técnicos da Rede IP Multisserviços

2.21. A Rede IP Multisserviços deve ser constituída por *backbone* e por redes de acessos que, em conjunto, oferecem conectividade IP fim a fim entre os ambientes de redes locais (LAN) das Unidades (UP ou UC).

2.22. A rede de acesso da Rede IP Multisserviços é o segmento de rede de telecomunicações que interliga a rede local de uma Unidade (UP ou UC) ao *backbone* da Rede IP Multisserviços.

2.23. A rede de acesso é constituída por CPE (*Customer Premises Equipment*) e por enlaces de comunicação projetados para atender aos requisitos técnicos da prestação dos serviços para a Unidade (UP ou UC).

2.23.1. O detalhamento da configuração é abordado no Acordo Operacional.

2.24. O *backbone* da Rede IP Multisserviços é o segmento de rede de telecomunicações responsável pela conectividade IP entre as redes de acesso com aplicação da tecnologia MPLS.

2.24.1. O *backbone* é constituído por equipamentos e por enlaces de comunicação projetados para atender às necessidades técnicas da prestação dos serviços pela Rede IP Multisserviços.

2.24.2. Os pontos de presença (PoP) do *backbone* utilizados para agregação da rede de acesso ao *backbone* são denominados de PE (*Provider Edge*).

2.24.3. O *backbone* da Rede IP Multisserviços deve possuir redundância automática, sendo cada PE interligado a pelo menos dois roteadores do *backbone*.

2.25. Devido a necessidade de integração da Rede IP Multisserviços com a infraestrutura do AS-GESP, a CONTRATADA deve instalar os PE do *backbone* da Rede IP Multisserviços nos respectivos *sites* do PoP 1 e PoP2 do AS-GESP, com dupla abordagem na interligação com os outros PoP do *backbone* e com exclusividade de uso para a Rede Intragov.

2.25.1. As interligações do PE ao BGP do AS-GESP e aos Concentradores SD-WAN devem ser em conexão local e em alta disponibilidade conforme topologia de referência apresentada no item 3.28.

2.25.2. Os projetos de interligação física e lógica da UP PRODESP e da UP SEFAZ à Rede IP Multisserviços devem ser feitos atendendo ao disposto no Plano de Transição.

2.26. A Rede IP Multisserviços deve ser mantida em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

2.27. A Rede IP Multisserviços deve ser dimensionada, anualmente, para a prestação do SCM na modalidade *multicast*, conforme disposto nos subitens que seguem.

2.27.1. Permitir a participação de hosts *multicast* dentro do limite estabelecido na tabela a seguir:

ANO	1º	2º	3º	4º	5º
HOSTS MULTICAST	4000	5000	6000	7000	8000

2.27.2. Atender, no mínimo, por VPN, à quantidade de sessões *multicast* simultâneas estabelecidas na tabela a seguir:

ANO	1º	2º	3º	4º	5º
SESSÕES MULTICAST SIMULTÂNEAS POR VPN	6	7	8	9	10

2.28. A Rede IP Multisserviços deve dar suporte para roteamento e transporte de pacotes IP em endereço IP privado ou endereço IP público, na versão IPv4 e na versão IPv6 *Dual Stack*, conforme recomendações das RFC 791 (*Internet Protocol Version 4 Specification*) e as atualizações pelas RFC 2474 , RFC 6864, RFC 6890 (*Special-Use IP Address Registries*) e atualizada pela RFC 8190, RFC 2460 (*Internet Protocol Version 6 Specification*), RFC 4291 (*Internet Protocol Version 6 Addressing Architecture*) e as atualizações pelas RFC 5952 , RFC 6052 , RFC 7136 , RFC 7346 , RFC 7371 , RFC 8064 e definições complementares da IANA (*Internet Assigned Numbers Authority*).

2.28.1. Para a prestação do SCM devem ser utilizados endereços IP privado e endereços IP público dos planos de endereçamento IP do Governo do Estado de São Paulo, sendo que o controle da distribuição dos referidos endereços IP é de responsabilidade da Administradora da Rede e Serviços.

2.28.2. Caso seja necessária a utilização de ambos os endereços para uma Unidade (UP ou UC), devem ser instalados dois SCM distintos, sendo um deles configurado com endereço IP privado e o outro configurado com endereço IP público.

2.28.3. A Rede IP Multisserviços deve dar suporte para o roteamento e para o transporte de pacotes IP gerados pela Unidade (UP ou UC) na versão IPv6.

2.28.4. Os serviços necessários para a plena operação da Rede IP Multisserviços, tais como gerenciamento, monitoramento e segurança, devem ser habilitados para IPv6.

2.28.5. Recomendações que devem ser suportadas no protocolo IPv6, RFC 4443 ICMPv6 (*Internet Control Message Protocol for the IPv6 Internet Protocol Version 6 Specification*) e atualizada pela RFC 4884, RFC 4861 NDP (*Neighbor Discovery for IP version 6*) e as atualizações pelas RFC 5942 , RFC 6980 , RFC 7048, RFC 7527 , RFC 7559 , RFC 8028 , RFC 8319 , RFC 8425, RFC 9131, RFC 5175 (*IPv6 Router Advertisement Flags Option*), RFC 4862 SLAAC (*IPv6 Stateless Address Autoconfiguration*) e atualizada pela RFC 7527, RFC 3315 DHCPv6 (*Dynamic Host Configuration Protocol for IPv6*) e as atualizações pelas RFC 4361, RFC 5494, RFC 6221, RFC 6422, RFC 6644, RFC 7083, RFC 7227, RFC 7283, RFC 7550.

2.29. A Rede IP Multisserviços deve ser isolada logicamente de outras redes de telecomunicações, privadas ou públicas, que tenham recursos físicos compartilhados com a Rede IP Multisserviços, de forma a manter a confidencialidade e a integridade das informações quando do transporte dos pacotes IP, durante o trajeto entre a origem e o destino.

2.30. A Rede IP Multisserviços deve ser dotada de funcionalidades do tipo "*Port Security e Broadcast/Multicast Storm Control*" consistente com o alto grau de disponibilidade requerido.

2.31. A rede de acesso (conexão CPE-PE) deve ser protegida de tráfego com endereço IP de origem forjado (IP *spoofing*) nos dois sentidos, utilizando os recursos uRPF (*unicast Reverse Path Forwarding*), lista de controle de acesso (*Access Control List* - ACL) ou outro com resultado equivalente.

2.32. A Rede IP Multisserviços deve utilizar a tecnologia IP VPN MPLS conforme definido nas RFC 4364 (BGP/MPLS VPNs) e as atualizações pelas RFC 4577, RFC 4684, RFC 5462, RFC 2983 (*Differentiated Services and Tunnels*), RFC 3031 (*Multiprotocol Label Switching Architecture*) e as atualizações pelas RFC 6178 , RFC 6790, visando à gestão da engenharia de tráfego para atendimento aos requisitos técnicos definidos para a prestação dos Serviços.

2.33. A Rede IP Multisserviços deve ser dotada de mecanismos para controle de tráfego, inibição de congestionamento e técnicas de enfileiramento para atendimento aos parâmetros de QoS correspondentes a cada classe de serviço, conforme disposto nas recomendações RFC 3550 (*RTP - A Transport Protocol for Real-Time Applications*) e as atualizações pelas RFC 5506 , RFC 5761 , RFC 6051 , RFC 6222 , RFC 7022 , RFC 7160 , RFC 7164 , RFC 8083 , RFC 8108 , RFC 8860, RFC 2212 (*Specification of Guaranteed Quality of Service*), RFC 2474 (*Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers*) e as atualizações pelas RFC 3168 , RFC 3260 , RFC 8436, RFC 2475 (*An Architecture for Differentiated Services*) e a atualizada pela RFC 3260, RFC 3270 (*Multi-Protocol Label Switching Support of Differentiated Services*) e atualizada pela RFC 5462, RFC 3564 (*Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*) e atualizada pela RFC 5462 , RFC 3754 (*IP Multicast in Differentiated Services Networks*).

2.34. A Rede IP Multisserviços deve implementar tráfego *multicast* sobre VPN IP MPLS.

2.35. Para a prestação do SCM na modalidade *multicast*, a Rede IP Multisserviços deve atender ao disposto nas recomendações RFC 1112 (*Host extensions for IP multicasting*) e atualizada pela RFC 2236, RFC 2730 (*Multicast Address Dynamic Client Allocation Protocol*), RFC 3550 (*RTP: A Transport Protocol for Real-Time Applications*), RFC 3551 (*RTP Profile for Audio and Video Conferences with Minimal Control*) e as atualizações pelas RFC 5761 , RFC 7007 , RFC 8860.

2.36. A Rede IP Multisserviços deve fazer uso do protocolo IGMPv3 (*Internet Group Management Protocol* versão 3), definido pela RFC 3376 e a atualização pela RFC 4604, para a gestão da dinâmica de alternância da função de geração entre os *hosts multicast* participantes de uma mesma sessão *multicast*, para o protocolo IPv4.

2.37. A Rede IP Multisserviços deve fazer uso do protocolo MLDv2 (*Multicast Listener Discovery* versão 2), definido pela RFC 3810 e atualizada pela RFC 4604, para a gestão da dinâmica de alternância da função de geração entre os *hosts multicast* participantes de uma mesma sessão *multicast*, para o protocolo IPv6.

2.38. A Rede IP Multisserviços deve fazer uso do protocolo PIM-SM (*Protocol Independent Multicast - Sparse Mode*), definido pela RFC 7761.

2.39. A Rede IP Multisserviços deve permitir o transporte de pacotes IP em caso de aplicações que utilizem o protocolo SIP (*Session Initiation Protocol*) ou qualquer protocolo do padrão H.323, tanto na modalidade *unicast* quanto na modalidade *multicast* da prestação do SCM.

2.40. A rede de acesso da Rede IP Multisserviços deve oferecer como padrão de SCM as alternativas de SCM sem redundância e de SCM com redundância.

2.40.1. O SCM sem redundância é constituído por um conjunto CPE/enlace conectado a um único PE do *backbone* da Rede IP Multisserviços.

2.40.2. O SCM com redundância é constituído por dois conjuntos CPE/enlace implantados com dupla abordagem ao prédio do OES, sem configurar ponto único de falha, em que cada conjunto é construído com recursos de transmissão distintos, onde cada conjunto é conectado ao respectivo PE, localizados em estações distintas do *backbone* da Rede IP Multisserviços.

2.41. O SCM redundante deve, quando contratado pelo OES, prover conexão entre os dois CPE do OES (*back-to-back*), para suportar falha cruzada entre a porta LAN de um CPE com uma porta WAN do outro CPE.

2.42. O SCM com redundância deve ser dotado de protocolo dinâmico que permita a comutação automática do fluxo de tráfego entre a Unidade e o *backbone* da Rede IP Multisserviços, no período máximo de 01 (um) minuto, em caso de falha de um dos elementos de rede do conjunto CPE/enlace em operação.

2.43. O SCM deve permitir a conectividade de uma Unidade (UP ou UC) com uso de endereçamento IP privado simultaneamente para a prestação do serviço na modalidade *unicast* e na modalidade *multicast*.

2.44. A instalação de equipamentos e a ativação dos serviços para uma UC devem ser feitas sem interrupção da conectividade das demais UC com a UP a que estas estiverem associadas.

2.45. Em casos previamente aprovados pela Administradora da Rede e Serviços, a ativação do SCM de uma UP pode ser feita com a participação conjunta da CONTRATADA e do OES, cabendo à CONTRATADA a instalação do enlace e ao OES a instalação do CPE.

2.45.1. Os parâmetros de QoS especificados para a prestação do serviço são válidos a partir da interface WAN do CPE instalado pelo OES.

2.45.2. O OES é responsável pela instalação de CPE que atenda aos requisitos técnicos e funcionais especificados neste documento, em conformidade com os serviços a serem prestados para a UP.

2.45.3. Cabe ao OES, além da instalação, a execução das atividades de configuração, operação, manutenção e gerenciamento do CPE.

2.46. O SCM de uma Unidade (UP ou UC) deve ser instalado com capacidade nominal de transmissão simétrica correspondente a um dos seguintes valores padrão de mercado: 64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, 10 Mbps, 16 Mbps, 34 Mbps, 60 Mbps, 100 Mbps, 155 Mbps, 300 Mbps, 622 Mbps, 1 Gbps, 2,5 Gbps, 5 Gbps, 10 Gbps, 20 Gbps, 40 Gbps e 100 Gbps.

2.47. A aplicação dos critérios de dimensionamento da capacidade nominal de transmissão do SCM é de responsabilidade do OES.

2.48. Ao definir a capacidade nominal do SCM de uma Unidade (UP ou UC), o OES deve atender ao critério de dimensionamento levando em consideração a soma das bandas úteis alocadas a cada classe de serviço e a banda útil alocada ao gerenciamento do SCM.

2.48.1. No dimensionamento da capacidade nominal do SCM a banda útil alocada à classe de serviço PADRÃO deve ser no mínimo 30% da capacidade nominal do SCM.

2.49. Nos casos de SCM com redundância cujos links façam uso de tecnologia *multilink*, o CPE deve ser configurado para gerar automaticamente um alarme sempre que uma interface lógica sofrer degradação motivada pela queda de um ou mais dos enlaces físicos que compõem o *multilink*.

2.49.1. Neste caso, deverá haver a comutação para o enlace de redundância.

2.50. Quando um SCM com capacidade nominal de até 8 Mbps, inclusive, for instalado com tecnologia *multilink*, os respectivos CPE e PE devem utilizar a técnica de fragmentação e intercalação de pacotes (*LFI - Link Fragmentation and Interleaving*).

2.51. Os SCM com capacidade de 10 Mbps e de 16 Mbps não podem ser atendidos com tecnologia *multilink*.

2.52. A utilização de satélite no enlace do SCM de uma Unidade ao *backbone* da Rede IP Multisserviços é permitida para a prestação de serviços exclusivamente nas classes de serviço Tempo Real – Voz, Tempo Real Vídeo (videomonitoramento) e Padrão, em SCM com capacidade nominal instalada de até 16 Mbps restrito a um salto por enlace.

2.52.1. A transmissão no enlace via satélite pode ser feita no modo assimétrico, desde que com taxa de transmissão de 25% (vinte cinco por cento) da capacidade nominal do SCM para o tráfego originado na Unidade (*upload*) e taxa de transmissão de 100% (cem por cento) da capacidade nominal do SCM para o tráfego destinado à Unidade (*download*).

2.52.2. Na transmissão no enlace via satélite, a capacidade garantida de transmissão deve ser, no mínimo, de 25% (vinte e cinco por cento) da capacidade nominal.

2.52.3. Serão aceitos no máximo 3 % do total de acessos, em meio satelital.

2.52.4. Os acessos satélites deverão ser substituídos por enlaces terrestres imediatamente, quando houver condições para tal.

2.52.4.1. A CONTRATADA deverá apresentar, periodicamente a cada 12 (doze) meses, ou quando solicitado pela CONTRATANTE, o plano de viabilidade dessas unidades, para ser aprovado pela Administradora da Rede e Serviços.

Requisitos Operacionais e Técnicos do CPE para o SCM

2.53. O CPE do SCM de uma Unidade (UP ou UC) deve suportar a funcionalidade, DHCP Relay, Server *e Agent*, devendo a CONTRATADA realizar sua configuração sempre que solicitado pela Administradora da Rede e Serviços ou pelo OES.

2.54. O CPE do SCM de uma Unidade (UP ou UC) deve suportar o VRRP (*Virtual Router Redundancy Protocol*), com extensões para IPv6 implementada conforme a RFC 3768.

2.55. O CPE do SCM de uma Unidade (UP ou UC) deve implementar roteamento estático, protocolo de roteamento dinâmico OSPFv3 e o protocolo de roteamento BGPv4.

2.56. O CPE do SCM de uma Unidade (UP ou UC) deve suportar roteamento estático para IPv6 e o protocolo de roteamento BGP com suporte a IPv6.

2.57. O CPE do SCM de uma Unidade (UP ou UC) deve suportar controle de tráfego com encapsulamentos GRE (*General Routing Encapsulation*), IGMPv1, IGMPv2 e IGMPv3 (*Internet Group Management Protocol*) e IPsec (*IP Security Protocol*).

2.58. O CPE do SCM de uma Unidade (UP ou UC) deve suportar LACP (*Link Aggregation Control Protocol*) padrões IEEE (IEEE 802.3ad ou 802.1AX).

2.59. O CPE do SCM de uma Unidade (UP ou UC) deve suportar Internet ICMPv6 (*Control Message Protocol Version* 6) com as funcionalidades, ICMP *Request / Reply*, NDP (*Neighbor Discovery Protocol*), ICMP MTU *Discovery*.

2.60. O CPE do SCM de uma Unidade (UP ou UC) deve suportar o método *Dual Stack* (IPv4 e IPv6).

2.61. O CPE do SCM de uma Unidade (UP ou UC) deve executar os mecanismos de QoS especificados para as classes de serviço.

2.61.1. O CPE do SCM da UC é responsável por executar a regra de condicionamento da entrada do tráfego IP na rede, executando a classificação e a marcação do tráfego oriundo da rede local da UC, cujo destino é a UP da VPN a que a UC está associada, cabendo aos demais elementos da Rede IP Multisserviços utilizar a marcação para manter a correta classificação, enfileiramento e descarte dos pacotes IP, de modo a atender aos parâmetros do QoS.

2.61.2. O CPE do SCM da UP é responsável por aplicar a mesma classificação e marcação ao tráfego que retorna da UP, decorrente da requisição feita pela UC, cabendo aos demais elementos da Rede IP Multisserviços manter a correta classificação, enfileiramento e descarte dos pacotes IP para atender aos parâmetros do QoS.

2.61.3. Quando solicitado pela Administradora da Rede e Serviços, o CPE da UP ou UC deve operar em modo *trust*, respeitando a marcação do pacote já realizada na LAN da Unidade.

2.61.4. O CPE da (UP ou UC) deve possuir a facilidade de priorização do tráfego através do protocolo IEEE 802.1p.

2.61.5. O CPE da (UP ou UC) deve suportar as funcionalidades de "*Traffic Shaping*" e "*Traffic Policing*".

2.62. Na execução dos mecanismos de QoS deve ser aplicada no CPE a combinação de critérios de classificação dos pacotes IP pela interpretação dos campos de endereçamento IP de origem ou de destino, pela associação da porta utilizada pela aplicação com o seu protocolo de transporte (TCP ou UDP) e pelo reconhecimento da interface física ou lógica utilizada para a entrada ou para a saída do tráfego.

2.62.1. A combinação dos critérios de classificação dos pacotes IP é definida por VPN, sendo aplicada a todos os CPE dos SCM das Unidades que participam da VPN.

2.63. A regra de atribuição de prioridade ao tráfego IP executada no CPE deve permitir a escolha de 6 (seis) diferentes códigos de marcação de prioridade para o modelo DSCP (*Differentiated Service Code Point*), cabendo à operadora a escolha do valor para a variável x, y, e z conforme especificado na tabela a seguir:

CLASSES DE SERVIÇO (CoS)	MARCAÇÃO DSCP
TEMPO REAL – VOZ	**EF**
TEMPO REAL – VÍDEO	**AF4x** **CS5**
MISSÃO CRÍTICA	**AF3y** **CS3**
SUPORTE À NEGÓCIO	**AF2z**
PADRÃO	**SEM MARCAÇÃO**

2.63.1. A classe TEMPO REAL – VOZ deve ser tratada com a política de enfileiramento de Prioridade Estrita (*PQ – Priority Queuing*).

2.63.2. Para o tráfego de videoconferência deve ser utilizada a classe de serviço TEMPO REAL – VÍDEO com marcação AF4x.

2.63.3. Para o tráfego de videomonitoramento deve ser utilizada a classe de serviço TEMPO REAL – VÍDEO com marcação CS5.

2.63.4. Para o tráfego de streaming de multimídia deve ser utilizada a classe de serviço MISSÃO CRÍTICA com marcação AF3y.

2.63.5. Para a sinalização de voz e vídeo e para o tráfego de gerência deve ser utilizada a marcação CS3 sem o descarte seletivo (*WRED – Weighted Random Early Discard*).

2.64. O CPE deve permitir a alocação dinâmica de banda respeitando a prioridade do tráfego IP de cada uma das classes de serviço.

2.65. Em situação de congestionamento na interface WAN do CPE, deve ser garantida a alocação de banda associada a cada classe de serviço, conforme a banda útil solicitada, por classe de serviço, para o SCM, sendo o tráfego excedente de qualquer das quatro primeiras classes alocado na classe PADRÃO para preservar o atendimento aos parâmetros de QoS das demais classes.

2.66. O CPE deve permitir, quando solicitado, a implantação de ACL (*Access Control List*) para fins de controle de acesso à rede local da Unidade (UP ou UC) ou a configuração de NAT (*Network Address Translation*) com a finalidade de compatibilizar a rede local da Unidade (UP ou UC) com a VPN da qual participa.

2.67. O CPE, conforme solicitação, deve ser instalado com uma ou mais interfaces LAN padrão Ethernet, com capacidade nominal de 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps ou 100 Gbps até o limite de quatro interfaces.

2.68. O CPE deve dar suporte ao encaminhamento de *Jumbo Frames* (*frames* de 9.018 bytes) quando o SCM possuir capacidade igual ou superior a 1 Gbps.

2.69. O CPE deve permitir, quando solicitado, a implantação do protocolo IEEE 802.1Q (VLAN) em sua interface LAN para fins de roteamento entre redes locais virtuais da Unidade (UP ou UC).

2.70. O CPE deve permitir, quando solicitado, o isolamento do tráfego das diversas sub-redes locais da Unidade (UP ou UC) nas VPN associadas, utilizando o protocolo IEEE 802.1Q.

2.71. Todas as informações necessárias para a configuração do CPE, tais como a faixa de endereçamento IP (IP privado ou IP público), interesse de tráfego com as demais UP de outras VPN, dentre outras, devem ser fornecidas pelo OES quando da solicitação dos serviços.

2.72. O CPE deve permitir a coleta de informações gerenciais de sua MIB (*Management Information Base*) por plataforma de gerenciamento, através de protocolo SNMP (*Simple Network Management Protocol*) versão v2c e v3, bem como permitir acesso às informações de configuração e do status de seus componentes, através de comando de linha CLI e Web, utilizando SSH (*Security Shell*) e HTTPS (*Hyper Text Transfer Protocol Secure*), com privilégios de leitura para a Administradora da Rede e Serviços.

Infraestrutura para a Prestação do Serviço de Comunicação Multimídia

2.73. Cabe ao OES a definição do local de instalação do CPE e do trajeto, desde o ponto de terminação da rede externa até o local de instalação do CPE, a ser seguido pela CONTRATADA para a instalação do enlace.

2.73.1. O OES é responsável pela segurança física do perímetro das suas Unidades.

2.74. A CONTRATADA deve prover os materiais e acessórios adequados às condições da infraestrutura disponível no local de instalação do CPE e no trajeto indicado pelo solicitante para a instalação do enlace.

2.74.1. A instalação do enlace deve ser feita em infraestrutura aparente, cabendo à CONTRATADA fornecer e instalar:

2.74.1.1. Cabos, fibras ópticas e demais meios de transmissão.

2.74.1.2. Conectores, amarradores, elementos de fixação com todas as partes e peças necessárias.

2.74.1.3. Materiais de encaminhamento (eletrodutos, junções e fixadores) até o local de instalação do CPE, exceto se houver disponibilidade no local e autorização do OES para o uso da sua infraestrutura interna de encaminhamento aparente.

2.74.2. Na execução de infraestrutura aparente, a CONTRATADA deve observar e seguir os padrões adotados pelo OES no local de instalação.

2.74.3. Cabe ao OES a execução de obras civis internas que eventualmente forem necessárias para a execução de infraestrutura aparente pela CONTRATADA.

2.74.4. Caso haja infraestrutura embutida com dutos disponíveis e adequados, e desde que autorizado pelo OES, a CONTRATADA pode fazer o uso da mesma para a instalação do enlace, cabendo-lhe fornecer e instalar cabos, fibras ópticas e conectores com todas as partes e peças necessárias.

2.74.5. Se a instalação do enlace tiver que ser feita parte em infraestrutura aparente e parte embutida, aplicam-se concomitantemente, no que couber, as regras definidas em todos os subitens acima.

2.75. A CONTRATADA deve construir base para instalação de antena de radioenlace ou satélite, em concreto, alvenaria ou qualquer outro material, bem como instalar para-raios, caso a instalação do enlace requeira tal infraestrutura.

2.76. Para a acomodação dos equipamentos que compõem a rede de acesso nas dependências dos OES, tais como modems, equipamentos de transmissão, roteadores, equipamento de aceleração, dentre outros, a CONTRATADA deve fornecer e instalar o rack padrão 19” no tamanho necessário para abrigar todos os equipamentos.

2.76.1. Desde que autorizada, a CONTRATADA pode acomodar os equipamentos no rack cedido pelo OES.

2.76.2. O OES deve fornecer as tomadas elétricas no padrão ABNT, na quantidade a ser definida pela CONTRATADA, condições ambientais, espaço e guarda apropriados para a instalação dos equipamentos da CONTRATADA.

2.76.3. O OES deve fornecer e instalar os cabos de interligação do(s) CPE aos equipamentos da sua rede local.

Aceleração de tráfego para o SCM em enlaces satélite

2.77. Para a prestação do SCM através de enlace satélite a CONTRATADA deve prover, adicionalmente, os recursos necessários para a aceleração de tráfego.

2.77.1. É facultado ao OES dispensar o emprego dos recursos para a aceleração em uma ou mais unidades de sob sua responsabilidade.

2.78. A solução deve ser baseada em elementos que operem aos pares (centralizado e remoto), em que um elemento comprime, acelera o tráfego WAN e o envia para o outro elemento, que o descomprime.

2.78.1. A função de aceleração deve estar ativa em ambos os sentidos da comunicação.

2.79. A solução de aceleração deve fazer o uso simultâneo das seguintes técnicas:

2.79.1. Otimização dos protocolos TCP, DNS, HTTP e FTP.

2.79.1.1. No caso do protocolo TCP, a otimização deve ser feita através de, no mínimo, as seguintes técnicas: aumento/diminuição do tamanho da janela inicial de transmissão; aumento da janela de transmissão para além do limite padrão de 64 KB; e retransmissão seletiva de segmentos em caso de perda de dados.

2.79.2. Aceleração do fluxo de pacotes de forma totalmente transparente e automática, eliminando os dados redundantes e realizando compressão de dados, sem a alteração dos cabeçalhos.

2.80. A capacidade de aceleração do elemento remoto deve ser suficiente para suportar toda a capacidade nominal contratada para o SCM.

2.81. A solução deve garantir que não haja interrupção no tráfego do SCM em caso de falha no elemento de aceleração (técnica conhecida como *bypass*).

2.82. O dispositivo de aceleração instalado nas unidades remotas pode ser:

2.82.1. Embarcado no sistema operacional do CPE (em *software*).

2.82.2. Um módulo de aceleração WAN adicionado ao CPE.

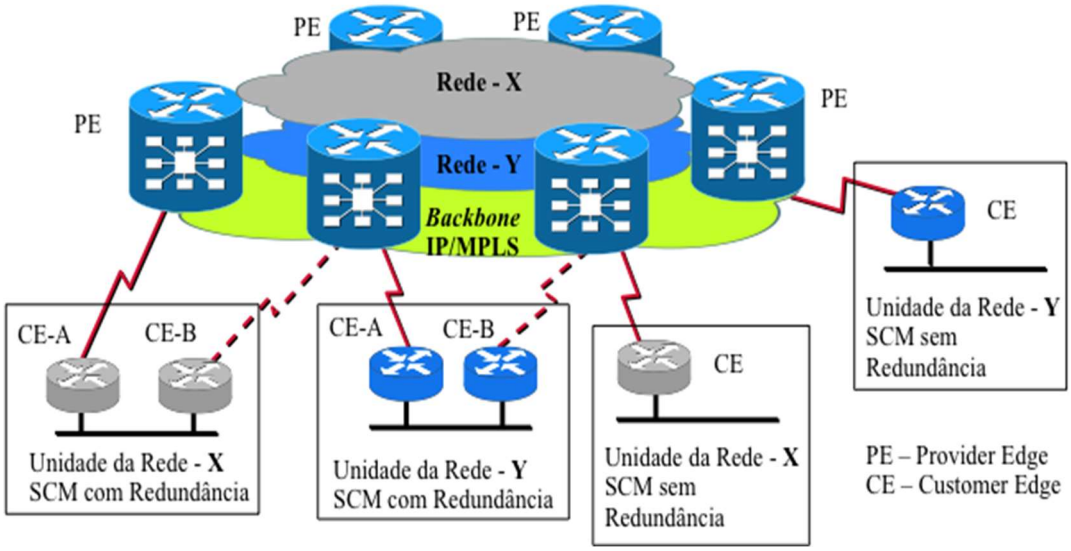
2.82.3. Um equipamento (*appliance*) dedicado externo ao CPE.

2.83. O elemento concentrador da solução de aceleração de tráfego deve ser instalado nas dependências da CONTRATADA.

2.84. A CONTRATADA deve disponibilizar para a Administradora da Rede e Serviços, via SEG, relatórios de otimização do tráfego, conforme procedimentos definidos no Acordo Operacional.

2.85. A falha da funcionalidade de aceleração do tráfego é tratada como incidente de degradação do SCM, desde que não cause interrupção total na prestação desse serviço.

2.86. Para fins de referência, a figura a seguir ilustra a topologia da Rede IP Multisserviços para a prestação do SCM.



III. DESCRIÇÃO DO SERVIÇO DE TRÂNSITO INTERNET (Lote 1)

Prestação do Serviço de Trânsito Internet

3.1. O Serviço de Trânsito Internet é prestado à Unidade (UP ou UC) que o tenha contratado e consiste no provimento de Trânsito Internet por dois AS da CONTRATADA para o AS GESP e para outros AS de governo que estiverem conectados a este.

3.1.1. A prestação do Serviço de Trânsito Internet para as Unidades (UP ou UC) que participam da VPN AS GESP pressupõe a prestação do SCM com o endereço IP público para essas Unidades.

3.1.2. A Rede IP Multisserviços deve dar suporte para o roteamento e para o transporte de pacotes IP gerados pelas UP participantes da VPN AS GESP com a implantação da técnica descrita na RFC 4241 (*A Model of IPv6/IPv4 Dual Stack Internet Access Service*), em que a conectividade entre o CPE da UP e a Internet é feita através de uma conexão fim a fim em IPv6 ou em IPv4.

3.2. O Serviço de Trânsito Internet deve ser prestado em conformidade com o previsto no Contrato, em especial atendendo às metas de qualidade da prestação dos serviços relacionadas aos indicadores de desempenho técnico-operacional do Acordo de Níveis de Serviços (SLA).

3.3. Para a prestação do Serviço de Trânsito Internet, os dois AS providos pela CONTRATADA devem anunciar os blocos CIDR (*Classless Inter-Domain Routing*) e ASN (*Autonomous System Number*) divulgados pelo AS GESP para os AS nacionais e AS internacionais participantes da Internet, tanto em IPv4 quanto em IPv6.

3.4. Para a prestação do Serviço de Trânsito Internet os dois AS providos pela CONTRATADA devem divulgar para o AS GESP todas as tabelas de roteamento da Internet por eles conhecidas (*full routing*).

3.4.1. No caso de divulgação parcial das rotas da Internet conhecidas (*partial routing*) pelos AS da CONTRATADA, devido a alguma anormalidade, a Administradora da Rede e Serviços pode solicitar que os AS da CONTRATADA passem a divulgar uma rota default (*next hop*) para o AS GESP até a normalização do serviço.

3.5. Na prestação do Serviço de Trânsito Internet, os dois AS providos pela CONTRATADA devem fazer uso do protocolo de roteamento BGP-4 (Border Gateway Protocol version 4) com extensões para o IPv6.

3.6. Para a prestação do Serviço de Trânsito Internet, a CONTRATADA pode fazer uso de dois AS próprios, de um AS próprio e de um AS de terceiro subcontratado ou de um AS próprio e de um AS de terceiro consorciado, denominados AS1 e AS2.

3.6.1. Cada um dos AS (AS1 e AS2) deve ter estrutura dualizada de roteadores BGP, implantada em endereços distintos, para fins de conexão com o AS GESP.

3.6.2. O AS1 deve ser interligado a dois outros AS distintos (AS11 e AS12) e o AS2 deve ser interligado a dois outros AS distintos dos primeiros (AS21 e AS22).

Infraestrutura para a Prestação do Serviço de Trânsito Internet

3.7. A banda inicial de Trânsito Internet para o AS GESP deve ser de 200Gbps, simétrica, para cada uma de suas conexões com o AS1, AS2 e IX.BR (antigo PTT Metro-SP).

3.8. A estrutura de roteamento BGP de cada AS deve ser dimensionada com capacidade nominal de Trânsito Internet para dar vazão plena ao tráfego do AS GESP com a Internet, incluindo o tráfego trocado no IX.BR.

3.9. A implantação da estrutura do AS GESP deve estar concluída no prazo de 90 (noventa) dias, ou sua adequação no prazo de 60 (sessenta) dias, a contar da data de assinatura do Contrato, conforme consta no Plano de Transição.

3.10. A CONTRATADA deve providenciar a ampliação da estrutura do AS GESP ou de suas conexões sempre que a média móvel trimestral no horário comercial de utilização de qualquer um desses recursos ultrapassar 50% de sua capacidade nominal ou quando o valor do 95º Percentil mensal, no horário comercial, de qualquer um desses recursos atingir ou ultrapassar 90% da sua capacidade nominal, o que ocorrer primeiro.

3.10.1. Para análise da ampliação da estrutura do AS GESP ou de suas conexões a CONTRATADA deve considerar o tráfego trocado entre o AS GESP e os AS de responsabilidade da CONTRATADA (AS1 e AS2) e o IX.BR.

3.11. Durante a vigência do Contrato, as ampliações dos recursos da estrutura do AS GESP devem estar disponíveis no prazo de 60 (sessenta) dias a contar da data de ocorrência do evento que lhe der causa, conforme critérios no item anterior.

3.12. O não cumprimento dos prazos de implantação, adequação ou ampliação dos recursos da estrutura do AS GESP ou de suas conexões sujeita a CONTRATADA à aplicação de penalidade por descumprimento contratual.

3.13. Como parte da prestação do Serviço de Trânsito Internet, a CONTRATADA deve prover recursos para constituir três pontos de presença do AS GESP, denominados PoP 1 do AS GESP, PoP 2 do AS GESP e PoP 3 do AS GESP.

3.14. Atualmente as localizações dos três pontos de presença do AS GESP correspondem a ambientes indicados, respectivamente, nos endereços PoP 1 do AS GESP na Rua Agueda Gonçalves, n° 240, Taboão da Serra – SP, PoP 2 do AS GESP na Secretaria da Fazenda, na Av. Rangel Pestana, n° 300, São Paulo – SP, e PoP 3 do AS GESP na Av. São Luís, 99, São Paulo – SP.

3.15. É facultada a alocação dos equipamentos que compõem cada PoP nas premissas atualmente em uso ou em um ou mais PoP nas premissas da CONTRATADA, por ocasião de sua ativação ou durante a vigência do contrato.

3.15.1. Caso opte por utilizar os PoP atuais, a CONTRATADA deve efetuar *site survey* para verificar as limitações físicas da área disponível nos ambientes para a instalação de no máximo 6 (seis) *racks* padrão 19”, devendo se ajustar às condições e exigências de cada PoP.

3.16. Caso a CONTRADADA opte por alocar um ou mais PoP em sua(s) premissa(s), como parte da prestação do Serviço de Trânsito Internet, a mesma deve prover todos os recursos especificados conforme o PoP substituído.

3.16.1. O local de cada PoP do AS GESP, utilizado pela CONTRATADA, deve estar alocado dentro do estado de São Paulo e possuir:

3.16.1.1. Certificação válida de nível *Tier* III, no mínimo, ou equivalente.

3.16.1.2. Certificação válida ISO 27001 emitida por organismo certificador em até 12 (doze) meses a partir da assinatura do Contrato.

3.17. Como parte da prestação do Serviço de Trânsito Internet, a CONTRATADA deve prover recursos para a interface de roteamento BGP do AS GESP, denominada de Borda BGP do AS GESP.

3.18. A Borda BGP do AS GESP deve ser localizada nos PoP 1 do AS GESP, PoP 2 do AS GESP e PoP 3 do AS GESP.

3.19. Os 3 (três) PoP do AS GESP devem ser dotados de 2 (dois) equipamentos, cada PoP, com funcionalidades de comutação e de roteamento, denominado roteador BGP, cada um deles com a configuração mínima de portas, conforme consta nas tabelas a seguir:

3.19.1. Cada roteador do PoP 1 do AS GESP têm a seguinte configuração:

Finalidade	Quantidade de Portas	Capacidade de cada Porta
Interligação ao PoP 2 e ao PoP 3 do AS GESP	4 (*)	100 Gbps
Interligação a um dos roteadores BGP do AS2	2	100 Gbps
Interligação ao PoP 1 do *backbone* da Rede IP Multisserviços	1	100 Gbps
Conexão local com roteador BGP redundante	2	100 Gbps
Conexão em âmbito local (LAN)	4(*) (**) 8	1 Gbps 10 Gbps

(*) Portas devem estar distribuídas em dois módulos distintos e independentes.
(**) 4 portas SFP 1000 Base-T / 1000 Base-SX.

3.19.2. Cada roteador do PoP 2 do AS GESP têm a seguinte configuração:

Finalidade	Quantidade de Portas	Capacidade de cada Porta
Interligação ao PoP 1 e ao PoP 3 do AS GESP	4 (*)	100 Gbps
Interligação a um dos roteadores BGP do AS1	2	100 Gbps
Interligação ao PoP 2 do *backbone* da Rede IP Multisserviços	1	100 Gbps
Conexão local com roteador BGP redundante	2	100 Gbps
Conexão de âmbito local (LAN)	4(*) (**) 8	1 Gbps 10 Gbps

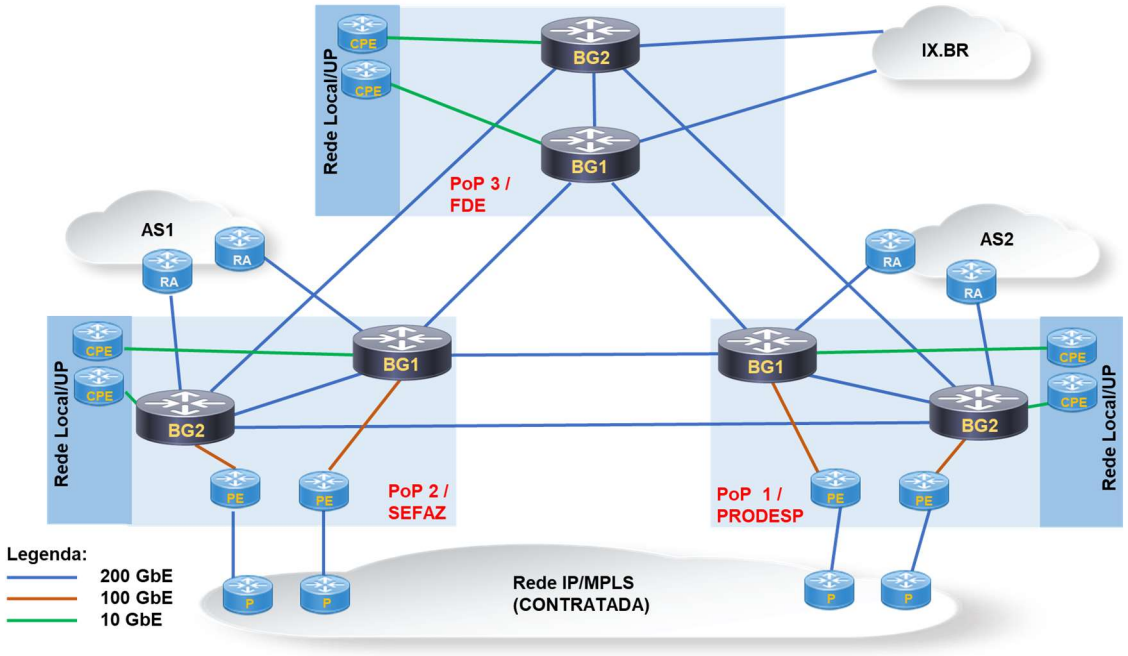
(*) Portas devem estar distribuídas em dois módulos distintos e independentes.
(**) 4 portas SFP 1000 Base-T / 1000 Base-SX.

3.19.3. Cada roteador do POP 3 do AS GESP têm a seguinte configuração:

Finalidade	Quantidade de Portas	Capacidade de cada Porta
Interligação ao PoP 1 e ao PoP 2 do AS GESP	4 (*)	100 Gbps
Interligação ao *switch* do IX.BR	2 (*)	100 Gbps
Conexão local com roteador BGP redundante	2	100 Gbps
Conexão de âmbito local (LAN)	4(*) (**) 1	1 Gbps 100 Gbps
Ampliação de capacidade ou redundância	1 (*)	100 Gbps

(*) Portas devem estar distribuídas em dois módulos distintos e independentes.
(**) 4 portas SFP 1000 Base-T / 1000 Base-SX.

3.20. Para fins de referência, a figura a seguir ilustra a topologia do AS GESP para a prestação do STI.



3.21. Os roteadores BGP devem ser idênticos em termos de marca, modelo e configuração mínima de hardware e de sistema operacional em sua versão mais atualizada, e devem atender, no mínimo, aos requisitos técnicos especificados nos subitens que seguem:

3.21.1. Dar suporte aos protocolos IPv4 e IPv6 *Dual Stack*.

3.21.2. Dar suporte aos protocolos BGP-4 (Border Gateway Protocol Version 4), OSPFv3 (Open Shortest Path First version 3) e VRRP (Virtual Router Redundancy Protocol), com extensões para o IPv6.

3.21.3. Ter capacidade de realizar roteamento pleno BGP-4 (*full routing*) com até cinco provedores de Trânsito Internet, além do roteamento entre os próprios roteadores BGP do AS GESP.

3.21.4. Dar suporte a *Link Aggregation* (IEEE 802.3ad/802.1AX), através das portas Gigabit Ethernet, possibilitando configuração de 8 (oito) grupos de até 8 (oito) portas agregadas por grupo.

3.21.5. O equipamento deve possuir arquitetura não bloqueante, tendo capacidade de encaminhamento *wire-speed* nas camadas 2 e 3 para *frames* a partir de 64 bytes de tamanho, de forma a suportar capacidade de encaminhamento de 100% (cem por cento) do número de interfaces, com capacidade de agregação mínima de comutação (*throughput*) de 100/400 Gbps (*half duplex / full duplex*).

3.21.6. Dar suporte ao encaminhamento de *Jumbo Frames* (*frames* de 9.018 bytes) nas portas Gigabit Ethernet.

3.21.7. Dar suporte às funcionalidades descritas nos padrões IEEE 802.3x (*Flow Control*), IEEE 802.1d (*Spanning Tree*), IEEE 802.1w (*Rapid Spanning Tree*), IEEE 802.1s (*Multiple Spanning Tree*), IEEE 802.1p (*Traffic Prioritization*), IEEE 802.1Q (VLAN) e IEEE 802.1X (*Access Control by Port*).

3.21.8. Dar suporte aos protocolos IGMPv3 (*Internet Group Management Protocol, Version 3*), DHCP (*Dynamic Host Configuration Protocol*) *snooping*, DHCP *Server*, DHCP *Relay Agent* e ao espelhamento (*Port Mirroring*) do tráfego de entrada e saída de múltiplas portas do *switch* em uma única porta.

3.21.9. Dar suporte aos protocolos IPv6, RFC 4443 ICMPv6 (*Internet Control Message Protocol for the IPv6 Internet Protocol Version 6 Specification*) e atualizada pela RFC 4884, RFC 4861 NDP (*Neighbor Discovery for IP version* 6) e as atualizações pelas RFC 5942 , RFC 6980 , RFC 7048 , RFC 7527 , RFC 7559 , RFC 8028 , RFC 8319 , RFC 8425 , RFC 9131, RFC 5175 (IPv6 *Router Advertisement Flags Option*) , RFC 4862 SLAAC (IPv6 *Stateless Address Autoconfiguration*) e atualizada pela RFC 7527, RFC 3315 DHCPv6 (*Dynamic Host Configuration Protocol for* IPv6) e as atualizações pelas RFC 4361, RFC 5494, RFC 6221, RFC 6422, RFC 6644, RFC 7083, RFC 7227, RFC 7283, RFC 7550.

3.21.10. Ter 16 (dezesseis) Gigabytes de memória RAM.

3.21.11. Dar suporte ao protocolo de gerenciamento SNMP (versão v2c e v3) e MIB.

3.21.12. Ter dimensões padronizadas para montagem em armário (*rack*) de 19”.

3.21.13. Possuir módulos de processamento, controle e fontes de alimentação redundantes (1+1) com tensão de alimentação de 100 a 127 VAC/60 Hz ou de 200 a 240 VAC/60 Hz, sendo que cada uma das fontes deve ter potência suficiente para suportar toda a carga do chassi em sua configuração máxima.

3.21.14. Permitir a substituição de módulos de processamento, controle, interface e fonte de alimentação sem a necessidade de desligamento do equipamento (*hot swap*).

3.22. Os 3 (três) PoP do AS GESP devem ser interligados, dois a dois, através de 6 (seis) circuitos digitais dedicados, ponto a ponto, atendendo às especificações técnicas do ITU-T.

3.22.1. Cada dois circuitos digitais entre dois PoP do AS GESP devem ser instalados em dupla abordagem.

3.22.1.1. Entende-se por dupla abordagem a utilização de meios físicos e elementos de infraestrutura distintos em todo o percurso externo ao endereço do PoP, não sendo permitido o compartilhamento de dutos, postes, radioenlace, cabos de fibra óptica, dentre outros, entre os seis circuitos.

3.22.1.2. Devem ser instalados meios físicos distintos no percurso interno ao endereço do PoP, desde a entrada até o local de instalação da terminação dos circuitos, fazendo uso da infraestrutura disponível nesse trajeto.

3.22.2. Cada circuito digital deve ser instalado com capacidade nominal adequada ao Trânsito Internet, utilizando-se de equipamento terminal distinto, devendo ser ajustado de forma consistente com a alteração da banda útil do Trânsito Internet.

3.22.3. Cada equipamento terminal deve ser interligado pela CONTRATADA a uma porta do roteador BGP nos PoP 1 do AS GESP, PoP 2 do AS GESP e PoP 3 do AS GESP, destinadas a essa finalidade.

3.22.4. Os circuitos digitais devem ser transparentes a códigos e a protocolos, configurados na modalidade ponto a ponto permanente e de uso exclusivo para a prestação do Serviço de Trânsito Internet.

3.23. A borda do AS GESP deve dar conectividade às Unidades que compõem o AS GESP através das interligações descritas a seguir:

3.23.1. A UP PRODESP deve ser interligada a dois CPE (em âmbito local, onde o endereço da UP é o mesmo do PoP 1 do AS GESP), cada qual conectados através de uma conexão aos dois roteadores BGP do PoP 1 do AS GESP, por meio da contratação do Serviço de Trânsito Internet sem o SCM.

3.23.2. A UP SEFAZ deve ser interligada a dois CPE (em âmbito local, onde o endereço da UP é o mesmo do PoP 2 do AS GESP), cada qual conectados através de uma conexão aos dois roteadores BGP do PoP 2 do AS GESP, por meio da contratação do Serviço de Trânsito Internet sem o SCM.

3.23.3. A UP FDE deve ser interligada em a dois CPE (em âmbito local, onde o endereço da UP é o mesmo do PoP 3 do AS GESP), cada qual conectados através de uma conexão aos dois roteadores BGP do PoP 3 do AS GESP, por meio da contratação do Serviço de Trânsito Internet sem o SCM.

3.23.4. Os CPE devem possuir conexão entre si (*back-to-back*), para suportar falha cruzada entre a porta LAN de um CPE com uma porta WAN do outro CPE.

3.23.5. Excepcionalmente, outras Unidades podem ser interligadas em âmbito local aos dois roteadores BGP do PoP 1 do AS GESP, do PoP 2 do AS GESP ou do PoP 3 do AS GESP, ainda que seus endereços sejam distintos do PoP, atendendo a eventuais solicitações para a prestação do Serviço de Trânsito Internet sem o SCM.

3.23.6. Cada um dos roteadores BGP do PoP 1 do AS GESP deve ser interligado em âmbito local a cada um dos PE do PoP do *backbone* da Rede IP Multisserviços para permitir a conectividade das demais Unidades do AS GESP que participam da VPN AS GESP.

3.23.7. Cada um dos roteadores BGP do PoP 2 do AS GESP deve ser interligado em âmbito local a cada um dos PE do PoP do *backbone* da Rede IP Multisserviços para permitir a conectividade das demais Unidades do AS GESP que participam da VPN AS GESP.

3.23.8. Por critério de engenharia de tráfego de rede, é facultado a CONTRATADA a possibilidade de conectar unidades contratantes do serviço SCM com STI com capacidade a partir 10 Gbps através de um circuito digital dedicado ponto a ponto, provisionado diretamente nos roteadores BGP do AS GESP, sem passar pelo *backbone* MPLS.

3.23.8.1. A redundância, se houver, da conectividade descrita acima deve ser implantada em PoP distinto da conexão principal.

3.23.8.2. A remuneração pela prestação dos serviços SCM com STI permanecerá a mesma, independentemente do tipo de transporte de rede utilizado.

3.24. A borda do AS GESP deve ser interligada aos AS que proveem trânsito ao AS GESP com IPv4 e com IPv6.

3.24.1. O PoP 2 do AS GESP deve ser interligado ao AS1 provido pela CONTRATADA, sendo cada um dos roteadores BGP interligado a cada um dos roteadores BGP do AS1, através de um circuito digital dedicado, ponto a ponto.

3.24.1.1. Os dois circuitos devem ser instalados em dupla abordagem.

3.24.2. O PoP 1 do AS GESP deve ser interligado ao AS2 provido pela CONTRATADA, sendo cada um dos roteadores BGP interligado a cada um dos roteadores BGP do AS2, através de um circuito digital dedicado, ponto a ponto.

3.24.2.1. Os dois circuitos devem ser instalados em dupla abordagem.

3.24.3. Cada circuito digital deve ser instalado com capacidade nominal adequada ao Trânsito Internet, utilizando-se de equipamento terminal distinto, devendo ser ajustado de forma consistente com a alteração da banda útil do Trânsito Internet.

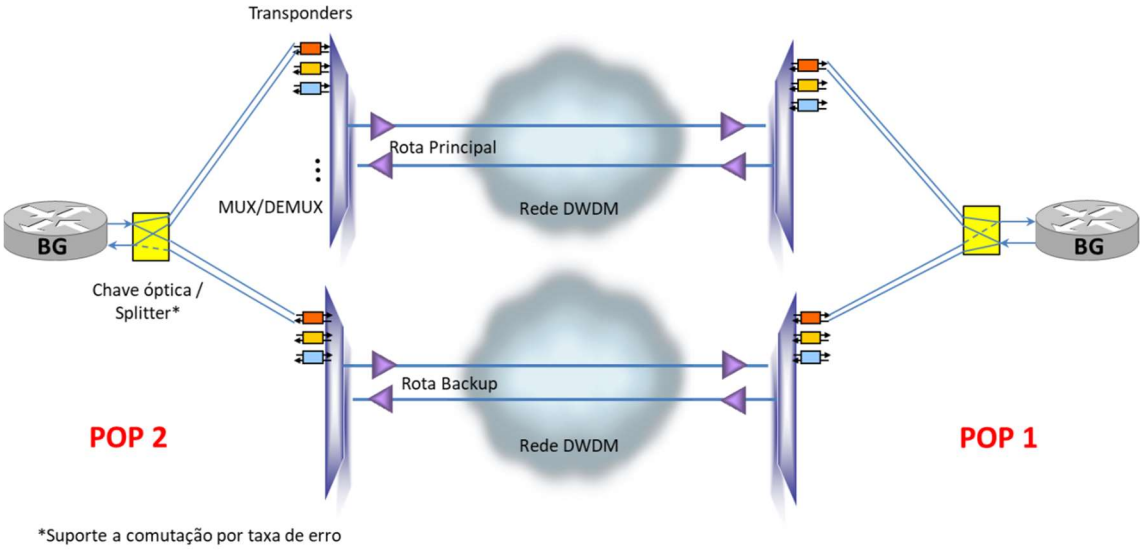
3.24.4. Cada equipamento terminal deve ser interligado pela CONTRATADA a uma porta do roteador BGP do PoP do AS GESP destinada a essa finalidade.

3.24.5. Os circuitos digitais devem ser transparentes a códigos e a protocolos, configurados na modalidade ponto a ponto permanente e de uso exclusivo para a prestação do Serviço de Trânsito Internet.

3.24.6. O PoP 3 do AS GESP deve ser interligado, pela CONTRATADA, ao IX-BR em âmbito local, sendo cada um dos roteadores BGP interligado ao PIX NIC-JD do IX-BR localizado em SP.

3.25. Para o provimento dos circuitos digitais dedicados ponto a ponto em dupla abordagem, cada circuito digital deve ter redundância por meio de equipamentos ópticos distintos, tais como multiplexadores, demultiplexadores, chave óptica, amplificadores ópticos e transponders utilizados em soluções DWDM.

3.25.1. Para fins de referência, a figura a seguir ilustra o circuito digital de uma das interligações do AS GESP, em que não há interseção entre a rota principal e a rota backup:

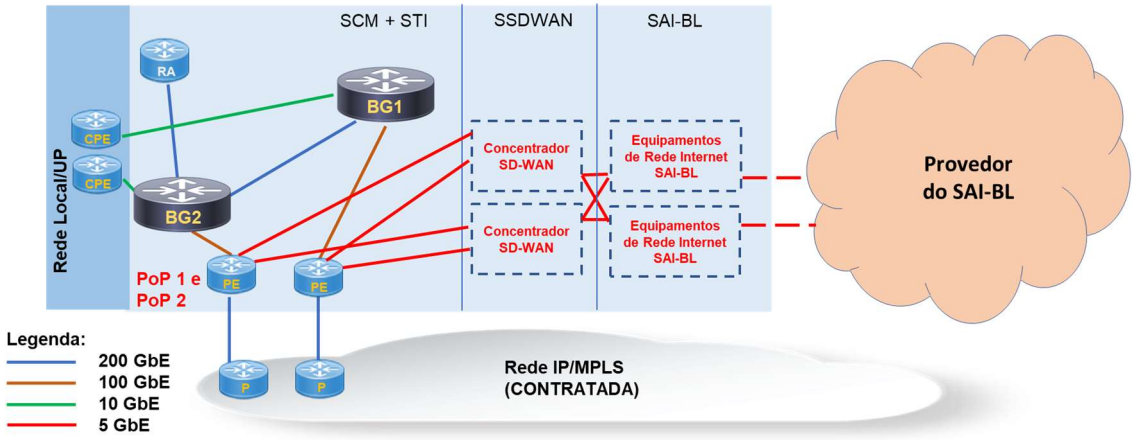


3.26. No caso da interligação entre os 3 (três) PoP do AS GESP e da interligação da borda do AS GESP aos AS que proveem Trânsito, o caminho da proteção de um circuito entre 2 (dois) PoP não pode passar pelo terceiro PoP (técnica também conhecida como *bypass*).

3.27. Cabe à CONTRATADA o fornecimento de todos os cabos e conectores nas dimensões e características adequadas para a interconexão dos roteadores BGP do PoP do AS GESP com as terminações dos circuitos digitais, bem como aqueles necessários à interconexão de âmbito local nos equipamentos.

3.28. Para fins de referência, a figura a seguir ilustra a topologia dos PoP 1 e PoP 2 do AS GESP para a prestação do STI e as integrações com o SCM, SSDWAN e SAI-BL.

3.28.1. Os elementos tracejados na figura indicam a os itens que não são de responsabilidade da CONTRATADA prestadora do STI.



3.29. A CONTRATADA deve prover no PoP 1 e PoP 2 espaço em rack padrão 19 polegadas e fornecimento de energia elétrica para acomodação e alimentação de todos os equipamentos da solução SD-WAN e equipamentos do SAI-BL para promover a interligação entre os dispositivos SD-WAN a Internet e a rede do SCM em alta disponibilidade, bem como deve fornecer todos os cabos, interfaces, *transceivers* ópticos e elétricos e executar todas as conexões necessárias para as interligações em âmbito local entre esses equipamentos (*colocation*, *golden jumpers*, cordões ópticos ou metálicos, entre outros).

3.29.1. A CONTRATADA deve providenciar, o que couber, a ampliação da banda de sua infraestrutura utilizada para a interligação, sempre que a média móvel trimestral no horário comercial de utilização ultrapassar 50% de sua capacidade nominal ou quando o valor do 95º Percentil mensal, no horário comercial atingir ou ultrapassar 90% da sua capacidade nominal, o que ocorrer primeiro.

3.29.2. Durante a vigência do Contrato, as ampliações necessárias na infraestrutura devem estar disponíveis no prazo de 90 (noventa) dias a contar da data de ocorrência do evento que lhe der causa.

Requisitos Operacionais para a Prestação do Serviço de Trânsito Internet

3.30. Os recursos utilizados para a prestação do Serviço de Trânsito Internet devem ser mantidos em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

3.31. Deve ser atribuído a cada um dos roteadores BGP dos PoP do AS GESP, a cada um dos circuitos digitais, bem como aos AS1 e AS2, um código de identificação (ID) a ser utilizado para se referir a esses elementos nos procedimentos estabelecidos no Acordo Operacional.

3.32. Os roteadores BGP dos PoP do AS GESP devem ser instalados, configurados e operados pela CONTRATADA e caso solicitado pela Administradora da Rede e Serviços, operados pela PRODESP com suporte da CONTRATADA, sendo de responsabilidade da CONTRATADA a manutenção dos equipamentos.

3.32.1. A partir da instalação e ativação da estrutura do AS GESP, será iniciado o período de operação assistida por 90 (noventa) dias, dentro do qual a CONTRATADA deve manter um especialista com qualificação técnica comprovada em protocolo de roteamento internet BGP na PRODESP, para atuação imediata, das 8:00 às 17:00 horas, em dias úteis, responsável por dar assistência à equipe da PRODESP na operação dos Roteadores BGP da infraestrutura de suporte ao Serviço de Trânsito Internet.

3.32.2. Fora do horário estipulado no item anterior, a CONTRATADA deve manter um especialista com qualificação técnica comprovada em BGP em regime de sobreaviso para ser acionado no caso de ocorrência de anormalidades dos roteadores BGP da infraestrutura de suporte ao Serviço de Trânsito Internet.

3.32.3. Nesse mesmo período os especialistas técnicos da CONTRATADA devem repassar conhecimentos na operação dos roteadores BGP como aperfeiçoamento à capacitação da equipe da PRODESP.

3.33. Após o período de operação assistida, a CONTRATADA deve manter o suporte técnico à equipe da PRODESP na operação dos roteadores BGP da infraestrutura de suporte ao Serviço de Trânsito Internet durante a vigência do Contrato, abrangendo os protocolos BGP-4, OSPFv3 e VRRP.

3.33.1. O suporte técnico deve ser dado por especialista certificado, através de atendimento telefônico imediato em horário comercial, sem limitação de chamadas, e de atendimento *in loco*, em horário comercial no primeiro horário do próximo dia útil imediatamente seguinte a solicitação feita pela PRODESP.

3.33.2. Fora do horário comercial, a CONTRATADA deve manter um especialista com qualificação técnica em BGP em regime de sobreaviso para ser acionado no caso de ocorrência de anormalidades dos roteadores BGP da infraestrutura de suporte ao Serviço de Trânsito Internet.

3.33.2.1. O suporte técnico BGP deverá ser iniciado no prazo de 30 (trinta) minutos, contados do momento do acionamento.

3.34. A CONTRATADA deve apresentar projeto executivo contendo a topologia física dos 6 (seis) circuitos digitais utilizados para a interligação dos PoP do AS GESP entre si e dos circuitos digitais utilizados para a interligação da Borda do AS GESP com os AS1, AS2 e o IX.BR, com a finalidade de demonstrar a conformidade com as especificações técnicas requeridas para a prestação do Serviço de Trânsito Internet, em especial quanto à dupla abordagem.

3.35. O projeto executivo contendo a topologia física dos circuitos digitais deve ser apresentado à Administradora da Rede e Serviços no prazo estabelecido no Plano de Transição, conforme disposto no Contrato.

3.36. Cabe à Administradora da Rede e Serviços efetuar a análise do projeto e aprová-lo, sendo-lhe facultada a realização de diligências para a comprovação do pleno atendimento aos requisitos contratuais.

3.36.1. Para fins de aceite da implantação da solução a CONTRATADA deve realizar testes de integração entre o STI, SCM, SAI-BL e SSDWAN.

3.37. A configuração inicial dos roteadores BGP dos PoP do AS GESP deve ser feita pela CONTRATADA em conformidade com as informações fornecidas pela PRODESP conforme previsto no Plano de Transição.

3.37.1. A CONTRATADA deve configurar o AS1 e o AS2 com base nessas informações fornecidas pela PRODESP.

3.37.2. Após a conclusão da configuração inicial dos roteadores BGP dos PoP do AS GESP, bem como do AS1 e AS2, a CONTRATADA deve efetuar, juntamente com a PRODESP, testes de conectividade, interoperabilidade e redundância automática entre a Borda do AS GESP e os AS1 e AS2.

3.38. A CONTRATADA deve realizar treinamento referente aos roteadores BGP e aos protocolos inerentes à solução do STI, atendendo ao disposto no Plano de Transição.

Funcionalidade de Monitoramento, Detecção e Mitigação de Ataques

3.39. Na prestação do Serviço de Trânsito Internet a CONTRATADA deve prover solução para o monitoramento, a detecção e a mitigação de ataques, em tempo real, de anomalias na rede causadas por ataques de várias naturezas oriundos da Internet e com destino ao AS GESP.

3.40. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes:

3.40.1. Ataques de negação de serviço (*DoS – Denial of Service*) e ataques distribuídos de negação de serviço (*DDoS – Distributed Denial of Service).*

3.40.2. Ataques de inundação (*Bandwidth Flood*), incluindo *Flood* de UDP e ICMP.

3.40.3. Ataques à pilha TCP, incluindo mau uso das *Flags TCP*, ataques de RST e FIN, *SYN Flood* e *TCP Idle Resets*.

3.40.4. Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.

3.40.5. Ataques de *Botnets, Worms* e ataques que utilizam falsificação de endereços IP, de DNS e de e-mails (*IP Spoofing*).

3.40.6. Ataques à camada de aplicação, incluindo protocolos HTTP e DNS.

3.40.7. Ataques por manipulação de URL (*Uniform Resource Locator).*

3.41. A solução deve implementar múltiplas técnicas de detecção de ataques, incluindo análise de mau uso de protocolos, verificação de assinaturas de ataques, análise de comportamento do tráfego comparado com linhas de base históricas, validação de sessões TCP, dentre outras.

3.42. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como ACL (*Access Control List*), limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

3.43. A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

3.44. A solução deve possuir tecnologia com capacidade de bloqueio e gerenciamento de grandes blocos de IP, considerando tabelas com mais de 2 (dois) milhões de blocos IP.

3.45. O sistema deve ser capaz de detectar anomalias de tráfego, pacotes ou protocolo, tanto para entidades previamente definidas (objetos gerenciados) quanto para não previamente definidas, como também ser capaz de criar uma linha de base (*baseline*) para cada entidade monitorada, de forma que possa aprender e relatar dinamicamente eventuais mudanças nos comportamentos de tráfego.

3.46. 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 CONTRATADA.

3.46.1. Por solicitação da Administradora da Rede e Serviços ou do OES, a CONTRATADA deve inserir ou excluir endereços IP em até 30 minutos após o registro do incidente, conforme disposto no Acordo Operacional.

3.47. A solução de monitoramento, detecção e mitigação de ataques deve ser implementada internamente ao AS da CONTRATADA.

3.48. No AS de terceiro a solução de monitoramento, detecção e mitigação de ataques pode ser implementada internamente a este AS ou de forma dedicada no PoP do AS GESP a ele conectado.

3.49. Deve ser implementada solução dedicada de monitoramento, detecção e mitigação de ataques no PoP 3 do AS GESP de modo a detectar os ataques provenientes das conexões com IX-BR.

3.50. A solução a ser utilizada para mitigação de ataques deve utilizar o modelo "*clean pipe*", no qual há somente o descarte de tráfego malicioso, sem afetar o tráfego válido, de modo que o tráfego seja entregue limpo ao AS GESP.

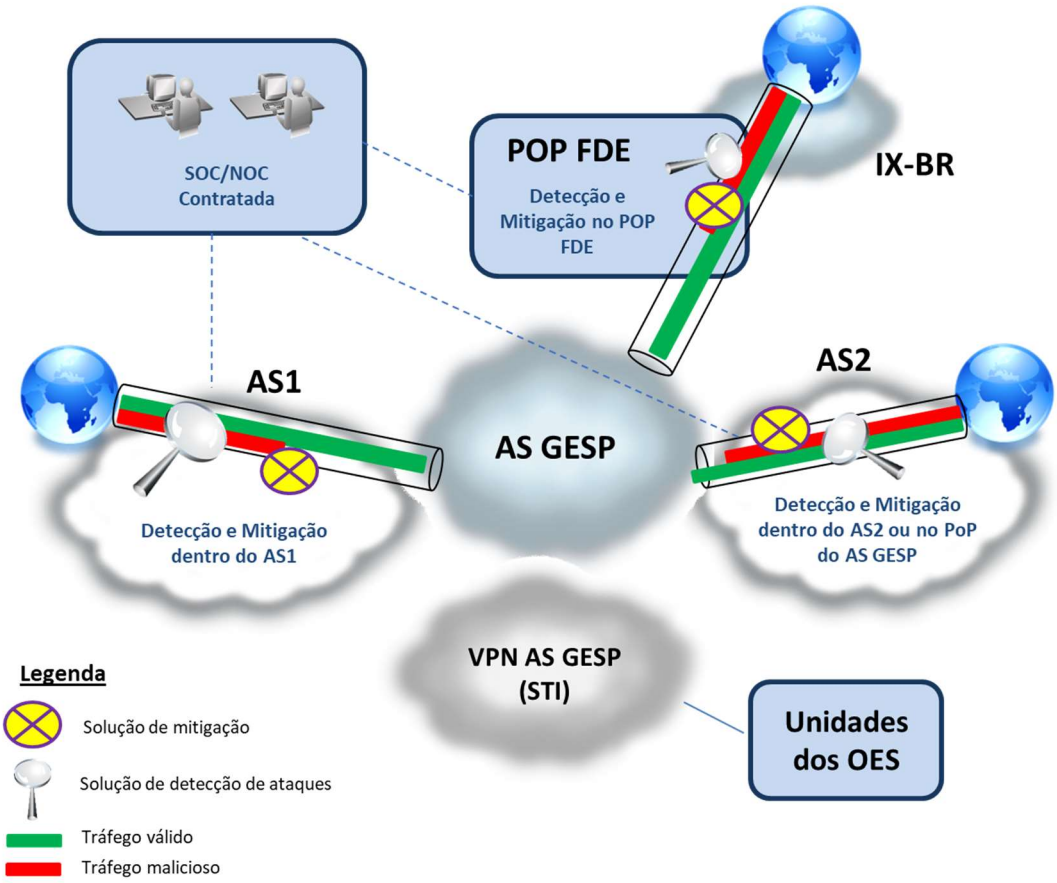
3.50.1. O tráfego malicioso deve ser descartado internamente ao AS ou nos equipamentos de mitigação instalados nos PoP do AS GESP, conforme for o caso.

3.51. A figura a seguir demonstra a solução de monitoramento, detecção e mitigação de ataques, na qual o AS GESP somente recebe tráfego válido proveniente da Internet, através das seguintes opções de detecção e mitigação:

3.51.1. Solução a ser implementada no AS da CONTRATADA.

3.51.2. Solução a ser implementada no AS de terceiro ou no PoP do AS GESP a ele conectado.

3.51.3. Solução dedicada a ser implementada no PoP 3 do AS GESP para proteção das conexões com o IX.BR.



3.52. A solução de monitoramento, detecção e mitigação de ataques provida através dos AS1 e AS2 deve suportar ataques de até 4 (quatro) vezes a capacidade nominal das conexões do AS GESP, entregando um canal limpo (*clean pipe*) no valor nominal das conexões do AS GESP, inclusive no caso de tráfego com pacotes de 64 bytes.

3.53. No caso ter da solução de monitoramento, detecção e mitigação de ataques implementada de forma dedicada nos PoP do AS GESP, a solução deve suportar ataques no valor da capacidade nominal das conexões do AS GESP, entregando um canal limpo (*clean pipe*) equivalente a banda útil das conexões do AS GESP.

3.54. As soluções de mitigação devem suportar as capacidades especificadas, sendo que não deve ser considerada como opção o desligamento de qualquer uma das conexões para a contenção desses ataques.

3.55. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS GESP 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 a *Remote Triggered Black Hole*, conforme detalhado na RFC 5635.

3.55.1. Adicionalmente, caso a solução de monitoramento, detecção e mitigação para o AS de terceiro seja implementada no PoP do AS GESP, pode ser realizado, a critério da Administradora da Rede e Serviços, o desvio do tráfego do ataque que esteja ocorrendo através desse AS para mitigação pelo AS da CONTRATADA através de manipulação de rotas no protocolo BGP do AS GESP.

3.55.2. A proposta de contramedidas a serem tomadas pela CONTRATADA deve ser previamente submetida à validação por parte do OES impactado com cópia para a Administradora da Rede e Serviços.

3.56. O tráfego tratado pela solução de mitigação e identificado como válido deve ser encaminhado ao AS GESP, mantendo-se a visibilidade do IP de origem (tráfego limpo sem modificação).

3.57. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.

3.58. A CONTRATADA deve disponibilizar um Centro Operacional de Segurança (ou SOC – *Security Operations Center*) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone fixo na área local 11, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

3.59. O monitoramento para detecção de ataques não deve inserir pontos de falha à rede, devendo ser baseado em tecnologias que utilizam informações de fluxos enviadas pelos roteadores (p.ex.: IPFIX), espelhamento através de cabos Y, espelhamento com *bypass* (em caso de falha de hardware) ou em tecnologias equivalentes.

3.60. 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.

3.60.1. A critério da CONTRATADA, a mitigação de ataques pode ser baseada em arquitetura na qual os equipamentos da solução são instalados em linha com o AS GESP, desde que esses equipamentos possuam a funcionalidade de *bypass* em caso de falha de *hardware* ou na alimentação elétrica.

3.61. Para a mitigação dos ataques não será permitido o modelo Proxy, o qual é baseado em redirecionamento de FQDN (*Fully Qualified Domain Name*) através da alteração de endereço(s) IP de host(s) no serviço de DNS (*Domain Name System*), nem o modelo roteado baseado em túneis IP ou GRE (*Generic Routing Encapsulation*).

3.62. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego do AS GESP para limpeza fora do território brasileiro.

3.63. A implantação e ativação das soluções de monitoramento, detecção e mitigação de ataques deve estar concluída no prazo de 120 (cento e vinte) dias, ou sua adequação no prazo de 60 dias, a contar da data de assinatura do Contrato, conforme conste no Plano de Transição.

3.64. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

3.65. A CONTRATADA deve disponibilizar nas consoles do SEG, instalados na UPG e na PRODESP, as ferramentas necessárias ao monitoramento da solução e ao acompanhamento das atividades do SOC.

3.65.1. As ferramentas devem permitir a visualização do tráfego Internet, relatórios, alertas e informações sobre ataques.

3.65.2. Os relatórios têm a finalidade de dar subsídios para a análise do interesse de tráfego do AS GESP e fornecer informações sobre aplicações por porta/protocolo, roteador e interface.

3.66. A CONTRATADA deve realizar treinamento referente ao monitoramento inerente à solução, atendendo ao disposto no Plano de Transição.

3.67. A CONTRATADA deve prover a funcionalidade de monitoramento, detecção e mitigação de ataques atendendo aos parâmetros de SLA especificados.

3.68. A CONTRATADA deve disponibilizar um portal web que permita ao OES ter acesso a informações sobre os ataques relacionados a seus blocos IP utilizados na prestação do STI.

3.69. A CONTRATADA deve apresentar projeto executivo contendo a topologia completa da solução para monitoramento, detecção e mitigação de ataques, com a finalidade de demonstrar a conformidade com as especificações técnicas requeridas para esta solução.

3.69.1. O projeto executivo deve ser apresentado à Administradora da Rede e Serviços no prazo estabelecido no Plano de Transição.

3.70. Cabe à Administradora da Rede e Serviços efetuar a análise do projeto e aprová-lo, sendo-lhe facultada a realização de testes, incluindo os de ataques simulados visando validar o pleno atendimento aos requisitos contratuais.

3.70.1. Quando da realização dos testes de ataques simulados, a Administradora da Rede e Serviços comunicará à CONTRATADA para o devido planejamento, acompanhamento, cooperação e análise dos resultados, nos termos estabelecidos no Acordo Operacional.

3.70.2. Os testes de ataques podem ser realizados tanto para fins de aceite da implantação da solução como para verificação do atendimento aos requisitos no decorrer da vigência do Contrato.

IV. DESCRIÇÃO DO SERVIÇO DE ACESSO À INTERNET BANDA LARGA (Lote 2)

Prestação do Serviço de Acesso à Internet Banda Larga

4.1. O Lote 2 contempla o atendimento do Serviço de Acesso à Internet Banda Larga em duas modalidades:

4.1.1. Serviço de Acesso à Internet Banda Larga (SAI-BL) para o atendimento de unidades pertencentes aos OES;

4.1.2. Serviço de Acesso à Internet Banda Larga Itinerante (SAI-BLI) para o atendimento de casos especiais como casos emergenciais e itinerantes, que nesta modalidade, serão solicitados sob demanda.

4.2. O SAI-BL deve ser atendido com infraestrutura terrestre. Em caso da falta de viabilidade técnica para o atendimento com infraestrutura terrestre, será aceita a implementação com enlace satélite limitado a 10% da planta ativa.

4.3. O SAI-BLI deve obrigatoriamente ser atendido por um acesso satélite de baixa órbita (LEO) e é limitado a 1% da planta ativa.

4.4. O Serviço de Acesso à Internet Banda Larga (SAI-BL) é prestado à Unidade (UP ou UC) que o tenha contratado e consiste na oferta de acesso à Internet.

4.5. Para o SAI-BL e para o SAI-BLI as capacidades nominais são as larguras de banda mínimas contratadas que deverão ser garantidas pela CONTRATADA na prestação do serviço.

4.6. Para o SAI-BL, a capacidade de upload garantida deve ser igual ou superior a 50% àquela solicitada como capacidade nominal, que é a largura mínima de banda de download.

4.7. Para o SAI-BL atendido por satélite e para o SAI-BLI, a transmissão no enlace via satélite pode ser feita no modo assimétrico, desde que com taxa de transmissão de 20% (vinte por cento) da capacidade nominal do SAI-BLI para o tráfego originado na Unidade (*upload*) e taxa de transmissão de 100% (cem por cento) da capacidade nominal do SAI-BLI para o tráfego destinado à Unidade (*download*).

4.8. O OES deve solicitar o SAI-BL ou o SAI-BLI para uma Unidade escolhendo uma dentre as capacidades nominais de 30 Mbps, 50 Mbps, 100 Mbps, 150 Mbps, 200 Mbps, 300 Mbps, 500 Mbps, 700 Mbps e 1 Gbps.

4.9. A CONTRATADA deve utilizar equipamentos e *softwares* que suportem nativamente o protocolo IPv4 e IPv6 *Dual Stack*, conforme a solicitação feita pelo OES ou pela Administradora da Rede e Serviços.

4.10. Não são aplicáveis franquias de consumo de volume de dados ao SAI-BL.

4.11. Para o atendimento do SAI-BL ou SAI-BLI por satélite deve ser considerado o serviço sem franquia (com acesso ilimitado).

4.12. Os terminais LEO do SAI-BLI devem possuir 2 interfaces GigabitEthernet para conexão com a LAN;

4.13. O SAI-BLI deve estar disponível em todo o estado de São Paulo e em Brasília;

4.14. A instalação e tratamento de incidentes do SAI-BLI deverá sempre ser realizada em uma unidade do Governo do Estado de São Paulo pertencente à OES solicitante, ou em uma unidade de outro OES em comum acordo entre OES;

4.15. Todos os componentes físicos (hardware) utilizados no SAI-BLI devem estar homologados para uso em território nacional pela ANATEL.O Serviço de Acesso à Internet deve ser prestado em conformidade com o previsto no Contrato, em especial atendendo às metas de qualidade da prestação dos serviços relacionadas aos indicadores de desempenho técnico-operacional do Acordo de Níveis de Serviços (SLA).

4.16. O Serviço de Acesso à Internet Banda Larga deve ser provido somente para os endereços IP da rede local da Unidade informados dentre as alternativas possíveis, que abrangem a totalidade dos endereços IP da rede local, blocos de endereços IP, endereços IP individuais ou combinações das duas últimas opções.

4.16.1. O Serviço de Acesso à Internet Banda Larga deve ser provido sem a necessidade de autenticação de usuário e sem a necessidade de execução de comandos de desconexão.

4.17. A tradução dos endereços IPv4 privados (RFC 1918) aptos de cada Unidade deve ser executada para um ou mais endereços IPv4 e IPv6 públicos da CONTRATADA (NAT), de uso exclusivo e permanente vinculado a cada Unidade a que for prestado o Serviço de Acesso à Internet.

4.17.1. A quantidade de endereços IPv4 e IPv6 públicos utilizada deve ser suficiente para suportar a demanda por sessões simultâneas, considerando os momentos de pico de tráfego.

4.17.2. Em caso de recebimento de notificação judicial sobre o uso indevido da Internet através de endereço IPv4 público do SAI-BL, a CONTRATADA deve identificar o ID da Unidade vinculada e comunicar, por escrito, ao OES responsável para as providências cabíveis, com cópia para a Administradora da Rede e Serviços, anexando cópia da respectiva notificação.

4.18. A CONTRATADA deve prestar o SAI-BL na quantidade de até 400 acessos de capacidade de 100 Mbps para Unidades Cliente, cujos serviços devem ser prestados a título gratuito em qualquer dos municípios do âmbito da sua prestação e com capacidade dentre os valores definidos na Cláusula Social do Contrato.

Infraestrutura para a Prestação do Serviço de Acesso à Internet

4.19. Cabe ao OES a definição do local de instalação do CPE e do trajeto, desde o ponto de terminação da rede externa até o local de instalação do CPE, a ser seguido pela CONTRATADA para a instalação do enlace.

4.19.1. O OES é responsável pela segurança física do perímetro das suas Unidades.

4.19.2. Para o SAI-BLI, cabe ao OES a definição do local de instalação da antena/modem e a interconexão da terminação da rede externa até o local de instalação do modem/CPE.

4.19.3. Caso o SAI-BLI seja instalado em uma unidade móvel de atendimento, a mesma deverá estar presente fisicamente na unidade do OES informada na solicitação de ativação do serviço, assim como para o tratamento de incidentes, quando necessário.

4.20. A CONTRATADA deve prover os materiais e acessórios adequados às condições da infraestrutura disponível no local de instalação do CPE e no trajeto indicado pelo solicitante para a instalação do enlace.

4.20.1. A instalação do enlace deve ser feita em infraestrutura aparente, cabendo à CONTRATADA fornecer e instalar:

4.20.1.1. Cabos, fibras ópticas e demais meios de transmissão.

4.20.1.2. Conectores, amarradores, elementos de fixação com todas as partes e peças necessárias.

4.20.1.3. Materiais de encaminhamento (eletrodutos, junções e fixadores) até o local de instalação do CPE, exceto se houver disponibilidade no local e autorização do OES para o uso da sua infraestrutura interna de encaminhamento aparente.

4.20.2. Na execução de infraestrutura aparente, a CONTRATADA deve observar e seguir os padrões adotados pelo OES no local de instalação.

4.20.3. Cabe ao OES a execução de obras civis internas que eventualmente forem necessárias para a execução de infraestrutura aparente pela CONTRATADA.

4.20.3.1. A CONTRATADA deve construir base para instalação de antena de radioenlace ou satélite, em concreto, alvenaria ou qualquer outro material, bem como instalar para-raios, caso a instalação do enlace requeira tal infraestrutura.

4.20.3.2. Na instalação de enlace satélite é responsabilidade da CONTRATADA a instalação de base de fixação, antena, modem satelital, acessórios, cabos e todos materiais necessários para a disponibilização do serviço na unidade.

4.20.4. Caso haja infraestrutura embutida com dutos disponíveis e adequados, e desde que autorizado pelo OES, a CONTRATADA pode fazer o uso dela para a instalação do enlace, cabendo-lhe fornecer e instalar cabos, fibras ópticas e conectores com todas as partes e peças necessárias.

4.20.5. Se a instalação do enlace tiver que ser feita parte em infraestrutura aparente e parte embutida, aplicam-se concomitantemente, no que couber, as regras definidas em todos os subitens acima.

4.21. A CONTRATADA deve construir base em concreto, alvenaria ou qualquer outro material para instalação de antena, bem como instalar para-raios, caso a instalação do enlace requeira tal infraestrutura.

4.22. O OES deve fornecer as tomadas elétricas no padrão ABNT, na quantidade a ser definida pela CONTRATADA, condições ambientais, espaço e guarda apropriados para a instalação dos equipamentos da CONTRATADA.

4.23. O OES deve fornecer e instalar os cabos de interligação do(s) CPE aos equipamentos da sua rede local.

4.24. Para o provimento do SAI-BL, a CONTRATADA deve fornecer links para interligar o seu backbone Internet ao PoP 1 e ao PoP 2 do AS-GESP em arquitetura de alta disponibilidade conforme topologia de referência apresentada no item 3.28.

4.24.1. Estes links Internet não deverão ser renumerados, tendo seus custos diluídos pela solução do SAI-BL.

4.24.2. As conexões devem ser redundantes com banda inicial de 5 Gbps cada, adequada à vazão do tráfego entre as unidades remotas e o dispositivo central SD-WAN.

4.24.3. A infraestrutura da prestação do SAI-BL deve ser ampliada a fim de acompanhar o crescimento da utilização do serviço ao longo do período de execução contratual.

4.24.3.1. A CONTRATADA deve providenciar, o que couber, a ampliação da banda de sua infraestrutura utilizada para a interligação, sempre que a média móvel trimestral no horário comercial de utilização ultrapassar 50% de sua capacidade nominal ou quando o valor do 95º Percentil mensal, no horário comercial atingir ou ultrapassar 90% da sua capacidade nominal, o que ocorrer primeiro.

4.24.3.2. Durante a vigência do Contrato, as ampliações necessárias na infraestrutura e links devem estar disponíveis no prazo de 90 (noventa) dias a contar da data de ocorrência do evento que lhe der causa.

4.24.4. A implantação dos links deve estar concluída no prazo de 90 (noventa) dias a contar da data de assinatura do Contrato, conforme consta no Plano de Implantação.

Requisitos Operacionais e Técnicos para a Prestação do Serviço de Acesso à Internet Banda Larga

4.25. Deve ser atribuído aos acessos códigos de identificação (ID) a serem utilizados para se referir a esses elementos nos procedimentos estabelecidos no Acordo Operacional.

4.26. As conexões devem ser gerenciadas pela CONTRATADA para a prestação do serviço e para o planejamento da capacidade nominal desses recursos.

4.27. A CONTRATADA é responsável pela operação e manutenção, corretiva ou preventiva de suas conexões.

4.28. Para a prestação do SAI-BL, a CONTRATADA deve instalar na Unidade um CPE.

4.29. O CPE SAI-BL deve ser capaz de realizar NAT (*Network Address Translation*).

4.30. O CPE SAI-BL deve possuir interface *Ethernet* elétrica GE (*Gigabit Ethernet*) RJ45, para conexão com a LAN da Unidade.

4.31. Todas as interfaces LAN não utilizadas, incluindo eventual interface Wi-Fi, devem ser desabilitadas.

4.32. As informações de usuário e senha de administração do CPE não podem ser iguais (tipo admin/admin), padrão do fabricante ou com senha em branco e não devem estar informadas no chassi do equipamento.

4.33. A prestação do SAI-BL deve ser feita atendendo aos parâmetros de Qualidade de Serviço (QoS) apresentados a seguir:

4.33.1. Latência ESAQ: no máximo 100 ms (conforme Entidade Aferidora da Qualidade de Banda Larga - ESAQ).

4.33.2. *Jitter*: no máximo 30 ms (conforme Entidade Aferidora da Qualidade de Banda Larga - ESAQ).

4.33.3. Perda de pacotes: no máximo 1% (conforme Entidade Aferidora da Qualidade de Banda Larga - ESAQ).

4.33.4. Caso o SAI-BL seja atendido com acesso satélite, devem ser atendidos os parâmetros de Qualidade de Serviço (QoS) apresentados a seguir:

4.33.4.1. Se utilizado satélite geoestacionário, latência máxima de 800ms (conforme Entidade Aferidora da Qualidade de Banda Larga - ESAQ);

4.33.4.2. Se utilizado satélite de baixa órbita, latência máxima de 150ms (conforme Entidade Aferidora da Qualidade de Banda Larga - ESAQ).

V. DESCRIÇÃO DO SERVIÇO DE SD-WAN (Lote 3)

Prestação do Serviço de SD-WAN

5.1. ESCOPO GERAL

5.1.1. O Serviço de SD-WAN (SSDWAN) consiste na oferta de um sistema de gerenciamento, controle e orquestração centralizado por software e de um conjunto de dispositivos SD-WAN que serão instalados nas Unidades Cliente (UC) e nas Unidades Provedoras (UP).

5.1.1.1. O serviço SD-WAN deve permitir o gerenciamento da conectividade utilizando-se de diferentes serviços de comunicação entre as unidades, como, por exemplo, enlaces do SCM, do SAI-BL, entre outros.

5.1.1.2. O serviço deve gerenciar o encaminhamento de tráfego de acordo com as políticas de encaminhamento e as políticas de segurança, a serem definidas de acordo com a necessidade de cada órgão.

5.1.2. O SSDWAN deve ser prestado em todos os municípios do território do Estado de São Paulo e em Brasília-DF.

5.1.3. O SSDWAN deve ser prestado em conformidade com as especificações técnicas e operacionais que constam neste capítulo (REQUISITOS TÉCNICOS SD-WAN).

5.1.4. Será permitida a subcontratação parcial de serviços de terceiros, por parte da CONTRATADA relacionada ao Serviço de SD-WAN.

5.1.5. A CONTRATADA deve fornecer treinamentos técnicos em conformidade aos requisitos que constam na seção Treinamento deste capítulo.

5.1.6. O SSDWAN deve ser prestado em conformidade com os parâmetros associados às especificações técnicas e operacionais que constam do capítulo VI - Acordo de Níveis de Serviços (SLA), seção SD-WAN, deste documento.

5.1.7. O SSDWAN deve ser gerenciado em conformidade com as especificações técnicas e operacionais que constam do capítulo VII Gerenciamento, seção SDWAN, deste documento.

5.1.8. O SSDWAN é objeto de monitoramento por parte da Administradora da Rede e Serviços em conformidade com as especificações técnicas e operacionais que constam do capítulo VIII – Monitoramento, seção SD-WAN, deste documento.

5.1.9. A CONTRATADA deve fornecer as informações relativas à prestação do SSDWAN especificados neste documento, em conformidade com as especificações técnicas e operacionais que constam do capítulo IX – Fornecimento de Informações, seção SD-WAN, deste documento.

5.1.10. O Acordo Operacional, firmado entre a CONTRATADA e a Administradora da Rede e Serviços nos termos do capítulo relativo do Contrato, estabelece os procedimentos operacionais e administrativos associados à prestação do SSDWAN a serem observados pela CONTRATADA, pela Administradora da Rede e Serviços, pelos OES e pelas Unidades indicadas pelos mesmos, com o suporte do Sistema de Apoio Operacional e Gestão (SAOG) da PRODESP.

5.1.11. A CONTRATADA deve atender às solicitações sobre incidentes na prestação do SSDWAN, conforme disposto no Acordo Operacional, por meio de telefone com **número 0800**, disponível durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

5.1.12. A CONTRATADA deve manter a tecnologia sempre atualizada para atender aos requisitos de disponibilidade, de confiabilidade, de integridade, de segurança e de qualidade definidos para a prestação do SSDWAN.

5.1.13. Eventuais substituições e/ou atualizações das RFC (*Request for Comments*) e/ou recomendações e/ou normas constantes neste documento de especificação técnica devem ser observadas pela CONTRATADA visando a manutenção desses requisitos e a continuidade na prestação do SSDWAN.

5.1.14. A PRODESP exerce as funções de administração da Rede e Serviços, sendo neste caso referida como Administradora da Rede e Serviços, devendo ser representada por empregado indicado como Administrador da Rede e Serviços, enquanto a CONTRATADA deve indicar um empregado para representá-la como Gestor da Rede e Serviços, visando interagir com o Administrador da Rede e Serviços no exercício de suas atribuições, conforme previsto neste Contrato e em seus anexos.

5.1.15. A prestação do SSDWAN pode vir a ser objeto de avaliação visando garantir a manutenção dos requisitos e a continuidade de sua prestação, em consonância com os critérios e condições descritos a seguir:

5.1.15.1. A avaliação será feita pela Administradora da Rede e Serviços em conjunto com a CONTRATADA, a qualquer tempo, de forma remota ou nas dependências da CONTRATADA, por iniciativa da Administradora da Rede e Serviços ou de qualquer OES que a solicite.

5.1.15.2. A decisão de efetuar a avaliação deve ser comunicada à CONTRATADA, via correspondência oficial, com antecedência de 5 (cinco) dias corridos, na qual devem constar o motivo e o objeto da avaliação.

5.1.15.3. A CONTRATADA deve disponibilizar todas as informações e os meios necessários, bem como cooperar para o bom andamento das atividades inerentes a esta avaliação.

5.1.15.4. No decorrer da avaliação, serão realizados diagnósticos e estabelecidas ações com prazos para a solução das questões levantadas.

5.1.15.5. A divulgação dos resultados será feita por meio de relatório validado pelos avaliadores, Administrador da Rede e Serviços, e pelo Gestor da Rede.

5.1.16. A CONTRATADA é responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos e recursos que forem necessários para o provimento do SSDWAN.

5.1.17. A CONTRATADA deve efetuar, quando solicitado pela Administradora da Rede e Serviços, e com sua supervisão ou de seu preposto, testes de verificação da qualidade e segurança do serviço prestado, de forma a identificar eventuais falhas ou situações que possam influenciar nos níveis de serviço.

5.1.18. A CONTRATADA deve prestar o SSDWAN na quantidade de até 40 dispositivos categoria 1 para Unidades Cliente, cujos serviços devem ser prestados a título gratuito em qualquer dos municípios do âmbito da sua prestação e com capacidade dentre os valores definidos na Cláusula Social do Contrato.

5.1.19. Os recursos utilizados para a prestação da solução SD-WAN em acordo com o objeto do Contrato devem ser integrados à Rede IP Multisserviços e à Rede do Serviço de Acesso à Internet Banda Larga, gerenciando de forma centralizada os distintos enlaces de rede de telecomunicações que propiciam a integração entre os recursos de tecnologia de informação e comunicação das Unidades, bem como sua conectividade com a Internet e com outras redes públicas e privativas para navegação e acessibilidade ao conteúdo de bases de dados de interesse público.

5.1.20. A CONTRATADA e o FABRICANTE da solução de SD-WAN deve apresentar o projeto executivo da solução SD-WAN, contendo a topologia e os dispositivos de hardware e software que pretende empregar na prestação do SSDWAN, bem como suas funcionalidades e facilidades de configuração, gerenciamento, monitoramento, etc., com a finalidade de demonstrar o pleno atendimento às especificações técnicas contidas no termo de referência deste serviço.

5.1.20.1. O projeto executivo deve ser apresentado à Administradora da Rede e Serviços no prazo estabelecido no Plano de Implantação.

5.1.20.2. Cabe à Administradora da Rede e Serviços efetuar a análise do projeto e aprová-lo, sendo-lhe facultada requerer a realização de testes prévios de homologação na solução a ser empregada pela CONTRATADA, visando verificar o pleno atendimento aos requisitos contratuais.

5.1.20.3. Quando da realização dos testes, a Administradora da Rede e Serviços comunicará à CONTRATADA para ela providencie o ambiente de homologação e apresente o respectivo planejamento, acompanhamento, cooperação e análise dos testes e seus resultados, nos termos estabelecidos no Acordo Operacional.

5.1.20.4. A critério da Administradora da Rede e Serviços, os testes também podem ser realizados para fins de aceite da implantação da solução e para verificação do atendimento aos requisitos no decorrer da vigência do Contrato.

5.1.20.5. Para fins de aceite da implantação da solução a CONTRATADA deve realizar testes de integração entre o SSDWAN, SCM, STI e SAI-BL.

5.1.21. A solução deve ser composta por dispositivos SD-WAN que executem de forma integrada todas as funcionalidades e requisitos de conectividade, encaminhamento e segurança.

5.1.22. A solução deve ser constituída por dispositivos SD-WAN e Console de Gerência Centralizada.

5.1.22.1. Os grupos de gerenciamento, de Controle e de Dados devem ser segregados, de modo que a indisponibilidade de um grupo não comprometa a disponibilidade dos demais.

5.1.22.2. O gerenciamento centralizado deve se comunicar com os dispositivos por meio do SCM e Internet de forma segura e concomitante.

5.1.22.3. A solução de gerenciamento deve segregar a as funções de SD-WAN e segurança, de modo que possam ter diferentes administradores de acordo com a gestão e responsabilidades.

5.1.22.4. Todos os componentes utilizados na prestação do SSDWAN devem ser do mesmo fabricante, inclusive o sistema de gerência/orquestração, para que se mantenha a compatibilidade e as funcionalidades específicas exigidas.

5.1.22.5. Caso o elemento da solução não seja do mesmo fabricante, a CONTRATADA deverá apresentar atestado de homologação oficial emitido pelo fabricante.

5.1.22.6. Todos os componentes Físicos (*hardware*) da solução de SD-WAN e segurança devem ser homologados pela Anatel.

5.1.22.7. Não serão aceitos componentes operando em *desktop*, *white box, appliances* desenvolvidos por terceiros e soluções *open source*.

5.1.22.8. O fabricante da solução ofertada deve ser qualificado no relatório Magic Quadrant for SD-WAN Gartner 2023

5.1.23. A solução deve consistir em plataforma baseada em dispositivo físico com funcionalidades de SD-WAN (*Software-Defined WAN*) e *Firewall Stateful* com visibilidade de camada 7.

5.1.24. A solução SD-WAN deve suportar a interconexão com outros serviços de Internet banda larga contratados pelas Unidades fora do âmbito da Rede Intragov, respeitando o limite de interfaces de rede especificadas para cada categoria do dispositivo SD-WAN

5.1.25. O SSDWAN deve ser prestado por meio de dispositivos SD-WAN e sistema de gerência centralizado que possibilite a criação de instâncias de gerenciamento distintas por OES ou grupos de Unidades conforme necessidades dos OES e da Administradora da Rede e Serviços.

5.1.26. Quando da contratação do SSDWAN, devem ser observadas as seguintes características da solução proposta:

5.1.26.1. Deve oferecer possibilidade de configuração de redundância e de comunicação de alta disponibilidade operando com links ativos de acordo com cada cenário de rede e políticas de encaminhamento a serem definidos durante a prestação do serviço.

5.1.26.2. Deve permitir a configuração de políticas de gerenciamento de tráfego distintas por unidade de acordo com as necessidades específicas de cada OES.

5.1.27. A CONTRATADA deve manter a tecnologia sempre atualizada para atender aos requisitos de disponibilidade, de confiabilidade, de integridade, de segurança e de qualidade definidos para a prestação dos serviços SD-WAN.

5.1.28. A CONTRATADA deve conectar as unidades de interesse de cada OES conforme o modelo de rede overlay definido no projeto executivo.

5.1.28.1. A CONTRATADA deve conectar as unidades contratadas por meio de VPN *client-to-site ou site-to-site* de interesse de cada OES, respeitando-se as quantidades de túneis definidas por modelo.

5.1.29. A prestação dos serviços pode vir a ser objeto de avaliação visando garantir a manutenção dos requisitos e a continuidade na prestação dos serviços, em consonância com os critérios e condições descritas a seguir:

5.1.29.1. A avaliação será feita pela Administradora da Rede e Serviços em conjunto com a CONTRATADA, a qualquer tempo, de forma remota ou nas dependências da CONTRATADA, por iniciativa da Administradora da Rede e Serviços ou de qualquer OES que a solicite.

5.1.29.2. A decisão de efetuar a avaliação deve ser comunicada à CONTRATADA, via correspondência oficial, com antecedência de 5 (cinco) dias corridos, na qual devem constar o motivo e o objeto da avaliação.

5.1.29.3. A CONTRATADA deve disponibilizar todas as informações e os meios necessários, bem como cooperar para o bom andamento das atividades inerentes a esta avaliação.

5.1.29.4. No decorrer da avaliação, serão realizados diagnósticos e estabelecidas ações com prazos para a solução das questões levantadas.

5.1.29.5. A divulgação dos resultados deve ser feita através de relatório validado pelos avaliadores, pelo Administrador da Rede e pelo Gestor da Rede.

5.1.30. O sistema de gerência SD-WAN centralizado deve permitir o provisionamento *zero touch* dos dispositivos SD-WAN com a possibilidade de se utilizar *templates* para otimizar a implantação.

5.1.31. Caso solicitado na contratação pelo OES CONTRATANTE, o SSD-WAN deve atender ao requisito de alta disponibilidade.

5.1.31.1. Para o SSDWAN em alta disponibilidade o OES contratará dois serviços SD-WAN (com dispositivos distintos) com indicação de configuração em alta disponibilidade.

5.1.31.2. Os dispositivos SD-WAN deverão operar em grupos de pelo menos 2 equipamentos em alta disponibilidade.

5.1.31.3. Caso sejam compostos por mais de um equipamento, cada elemento dessa composição deve ser duplicado.

5.1.31.4. Deve operar em modo de tolerância a falhas (Alta Disponibilidade) de forma a garantir que, se um dos dispositivos parar de funcionar, os demais equipamentos do cluster deverão assumir automaticamente, suportando todo o tráfego.

5.1.31.5. Esta solução deve permitir a função de tolerância a falhas, nos modos Ativo/Passivo e Ativo/Ativo, com todas as licenças de software habilitadas para tal, de forma a garantir que, se um dos equipamentos parar de funcionar, os demais deverão assumir automaticamente, suportando todo o tráfego com todas as funcionalidades de segurança ativas.

5.1.32. A CONTRATADA deve disponibilizar um cluster de concentradores SD-WAN no PoP 1 e outro no PoP 2 do AS-GESP em arquitetura de alta disponibilidade conforme topologia de referência apresentada no item 3.28.

5.1.33. Estes dispositivos serão utilizados como redundância em caso de falha no SCM das unidades remotas, de modo que o tráfego da comunicação entre a Rede Multisserviço e a unidade remota fluirá através da rede do serviço SAI-BL, por meio de VPN seguras estabelecidas pelo serviço SSDWAN.

5.1.34. As interligações em âmbito local com os roteadores PE (SCM) e com os CPE do SAI-BL devem ser dualizadas.

5.1.35. A CONTRATADA deve gerenciar os ativos de rede e as ferramentas de segurança, com completa visibilidade e controle de toda essa infraestrutura de rede, mantendo-a atualizada e em conformidade com todos normativos e requisitos de segurança da rede.

5.1.36. A CONTRATADA deverá realizar análises periódicas nos segmentos da rede da CONTRATANTE, visando detectar possíveis falhas de segurança da rede e fornece relatórios contendo os resultados das análises realizadas e situação atual da rede contratada, sempre que solicitado pela CONTRATANTE.

5.1.37. Após a ocorrência de incidente ou ataque, a CONTRATADA deve reestabelecer a comunicação da rede.

5.1.38. A CONTRATADA deve fazer a investigação das causas dos incidentes de segurança na rede.

5.1.39. A CONTRATADA deve criar e configurar as políticas de segurança a serem aplicadas na rede (elementos ativos e serviços).

5.1.40. A CONTRATADA é responsável pela geração e divulgação de relatórios dos ataques e incidentes de segurança, os quais devem ser disponibilizados para acesso on-line pelo CONTRATANTE.

5.1.41. Devem ser fornecidos relatórios em formato HTML e PDF, dos eventos de IPS/IDS e antimalware.

5.1.42. A CONTRATADA deve elaborar e acompanhar o plano de tratamento de riscos.

5.1.43. Os serviços e o monitoramento de segurança devem estar disponíveis em regime de operação 24x7 durante toda a vigência do contrato.

5.1.44. A CONTRATADA e o FABRICANTE da solução de SD-WAN devem possuir centro de atendimento no Brasil, com equipe técnica especializada em SD-WAN e Segurança para abertura e gerenciamento chamados.

5.1.45. A CONTRATADA deve detectar ameaças, e mitigar ataques e incidentes de segurança na rede junto com o FABRICANTE.

5.1.46. A CONTRATADA colocará à disposição da PRODESP, pessoal técnico especializado necessário do FABRICANTE da solução, para a prestação do serviço de apoio.

5.1.47. A CONTRATADA deve prover formação oficial online certificada da FABRICANTE, incluindo vouchers de certificação, para 14 colaboradores da CONTRATANTE.

5.1.48. Devem incluir a nomeação de um engenheiro líder do FABRICANTE na região responsável pela gestão de tickets gerados pela CONTRATANTE ou alguém indicado, no regime em horário comercial 8x5.

5.1.49. Deve incluir a designação de um gerente de serviços do FABRICANTE como ponto único de contato para consultas de serviços, acompanhamento na resolução de incidentes nos horários estabelecidos e prestação de serviços em geral em horário comercial 8x5.

5.1.50. Deve fornecer relatórios de análise de causa raiz (RCA) para incidentes críticos (Prioridade 1 e 2) emitidos pelo FABRICANTE.

5.1.51. Deve fornecer revisão da plataforma com relatórios trimestrais indicando as melhores práticas, recomendações e saúde da plataforma pelo FABRICANTE

5.1.52. Deve incluir teleconferências periódicas para acompanhamento dos tickets abertos com a CONTRATADA e o FABRICANTE.

5.1.53. A PRODESP deve ter a opção de solicitar recomendação de upgrade de software para o FABRICANTE da solução de SD-WAN com base em correções de bugs e requisitos operacionais.

5.1.54. O FABRICANTE deve comunicar à Entidade Compradora qualquer questão crítica aberta que possa afetar o seu ambiente.

5.1.55. O FABRICANTE deverá realizar pelo menos uma reunião ou assistência técnica presencial PRODESP.

5.1.56. O FABRICANTE deverá incluir um workshop personalizado sobre a solução de SD-WAN, a sessão deve incluir resolução de problemas e recomendações para problemas comumente vistos, a sessão deve ser remota e prática para 3 funcionários da entidade.

5.1.57. Deve permitir pelo menos duas assistências remotas anuais do FABRICANTE, fora do horário de expediente, para as janelas de manutenção indicadas pela PRODESP.

Concentradores

5.1.58. A CONTRATADA deverá implantar Clusters de concentradores, com no mínimo dois appliances em alta disponibilidade em modo Ativo/Passivo e/ou Ativo/Ativo da rede SD-WAN em cada um dos POPs indicados conforme topologia de referência apresentada no item 3.28;

5.1.59. A CONTRATADA deverá garantir a interconexão entre a rede, rede VPN IP do CONTRATANTE e a rede da PRODESP.

5.1.60. A CONTRATADA deverá prover em cada concentrador a solução SD-WAN, em alta disponibilidade (ativo/passivo ou ativo/ativo) e de acordo com as especificações definidas neste Termo de Referência;

5.1.61. Os Clusters de Concentradores SD-WAN e demais equipamentos que componham esta finalidade, devem ser do mesmo fabricante da solução de SD-WAN;

5.1.62. Os Concentradores podem ser entregues em 1 (um) ou mais equipamentos, aplicando o conceito múltiplos Clusters para atender grupos de OES.

5.1.63. O Concentrador e seus respectivos elementos, devem ser entregues com no mínimo a somatória dos requisitos abaixo

5.1.63.1. Throughput de, no mínimo, 400 Gbps com a funcionalidade de Firewall;

5.1.63.2. Throughput de, no mínimo, 200 Gbps de VPN IPSec;

5.1.63.3. Throughput de, no mínimo, 60 Gbps de Threat Prevention;

5.1.63.4. Possuir ao menos 30 interfaces 10 GE SFP+ com seus respectivos transceivers;

5.1.63.5. Possuir ao menos 4 interfaces 100 GE QSFP28 com seus respectivos transceivers;

5.1.63.6. As interfaces de utilizadas para comunicação interna dos elementos do Concentrador, não devem contar para os dois itens acima. Ou seja, além das interfaces utilizadas para comunicação dos elementos do Concentrador, devem ser entregues também ao menos 30 interfaces 10 GE SFP+ e ao menos 4 interfaces 100 GE QSFP28 para comunicação do concentrador com as demais redes;

5.1.63.7. Todos os elementos do concentrador devem ser entregues em Alta Disponibilidade;

5.1.63.8. Todos os elementos do concentrador devem possuir fonte redundante hot-swap.

Gerência Centralizada SD-WAN

5.1.64. A solução SD-WAN deverá possuir gerência centralizada;

5.1.65. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de *end-of-life, end-of-sale e end-of-support.*

5.1.66. As licenças de uso de software serão cedidas e atualizadas durante toda a vigência contratual. A solução de SD-WAN, Gerência Centralizada e todas as funcionalidades que compõe as soluções, exceto filtro de conteúdo web e serviço ATP, deverão estar funcionais e acessíveis, mesmo que incapaz de atualizar softwares e assinaturas, após o término do período contratado.

5.1.67. O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e API aberta.

5.1.68. Os elementos da gerência da solução SD-WAN poderão ser entregues na forma de servidores dedicados ou virtualizados, não sendo permitida a entrega em nuvem ou datacenter de terceiros a PRODESP;

5.1.68.1. Em caso de entrega da solução de gerenciamento em modo virtualizado, deverá ser entregue o hardware e qualquer outra licença necessária para o pleno funcionamento da máquina virtual da solução.

5.1.69. O gerenciamento da solução deve possuir, no mínimo, 400 Terabytes de armazenamento;

5.1.70. O gerenciamento da solução de suportar, no mínimo, 120.000 logs/segundo.

5.1.71. Deverá possuir pelo menos duas camadas para tratamentos de logs, uma para coleta e a outra para análise e correlação de eventos e relatórios.

5.1.72. O sistema deverá suportar contas de usuário/senha estáticas.

5.1.73. Deverá possuir token para MFA para no mínimo 50 usuários administradores;

5.1.73.1. Os tokens devem ser compatíveis com sistemas operacionais Android ou Apple IOS;

5.1.73.2. Não serão permitidos utilização de tokens que necessitem cadastro em plataformas de SaaS e/ou Provedores de Identidades públicos;

5.1.73.3. Os usuários e tokens devem ser administrados pela plataforma de gerência centralizada;

5.1.74. Devem ser entregues no mínio 50 tokens físicos para no mínimo 50 usuários e administradores, para acesso a plataforma de gerência;

5.1.75. O Sistema de gerência centralizada SD WAN deve permitir acesso concorrente de administradores.

5.1.76. O Sistema deverá garantir a integridade das configurações, através de bloqueio de alterações em caso de acesso simultâneo de dois ou mais administradores no mesmo equipamento ou Cluster.

5.1.77. A gerência centralizada SD-WAN deve permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações.

5.1.78. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor Radius e Tacacs+.

5.1.79. A solução deverá suportar a automação/integração da rede e as comunicações deverão ser protegidas e criptografadas.

5.1.80. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento.

5.1.81. Todas as alterações de configuração deverão ser registadas e arquivadas para fins de auditoria.

5.1.82. A solução deve incluir PKI integrada para emissão automática de certificados digitais utilizados durante autenticação dos túneis VPN.

5.1.83. Os dispositivos SD-WAN deverão suportar SNMP, syslog e restAPI.

5.1.84. A Gerência SD-WAN deverá ter a capacidade de enviar mensagens syslog referentes aos equipamentos SD-WAN para um servidor syslog da CONTRATANTE.

5.1.85. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada dispositivo SDWAN a cada 5 (cinco) minutos no mínimo.

5.1.86. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN.

5.1.87. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visão geral da saúde dos links, desempenho da aplicação, utilização da largura de banda e conformidade do nível de serviço definido.

5.1.88. A solução de gerência SD-WAN deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros.

5.1.89. Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN.

5.1.90. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação.

5.1.91. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Web filtering.

5.1.92. A solução de gerenciamento deve permitir a identificação de quais regras de um objeto estão sendo utilizadas.

5.1.93. A solução de gerenciamento deve permitir criação de regras que fiquem ativas em horário definido.

5.1.94. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos *appliances.*

5.1.95. A solução de gerenciamento deve ser capaz de gerar relatórios ou exibir comparativos entre duas configurações diferentes, resumindo as alterações efetuadas.

5.1.96. Desejável que a solução de gerenciamento permita criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas elas somente sejam aplicadas após aprovação de outro administrador.

5.1.97. A solução de gerência deve adicionar os dispositivos SD-WAN de forma automática.

5.1.98. A solução deve permitir a adição de políticas e objetos para os dispositivos.

5.1.99. A solução deve permitir Webhook para plataformas de terceiros, incluindo ServiceNow;

5.1.100. A solução de gerenciamento deve permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, IP de gerência, licenças, horário do sistema e firmware.

5.1.101. A solução de gerenciamento deve permitir a instalação de políticas e configurações dos dispositivos por meio de "wizard", templates ou outros meios.

5.1.102. A solução deve permitir criar na solução de gerência *templates* de configuração dos dispositivos.

5.1.103. A solução deve permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados.

5.1.104. Deve possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência.

5.1.105. Deve realizar o backup das configurações com número de revisão que permita a visibilidade nas alterações e o retorno de configuração no plano de volta.

5.1.106. A solução deve permitir a operação e configurações diretamente no equipamento SD-WAN remotos mesmo que gerenciado centralmente, todas as configurações aplicadas devem ser autorizadas ou recusadas pela plataforma de gerência.

5.1.107. A solução deve permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada.

5.1.108. A solução deve permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos.

5.1.109. A solução deve permitir criar regras anti DoS de forma centralizada para os concentradores.

5.1.110. A solução deve permitir criar os objetos que serão utilizados nas políticas de forma centralizada.

5.1.111. A solução deve permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia.

5.1.112. A solução deve permitir provisionamento do Zero Touch que deverá funcionar de tal forma que dispositivos SD-WAN sejam enviados diretamente do fornecedor para um endereço de interesse do CONTRATANTE sem a necessidade de configuração prévia do dispositivo de acesso.

5.1.113. A solução deve ser entregue em alta disponibilidade, distribuídos entre dois data centers da CONTRATANTE.

Requisitos Técnicos SD-WAN

5.1.114. A solução de comunicação de dados utilizará a tecnologia SD-WAN com o objetivo de balancear o tráfego de forma inteligente para otimizar ao máximo o uso da rede.

5.1.115. O tráfego de saída de Internet deverá ser descentralizado em todas as unidades dos órgãos atendidos por essa rede, Unidades Clientes e Unidades Provedoras.

5.1.116. Todos os tuneis criptografados da solução de SD-WAN, devem usar autenticação por certificado digital, emitidos pela PKI da Gerência Solução.

5.1.117. Todas as UCs quanto as UPs estarão contempladas pela rede contratada e em cada unidade deverá ser instalado o equipamento SD-WAN e os links de MPLS e/ou de internet banda larga, conforme disposto neste documento e no Termo de Referência.

5.1.118. Os concentradores SD WAN devem ser instalados nos datacenters da PRODESP. A forma de roteamento desse tráfego será definida no projeto executivo.

5.1.119. Os concentradores deverão encaminhar o tráfego corporativo para PRODESP.

5.1.120. O contingenciamento dos concentradores deverá prever o encaminhamento do tráfego para os demais concentradores ativos, conforme será definido no projeto executivo.

5.1.121. O plano de endereçamento IP será definido no projeto executivo.

5.1.122. A rede contratada deverá se conectar com a estrutura de nuvem do prestador que atende a CONTRATANTE diretamente pela Internet ou pela rede da PRODESP, conforme será definido no Projeto Executivo. A CONTRATADA deverá conectar todas as unidades ao ambiente de nuvem contratado pela PRODESP por meio de VPN site-to-site, utilizando os links de Internet que saem dos concentradores da rede ou conforme será definido no Projeto Executivo.

5.1.123. A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita utilizando a solução SD-WAN.

5.1.124. O serviço de DHCP relay das redes locais das unidades deverá ser provido pelo equipamento SD-WAN.

5.1.125. Todos os dispositivos SD-WAN da rede de acesso devem ser dimensionados de forma que tenham capacidade de processamento compatíveis com as velocidades dos links WAN conectados.

5.1.126. O CONTRATANTE deverá ter acesso do tipo leitura nos equipamentos da rede de acesso instalados nos seus endereços de interesse. Por acesso entende-se permissão de ingresso utilizando interface web, protocolo https, linha de comando utilizando ssh e possibilidade de obtenção de dados via SNMP e syslog.

5.1.127. Todos os equipamentos compostos no projeto de SD-WAN, deverão ser acessíveis a partir de plataformas de gerenciamento SNMP, syslog localizadas na rede interna da PRODESP.

5.1.128. Os equipamentos SD-WAN com segurança devem ser fornecidos em formato de equipamento físico dedicado, devendo ser implementadas as funcionalidades de SD-WAN e segurança em um mesmo hardware. Um mesmo equipamento deve implementar todas as funcionalidades de roteamento, SD-WAN e segurança.

5.1.129. A solução SD-WAN deverá ser composta por dispositivos SD-WAN (SD-WAN Appliances) e Console de Gerência Centralizada.

5.1.130. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação.

5.1.131. Deve ser possível criar políticas para modelagem do tráfego definido pelo menos os parâmetros:

5.1.131.1. IP de origem;

5.1.131.2. VLAN de origem;

5.1.131.3. IP de destino;

5.1.131.4. Porta TCP/UDP de destino;

5.1.131.5. Domínio e URL de destino;

5.1.131.6. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

5.1.131.7. Grupos de categorias de aplicação de camada 7 (Colaboração, SaaS etc);

5.1.131.8. Tráfego multicast controlado pelas políticas de SD-WAN

5.1.132. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp.

5.1.133. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente.

5.1.134. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo.

5.1.135. A solução deve permitir a definição do roteamento para cada aplicação.

5.1.136. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação.

5.1.137. A solução deve possibilitar a definição do link de saída para uma aplicação específica.

5.1.138. A solução deve implementar balanceamento de link por hash do IP de origem e destino;

5.1.139. A solução deve implementar balanceamento de link por volume. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

5.1.140. A solução de SD-WAN deve suportar o encapsulamento de VRFs entre HUB e Spokes, segregando logicamente a tabela de roteamento nas VRFs entre tuneis IPSec.

5.1.141. A solução de SD-WAN deve suportar a funcionalidade de route leaking entre as VRFs permitindo comunicação entre diferentes tabelas de roteamento, segmentos e acesso internet local.

5.1.141.1. A solução de SD-WAN deve suportar interfaces lógicas com diferentes encapsulamentos VLANs (802.1Q), IPSec, GREs, Ethernet.

5.1.142. A solução de SD-WAN deve suportar IPv6.

5.1.143. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

5.1.144. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding.

5.1.145. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

5.1.146. Para IPv6, deve suportar roteamento estático e dinâmico (BGP e OSPF);

5.1.147. Deve suportar multicast PIM-DM e PIM-SM;

5.1.148. A solução deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote ou sessão entre eles.

5.1.149. A solução deve possuir recurso para correção de erro, possibilitando a redução das perdas de pacotes nas transmissões.

5.1.150. A solução deve permitir a customização dos *timers* para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido.

5.1.151. 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 tera capacidade de controlá-las por políticas de *shaping*. Dentre as tratativas possíveis, a solução deve contemplar o suporte a criação de políticas Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações, categoria de URL, protocolos UDP/TCP e portas.

5.1.152. O Traffic Shaping deve possibilitar a definição de tráfego com banda garantida, máxima, prioridade (baixa/media/alta) e marcação DSCP. Ex: banda mínima disponível e máxima para aplicações de negócio.

5.1.153. Os Concentradores de SD-WAN, devem realizar testes de velocidade no overlay, com a finalidade de obter o real valor do Link com o spoke dinamicamente. O resultado deve ser armazenado para uso futuro e ser utilizado dinamicamente na política de Traffic shaping de saída.

5.1.154. O Traffic shaping deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best- effort/não corporativas, tais como Youtube, Facebook etc.

5.1.155. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda.

5.1.156. O Traffic Shaping deve possibilitar a definição de filas.

5.1.157. O Traffic Shaping deve ser definido utilizando categoria de aplicações.

5.1.158. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

5.1.159. A solução deve ter a capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço.

5.1.160. Deve possibilitar a definição de bandas distintas para download e upload.

5.1.161. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência).

5.1.162. A solução deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN.

5.1.163. O dispositivo SD WAN deve ter suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo.

5.1.164. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN.

5.1.165. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site.

5.1.166. A solução deve ter a funcionalidade de bloqueio de acesso à aplicações.

5.1.167. A solução deve suportar NAT dinâmico bem como NAT de saída.

5.1.168. Deve suportar balanceamento de tráfego por sessão ***ou*** pacote.

5.1.169. O dispositivo SD-WAN deverá possuir serviço de servidor DHCP.

5.1.170. O dispositivo SD-WAN deverá possuir serviço de DHCP relay.

5.1.171. O dispositivo SD-WAN deverá suportar Agregação de links 802.3ad (LACP).

5.1.172. Deve possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link.

5.1.173. O dispositivo SD-WAN deverá suportar vários links de acesso, como Internet dedicada e Internet com garantia de banda por meio privativo e independente.

5.1.174. O equipamento SD WAN deverá ter capacidade para utilizar as tecnologias 3G/4G por meio de modens da CONTRATANTE, ADSL ou similar. Caso necessário, a pedido do CONTRATANTE, a CONTRATADA deverá efetuar todas as configurações necessárias, no equipamento e na rede, para efetiva utilização dessas tecnologias, com todas as funcionalidades disponíveis na solução SD WAN.

5.1.175. A solução deve possuir capacidade de agregar e balancear, no mínimo, 8 circuitos de dados, sendo físico ou lógico.

5.1.176. A solução deve permitir a configuração de ISP (rota default estática) com a utilização de probe ou de forma similar para verificar a disponibilidade do provedor. A *probe* ou similar deve permitir verificar o acesso a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência).

5.1.177. Deve ter funcionalidade de inspeção via web filter transparente para navegação a sites HTTP/HTTPS (situação em que o cliente não precisa encaminhar o tráfego para o IP do proxy, de modo que o cliente acredita estar acessando diretamente o conteúdo desejado).

5.1.178. Os equipamentos SD-WAN deverão suportar e estar licenciados para operarem em alta disponibilidade Ativo/Passivo e Ativo/Ativo;

5.1.179. A configuração em alta disponibilidade deve sincronizar sessões, configurações, incluindo políticas de Firewall, NAT e objetos de rede, certificados VPNs e SD-WAN.

5.1.180. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

5.1.181. Os dispositivos devem ser destinados ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação), e suportar temperatura ambiente de armazenamento entre 0ºC e 50ºC.

5.1.182. Entende-se por *Threat Prevention* as funcionalidades de Controle de Aplicação, IPS e Antimalware habilitadas com logs.

5.1.183. Os dispositivos de comunicação de dados utilizados pela CONTRATADA na solução, devem estar em conformidade com os normativos regulatórios nacionais, incluindo homologação válida e emitida pela ANATEL na data da abertura do certame.

5.1.184. Não serão aceitas funcionalidades que estão previstas somente em Roadmap ou versão pré-produção, sem pleno suporte pelo fabricante.

Dispositivos SD-WAN

5.1.185. O SSDWAN é contratado para Unidade do OES dentre 7 categorias distintas, de acordo com a demanda e porte da unidade, conforme descrito nos itens a seguir.

5.1.186. Os valores de capacidades indicados para as categorias superiores (6 e 7) podem ser compostas por estratégia de cluster, viabilizado pelo crescimento horizontal.

5.1.187. Equipamento SD-WAN categoria 1 - atendendo aos seguintes requisitos:

5.1.187.1. Throughput de, no mínimo, 150 Mbps de Threat Prevention;

5.1.187.2. Throughput de, no mínimo, 200 Mbps de Inspeção SSL;

5.1.187.3. Throughput de, no mínimo, 800 Mbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.187.4. Throughput de, no mínimo, 3.3 Gbps de VPN IPSec;

5.1.187.5. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.187.6. Possuir ao menos 5 (cinco) interfaces 1 GE RJ45;

5.1.187.7. Possuir fonte de alimentação externa;

5.1.188. Equipamento SD-WAN categoria 2 - atendendo aos seguintes requisitos:

5.1.188.1. Throughput de, no mínimo, 300 Mbps de Threat Prevention;

5.1.188.2. Throughput de, no mínimo, 400 Mbps de Inspeção SSL;

5.1.188.3. Throughput de, no mínimo, 1 Gbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.188.4. Throughput de, no mínimo, 4 Gbps de VPN IPSec;

5.1.188.5. Estar licenciado para, ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.188.6. Possuir ao menos 8 interfaces 1 GE RJ45;

5.1.188.7. Possuir fonte de alimentação externa;

5.1.189. Equipamento SD-WAN categoria 3 - atendendo aos seguintes requisitos:

5.1.189.1. Throughput de, no mínimo, 500 Mbps de Threat Prevention;

5.1.189.2. Throughput de, no mínimo, 600 Mbps de Inspeção SSL;

5.1.189.3. Throughput de, no mínimo, 1 Gbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.189.4. Throughput de, no mínimo, 4.5 Gbps de VPN IPSec;

5.1.189.5. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.189.6. Possuir ao menos 8 interfaces 1 GE RJ45;

5.1.189.7. Possuir fonte de alimentação externa.

5.1.190. Equipamento SD-WAN categoria 4 - atendendo aos seguintes requisitos:

5.1.190.1. Throughput de, no mínimo, 1 Gbps de Threat Prevention;

5.1.190.2. Throughput de, no mínimo, 2 Gbps de Inspeção SSL;

5.1.190.3. Throughput de, no mínimo, 1.6 Gbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.190.4. Throughput de, no mínimo, 8.5 Gbps de VPN IPSec;

5.1.190.5. Estar licenciado para, ou suportar sem o uso de licença, 1800 túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.190.6. Possuir ao menos 10 interfaces 1 GE RJ45;

5.1.190.7. Possuir ao menos 2 interfaces 10 Gbps SFP+ e seus respectivos adaptadores.

5.1.190.8. Possuir 2 fontes de alimentação internas, redundantes.

5.1.191. Equipamento SD-WAN categoria 5 - atendendo aos seguintes requisitos:

5.1.191.1. Throughput de, no mínimo, 10 Gbps de Threat Prevention;

5.1.191.2. Throughput de, no mínimo, 10 Gbps de Inspeção SSL;

5.1.191.3. Throughput de, no mínimo, 15 Gbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.191.4. Throughput de, no mínimo, 40 Gbps de VPN IPSec;

5.1.191.5. Estar licenciado para, ou suportar sem o uso de licença, 20.000 túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.191.6. Possuir ao menos 8 interfaces 1 GE RJ45;

5.1.191.7. Possuir ao menos 8 interfaces 1 GE SFP;

5.1.191.8. Possuir ao menos 06 interfaces 10 GE SFP+ com seus respectivos transceivers;

5.1.191.9. Possuir 2 fontes de alimentação internas, redundantes e hot-swap;

5.1.192. Equipamento SD-WAN categoria 6 - atendendo aos seguintes requisitos:

5.1.192.1. Throughput de, no mínimo, 20 Gbps de Threat Prevention;

5.1.192.2. Throughput de, no mínimo, 25 Gbps de Inspeção SSL;

5.1.192.3. Throughput de, no mínimo, 30 Gbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.192.4. Throughput de, no mínimo, 80 Gbps de VPN IPSec;

5.1.192.5. Estar licenciado para, ou suportar sem o uso de licença, 30.000 túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.192.6. Possuir ao menos 10 interfaces 10 GE SFP+ com seus respectivos transceivers;

5.1.192.7. Possuir ao menos 4 interfaces 100 GE QSFP28 com seus respectivos transceivers;

5.1.192.8. Possuir 2 fontes de alimentação internas, redundantes e hot-swap;

5.1.193. Equipamento SD-WAN categoria 7 - atendendo aos seguintes requisitos:

5.1.193.1. Throughput de, no mínimo, 50 Gbps de Threat Prevention;

5.1.193.2. Throughput de, no mínimo, 55 Gbps de Inspeção SSL;

5.1.193.3. Throughput de, no mínimo, 60 Gbps com a seguinte classificação de segurança, NGFW, composto por Firewall, IPS e controle de aplicações habilitadas;

5.1.193.4. Throughput de, no mínimo, 150 Gbps de VPN IPSec;

5.1.193.5. Estar licenciado para, ou suportar sem o uso de licença, 40.000 túneis de VPN IPSEC Site-to-Site simultâneos;

5.1.193.6. Possuir ao menos 8 interfaces 10 GE SFP+ com seus respectivos transceivers;

5.1.193.7. Possuir ao menos 4 interfaces 100 GE QSFP28 com seus respectivos transceivers;

5.1.193.8. Possuir 2 fontes de alimentação internas, redundantes e hot-swap;

Políticas de encaminhamento

5.1.194. A solução SD-WAN deverá ser capaz de balancear o tráfego das aplicações entre múltiplos links simultaneamente.

5.1.195. A Solução SD-WAN deverá analisar o fluxo do tráfego em tempo real e realizar a duplicação de pacotes através de regras, distribuir em múltiplos links simultaneamente, realizar a reordenação dos pacotes no outro extremo.

5.1.196. A Solução SD-WAN deve monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente.

5.1.197. A Solução SD-WAN deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos CPEs, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas.

5.1.198. A Solução deverá permitir que os endereços de interesse do CONTRATANTE acessem sites VPN legados (não-SD-WAN) sem fazer backhauling do tráfego de aplicativos por meio de um hub SD-WAN.

5.1.199. A solução deve permitir criar políticas para a modelagem do tráfego.

5.1.200. A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas, respeitando o tempo limite de expiração dessas sessões

5.1.201. A rede deve suportar o roteamento das unidades para os concentradores pela métrica de intenção de tráfego.

Tunelamento e Criptografia

5.1.201.1. A solução deverá permitir a comunicação indireta entre localidades por meio de topologia “hub and spoke”.

5.1.201.2. A solução deverá permitir a comunicação por meio de localidades em que se faz necessária a centralização do tráfego utilizando uma topologia “hub and spoke”.

5.1.201.3. A solução SD-WAN deverá criar dinamicamente os túneis criptografados entre as localidades que possuam SD-WAN.

5.1.201.4. Os equipamentos utilizados na solução SD-WAN deverão implementar túneis VPN IPSEC com capacidade de integração com equipamentos de outros fabricantes.

Conectividade em nuvens públicas (SAAS)

5.1.202. A solução SD-WAN deve possuir mecanismos de monitoração PASSIVA da qualidade dos enlaces disponíveis na unidade (Identificar o estado real entre as estações) até as aplicações SaaS;

5.1.203. A solução SD-WAN deve suportar segregação de fluxo através de zonas locais (DIA) direct internet access, permitindo a comunicação com aplicações de software como serviços em nuvem pública;

5.1.204. A solução deve suportar a conectividade local via zona DIA (direct Internet access) para aplicações corporativas, como Webex, Teams, Salesforce, Sap, Oracle;

5.1.205. A solução deve possuir uma lista dinâmica e atualizada pelo Fabricante para aplicações corporativas, como Microsoft, Office 365,Teams, salesforce, sap, Oracle, Webex.

Conectividade com nuvens públicas (IAAS)

5.1.206. A conectividade com as nuvens públicas deve ser provida por meio de serviço do mesmo Fabricante, permitindo a inclusão de dispositivos SD-WAN virtuais nos principais provedores de nuvem pública (AWS, Azure, GCP e OCI), garantindo a comunicação direta das unidades com as aplicações de software como serviço em nuvens públicas de forma segura;

5.1.207. A solução SD-WAN deverá fornecer integração NATIVA com no mínimo (quatro) das principais nuvens públicas (AWS, Google, Azure e OCI), permitindo o reconhecimento de objetos SDN;

5.1.208. A solução SD-WAN deverá fornecer conector SDN nativo com no mínimo AWS, Google, Azure e OCI para identificar TAGs por tipos de instancias, segmentos de redes, nome de máquinas, tipos de ambientes ex. produção e QA.

Segurança

5.1.209. A solução deverá possuir as seguintes funcionalidades mínimas, porém não exaustivas, de segurança, em face da evolução contínua das boas práticas deste tipo de serviço:

5.1.209.1. Firewall stateful;

5.1.209.2. Controle de Aplicação, localmente integrado no próprio appliance de Firewall;

5.1.209.3. Controle de navegação Web Filtering, localmente integrado no próprio appliance de Firewall;

5.1.209.4. Sistema de Prevenção de Intrusão (IDS/IPS), localmente integrados no próprio appliance de firewall;

5.1.209.5. Antimalware / Antivírus Anti-Spyware localmente integrados no próprio appliance de firewall;

5.1.209.6. VPN IPSEC (Client-to-Site e Site-to-Site) e SSL/TLS;

5.1.209.7. Suporte a qualidade de serviço (QoS) com traffic shaping.

5.1.210. A solução deverá permitir minimamente a configuração dos perfis de segurança (IPS, Web Filter, SSL, Controle de Aplicação, AntiVirus) na mesma política de segurança.

5.1.211. A solução SD WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN.

5.1.212. A solução deve suportar VPNs do tipo Hub Spoke.

5.1.213. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de segurança avançada, não sendo permitido appliances virtuais ou solução open source (produto montado).

5.1.214. As funcionalidades de segurança devem ser fornecidas no dispositivo SD-WAN ofertado.

5.1.215. Por funcionalidades de segurança entende-se: Firewall, controle de aplicações, IPS, prevenção de ameaças e controle de navegação por categorias;

5.1.216. As funcionalidades de segurança que compõem a solução devem funcionar em equipamento único obedecendo a todos os requisitos desta especificação, com suporte de gerenciamento centralizado.

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

5.1.218. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) ou outro mecanismo de integração/interoperabilidade;

5.1.219. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast;

5.1.220. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

5.1.221. A solução deve suportar NAT dinâmico nos concentradores definidos na arquitetura da rede corporativa de dados;

5.1.222. A solução deve suportar NAT estático (1-to-1);

5.1.223. A solução deve suportar NAT estático bidirecional 1-to-1;

5.1.224. A solução deve suportar Tradução de porta (PAT);

5.1.225. A solução deve suportar NAT de Origem;

5.1.226. A solução deve suportar NAT de Destino;

5.1.227. A solução deve suportar NAT de Origem e NAT de Destino simultaneamente;

5.1.228. A solução deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

5.1.229. A solução deve suportar NAT64;

5.1.230. A solução deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

5.1.231. A solução deve possibilitar o envio de log para sistemas de monitoração externos, de forma segura, usando protocolo SSL, túneis IPSEC ou outro mecanismo de transporte de dados segura. Todos os equipamentos necessários a essa funcionalidade devem ser fornecidos, instalados, configurados e mantidos pela CONTRATADA

5.1.232. A solução deve ter funcionalidade de Proteção anti-spoofing;

5.1.233. A solução deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

5.1.234. A solução deve suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados e deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

5.1.235. A solução deve deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

5.1.236. A solução deve ter suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

5.1.237. O modo de Alta-Disponibilidade deve possibilitar monitoração de falha de link;

5.1.238. A solução deve possibilitar o controle de acesso, inspeções de segurança, SSL/TLS para tráfego de Saída (Outbound) no próprio dispositivo local das OES, não permitido envio para processamento externo em nuvem de terceiros ou do Fabricante. Exceto tráfego para análise em Sandbox, hospedado em nuvem do Fabricante da solução ofertada.

5.1.239. Não serão aceitas soluções baseadas em PCs de uso geral.

5.1.240. Os equipamentos devem ser novos, ou seja, de primeiro uso. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale. Devendo ser comprovado através de Declaração do Fabricante ofertado, direcionada a esse processo.

Políticas de Segurança

5.1.240.1. A solução deve suportar controles por zonas de segurança;

5.1.240.2. A solução deve suportar controles de políticas por porta e protocolo;

5.1.240.3. A solução deve suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

5.1.240.4. A solução deve possibilitar a definição de Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

5.1.240.5. A solução deve possibilitar o controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

5.1.240.6. A solução deve possibilitar o Controle, inspeção e descriptografia de SSL/TLS, por política, para tráfego de saída (Outbound), no próprio equipamento de Firewall. Não será permitido SSL em nuvem;

5.1.240.7. A inspeção SSL deve ser compatível com HTTP/3. Tal inspeção é essencial uma vez que uma grande quantidade de sítios públicos está utilizando o protocolo em questão, tais como serviços de compartilhamento de vídeos, sites de busca e redes sociais, os quais estão sendo diariamente consumidos por usuários corporativos e externos;

5.1.240.8. Deve permitir restringir o acesso Tenant SaaS a recursos como Microsoft Office 365, Google Workspace e Dropbox por locatário, para bloquear tentativas de login que não sejam da empresa e proteger os usuários contra o acesso a recursos de nuvem não aprovados, rescurso de inserção de cabeçalho http para o provedor SaaS;

5.1.240.9. A solução deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

5.1.240.10. A solução deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

5.1.240.11. A solução deve ter suporte a objetos e regras IPV6;

5.1.240.12. A solução deve ter suporte a objetos e regras multicast;

5.1.240.13. A solução deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

5.1.240.14. Identificação de usuários

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

5.1.240.14.2. A solução 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;

5.1.240.14.3. A solução deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior, Active Directory na nuvem e Ldap;

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

5.1.240.14.5. A solução deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

5.1.240.14.6. A solução deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

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

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

5.1.240.14.9. A solução deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

Filtro de conteúdo WEB

5.1.240.15. Possuir no mínimo 90 (noventa) categorias ou subcategorias de classificação de URL;

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

5.1.240.17. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

5.1.240.18. Criar políticas baseadas na visibilidade e controle de acesso que permite identificar usuários e URLs, através da integração com serviços de diretório (LDAP/Microsoft Active Directory) usando o protocolo kerberos e NTLM e base de dados local;

5.1.240.19. Permitir a configuração de busca segura minimamente nos sites (Google, Bing e Yahoo).

5.1.240.20. Permitir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

5.1.240.21. Possuir categoria específica para classificar domínios recém registrados;

5.1.240.22. Permitir a criação de categorias de URLs customizadas;

5.1.240.23. Possuir base ou cache de URLs local no appliance, evitando atraso de comunicação/validação das URLs;

5.1.240.24. Permitir a customização de página de bloqueio;

5.1.240.25. Proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com o Microsoft Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Microsoft Active Directory só possam enviar informações de login para sites autorizados na solução;

5.1.240.26. Permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

5.1.240.27. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

5.1.240.28. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

5.1.240.29. Salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos às URLs: UserAgent, Referer e X-Forwarded-For;

5.1.240.30. Possuir filtro do Youtube por conteúdo. Por exemplo: possibilidade de disponibilizar o acesso apenas para determinados canais da plataforma.

5.1.240.31. Toda inspeção e decisão de acesso deverá ser executada nos dispositivos locais das OES, devidamente licenciados para a funcionalidade. Não é permitido encaminhamento para proxy em nuvem de terceiro e do Fabricante. Exceto a consulta e atualizações de URLs e Categorias na base de inteligência do Fabricante da solução.

Controle de Aplicação

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

5.1.240.33. A solução deve possibilitar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

5.1.240.34. A solução deve reconhecer pelo menos 5.000 (cinco mil) 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;

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

5.1.240.36. A solução deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

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

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

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

5.1.240.40. A solução deve identificar o uso de táticas evasivas via comunicações criptografadas;

5.1.240.41. A solução deve ser capaz de atualizar a base de assinaturas de aplicações automaticamente;

5.1.240.42. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory.

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

5.1.240.44. A solução deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

5.1.240.45. A solução deve permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias;

5.1.240.46. A solução deve alertar o usuário quando uma aplicação for bloqueada utilizando http.

5.1.240.47. A solução deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

5.1.240.48. A solução deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Google Chat, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

5.1.240.49. A solução deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Microsoft Teams e bloquear a chamada de vídeo;

5.1.240.50. A solução deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.

5.1.240.51. A solução deve possibilitar a criação de grupos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

5.1.240.52. A solução deve possibilitar a criação de grupos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação.

5.1.240.53. A solução deve possibilitar a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação.

5.1.240.54. A solução deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir, acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao whatsapp mas bloquear a transferência de arquivos.

5.1.240.55. Deve ser capaz de reconhecer a aplicação ChatGTP da OpenAI, permitindo a liberação ou bloqueio da mesma, como também limitar somente o Login e o Post para esta aplicação;

5.1.240.56. Toda inspeção deverá ser executada nos dispositivos locais das OES, devidamente licenciados para a funcionalidade. Não é permitido encaminhamento para ambiente em nuvem do Fabricante.

IDS/IPS e APT

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

5.1.240.58. Deverá possuir os seguintes mecanismos de inspeção de IPS:

5.1.240.59. Análise de padrões de estado de conexões;

5.1.240.60. Análise de decodificação de protocolo;

5.1.240.61. Análise para detecção de anomalias de protocolo;

5.1.240.62. Remontagem de pacotes TCP;

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

5.1.240.64. Detectar e bloquear a origem de port scans;

5.1.240.65. Suportar bloqueio de arquivos por tipo;

5.1.240.66. Identificar e bloquear comunicação com botnets;

5.1.240.67. Deve suportar várias técnicas de prevenção, incluindo Drop (Cliente, Servidor e ambos);

5.1.240.68. Deve suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);

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

5.1.240.70. Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis;

5.1.240.71. Rastreamento de vírus em pdf;

5.1.240.72. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate, como: zip e gzip;

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

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

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

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

5.1.240.77. Deve permitir o bloqueio de vulnerabilidades;

5.1.240.78. Deve permitir o bloqueio de exploits conhecidos;

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

5.1.240.80. Bloquear ataques efetuados por worms conhecidos;

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

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

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

5.1.240.84. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, CIFS, SMTP e POP3, como também em protocolos criptografados como HTTPS, POP3S, SMTPS e FTPS;

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

5.1.240.86. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos, permitido envio de artefatos para análise em nuvem do Fabricante.

5.1.240.87. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

5.1.240.88. A proteção deve possuir capacidade de análise da reputação de endereços IP, possuindo base própria de informações, gerada durante a filtragem dos ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

5.1.240.89. Toda inspeção deverá ser executada nos dispositivos locais das OES, devidamente licenciados para a funcionalidade. Não é permitido encaminhamento para ambiente em nuvem do Fabricante, exceto artefatos mencionado no item 5.9.36.30.

5.1.240.90. A solução deve reconhecer pelo menos 11.000 (onze mil) assinaturas para prevenção de ameaças, IDS/IPS.

VPN

Características gerais

5.1.240.90.1. A solução deve suportar VPN IPSec Site-to-Site.

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

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

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

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

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

VPN SSL

5.1.240.91. Suporte a autenticação multifator integrado.

5.1.240.92. Suportar conexões VPN SSL/TLS.

5.1.240.93. Para VPN SSL/TLS deverá suportar:

5.1.240.93.1.1. Deverá suportar os padrões 3DES, AES128, AES192, AES256 e ECDSA;

5.1.240.93.1.2. Deverá suportar TLS 1.1, TLS 1.2 e TLS 1.3;

5.1.240.94. Deverá permitir criação de perfis e grupos de usuário.

5.1.240.95. Deverá suportar autenticação integrada com base local, LDAP e RADIUS.

5.1.240.96. Deverá permitir a criação de políticas de VPN distintas para cada perfil de usuário.

5.1.240.97. O software cliente VPN deverá ser compatível com os seguintes sistemas operacionais: Windows 10 ou edição superior, Linux e MacOS.

Treinamento

5.1.241. A CONTRATADA deve fornecer dois tipos de treinamento, um para a capacitação dos técnicos da Administradora da Rede e Serviços e outro para os administradores técnicos dos OES.

5.1.242. O treinamento deve capacitar os técnicos da Administradora da Rede e Serviços no entendimento da solução SD-WAN como um todo, considerando todas as funcionalidades disponíveis nos dispositivos SD-WAN, topologias, políticas de encaminhamento, políticas de segurança, uso do sistema de gerenciamento centralizado para monitoração e configuração.

5.1.243. Deverão ser ministrados treinamentos oficiais dos fornecedores da solução SD-WAN.

5.1.244. Deve ser ministrado treinamento oficial do fabricante da solução SD-WAN de no mínimo 80 horas, podendo ser divididos em módulos, para até 08 (oito) técnicos habilitando-os à operação e configuração dos equipamentos.

5.1.245. Os treinamentos para os técnicos da Administradora da Rede e Serviços devem ser realizados em local adequado (mesa, cadeira e um terminal para cada treinando) e que permita atividades do tipo hands-on em equipamentos compatíveis com o sistema a ser disponibilizado na implantação.

5.1.246. Os treinamentos para os técnicos da Administradora da Rede e Serviços deverão ser realizados para 3 turmas de até 8 pessoas cada.

5.1.247. A CONTRATADA deve realizar o treinamento técnico atendendo ao disposto no Plano de Implantação.

5.1.248. Todos os treinamentos devem ser ministrados em português por instrutor devidamente habilitado.

5.1.249. A CONTRATADA deve fornecer treinamentos técnicos oficiais ou homologados pelos fabricantes da solução SD-WAN.

5.1.250. A CONTRATADA deve elaborar e apresentar os conteúdos programáticos de cada treinamento, a ser realizado em módulos, sendo que os mesmos estarão sujeitos à análise e aprovação da PRODESP.

5.1.251. O material didático do treinamento para os técnicos da Administradora da Rede e Serviços deve estar preferencialmente em português Brasil.

5.1.252. O material disponibilizado deve ser oficial ou homologado pelo(s)/do(s) fabricante(s).

5.1.253. Em caso de não estar disponível material didático em português, o mesmo deve estar em língua inglesa.

5.1.254. O treinamento para os técnicos da Administradora da Rede e Serviços deve abordar, minimamente, os seguintes assuntos:

5.1.254.1. Dispositivos SD-WAN.

5.1.254.1.1. Configurar a rede básica do dispositivo a partir das configurações padrão de fábrica

5.1.254.1.2. Configure e controle o acesso do administrador ao dispositivo

5.1.254.1.3. Use a GUI e CLI para administração

5.1.254.1.4. Controlar o acesso à rede configurada usando políticas de firewall

5.1.254.1.5. Aplicar encaminhamento de porta, NAT de origem e NAT de destino

5.1.254.1.6. Análise uma tabela de rotas do dispositivo

5.1.254.1.7. Roteie pacotes usando rotas estáticas e baseadas em políticas para implantações de vários caminhos e com balanceamento de carga

5.1.254.1.8. Autenticar usuários usando políticas de firewall

5.1.254.1.9. Monitore usuários de firewall a partir da GUI do dispositivo

5.1.254.1.10. Compreenda certificados e criptografia

5.1.254.1.11. Inspecione o tráfego protegido por SSL/TLS para evitar que a criptografia seja usada para ignorar políticas de segurança

5.1.254.1.12. Configure perfis de segurança para neutralizar ameaças e uso indevido, incluindo vírus, torrents e sites inadequados

5.1.254.1.13. Aplicar técnicas de controle de aplicativos para monitorar e controlar aplicativos de rede que possam usar protocolos e portas padrão ou não padrão

5.1.254.1.14. Ofereça uma VPN SSL para acesso seguro à sua rede privada

5.1.254.1.15. Estabeleça um túnel VPN IPsec entre dois dispositivos

5.1.254.1.16. Configurar roteamento estático

5.1.254.1.17. Configurar subjacência, sobreposição e breakout local de SD-WAN

5.1.254.1.18. Implante dispositivos como um cluster HA para tolerância a falhas e alto desempenho

5.1.254.1.19. Diagnosticar e corrigir problemas

5.1.254.2. SDWAN

5.1.254.2.1. Recursos da SD-WAN

5.1.254.2.2. Configurar recursos básicos de SD-WAN

5.1.254.2.3. Configure recursos avançados de SD-WAN

5.1.254.2.4. Entenda a rota SD-WAN e o processo de pesquisa de regras

5.1.254.2.5. Compreenda os diferentes critérios e estratégias de regras disponíveis para direcionar o tráfego usando SD-WAN e como a SD-WAN responde às mudanças nas condições do link

5.1.254.2.6. Implante SD-WAN usando IPsec básico e configuração de roteamento

5.1.254.2.7. Implante SD-WAN usando IPsec avançado e configuração de roteamento

5.1.254.2.8. Solucionar problemas de roteamento SD-WAN e correspondência de regras

5.1.254.3. Gerenciamento de Configuração e relatórios do Sistema.

5.1.254.3.1. Descreve os principais recursos e capacidades

5.1.254.3.2. Entenda a API e os meta campos

5.1.254.3.3. Implante domínios administrativos

5.1.254.3.4. Restringir o acesso simultâneo ao domínios usando áreas de trabalho e modo de fluxo de trabalho

5.1.254.3.5. Use modelos de provisionamento para alterações no nível do dispositivo em vários dispositivos

5.1.254.3.6. Identifique os estados de sincronização e gerencie o histórico de revisões dos dispositivos gerenciados

5.1.254.3.7. Gerencie políticas de firewall em vários dispositivos usando pacotes de políticas com objetos compartilhados e dinâmicos

5.1.254.3.8. Implante políticas e objetos global

5.1.254.3.9. Descreve opções de alta disponibilidade (HA), backup e recuperação

5.1.254.3.10. Gerencie centralmente o firmware dos dispositivos suportados

5.1.254.3.11. Diagnosticar e solucionar problemas de importação e instalação

5.1.254.3.12. Descreve a finalidade de coletar e armazenar logs

5.1.254.3.13. Visualize e pesquise logs

5.1.254.3.14. Gerenciar eventos e manipuladores de eventos

5.1.254.3.15. Configurar e analisar incidentes

5.1.254.3.16. Execute tarefas de caça a ameaças

5.1.254.3.17. Personalize e crie gráficos e conjuntos de dados

5.1.254.3.18. Personalize e gere relatórios

5.1.254.3.19. Configurar armazenamento externo para relatórios

5.1.254.3.20. Anexe relatórios a incidentes

5.1.254.3.21. Resolver problemas de relatórios

5.1.254.3.22. Entenda os conceitos de Playbook

5.1.254.3.23. Crie e monitore PlayBooks

5.1.255. O treinamento dos administradores técnicos dos OES deve capacitá-los no entendimento, definição, controle e monitoramento do encaminhamento e segurança de suas unidades e deve ser no modo self-paced com acesso remoto, sem limite de quantidade de acessos ou de usuários.

5.1.255.1. Estes treinamentos têm o objetivo de capacitar os administradores dos OES para realizarem as atividades de monitoramento e configurações das políticas de segurança e encaminhamento.

5.1.255.2. O treinamento self-paced deve possuir todo o conteúdo necessário para a capacitação dos administradores dos OES, similar ao treinamento presencial.

5.1.255.3. Os treinamentos *self-paced* devem ficar disponíveis durante toda a vigência do contrato.

5.1.256. Treinamento especializado anual – Atualização tecnológica

5.1.256.1. O treinamento poderá ser presencial, com transmissão online, e ser realizado em Centro de Treinamento da CONTRATADA ou nas dependências do Fabricante. Treinamento deve ocorrer uma vez ao ano durante todo período de vigência do contrato.

Requisitos de Projeto e Implantação

5.1.257. Requisitos Gerais

5.1.257.1. Entende-se por instalação a montagem física dos equipamentos e acessórios fornecidos especificados nesse anexo, bem como a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATATANTE.

5.1.258. Das Reuniões Preparatórias

5.1.258.1. Após a assinatura do instrumento contratual, e até a entrega dos PRODUTOS, serão realizadas reuniões preparatórias, de forma remota, com a presença de integrantes da equipe técnica da CONTRATADA, da qual se lavrará ata, para permitir o acompanhamento criterioso da execução dessa proposta.

5.1.258.2. A CONTRATADA, na data da 1ª reunião de acompanhamento da execução do contrato, a ser definida pela CONTRATANTE, após a assinatura do contrato, apresentará sua equipe de trabalho.

5.1.259. Execução Dos Serviços

5.1.259.1. A equipe técnica da CONTRATADA que executará os serviços irá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de implantação com validações e acompanhamentos do FABRICANTE da solução ofertada.

5.1.259.2. Para cada local de instalação, a CONTRATADA enviará um questionário técnico, o qual a CONTRATANTE deverá preencher comprovando a disponibilidade técnica para a instalação;

5.1.259.3. A CONTRATANTE deverá acompanhar a visita da instalação física para constatar que os PRODUTOS foram instalados de acordo com o cenário requerido pela CONTRATANTE.

5.1.259.4. A CONTRATANTE providenciará a infraestrutura elétrica e a infraestrutura de dados nos locais de instalação dos PRODUTOS.

5.1.259.5. O serviço de instalação será executado pela CONTRATADA durante o horário comercial compreendido das 09h00 às 18h00, de segunda a sexta-feira, podendo eventualmente, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes.

5.1.259.6. Caso a CONTRATANTE solicitar atendimento em finais de semana e feriados para atendimento ou acompanhamento de implementações que necessitem ser executadas fora do horário comercial, a CONTRATADA cobrará uma taxa adicional.

5.1.259.7. A CONTRATANTE deverá informar com até 05 (cinco) dias de antecedência a CONTRATADA da necessidade de eventuais serviços a serem executados fora do horário de expediente normal.

5.1.259.8. A configuração lógica dos PRODUTOS será executada de forma remota.

5.1.259.9. A CONTRATADA se encarrega de instalar e configurar, a critério exclusivo da CONTRATANTE, as atualizações e correções de todos os softwares e firmwares fornecidos durante o projeto.

5.1.259.10. Os testes de pré-operação serão executados de forma remota.

5.1.259.11. Entende-se por testes de pré-operação que depois de concluído o serviço de instalação física e configuração lógica dos PRODUTOS, a CONTRATADA realizará, com o acompanhamento dos técnicos da CONTRATANTE e do FABRICANTE, testes de pré-operação para constatar que os PRODUTOS foram instalados e configurados de acordo com o cenário requerido pela CONTRATANTE.

5.1.259.12. Todo o processo de planejamento, instalação, configuração, integração à infraestrutura de Tecnologia de Informação existente no local de instalação dos PRODUTOS, como também os testes de pré-operação dos PRODUTOS serão conduzidos pela CONTRATADA e pelo FABRICANTE da solução ofertada.

5.1.259.13. Deverá ser entregue o projeto High Level Design (HLD) e Low Level Design (LLD) da solução centralizada e suas devidas configurações para as localidades remotas desenvolvido e validado pelo FABRICANTE.

5.1.259.14. Para a instalação das localidades remotas, deve ser entregue documentação com ao menos as seguintes informações: Topologia local, interconexões com a plataforma SD-WAN, fotos e todos os testes realizados.

5.1.259.15. Concluídos a instalação e os testes de funcionalidade, a CONTRATADA irá elaborar a DOUMENTAÇÃO TÉCNICA DA INSTALAÇÃO contendo todas as informações da implantação: aspectos de arquitetura implantada, configuração, descrição das características e recursos utilizados, testes e integração aos ambientes de redes locais da instalação.

5.1.259.16. A documentação será emitida com timbre da CONTRATADA e irá conter o nome, data e assinatura do responsável técnico da CONTRATADA.

5.1.259.17. A documentação será entregue via meio digital.

5.1.259.18. A CONTRATADA entregará a DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO, no prazo máximo de 5 (cinco) dias úteis, após a conclusão da instalação, configuração e testes de pré-operação dos PRODUTOS.

5.1.259.19. A documentação deverá ser validada pela equipe técnica da CONTRATANTE em até 05 (cinco) dias úteis. Expirando-se este prazo, a CONTRATADA dará por finalizada esta demanda.

5.1.259.20. Toda informação manuseada durante a instalação, configuração e testes serão de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA assume o compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE.

5.1.259.21. O técnico responsável da CONTRATADA, junto com o FABRICANTE, irá elaborar e manter, no local de serviço, Relatório de Instalação (RI), em formulário digital timbrado próprio da CONTRATADA, com registros das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do projeto.

5.1.259.22. Quando aprovado o funcionamento de todos os PRODUTOS, tendo como base os itens do RI para cada PRODUTO, esses PRODUTOS deverão ser considerados instalados e aptos a serem utilizados. Isso deverá ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI.

5.1.259.23. Durante a fase do projeto e quando não aprovado o funcionamento de qualquer PRODUTO, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação.

5.1.259.24. Não estão previstas a instalação física ou configuração lógica de PRODUTOS ou novos fluxos de processos mapeados durante a fase de pré-operação

5.1.260. Equipe de Trabalho

5.1.260.1. A CONTRATADA se compromete em manter em seu quadro de funcionários pelo menos 01 (um) técnico de TI certificado pela FABRICANTE nos PRODUTOS da solução ofertada.

5.1.260.2. Os serviços de instalação serão executados e/ou supervisionados por técnico certificado pela FABRICANTE nos PRODUTOS da solução proposta.

5.1.260.3. A CONTRATADA apresentará a relação nominal dos profissionais, explicitando as respectivas atribuições na execução dos serviços.

5.1.260.4. Os serviços de instalação dos equipamentos descritos nesse anexo poderão ser subcontratados, a critério da CONTRATADA, sem a necessidade de autorização previa por parte da CONTRATANTE.

5.1.260.5. A responsabilidade pela efetiva execução dos serviços perante a CONTRATANTE será da CONTRATADA.

5.1.260.6. Caso seja constatada, durante o exercício dos serviços contratados, a falta de qualificação ou inadequação do profissional da CONTRATADA, o mesmo será substituído no prazo máximo de 05 (cinco) dias a partir da solicitação da CONTRATANTE.

Garantia e Assistência Técnica

5.1.261. Todos os PRODUTOS especificados neste documento deverão possuir garantia e assistência técnica pelo período de 60 (sessenta) meses, para cada tipo de Solução SD-WAN e para cada tipo de Gerência, contados a partir do aceite deles.

5.1.262. A assistência técnica da garantia é de responsabilidade única e exclusiva da CONTRATADA e ocorrerá por conta da CONTRATADA, sem nenhum ônus adicional além do valor contratado, durante o período de vigência da garantia, para qualquer tipo de serviço necessário para o cumprimento do contrato.

5.1.263. A CONTRATADA deve ter acesso direto ao suporte técnico especializado do fabricante dos PRODUTOS (technical assistance center) para solução de problemas e encaminhamento de problemas ao setor competente do fabricante dos PRODUTOS.

5.1.264. A CONTRATADA será responsável pela abertura e acompanhamento de chamados técnicos junto aos centros de suporte técnico do fabricante, bem como o acompanhamento da resolução desses chamados e implantação das soluções sugeridas pelo fabricante.

5.1.265. O serviço de assistência técnica deverá ser prestado remotamente e caso identificado a necessidade de troca de peças, deverá ser prestado nos respectivos locais de instalação dos PRODUTOS (on-site).

5.1.266. O período de disponibilidade para execução, pela CONTRATADA, do serviço de assistência técnica on-site para todos os PRODUTOS é das 8h00 às 18h00, de segunda a sexta-feira, exceto feriados.

5.1.267. Com o objetivo de manter os equipamentos a serem fornecidos em boas condições de funcionamento ou restabelecê-lo a tais condições, a CONTRATADA prestará serviço de assistência técnica remoto e caso necessário, on-site durante o período de disponibilidade, estabelecido no subitem anterior.

5.1.268. O prazo para a CONTRATADA iniciar o atendimento remoto, via suporte telefônico, para diagnosticar o problema é de, no máximo, 90 (noventa) minutos, contado a partir da abertura do chamado e dentro do período de disponibilidade.

5.1.269. O atendimento no local (on-site) para reposição de peças danificadas deve cumprir o prazo de quatro horas, provida pelo Fabricante, na capital de São Paulo restringindo os Data Centers da CONTRATANTE.

5.1.270. Demais localidades, a reposição de peças danificadas, deve cumprir o prazo máximo será de ate 2(dois) dias uteis após o diagnóstico de identificação pelo FABRICANTE.

5.1.271. A assistência técnica da garantia deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, não se restringindo a substituição de peças, partes, componentes e acessórios.

5.1.272. A CONTRATADA será responsável pela entrega e instalação das peças de substituição, retirada das peças com defeitos e, se necessário, deverá efetuar a reinstalação e/ou reconfiguração do sistema operacional do equipamento.

5.1.273. Todas as peças serão fornecidas à base de permuta, sendo que a reposição deverá ser feita por peças enviadas pelo fabricante dos equipamentos, de especificações idênticas ou superiores às substituídas, como tipo, configuração e capacidade.

5.1.274. A assistência técnica on-site deverá ser executada por técnicos treinados e certificados, com qualificação técnica para diagnóstico e solução dos problemas, bem como para substituição das peças e reconfiguração dos equipamentos.

5.1.275. A CONTRATADA deverá possuir em seu quadro de funcionários pelo menos 2 (dois) técnicos de TI certificados pelo fabricante dos equipamentos na solução ofertada, durante toda a vigência da garantia.

5.1.276. Em caso de problemas de falhas de software (bugs), cuja solução dependa da liberação de nova versão ou patches de correção pelo fabricante, a CONTRATADA deve providenciar uma solução de contingência, no prazo máximo de 2 (dois) úteis contados a partir da abertura do chamado.

5.1.277. Solução de contingência é uma solução temporária para um problema que não elimina a sua causa raiz. Esta solução restabelece a disponibilidade do ambiente, possibilitando assim a execução plena de suas funções originais, mantendo o nível de desempenho anterior ao problema.

5.1.278. Em caso de adoção de solução de contingência, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emitir laudos, na periodicidade

5.1.279. exigida pela CONTRATANTE, informando sobre a evolução dos trabalhos para solucionar o problema de forma definitiva.

5.1.280. A solução de contingência não caracterizará a conclusão de um chamado, contudo suspenderá a contagem de tempo para a resolução de ocorrência.

5.1.281. Um chamado somente será considerado concluído (solução definitiva) ou contingência (solução temporária) com o aceite da CONTRATANTE.

5.1.282. A CONTRATADA deverá assegurar a assistência técnica necessária à satisfatória utilização dos equipamentos, no que consiste à manutenção de hardware, instalação, reinstalação e atualização de softwares/firmwares internos dos equipamentos.

5.1.283. Deve ser disponibilizado durante todo o período de vigência da garantia, acesso automático às documentações e às versões de manutenção e atualizações de softwares/firmwares dos PRODUTOS, via portal web Internet do fabricante, sob demanda, sem ônus adicional à CONTRATANTE.

5.1.284. A assistência técnica deve cobrir atendimento telefônico, sem limitação, durante a vigência da garantia.

5.1.285. Caso o equipamento, no todo ou em parte, tenha que ser retirado do local ou o tempo para reparo e solução, contado a partir do chamado, seja superior a 2 (dois) úteis, a CONTRATADA deverá substituir, no ato, o equipamento por outro equivalente (equipamento back-up), enquanto perdurar o conserto.

5.1.286. Em caso de necessidade de substituição temporária de algum equipamento, o substituto deverá ser de modelo equivalente, ser compatível e ter a mesma configuração ou superior.

5.1.287. Em qualquer um dos casos acima, a CONTRATANTE irá emitir laudo de recepção técnica atestando ou não o cumprimento dos requisitos.

5.1.288. A retirada do equipamento para reparo e manutenção fora das dependências da CONTRATANTE, deverá ser comunicada pela CONTRATADA, e somente se efetivará quando do preenchimento e protocolo dos documentos específicos de retirada pelos prepostos da CONTRATADA.

5.1.289. Correm por conta exclusiva da CONTRATADA as responsabilidades decorrentes pela retirada e devolução do equipamento, bem como todas as despesas de transporte, frete e seguro correspondentes.

5.1.290. O equipamento back-up deverá ser de propriedade da CONTRATADA ou por ela locado, não cabendo à CONTRATANTE, nenhuma responsabilidade na disponibilização do mesmo.

5.1.291. A substituição temporária de equipamento original por equipamento back-up não caracterizará a conclusão de um chamado. Isto acontecerá quando o equipamento original retornar em perfeito estado de funcionamento à instalação de origem.

5.1.292. O equipamento original deve retornar à instalação de origem, em pleno funcionamento, no prazo máximo de até 30 (trinta) dias úteis a contar da data de sua retirada para reparo.

5.1.293. A CONTRATADA prestará os serviços de garantia apenas dos acessórios e equipamentos instalados e homologados pela equipe da CONTRATADA.

5.1.294. A CONTRATADA providenciará, a qualquer tempo, revisões de engenharia que forem classificadas como mandatórias pelo fabricante dos equipamentos, durante a vigência da garantia.

Local e prazo de entrega

5.1.295. Os PRODUTOS da presente contratação deverão ser entregues, pela CONTRATADA, na unidade administrativa/almoxarifado dos órgãos contratantes.

5.1.296. O prazo máximo para entrega dos PRODUTOS especificados neste documento é de 90 (noventa) dias a contar da data de assinatura do contrato de fornecimento.

5.1.297. O prazo máximo para agendamento da INSTALAÇÃO dos PRODUTOS especificados neste documento é de 30 (trinta) dias a contar do aceite de recebimento do equipamento de cada localidade para REGIÃO METROPOLITANA e de 60 (sessenta) dias para REGIÃO DO INTERIOR.

5.1.298. As localidades que os Links não estiverem disponíveis a Contratada deverá entrega (pré configurado) e energiza-lo e alocá-lo no Rack, garantindo assim a conexão quando os links estiverem entregues.

5.1.299. A CONTRATANTE deverá ser comunicada com antecedência de 1 (um) dia, da data de realização da entrega, pela CONTRATADA.

Suporte Assistido aos ativos de redes da contratada

5.1.300. Os recursos humanos a serem disponibilizados pela CONTRATADA deverão possuir as seguintes formações:

5.1.301. RECURSOS INTERMEDIÁRIOS

5.1.301.1. Diploma de Curso de Nível Superior na área de Tecnologia da Informação, Engenharia da Computação ou Análise de Sistemas;

5.1.301.2. Certificação Intermediária do fabricante para os equipamentos e softwares de rede fornecidos pela CONTRATADA;

5.1.301.3. Experiência mínima de 3 anos, comprovada em carteira, atuando em operação e administração redes de dados e infraestrutura de telecomunicações do fabricante da rede da CONTRATADA.

5.1.302. RECURSO AVANÇADO

5.1.302.1. Graduação Técnica de Nível Superior;

5.1.302.2. Certificação Avançada do fabricante para os equipamentos e softwares de rede fornecidos pela CONTRATADA;

5.1.302.3. Conhecimento e experiência em implementação de controles de segurança da informação de redes de telecomunicações;

5.1.302.4. Experiência mínima de 5 anos, comprovada em carteira, atuando em redes de dados e infraestrutura de telecomunicações do fabricante da rede da CONTRATADA.

5.1.302.5. As atribuições dos técnicos, que atuarão sempre em conjunto, contemplam:

5.1.302.5.1. Realizar junto ao CONTRATANTE as configurações necessárias nos ativos de rede sob responsabilidade da CONTRATADA, nas instalações do PRODESP;

5.1.302.5.2. Manter e operacionalizar todas as ferramentas da solução de gerência;

5.1.302.5.3. Auxílio no gerenciamento e monitoramento da rede e dos dispositivos;

5.1.302.5.4. Auxílio no controle de agendamento e interrupções;

5.1.302.5.5. Auxílio no controle de níveis de serviço;

5.1.302.5.6. Auxílio no controle de níveis de desempenho;

5.1.302.5.7. Atendimento via telefone, e-mail, web de clientes da PRODESP; nas respostas a incidentes;

5.1.302.5.8. Auxílio no controle de mudanças;

5.1.302.5.9. Auxiliar na manutenção e documentação dos ativos que compõem a infraestrutura da Solução

5.1.302.5.10. Reportar-se à Gerência de Redes e Telecomunicações da CONTRATANTE;

5.1.302.5.11. Elaborar relatório técnico mensal sobre as suas atividades;

5.1.302.5.12. Elaborar projetos de rede, relatórios gerenciais ou qualquer instrumento de auxílio à tomada de decisões no que tange à melhoria contínua da Rede da PRODESP;

5.1.302.5.13. Garantir que a rede PRODESP esteja em constante evolução tecnológica e aderente às melhores práticas de mercado e do fabricante dos equipamentos da rede.

Suporte assistido de segurança de redes

5.1.303. Os recursos humanos a serem disponibilizados pela CONTRATADA deverão possuir as seguintes formações:

5.1.304. Avançados, mínimo 2 (dois)

5.1.304.1.1. Graduação Técnica de Nível Superior;

5.1.304.1.2. Certificação Avançada do fabricante para os equipamentos e softwares de segurança de rede fornecidos pela CONTRATADA;

5.1.304.1.3. Conhecimento e experiência avançados em implementação de controles de segurança da informação de redes de telecomunicações, auditoria de logs, identificação de ameaças e vulnerabilidades, prevenção de ataques, e demais atribuições pertinentes;

5.1.304.1.4. Experiência mínima de 5 anos, comprovada em carteira, atuando em segurança de redes de dados e infraestrutura de telecomunicações composta de equipamentos do fabricante fornecidos pela CONTRATADA.

5.1.304.1.5.

5.1.304.1.6. As atribuições dos técnicos, que atuarão sempre em conjunto, contemplam:

5.1.304.1.7. Auxiliar o cliente final nas configurações necessárias nas instalações do Data Center do PRODESP;

5.1.304.1.8. Auxiliar na manutenção e operação de todas as ferramentas das soluções de segurança da informação;

5.1.304.1.9. Auxílio no gerenciamento e monitoramento da rede e dos dispositivos;

5.1.304.1.10. Auxílio na detecção de riscos e ameaças;

5.1.304.1.11. Auxílio na prevenção de ataques cibernéticos;

5.1.304.1.12. Auxílio nas respostas a incidentes;

5.1.304.1.13.

5.1.304.1.14. Auxílio no controle de mudanças;

5.1.304.1.15. Auxiliar na manutenção e documentação os ativos que compõem a infraestrutura da PRODESP;

5.1.304.1.16. Reportar-se à Gerência de Redes e Telecomunicações da CONTRATANTE;

5.1.304.1.17. Elaborar relatório técnico mensal sobre os incidentes, vulnerabilidades e ameaças detectadas;

5.1.304.1.18. Elaborar projetos de segurança rede, relatórios gerenciais ou qualquer instrumento de auxílio à tomada de decisões no que tange à melhoria contínua da Rede PRODESP;

5.1.304.1.19. Garantir que a rede PRODESP esteja em constante evolução tecnológica e aderente às melhores práticas de segurança da informação de mercado e do fabricante dos equipamentos da rede.

Suporte Assistido de telecomunicações

5.1.305. O Recurso Humano a ser disponibilizado pela CONTRATADA deverá possuir a seguinte formação:

5.1.306. As atribuições deste técnico serão:

5.1.307. Auxiliar na supervisão da qualidade e disponibilidade dos circuitos;

5.1.308. Acompanhar os chamados técnicos para recuperação de circuitos;

5.1.309. Interceder junto à contratada quando solicitado;

5.1.310. Auxiliar na manutenção e documentação dos racks dos equipamentos;

5.1.311. Efetuar os remanejamentos de circuitos, quando solicitado pelo PRODESP;

5.1.312. Reportar-se à Gerência de Redes e Telecomunicações

5.1.313. Elaborar relatório técnico mensal sobre as suas atividades.

Acomodação dos equipamentos

5.1.314. A CONTRATADA deverá instalar os equipamentos no ambiente indicado pela CONTRATANTE;

5.1.315. O ambiente disponibilizado pela CONTRATANTE dispõe da infraestrutura adequada (espaço físico, rack, bandeja, energia e climatização) para acomodação dos equipamentos da CONTRATADA.

Da reunião de alinhamento

5.1.316. Homologado o resultado da licitação e tendo o contrato assinado, deverá ser realizada até o 15º (décimo quinto) dia útil após a assinatura do Contrato, uma reunião presencial de alinhamento, na sede do CONTRATANTE, com o objetivo de se apresentar o preposto, identificar as expectativas e diretrizes para elaborar o Projeto de Implantação, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas do objeto, conforme agendamento efetuado pelo Gestor do Contrato;

5.1.317. O Projeto de Implantação deverá indicar o Cronograma de Implantação com as entregas intermediárias e será elaborado de comum acordo entre a CONTRATADA e o CONTRATANTE, desde que observado o prazo máximo de entrega total do serviço contratado.

Do projeto de implantação

5.1.318. A CONTRATADA deverá apresentar, ao Gestor do Contrato, em até 30 (trinta) dias consecutivos, contados a partir do primeiro dia útil seguinte à data da realização da reunião de alinhamento, o Projeto de Implantação dos serviços contratados, contendo no mínimo:

5.1.319. O detalhamento das etapas que serão seguidas, datas de início e fim de cada atividade, conforme Cronograma de Implantação aprovado na reunião de alinhamento;

5.1.320. Quando couber, a definição das marcas e modelos de equipamentos que serão utilizados.

VI. ACORDO DE NÍVEIS DE SERVIÇOS / SLA (Lotes 1, 2 e 3)

6.1. O Acordo de Níveis de Serviços, ou *Service Level Agreement* (SLA), tem como objetivo estabelecer as metas de qualidade da prestação dos serviços relacionadas aos indicadores de desempenho técnico-operacional.

6.2. A CONTRATADA assume o compromisso de prestar os serviços atendendo às metas de qualidade estabelecidas neste acordo, inclusive para aqueles prestados sob as condições da Cláusula Social do Contrato.

6.3. A CONTRATADA é responsável pelo cumprimento das metas de qualidade estabelecidas neste acordo, durante todo o prazo de prestação dos serviços.

6.4. O não cumprimento aos indicadores de SLA sujeita a CONTRATADA às penalidades estabelecidas no Contrato.

6.5. A CONTRATADA deve apurar mensalmente os indicadores do SLA com base nas informações provenientes dos elementos gerenciados utilizados para a prestação dos serviços e dos procedimentos administrativos aplicáveis na prestação dos serviços.

6.6. A Administradora da Rede e Serviços apurará mensalmente os indicadores do SLA utilizando informações de seus sistemas e de informações recebidas da CONTRATADA.

6.6.1. A notificação para aplicação de penalidades é feita com base nos resultados da apuração mensal dos indicadores que constam nos relatórios previstos no Acordo Operacional.

6.7. Para fins das disposições deste SLA, entende-se por “incidente” uma interrupção não planejada ou uma redução da qualidade do serviço prestado a Unidade, cuja causa raiz e responsabilidade pela sua ocorrência devem ser devidamente identificadas pela CONTRATADA quando do seu atendimento e encerramento.

6.8. Em caso de mais de 2 (dois) incidentes associados a um mesmo ID, ocorridos em período mensal, a CONTRATADA deve entregar ao respectivo OES e à Administradora da Rede e Serviços um relatório de análise de causa raiz com proposta de solução.

6.9. As informações referentes a cada incidente devem ser agrupadas em um registro denominado de Registro de Incidente, aberto quando da identificação da ocorrência e fechado quando do restabelecimento da normalidade da prestação do serviço.

6.10. Em cada Registro de Incidente deve constar a data (dd:mm:aa) e o horário (hh:mm) de sua abertura e a data (dd:mm:aa) e o horário (hh:mm) de seu fechamento, que delimitam o Período de Tratamento do Incidente (PTI).

6.11. Sempre que a CONTRATADA julgar que não é a responsável por um incidente, cabe a ela o ônus da prova, devendo apresentar testes comprobatórios, registros, relatórios específicos ou quaisquer outras evidências que julgar suficientes para afastar a sua responsabilidade.

Indicadores para o SCM e STI (Lote 1)

Frequência de Registros de Incidente SCM por ID

6.12. A Frequência de Registro de Incidentes SCM por ID corresponde ao número total de registros abertos de forma proativa ou de forma reativa, por mês.

6.12.1. A apuração do indicador deve ser feita com base nas informações de abertura de registro de incidentes.

6.13. A Quantidade máxima de abertura de Registros de Incidentes por ID por mês está descrita na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente SCM por ID	2	Registros

Frequência de Registros de Incidente do SCM

6.14. A Frequência de Registros de Incidente do SCM, por cem ID, corresponde ao número total de Registros de Incidente relativos ao Serviço de Comunicação Multimídia, fechados no mês, cuja causa é de responsabilidade da CONTRATADA, dividido pela quantidade de ID ativados até o último dia do mês, multiplicado por cem.

6.15. A frequência máxima de Registros de Incidente do SCM é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE

Frequência de Registros de Incidente do SCM	5	%

Prazo para Solução de Incidente em Serviços ou em recursos

6.16. O prazo para Solução de Incidente em Serviços ou em recursos, cuja causa é de responsabilidade da CONTRATADA, corresponde ao valor máximo admissível do PTI relativo aos serviços SCM e STI ou aos recursos: do *backbone* IP-MPLS ou do AS GESP.

6.17. O prazo para Solução de Incidentes em Serviços ou em recursos é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Solução de Incidentes em Serviços SCM em área urbana e STI, ou em recursos: do *backbone* IP-MPLS ou do AS GESP	240	Minutos
Prazo para Solução de Incidentes no SCM em área rural	360	Minutos

Indisponibilidade de Serviço

6.18. A Indisponibilidade de Serviço corresponde ao período de tempo total no mês, em que cada um dos serviços contratados permanece indisponível para ser utilizado pela Unidade (UP ou UC) que o contratou.

6.19. A apuração da Indisponibilidade de Serviço deve considerar os incidentes cuja causa é de responsabilidade da CONTRATADA.

6.20. Para o cálculo da Indisponibilidade do Serviço, deve ser considerado o PTI referente ao incidente em que houve interrupção da prestação do serviço, de cada Registro de Incidente fechado no mês calendário.

Indisponibilidade do Serviço SCM por Unidade

6.21. A Indisponibilidade do SCM, por Unidade, se desdobra em Indisponibilidade do SCM com redundância e Indisponibilidade do SCM sem redundância.

6.21.1. A Indisponibilidade do SCM com redundância corresponde ao período de tempo total no mês, por Unidade, em que ambos os conjuntos CPE/enlace da rede de acesso ou o *backbone* da Rede IP Multisserviços não se encontram aptos, física ou logicamente, para a prestação do SCM.

6.21.1.1. A prestação do SCM com redundância pressupõe a comutação automática do roteamento de um conjunto CPE/enlace para o outro em caso de falha de um dos elementos de rede do conjunto em operação, sem causar interrupção na prestação do serviço além do limite disposto na especificação técnica do SCM.

6.21.1.2. A interrupção na prestação do SCM que ultrapasse o limite estabelecido é considerada incidente e passível de registro para que conste na apuração desse indicador de SLA.

6.21.2. A Indisponibilidade do SCM sem redundância corresponde ao período de tempo total no mês, por Unidade, em que o conjunto CPE/enlace da rede de acesso ou o *backbone* da Rede IP Multisserviços não se encontram aptos, física ou logicamente, para a prestação do SCM.

6.22. A Indisponibilidade do SCM é expressa em horas através da seguinte fórmula:

Indisponibilidade do SCM (horas) = ISCM /60
Em que:
ISCM - período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do SCM, por Unidade, no mês, de responsabilidade da CONTRATADA.

6.23. A Indisponibilidade de Serviço, por mês, é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do SCM sem redundância, por unidade	8	Horas
Indisponibilidade do SCM com redundância, por unidade	0,5	Hora

Indisponibilidade de recursos: do backbone IP-MPLS ou do AS GESP

6.24. Indisponibilidade de recursos: do *backbone* IP-MPLS ou do AS GESP, corresponde ao período de tempo total no mês, em que há interrupção da prestação do serviço correlacionado ao recurso para a totalidade das Unidades que o contrataram.

6.25. A apuração da indisponibilidade de recursos: do *backbone* IP-MPLS ou do AS GESP, deve considerar os incidentes cuja causa é de responsabilidade da CONTRATADA.

6.26. Para o cálculo da indisponibilidade de recursos: do *backbone* IP-MPLS ou do AS GESP, deve ser considerado o PTI referente ao incidente associado ao ID do recurso, de cada Registro de Incidente fechado no mês calendário.

6.27. A indisponibilidade de recursos do *backbone* IP-MPLS é expressa em horas através da seguinte fórmula:

Indisponibilidade de recursos do *backbone* IP-MPLS (horas) = IBIP/ 60

Em que:

IBIP – período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do SCM simultaneamente para todas as Unidades que a contrataram, no mês, de responsabilidade da CONTRATADA.

6.28. A indisponibilidade de recursos do AS GESP é expressa em horas através da seguinte fórmula:

Indisponibilidade de recursos do AS GESP (horas) = IASG / 60

Em que:

IASG – período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do STI simultaneamente para todas as Unidades que a contrataram, no mês, de responsabilidade da CONTRATADA.

6.29. A indisponibilidade de recursos: do *backbone* IP-MPLS ou do AS GESP, por mês, é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do *backbone* IP-MPLS	0,5	Hora
Indisponibilidade do AS GESP		

Nível da Qualidade do SCM

6.30. O Nível da Qualidade do Serviço de Comunicação Multimídia corresponde ao percentual de SCM em conformidade com os parâmetros de QoS avaliados com a aplicação de testes de conformidade, pela CONTRATADA, em uma amostra de ID selecionados periodicamente pela Administradora da Rede e Serviços.

6.31. A apuração deste indicador é feita com a aplicação da seguinte fórmula:

NQSCM = [(TTA-TTF)/TTA]*100

Em que:

NQSCM – Nível da Qualidade do Serviço de Comunicação Multimídia.

TTA – Total de ID da amostra.

TTF – Total de ID da amostra com resultado de teste de conformidade fora dos limites em pelo menos um dos parâmetros de QoS.

6.32. O valor mínimo do Nível da Qualidade do Serviço de Comunicação Multimídia é o que consta na tabela abaixo.

INDICADOR	VALOR	UNIDADE
Nível da Qualidade do SCM	93	%

6.33. O ID em que um ou mais testes de conformidade não atender aos parâmetros de QoS especificados é considerado como fora dos limites para fins de apuração do indicador.

6.34. A quantidade de ID da amostra consta no Acordo Operacional.

6.35. Os testes de conformidade a serem aplicados nos ID selecionados que compõem a amostra, se referem aos parâmetros de QoS de latência, *jitter* e perda de pacotes, especificados nos itens que seguem.

6.35.1. Devem ser realizadas medidas usando as fórmulas dos parâmetros para cada uma das classes de serviço definidas na descrição do Serviço de Comunicação Multimídia deste documento.

6.35.2. Os valores máximos dos parâmetros, a serem considerados, são os que constam, por classe de serviço, na descrição do Serviço de Comunicação Multimídia deste documento.

Latência

6.36. A latência corresponde ao período de tempo expresso em milissegundos para transportar um pacote IP de um CPE de origem até um CPE de destino na Rede IP Multisserviços e transportar o respectivo pacote de resposta até o CPE de origem, sendo para o seu cálculo adotada a seguinte fórmula:

L = RTT

Em que:

L – Latência, em milissegundos (ms).

RTT – *Round Trip Time*, período de tempo entre a ida e a volta de um pacote, em milissegundos (ms).

Jitter

6.37. O *jitter* ou variação do atraso, expresso em milissegundos, corresponde à variação máxima de retardo entre pacotes IP sucessivos de um fluxo de pacotes IP transportados pela Rede IP Multisserviços entre o CPE de origem e o CPE de destino, sendo para o seu cálculo adotada a seguinte fórmula:

J = Dn - D(n-1)

Onde:

J – *Jitter* entre dois CPE, em milissegundos (ms).

Dn - atraso total do "enésimo" pacote (em milissegundos - ms).

D(n-1) - atraso total do "enésimo menos 1" pacote (em milissegundos - ms).

6.37.1. Como o *jitter* é um parâmetro de QoS exigido apenas para a Classe de Serviço TEMPO REAL – VOZ e TEMPO REAL - VÍDEO, sua apuração se restringe a acessos em que ocorre a prestação de serviços que demandam essa Classe de Serviço.

Perda de Pacotes

6.38. A perda de pacotes, expresso em porcentagem, corresponde à quantidade de pacotes IP não recebidos no CPE de destino em relação ao total de pacotes IP enviados pelo CPE de origem, sendo para o seu cálculo adotada a seguinte fórmula:

PP (%) = [(NP origem – NP destino) / NP origem]*100

Em que:

PP – Perda de Pacotes (%).

NP origem – Nº de pacotes na origem.

NP destino – Nº de pacotes no destino.

Prazo para atendimento à Solicitação de Ativação de Serviços

6.39. O prazo para atendimento à Solicitação de Ativação de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação pelo OES e a data do envio dos resultados dos testes de ativação do ID realizados pela CONTRATADA, desde que tenha sido dado o aceite pelo OES.

6.40. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.41. O prazo para atendimento à Solicitação de Ativação de Serviços consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Ativação de Serviços em Área Urbana com ou sem Redundância.	90	Dias corridos
Prazo para Ativação de Serviços em Área Rural com ou sem Redundância.	135	Dias corridos

Prazo para atendimento à Solicitação de Alteração da Prestação de Serviços

6.42. O prazo para atendimento a uma Solicitação de Alteração da Prestação de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação e a data do aceite pelo OES.

6.43. O atendimento, pela CONTRATADA, à Solicitação de Alteração da Prestação de Serviços deve ser realizado no prazo máximo descrito na tabela a seguir:

INDICADOR		
Prazo para Alteração da Prestação de Serviços	VALOR	UNIDADE
Sem alteração da capacidade nominal do SCM	30	Dias corridos
Com alteração da capacidade nominal do SCM em Área Urbana	90	Dias corridos
Com alteração da capacidade nominal do SCM em Área Rural	135	Dias corridos

Prazo para Atendimento a Solicitação de Alteração de Padrão de SCM

6.44. O prazo para atendimento a uma Solicitação de Alteração de Padrão de SCM corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação e a data do aceite pelo OES.

6.45. O atendimento, pela CONTRATADA, à Solicitação de Alteração de Padrão de SCM deve ser realizado no prazo máximo descrito na tabela a seguir:

INDICADOR		
Prazo para Alteração de Padrão de SCM	VALOR	UNIDADE
De sem redundância para com Redundância em Área Urbana.	90	Dias corridos
De sem redundância para com Redundância em Área Rural.	135	Dias corridos

6.46. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

Prazo para atendimento à Solicitação de Alteração de Configuração de CPE

6.47. O prazo para atendimento a uma Solicitação de Alteração de Configuração de CPE corresponde ao período de tempo, expresso em dias corridos, entre o momento da emissão da solicitação e o aceite pelo OES.

6.48. Entre as atividades previstas neste indicador estão a configuração de Classes de Serviço (CoS) e marcação de pacotes e a configuração de DHCP relay ou server, entre outras alterações lógicas no CPE.

6.49. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.50. O atendimento, pela CONTRATADA, à Solicitação de Alteração de Configuração de CPE para UP ou UC deve ser realizado no prazo máximo descrito na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Configuração de CPE	2	Dias corridos

Prazo para atendimento à Solicitação de Alteração da Infraestrutura de Instalação

6.51. O prazo para atendimento à Solicitação de Alteração da Infraestrutura de Instalação do SCM corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação pelo OES e a data do envio dos resultados dos testes realizados pela CONTRATADA, desde que tenha havido aceite pelo OES.

6.52. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.53. O prazo para a aprovação de GMUD não deve ser considerado para efeito de cálculo do indicador.

6.54. O prazo para atendimento à Solicitação de Alteração da Infraestrutura de Instalação do SCM é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração da Infraestrutura de Instalação do SCM em UC em área urbana	15	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UP em área urbana	30	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UC em área rural	22	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UP em área rural	45	Dias corridos

6.55. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.56. O prazo para a aprovação de GMUD não deve ser considerado para efeito de cálculo do indicador.

Prazo para atendimento à Solicitação de Alteração de Dados Cadastrais

6.57. O prazo para atendimento à Solicitação de Alteração de Dados Cadastrais corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data da execução da alteração pela mesma.

6.58. O prazo para atendimento à Solicitação de Alteração de Dados Cadastrais é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Dados Cadastrais	10	Dias corridos

Prazo para atendimento à Solicitação de Alteração de Titularidade do ID

6.59. O prazo para atendimento à Solicitação de Alteração de Titularidade do ID, de UP ou de UC, corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data da execução da alteração pela mesma.

6.60. O prazo para atendimento à Solicitação de Alteração de Titularidade do ID é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Titularidade do ID	10	Dias corridos

Frequência de Faturas Contestadas Procedentes

6.61. A Frequência de Faturas Contestadas Procedentes corresponde ao percentual das faturas contestadas procedentes em relação às faturas emitidas, durante o período de um mês, tendo como base as informações dos registros de Solicitação de Contestação de Faturas.

6.62. A apuração deste indicador é feita pela aplicação da seguinte fórmula:

FFCP (%) = (FCP / TFE)*100

Em que:

FFCP – Frequência de Faturas Contestadas Procedentes, no mês calendário.

FCP – Faturas Contestadas Procedentes, no mês calendário.

TFE – Total de Faturas Emitidas, no mês calendário.

6.63. O valor máximo para a Frequência de Faturas Contestadas Procedentes é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Faturas Contestadas Procedentes	3	%

Prazo para Reação e Mitigação de Ataques

6.64. O prazo para reação e mitigação de ataques corresponde ao limite de tempo no qual a CONTRATADA deve reagir para iniciar o processo de mitigação de ataques, de forma a garantir uma mitigação efetiva e não mera reação que traga resultado insatisfatório.

6.65. O indicador deve ser medido, por evento, entre o início da ocorrência dos ataques e o início da efetiva mitigação dos mesmos pela CONTRATADA.

6.66. O Ataque ao AS GESP corresponde ao evento de ataque cujo destino seja um ou mais alvos dentro do recurso agregado utilizado para a prestação do STI ou ao evento de ataque que indiretamente afete as conexões desse AS, devendo o incidente ser registrado para o(s) ID do(s) recurso(s) afetado(s).

6.67. O Ataque ao OES corresponde ao evento de ataque cujo destino seja um ou mais alvos dentro da estrutura de uma mesma Unidade do OES, a qual tenha contratado o STI, devendo o incidente ser registrado para o ID afetado.

6.68. Caso ocorra um ou mais eventos simultâneos de Ataque ao OES que ocasione a saturação de qualquer uma das conexões do AS GESP, prevalecerá, para fins de apuração, o incidente relacionado com o Ataque ao AS GESP, independente de quantos incidentes sejam registrados para os eventos de Ataque ao OES.

6.69. O valor máximo admitido para este indicador consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Reação e Mitigação de Ataque ao OES, por evento	30	Minutos
Prazo para Reação e Mitigação de Ataque ao AS GESP, por evento	30	Minutos

Prazo para entrega de relatórios

6.70. O prazo para entrega dos relatórios previstos neste Contrato, em meio eletrônico, é o que consta na tabela abaixo.

INDICADOR	VALOR	UNIDADE
Prazo para entrega de relatórios em meio eletrônico (no mês subsequente ao mês da apuração)	15	Dias corridos

Resumo dos Indicadores do SLA para a prestação do SCM e o STI

6.71. Os indicadores do SLA se encontram agrupados na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente SCM por ID	2	Registros
Frequência de Registros de Incidente do SCM	5	%
Prazo para Solução de Incidentes em Serviços SCM em área urbana e STI, ou em recursos: do *backbone* IP-MPLS ou do AS GESP	240	Minutos
Prazo para Solução de Incidentes no SCM em área rural	360	Minutos
Indisponibilidade do SCM sem redundância, por unidade	8	Horas
Indisponibilidade do SCM com redundância, por unidade	0,5	Hora
Indisponibilidade de recursos: do *backbone* IP-MPLS ou do AS GESP	0,5	Hora
Nível da Qualidade do SCM	93	%
Prazo para Ativação de Serviços em Área Urbana com ou sem Redundância	90	Dias corridos
Prazo para Ativação de Serviços em Área Rural com ou sem Redundância	135	Dias corridos
Prazo para Alteração da Prestação de Serviços sem alteração da capacidade nominal do SCM	30	Dias corridos
Prazo para Alteração da Prestação de Serviços com alteração da capacidade nominal do SCM em Área Urbana	90	Dias corridos
Prazo para Alteração da Prestação de Serviços com alteração da capacidade nominal do SCM em Área Rural	135	Dias corridos
Prazo para Alteração de Padrão de SCM de sem redundância para com redundância em Área Urbana	90	Dias corridos
Prazo para Alteração de Padrão de SCM de sem redundância para com redundância em Área Rural	135	Dias corridos
Prazo para Alteração da Configuração de CPE	2	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UC em área urbana	15	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UP em área urbana	30	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UC em área rural	22	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SCM em UP em área rural	45	Dias corridos
Prazo para Alteração de Dados Cadastrais	10	Dias corridos

Prazo para Alteração de Titularidade do ID	10	Dias corridos
Frequência de Faturas Contestadas Procedentes	3	%
Prazo para Reação e Mitigação de Ataque ao OES, por evento	30	Minutos
Prazo para Reação e Mitigação de Ataque ao AS GESP, por evento	30	Minutos
Prazo para entrega de relatórios	15	Dias corridos

Indicadores para o SAI-BL (Lote 2)

Frequência de Registros de Incidente do SAI-BL

6.72. A Frequência de Registros de Incidente do SAI-BL e SAI-BLI, por cem ID, corresponde ao número total de Registros de Incidente relativos ao Serviço de Acesso à Internet de Banda Larga Fixa e ao Serviço de Acesso à Internet de Banda Larga Itinerante, fechados no mês, cuja causa é de responsabilidade da CONTRATADA, dividido pela quantidade de ID ativados até o último dia do mês, multiplicado por cem.

6.73. A frequência máxima de Registros de Incidente do SAI-BL e do SAI-BLI é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente do SAI-BL e SAI-BLI	5	%

Prazo para Solução de Incidente em Serviços ou em recursos

6.74. O prazo para Solução de Incidente em Serviços ou em recursos, cuja causa é de responsabilidade da CONTRATADA, corresponde ao valor máximo admissível do PTI relativo ao serviço SAI-BL e SAI-BLI.

6.75. O prazo para Solução de Incidentes em Serviços ou em recursos é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Solução de Incidentes no SAI-BL e SAI-BLI em área urbana	24	Horas
Prazo para Solução de Incidentes no SAI-BL e SAI-BLI em área rural	36	Horas

Indisponibilidade de Serviço

6.76. A Indisponibilidade de Serviço corresponde ao período de tempo total no mês, em que cada um dos serviços contratados permanece indisponível para ser utilizado pela Unidade (UP ou UC) que o contratou.

6.77. A apuração da Indisponibilidade de Serviço deve considerar os incidentes cuja causa é de responsabilidade da CONTRATADA.

6.78. Para o cálculo da Indisponibilidade do Serviço, deve ser considerado o PTI referente ao incidente em que houve interrupção da prestação do serviço, de cada Registro de Incidente fechado no mês calendário.

Indisponibilidade do Serviço SAI-BL e SAI-BLI por Unidade

6.79. A Indisponibilidade do SAI-BL e do SAI-BLI corresponde ao período de tempo total no mês, por Unidade, em que não há oferta de acesso à Internet Banda Larga Fixa ou Interativa, para a Unidade que contratou o SAI-BL ou o SAI-BLI.

6.80. A Indisponibilidade do SAI-BL e do SAI-BLI é expressa em horas através da seguinte fórmula:

Indisponibilidade do SAI-BL (horas) = ISAI-BL /60
Em que:
ISAI-BL - período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do Serviço SAI-BL, por Unidade, no mês, de responsabilidade da CONTRATADA.

Indisponibilidade do SAI-BLI (horas) = ISAI-BLI /60
Em que:
ISAI-BLI - período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do Serviço SAI-BLI, por Unidade, no mês, de responsabilidade da CONTRATADA.

6.81. A Indisponibilidade de Serviço, por mês, é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do SAI-BL, por unidade	48	Horas
Indisponibilidade do SAI-BLI, por unidade	8	Horas

Prazo para atendimento à Solicitação de Ativação de Serviços

6.82. O prazo para atendimento à Solicitação de Ativação de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação pelo OES e a data do envio dos resultados dos testes de ativação do ID realizados pela CONTRATADA, desde que tenha sido dado o aceite pelo OES.

6.83. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.84. O prazo para atendimento à Solicitação de Ativação de Serviços consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Ativação do SAI-BL e SAI-BLI em Área Urbana	30	Dias corridos
Prazo para Ativação do SAI-BL e SAI-BLI em Área Rural	45	Dias corridos

Prazo para atendimento à Solicitação de Alteração da Prestação de Serviços

6.85. O prazo para atendimento a uma Solicitação de Alteração da Prestação de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação e a data do aceite pelo OES.

6.86. O atendimento, pela CONTRATADA, à Solicitação de Alteração da Prestação de Serviços deve ser realizado no prazo máximo descrito na tabela a seguir:

INDICADOR		
Prazo para Alteração da Prestação de Serviços	VALOR	UNIDADE
Com ou sem alteração da capacidade nominal do SAI-BL e SAI-BLI em Área Urbana	10	Dias corridos
Com ou sem alteração da capacidade nominal do SAI-BL e SAI-BLI em Área Rural	15	Dias corridos

Prazo para atendimento à Solicitação de Alteração de Configuração de CPE

6.87. O prazo para atendimento a uma Solicitação de Alteração de Configuração de CPE corresponde ao período de tempo, expresso em dias corridos, entre o momento da emissão da solicitação e o aceite pelo OES.

6.88. Entre as atividades previstas neste indicador estão a configuração de desabilitação/habilitação de interface LAN entre outras alterações lógicas no CPE.

6.89. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.90. O atendimento, pela CONTRATADA, à Solicitação de Alteração de Configuração de CPE para UP ou UC deve ser realizado no prazo máximo descrito na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Configuração de CPE do SAI-BL e SAI-BLI	2	Dias corridos

Prazo para atendimento à Solicitação de Alteração da Infraestrutura de Instalação

6.91. O prazo para atendimento à Solicitação de Alteração da Infraestrutura de Instalação do SAI-BL e SAI-BLI corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação pelo OES e a data do envio dos resultados dos testes realizados pela CONTRATADA, desde que tenha havido aceite pelo OES.

6.92. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.93. O prazo para a aprovação de GMUD não deve ser considerado para efeito de cálculo do indicador.

6.94. O prazo para atendimento à Solicitação de Alteração da Infraestrutura de Instalação do SAI-BL e SAI-BLI é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração da Infraestrutura de Instalação do SAI-BL e SAI-BLI em Área Urbana	7	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SAI-BL e SAI-BLI em Área Rural	11	Dias corridos

Prazo para atendimento à Solicitação de Alteração de Dados Cadastrais

6.95. O prazo para atendimento à Solicitação de Alteração de Dados Cadastrais corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data da execução da alteração pela mesma.

6.96. O prazo para atendimento à Solicitação de Alteração de Dados Cadastrais é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Dados Cadastrais	10	Dias corridos

Prazo para atendimento à Solicitação de Alteração de Titularidade do ID

6.97. O prazo para atendimento à Solicitação de Alteração de Titularidade do ID, de UP ou de UC, corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data da execução da alteração pela mesma.

6.98. O prazo para atendimento à Solicitação de Alteração de Titularidade do ID é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Titularidade do ID	10	Dias corridos

Frequência de Faturas Contestadas Procedentes

6.99. A Frequência de Faturas Contestadas Procedentes corresponde ao percentual das faturas contestadas procedentes em relação às faturas emitidas, durante o período de um mês, tendo como base as informações dos registros de Solicitação de Contestação de Faturas.

6.100. A apuração deste indicador é feita pela aplicação da seguinte fórmula:

FFCP (%) = (FCP / TFE)*100

Em que:

FFCP – Frequência de Faturas Contestadas Procedentes, no mês calendário.

FCP – Faturas Contestadas Procedentes, no mês calendário.

TFE – Total de Faturas Emitidas, no mês calendário.

6.101. O valor máximo para a Frequência de Faturas Contestadas Procedentes é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Faturas Contestadas Procedentes	3	%

Prazo para entrega de relatórios

6.102. O prazo para entrega dos relatórios previstos neste Contrato, em meio eletrônico, é o que consta na tabela abaixo.

INDICADOR	VALOR	UNIDADE
Prazo para entrega de relatórios em meio eletrônico (no mês subsequente ao mês da apuração)	15	Dias corridos

Resumo dos Indicadores do SLA para a prestação do SAI-BL

6.103. Os indicadores do SLA se encontram agrupados na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente do SAI-BL e SAI-BLI	5	%
Prazo para Solução de Incidentes no SAI-BL e SAI-BLI em área urbana	24	Horas
Prazo para Solução de Incidentes no SAI-BL e SAI-BLI em área rural	36	Horas
Indisponibilidade do SAI-BL, por unidade	48	Horas
Indisponibilidade do SAI-BLI, por unidade	8	Horas
Prazo para Ativação do SAI-BL e SAI-BLI em Área Urbana	30	Dias corridos
Prazo para Ativação do SAI-BL e SAI-BLI em Área Rural	45	Dias corridos
Prazo para Alteração da Prestação de Serviços com ou sem alteração da capacidade nominal do SAI-BL e SAI-BLI em Área Urbana	10	Dias corridos
Prazo para Alteração da Prestação de Serviços com ou sem alteração da capacidade nominal do SAI-BL e SAI-BLI em Área Rural	15	Dias corridos
Prazo para Alteração da Configuração de CPE	2	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SAI-BL e SAI-BLI em Área Urbana	7	Dias corridos
Prazo para Alteração da Infraestrutura de Instalação do SAI-BL e SAI-BLI em Área Rural	11	Dias corridos
Prazo para Alteração de Dados Cadastrais	10	Dias corridos
Prazo para Alteração de Titularidade do ID	10	Dias corridos
Frequência de Faturas Contestadas Procedentes	3	%
Prazo para entrega de relatórios em meio eletrônico	15	Dias corridos

Indicadores para o SSDWAN (Lote 3)

Frequência de Registros de Incidente por ID para o SSDWAN

6.104. Frequência de Registro de Incidentes por ID para o SSDWAN corresponde ao número total de registros abertos de forma proativa ou de forma reativa, por mês.

6.105. A apuração do indicador deve ser feita com base nas informações de abertura de registro de incidentes.

6.106. A Quantidade máxima de abertura de Registros de Incidentes por ID por mês está descrita na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente por ID para o SSDWAN	3	Registro

Frequência de Registros de Incidente do SSDWAN

6.107. A Frequência de Registros de Incidente do SSDWAN, por cem ID, corresponde ao número total de Registros de Incidente relativos ao Serviço de SD-WAN, fechados no mês, cuja causa é de responsabilidade da CONTRATADA, dividido pela quantidade de ID ativados até o último dia do mês, multiplicado por cem.

6.108. A frequência máxima de Registros de Incidente do SSDWAN é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente do SSDWAN	5	%

Prazo para Solução de Incidente no SSDWAN

6.109. O prazo para Solução de Incidente no SSDWAN, cuja causa é de responsabilidade da CONTRATADA, corresponde ao valor máximo admissível do período de tratamento do incidente relativo ao SSDWAN e todos os recursos utilizados para prestação do serviço.

6.110. O prazo para Solução de Incidente é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Solução de Incidente no SSDWAN (categorias 1 a 7) em área urbana	320	Minutos
Prazo para Solução de Incidente no SSDWAN (categorias 1 a 7) em área rural	480	Minutos

Indisponibilidade Mensal do Sistema de Gerência e Monitoramento do SSDWAN

6.111. Percentual de tempo, durante o período do mês de operação, em que os relatórios e serviços de gerência, monitoramento e operação da solução do SSDWAN, assim como o acesso ao sistema de gerência venham a permanecer em condições não normais de funcionamento.

6.112. Para a aferição da indisponibilidade mensal do sistema de gerência e monitoramento SSDWAN, devem ser consideradas todas as instâncias de gerenciamento por grupos disponibilizadas pela CONTRATADA.

6.113. A indisponibilidade do Sistema de Gerência e Monitoramento do SSDWAN é expressa em horas através da seguinte fórmula:

Indisponibilidade do Sistema de Gerência e Monitoramento do SSDWAN (horas) = GEREN/ 60
Em que:
GEREN – período de tempo total, expresso em minutos, correspondente à soma da interrupção na prestação dos Serviços de Gerência e Monitoramento do SSDWAN simultaneamente para todas as instâncias de gerenciamento por grupo, no mês, de responsabilidade da CONTRATADA.

6.114. A indisponibilidade dos Sistema de Gerência e Monitoramento é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do Sistema de Gerência do SSDWAN	4	Horas

Indisponibilidade do SSDWAN

6.115. Percentual de tempo, durante o período do mês de operação, em que o SSDWAN venha a permanecer em condições não normais de funcionamento.

6.116. Para este indicador deve ser considera a indisponibilidade de qualquer elemento que componha o SSDWAN (CPE, firewalls e/ou outros dispositivos).

6.117. A indisponibilidade do SSDWAN é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do SSDWAN	8	Horas
Indisponibilidade do SSDWAN em alta disponibilidade	4	Hora

Prazo para Solução de Incidente em qualquer elemento do Sistema de Servidores da Solução SD-WAN

6.118. O prazo para Solução de Incidente em qualquer elemento do Sistema de servidores da solução SD-WAN (para implementação das instâncias de gerência ou qualquer outro servidor que componha a solução SD-WAN), cuja causa é de responsabilidade da CONTRATADA, corresponde ao valor máximo admissível para os serviços disponibilizados.

6.119. O prazo para Solução de Incidentes em qualquer elemento do Sistema de servidores da Solução SD-WAN é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para solução de Incidente em qualquer elemento do Sistema de Servidores da Solução SD-WAN	6	Horas

Indisponibilidade do Sistema de Servidores do SSDWAN

6.120. Tempo, durante o período do mês de operação, em que o Sistema de servidores (orquestrador, controlador, etc.) utilizados na prestação do SSDWAN venham a permanecer em condições não normais de funcionamento.

6.121. A indisponibilidade dos servidores do SSDWAN é a que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do Sistema de Servidores do SSDWAN	120	Minutos

Prazo para atendimento à Solicitação de Ativação ou Adição de Serviço para elementos SD-WAN das categorias 1,2, 3 e 4

6.122. O prazo para atendimento à Solicitação de Ativação ou Adição de Serviço corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação pelo OES e a data do envio dos resultados dos testes de ativação do ID realizados pela CONTRATADA, desde que tenha sido dado o aceite pelo OES.

6.123. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.124. O prazo para atendimento à Solicitação de Ativação ou Adição de Serviço SD-WAN consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para atendimento à Solicitação de Ativação ou Adição de Serviço para elementos SD-WAN das categorias 1, 2, 3 e 4.	60	Dias corridos

Prazo para atendimento à Solicitação de Ativação ou Adição de Serviço para elementos SD-WAN das categorias 5, 6 e 7

6.125. O prazo para atendimento à Solicitação de Ativação ou Adição de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação e a data do aceite pelo OES.

6.126. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.127. O prazo para atendimento à Solicitação de Ativação ou Adição de Serviços consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para atendimento à Solicitação de Ativação ou Adição de Serviço para elementos SD-WAN das categorias 5, 6 e 7.	90	Dias corridos

Prazo para atendimento à Solicitação de Alteração de Configuração do dispositivo SD-WAN

6.128. O prazo para atendimento à Solicitação de Ativação ou Adição de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação e a data do aceite pelo OES.

6.129. A alteração de configuração pode ser uma solicitação relacionada à alteração das políticas de encaminhamento, políticas de segurança, relacionada à integração de um novo enlace no dispositivo SD-WAN (desde que o dispositivo atual possua porta disponível) ou qualquer outra alteração de configuração necessária para adequação dos serviços SD-WAN na OES.

6.130. As alterações devem ser realizadas no dispositivo SD-WAN (CPE SD-WAN e/ou dispositivos de segurança) conforme a necessidade associada à solicitação de alteração de configuração.

6.131. O prazo para atendimento à Solicitação de Alteração de Configuração do dispositivo SD-WAN consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para atendimento à Solicitação de Alteração de Configuração no dispositivo SD-WAN	48	Horas

Prazo para atendimento à Solicitação de Alteração de Localização Física de dispositivo SD-WAN

6.132. O prazo para atendimento à Solicitação de Alteração de Localização Física do dispositivo SD-WAN corresponde ao período de tempo, expresso em dias corridos, entre a data da emissão da solicitação e a data do aceite pelo OES.

6.133. Quando de ocorrências em que a execução de atividades, pela CONTRATADA, no local de instalação do ID, for condicionada a agendamento definido junto ao OES, em decorrência de seus critérios operacionais e de segurança, o tempo de interrupção das atividades da CONTRATADA não deve ser considerado para efeito de cálculo do indicador.

6.134. O prazo para a aprovação de GMUD não deve ser considerado para efeito de cálculo do indicador.

6.135. O prazo para atendimento à Solicitação de Alteração de Localização Física do dispositivo SD-WAN é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Localização Física do dispositivo SD-WAN	15	Dias corridos

Prazo para entrega de relatórios mensais em meio digital

6.136. O prazo para entrega dos relatórios previstos neste Contrato, em meio eletrônico, é o que consta na tabela abaixo.

INDICADOR	VALOR	UNIDADE
Prazo para entrega de relatórios em meio eletrônico (no mês subsequente ao mês da apuração)	15	Dias corridos

Prazo para Alteração de Dados Cadastrais

6.137. O prazo para atendimento à Solicitação de Alteração de Dados Cadastrais corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data da execução da alteração pela mesma.

6.138. O prazo para atendimento à Solicitação de Alteração de Dados Cadastrais é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Dados Cadastrais	10	Dias corridos

Frequência de Registros de Incidente de Incidentes devido a indisponibilidade de Informações no Sistema de Gerenciamento SD-WAN

6.139. Frequência de Registro de Incidentes relacionados às falhas sobre informações disponibilizadas pelo sistema de gerenciamento SD-WAN.

6.139.1. Serão consideradas falhas de informações quando houver acesso ao sistema de gerência e a informação disponibilizada não estiver atualizada ou não estiver disponível para consulta.

6.139.2. Este indicador corresponde ao número total de registros abertos de forma proativa ou de forma reativa, por mês.

6.140. A apuração do indicador deve ser feita com base nas informações de abertura de registro de incidentes.

6.141. A Quantidade máxima de abertura de Registros de Incidentes de Indisponibilidade de Informações no Sistema de Gerenciamento SD-WAN por mês está descrita na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente de Incidentes devido a indisponibilidade de Informações no Sistema de Gerenciamento SD-WAN	3	Registro

Resumo dos Indicadores do SLA para a prestação do SSDWAN

6.142. Os indicadores do SLA para a solução SD-WAN se encontram agrupados na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente por ID para o SSDWAN	3	Registros
Frequência de Registros de Incidente do SSDWAN	5	%
Prazo para Solução de Incidente no SSDWAN (categorias 1 a 7)	320	Minutos
Prazo para Solução de Incidente no SSDWAN (categorias 1 a 7) em área rural	480	Minutos
Indisponibilidade do Sistema de Gerência e Monitoramento do SSDWAN	4	Horas
Indisponibilidade do SSDWAN	8	Horas
Indisponibilidade do SSDWAN em alta disponibilidade	4	Hora
Prazo para Solução de Incidente em qualquer elemento do Sistema de Servidores da Solução SD-WAN	6	Horas
Indisponibilidade do Sistema de Servidores do SSDWAN	120	Minutos
Prazo para atendimento à Solicitação de Ativação ou Adição de Serviço para elementos SD-WAN das categorias 1, 2, 3 e 4.	60	Dias Corridos
Prazo para atendimento à Solicitação de Ativação ou Adição de Serviço para elementos SD-WAN das categorias 5, 6 e 7.	90	Dias Corridos
Prazo para atendimento à Solicitação de Alteração de Configuração do dispositivo SD-WAN	48	Horas
Prazo para atendimento à Solicitação de Alteração de Localização Física do elemento de dispositivo SD-WAN	15	Dias Corridos
Prazo para entrega de relatórios mensais em meio digital (no mês subsequente ao mês da apuração)	15	Dias Corridos
Prazo para Alteração de Dados Cadastro	10	Dias Corridos
Frequência de Registros de Incidente de Incidentes devido a indisponibilidade de Informações no Sistema de Gerenciamento SD-WAN	3	Incidentes

VII. GERENCIAMENTO

DA REDE IP MULTISSERVIÇOS E DE SEUS RECURSOS AGREGADOS (Lote 1)

7.1. O gerenciamento da Rede IP Multisserviços e dos recursos de *hardware* e *software* a esta agregados para a prestação dos serviços SCM e STI, referido nesta seção do documento como Gerenciamento, consiste na execução das atividades compreendidas nas áreas funcionais da Gerência de Configuração, Gerência de Incidentes, Gerência de Desempenho e Gerência de Segurança.

7.2. As unidades organizacionais *Network Operation Center* (NOC) e Unidade Provedora de Gerenciamento (UPG), sob a coordenação da primeira, são incumbidas da execução das atividades compreendidas nas áreas funcionais da Gerência de Configuração, Gerência de Incidentes, Gerência de Desempenho e Gerência de Segurança.

7.3. O Gerenciamento tem como objetivo a continuidade da prestação dos serviços dentro dos parâmetros de desempenho técnico-operacional estabelecidos no Acordo de Nível de Serviço (SLA).

7.4. As atividades de Gerenciamento devem ser executadas de forma proativa e transparente para a prestação dos serviços, sem causar sua interrupção ou a degradação de sua qualidade.

7.5. O Gerenciamento deve se apoiar na utilização de recursos de *hardware* e *software*, constituídos por plataformas de gerenciamento referidas neste documento como Sistemas Especialistas de Gerenciamento (SEG), que dá suporte à formação da base de dados de gerenciamento.

7.5.1. O SEG e todos os elementos por ele gerenciados devem estar com a data e hora sincronizada através de NTP (*Network Time Protocol*).

7.6. A base de dados de gerenciamento utilizada pelo NOC e pela UPG deve conter, dentre outras, as informações de configuração de cada elemento de rede, as informações dos elementos gerenciados, o histórico de alarmes, histórico de eventos, o histórico das ações executadas e o histórico dos indicadores de desempenho.

7.6.1. Deve ser praticada rotina de *backup* que possibilite recuperação rápida, segura e consistente dessas informações pelo período de 36 (trinta e seis) meses.

7.7. O SEG deve efetuar a coleta e atualização das informações disponíveis de cada elemento gerenciado, dentro do intervalo máximo de 15 (quinze) minutos.

7.7.1. Os elementos gerenciados da Rede IP Multisserviços são o P (*Provider*) e o PE (*Provider Edge*), do *backbone*, e o CPE (*Customer Premises Equipment*).

7.7.2. Os elementos gerenciados da infraestrutura para a prestação do Serviço de Trânsito Internet (STI) são os equipamentos de terminação dos circuitos digitais, roteadores, portas Internet e dispositivos da solução de monitoramento, detecção e mitigação de ataques instalados nos PoP do AS GESP.

7.7.3. Os elementos gerenciados da função de aceleração WAN são os recursos responsáveis pela implementação desta funcionalidade.

7.8. Cada elemento gerenciado deve transmitir para o SEG, de imediato, os alarmes gerados em decorrência de alterações nas condições de operação dos elementos, como por exemplo, alterações do estado operacional do link (link *up/down*), alarmes de desempenho de violação de utilização de processador, alarmes de desempenho de violação de limites de parâmetros de QoS, entre outros, de tal forma que o SEG tome conhecimento dos eventos mais significativos e consiga atuar de forma proativa que garanta o SLA contratado.

7.9. A execução das atividades de Gerenciamento não pode comprometer mais do que 16 Kbps da capacidade nominal do SCM.

7.10. O SEG deve ser escalável, flexível e capaz de atender à expansão da quantidade de elementos gerenciados, decorrentes da ampliação da prestação dos serviços ao longo do período de vigência do Contrato.

7.11. É responsabilidade da CONTRATADA prover as plataformas de Gerenciamento do SEG.

7.12. É responsabilidade da CONTRATADA, sempre que houver reconfiguração ou substituição do elemento gerenciado, proceder, se necessário, com a remodelagem desse elemento nas plataformas de Gerenciamento do SEG, bem como comunicar de imediato à Administradora da Rede e Serviços para que ela possa também remodelar, se necessário, na sua plataforma de monitoramento.

7.13. A Gerência de Configuração é responsável por manter o controle quantitativo e qualitativo de cada um dos elementos gerenciados, por manter o controle da operação e da manutenção desses elementos e por manter o histórico das mudanças na estrutura física e lógica da Rede IP Multisserviços e dos recursos agregados.

7.14. A Gerência de Configuração compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.14.1. Modelagem na plataforma de gerenciamento (SEG) dos elementos gerenciados e da conectividade entre eles.

7.14.2. Coleta de informações sobre a configuração dos dispositivos e atribuição dos valores iniciais aos parâmetros dos elementos gerenciados, conforme modelo da plataforma de gerenciamento.

7.14.3. Gestão da configuração dos elementos gerenciados e associados à prestação dos serviços, com a aplicação de métodos e processos para a identificação e registro das características físicas (estrutura de interconexão) e lógicas (relacionamento) dos elementos gerenciados, bem como das alterações dessas características (MAC – *Moves, Adds and Changes*).

7.14.4. Execução de teste funcional para verificar a alcançabilidade dos endereços IP de destinos configurados no CPE, do ID de modo a confirmar a conectividade inerente à prestação do SCM.

7.14.5. Coleta e geração de informações para a emissão de relatórios gerenciais.

7.14.6. Geração e envio de informações para os sistemas internos da CONTRATADA.

7.14.7. Acompanhamento da execução das ações coordenadas por essa gerência.

7.15. A Gerência de Incidentes é responsável pelo acompanhamento das ocorrências de alarmes, pela detecção de falha na Rede IP Multisserviços e nos recursos agregados, pelo isolamento da falha e pelas decisões que devem ser tomadas para o restabelecimento da normalidade de funcionamento contínuo em casos de degradação, interrupção parcial ou interrupção total na prestação dos serviços.

7.16. A Gerência de Incidentes compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.16.1. Controle do nível de severidade de alarmes nos elementos gerenciados com funcionamento anormal, parcial ou fora de operação.

7.16.2. Análise e diagnóstico de incidentes, aplicação de técnicas de correlação de eventos e de testes funcionais nos elementos gerenciados para localização, identificação de causas e isolamento de falhas.

7.16.3. Comparação entre a configuração corrente do elemento gerenciado com as configurações armazenadas na base de dados de gerenciamento, para detecção de divergências que possam dar causa a falha.

7.16.4. Intervenção nos elementos gerenciados para ajustes em sua configuração com a finalidade de isolamento ou de solução de falha, inclusive efetuando, se for o caso, *roll-back* de configuração.

7.16.5. Acionamento das equipes de manutenção corretiva para solução de falhas e acompanhamento das ações para o restabelecimento da normalidade do funcionamento dos elementos que apresentarem falhas.

7.16.6. Execução de testes funcionais para verificação das condições normais de funcionamento dos recursos inerentes à prestação dos serviços, inclusive quanto à alcançabilidade dos endereços IP de destinos configurados no CPE, do ID de modo a confirmar a conectividade inerente à prestação do SCM.

7.16.7. Registro e controle, em base de dados, das informações de falhas nos recursos inerentes à prestação dos serviços para permitir a emissão de relatórios gerenciais.

7.16.8. Geração e envio de informações de falhas para os sistemas internos da CONTRATADA.

7.16.9. Acompanhamento da execução das ações coordenadas por essa gerência.

7.17. Para a execução das funções da Gerência de Incidentes, deve ser utilizado um sistema de apoio para o Registro de Incidente que, dentre outras facilidades, permita a abertura de Registro de Incidente detectado pelo SEG ou comunicado pelo solicitante, o acompanhamento e o encerramento de comunicação associada ao Registro de Incidente, a consulta ao histórico dos incidentes para análise e solução de incidente e o escalonamento de Registro de Incidente para equipe especializada na resolução de falhas.

7.18. A Gerência de Desempenho é responsável pelo monitoramento dos indicadores de desempenho especificados no SLA, pela avaliação desses indicadores de desempenho, pela solução de deficiências de desempenho e planejamento de capacidade nominal dos recursos, conforme requisitos da prestação dos serviços.

7.19. A Gerência de Desempenho compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.19.1. Gestão dos limiares para os parâmetros de monitoramento dos elementos gerenciados, incluindo um intervalo de valores aceitável (*threshold*), um valor de alerta e um valor em que se remove a situação de alerta, tendo por base o atendimento aos indicadores definidos para a Qualidade dos Serviços (QoS) prestados.

7.19.2. Monitoramento contínuo e em tempo real dos elementos gerenciados para identificação de taxas crescentes de utilização, taxas crescentes de erro, atrasos de transmissão, dentre outras anormalidades, visando evitar a ocorrência de alarmes decorrentes de valores dos parâmetros fora dos limites estabelecidos (*thresholds*).

7.19.3. Execução de testes entre dois acessos da Rede IP Multisserviços para verificar o atendimento aos parâmetros de QoS associados aos serviços prestados nesses acessos.

7.19.4. Análise das tendências do desempenho dos elementos gerenciados.

7.19.5. Gestão da capacidade nominal dos recursos inerentes à prestação dos serviços.

7.19.6. Análise dos parâmetros de configuração, dos valores limites dos parâmetros e do regime de coleta de informações dos elementos gerenciados.

7.19.7. Registro e controle, em base de dados, das informações de desempenho dos elementos gerenciados para a emissão de relatórios gerenciais.

7.19.8. Geração e envio de informações de desempenho para os sistemas internos da CONTRATADA.

7.19.9. Acompanhamento da execução das ações coordenadas por essa gerência.

7.20. A Gerência de Segurança é responsável pela segurança do transporte de informações através dos recursos utilizados para a prestação dos serviços, pela detecção de qualquer evento adverso, confirmado ou sob suspeita, de tentativa de violação dos recursos e pela geração de alarmes sempre que ocorra evento dessa natureza.

7.21. A Gerência de Segurança compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.21.1. Configuração de disparo de alarme de violação de segurança.

7.21.2. Controle de Permissão de Acesso (*Access Control*) aos recursos utilizados para a prestação dos serviços.

7.21.3. Controle da confidencialidade das informações transportadas (*confidentiality*).

7.21.4. Controle da integridade das informações transportadas (*integrity*).

7.21.5. Monitoramento e análise contínuos dos recursos associados à prestação dos serviços, incluindo a supervisão do status dos alarmes de violação de segurança, quanto aos riscos inerentes às tentativas de acesso não autorizado, aos ataques de negação de serviço (DoS), de uso ou acesso não autorizado ou de modificações nos recursos sem o conhecimento ou consentimento prévio do solicitante.

7.21.6. Bloqueio e desbloqueio de segurança de um endereço IP ou de um bloco de endereços IP, de origem ou de destino, no CPE da rede de acesso da Rede IP Multisserviços, executado com a inclusão ou com a exclusão do endereço na lista de controle de acesso (ACL) do CPE.

7.21.7. Geração de registro de incidente de segurança, incluindo as tentativas de acesso negadas e os ataques bem-sucedidos, em base de dados, contendo informações de data e horário da ocorrência, endereço IP de origem da atividade, protocolo utilizado e portas envolvidas.

7.21.8. Análise dos registros de incidente de segurança para a emissão de relatórios gerenciais.

7.21.9. Geração e envio de informações de segurança para os sistemas internos da CONTRATADA.

7.21.10. Acompanhamento da execução das ações coordenadas por essa gerência.

7.22. O NOC e a UPG devem assegurar a alta disponibilidade dos recursos utilizados na prestação dos serviços, atuando com eficácia na identificação das causas de degradação e de interrupção da prestação dos serviços e na execução das ações para restaurar as condições de qualidade requisitadas para a prestação dos serviços.

7.23. O NOC deve atuar, com exclusividade, sobre os elementos gerenciados do *backbone* da Rede IP Multisserviços, P (*Provider*) e PE (*Provider Edge*), e no CPE da rede de acesso, caso seja necessário complementar a atuação da UPG.

7.24. O NOC deve atuar, com exclusividade, sobre os elementos gerenciados das estruturas agregadas à Rede IP Multisserviços para a prestação do Serviço de Trânsito Internet.

7.24.1. A Gerência de Configuração e a Gerência de Segurança dos roteadores da Borda BGP do AS GESP utilizados na prestação do STI são de responsabilidade da CONTRATADA podendo, caso solicitado pela Administradora da Rede e Serviços, ser transferida para a PRODESP.

7.25. A UPG deve atuar, com prioridade em relação ao NOC, sobre os CPE (*Customer Premises Equipment*) da rede de acesso da Rede IP Multisserviços.

7.26. A UPG deve monitorar os seguintes recursos:

7.26.1. Infraestrutura do STI.

7.26.2. Dispositivos de aceleração WAN.

7.26.3. Recursos da funcionalidade de monitoramento, detecção e mitigação de ataques.

7.27. A UPG deve apresentar os relatórios referentes aos indicadores do Nível de Qualidade do Serviço de Comunicação Multimídia (NQSCM), conforme disposto no Acordo Operacional.

7.28. A CONTRATADA deve manter o SEG operacional e atualizado, propiciando condições necessárias para a execução do Gerenciamento pelo NOC e pela UPG.

7.29. O NOC deve contar com equipe de técnicos especializados e operar em regime de 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, sendo de responsabilidade da CONTRATADA a instalação, operação e manutenção dos recursos de infraestrutura necessários ao seu funcionamento nas dependências da CONTRATADA.

7.30. A UPG deve contar com equipe de técnicos especializados nas tecnologias utilizadas na rede de acesso e operar em regime de 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, nas dependências da PRODESP no município de Taboão da Serra – SP, para atendimento exclusivo à Rede Intragov.

7.31. A equipe técnica da UPG deve ser composta por um gerente, um coordenador e por atendentes, cuja qualificação profissional deve atender aos perfis que constam nos subitens que seguem:

7.31.1. Gerente – profissional com experiência em projetar, instalar, configurar e operar redes de telecomunicações de médio ou grande porte e com conhecimento do CPE da rede de acesso da Rede IP Multisserviços.

7.31.1.1. O Gerente deve permanecer na UPG com a frequência mínima de uma vez a cada 15 dias, em dia combinado previamente com a ADMINISTRADORA, ou quando solicitado pelo Administrador da Rede, em horário comercial.

7.31.2. Coordenador – profissional com experiência em coordenação de equipe de atendimento de redes de telecomunicações e com certificação técnica para instalação, configuração e operação em redes que utilizem o CPE da rede de acesso da Rede IP Multisserviços.

7.31.2.1. O Coordenador deve executar atividades exclusivas à UPG, comparecendo nesta unidade todos os dias úteis da semana, em horário comercial.

7.31.3. Atendente – profissional com certificação técnica para instalação, configuração e operação em redes de telecomunicações que utilizem o CPE da rede de acesso da Rede IP Multisserviços.

7.31.3.1. A equipe de atendentes deve permanecer na PRODESP em regime de 24x7.

7.32. Na ausência do Gerente ou do Coordenador, deve ser indicado, com no mínimo 5 (cinco) dias de antecedência, um substituto qualificado.

7.33. A equipe de atendentes da UPG deve ser dimensionada, a critério da CONTRATADA, para a execução de suas atribuições até o limite de 8 (oito) posições para consoles de operação a serem instaladas no ambiente cedido pela PRODESP.

7.34. A equipe da UPG deve acionar o NOC quando necessário de modo a escalar ou cooperar na solução de incidentes cuja complexidade requeira suporte especializado.

7.35. A equipe da UPG deve acionar o SOC quando necessário nos casos de incidentes relacionados à ataques na infraestrutura do STI.

7.36. A equipe da UPG deve dispor de consoles de operação integrada ao SEG, em tempo real, instaladas, operadas e mantidas pela CONTRATADA, em quantidade suficiente para o desempenho de suas atividades de Gerenciamento.

7.37. A interligação das consoles de operação da UPG ao SEG deve ser feita através de um circuito digital redundante e dedicado com capacidade a ser definida pela CONTRATADA, de modo a garantir o desempenho e a disponibilidade mensal de 99,95% (noventa e nove por cento e noventa e cinco centésimos).

7.37.1. A CONTRATADA deve providenciar a ampliação da capacidade nominal do circuito digital sempre que a média móvel trimestral no horário comercial de utilização de qualquer um desses recursos ultrapassar 50% de sua capacidade nominal ou quando o valor do 95º Percentil mensal, no horário comercial, de qualquer um desses recursos atingir ou ultrapassar 90% da sua capacidade nominal, o que ocorrer primeiro.

7.37.2. A implantação ou a adequação da estrutura necessária para a interligação das consoles de operação da UPG ao SEG deve estar concluída no prazo de 90 (noventa) dias ou de 60 (sessenta) dias, respectivamente, a contar da data de assinatura do Contrato, conforme conste no Plano de Transição.

7.37.3. Durante a vigência do Contrato, as ampliações necessárias na estrutura de interligação das consoles de operação da UPG ao SEG devem estar disponíveis no prazo de 60 (sessenta) dias a contar da data de ocorrência do evento que lhe der causa.

7.37.4. O não cumprimento dos prazos pode implicar na aplicação de penalidade por descumprimento contratual.

7.38. Além das consoles de operação, a CONTRATADA é responsável pelas licenças de *softwares*, pelos recursos de infraestrutura de rede local e comunicação e pelo fornecimento de bens de consumo, todos para a sua utilização, necessários ao funcionamento da UPG nas dependências da PRODESP.

7.39. A UPG deve ser implantada em área de acesso restrito, em condições adequadas de iluminação e climatização, cedida pela PRODESP para uso da CONTRATADA.

7.40. Para o funcionamento da UPG, a PRODESP é responsável pela cessão de área para instalação de até 8 (oito) consoles de operação, pelo mobiliário, pelo fornecimento de energia elétrica, pela guarda e integridade dos equipamentos instalados e pela permissão de acesso dos profissionais credenciados à área de acesso restrito.

7.41. Para a execução das funções da Gerência de Desempenho e da Gerência de Incidentes, pela equipe da UPG, as informações relativas ao CPE devem ser agrupadas e apresentadas na console de operação, através de interface gráfica, sob visão topológica da rede de acesso por PE, apresentando o CPE, o enlace e a respectiva interface do PE, e sob visão geográfica da rede de acesso por localidade, apresentando os CPE instalados em cada localidade.

7.42. As informações relativas ao CPE que devem ser apresentadas nas consoles de operação são as que constam nos subitens que seguem:

7.42.1. Roteamento da VPN configurada no PE associado ao CPE.

7.42.2. Status do CPE da rede de acesso e de suas interfaces.

7.42.3. Alarmes e eventos ocorridos no CPE da rede de acesso, com informações de data e hora de cada ocorrência.

7.42.4. Tráfego em curso, por interface do CPE da rede de acesso.

7.43. As informações relativas ao recurso de aceleração WAN que devem ser apresentadas nas consoles de operação são as que constam nos subitens que seguem:

7.43.1. Alarmes associados ao equipamento de aceleração WAN.

7.43.2. Medidas de desempenho de recursos computacionais tais como CPU e memória.

7.43.3. Medições da eficiência do processo de aceleração.

7.44. As informações relativas a funcionalidade de monitoramento, detecção e mitigação de ataques que devem ser apresentadas nas consoles de operação são os alarmes associados aos dispositivos da solução instalados nos PoP do AS GESP.

7.45. A CONTRATADA deve atuar de forma preventiva, evitando a degradação ou a interrupção na prestação dos serviços ou minimizando seus efeitos, com base nas informações relativas ao CPE, apresentadas nas consoles de operação.

7.46. A CONTRATADA deve utilizar uma solução especializada para testes de desempenho e qualidade em redes IP com capacidade de geração de tráfego e coleta de informações na execução de testes funcionais em um ID específico da Rede IP Multisserviços, com o objetivo de verificar os níveis da qualidade da prestação dos serviços com base nos parâmetros de QoS associados aos serviços prestados no SCM, comprovar a priorização de pacotes conforme as classes de QoS, e a medição de, no mínimo, os parâmetros latência bidirecional, *jitter*, perda de pacotes e vazão máxima em TCP e UDP.

7.46.1. A solução deve:

7.46.1.1. Realizar o teste entre a Unidade (UP ou UC) e um ponto da própria rede da CONTRATADA.

7.46.1.2. Se basear em duas *probes* (*appliance* ou *software*+computador), sendo uma delas conectada, preferencialmente, diretamente ao CPE da Unidade, enquanto a outra *probe* deve ser conectada dentro da rede da CONTRATADA.

7.46.1.3. Ser capaz de gerar tráfego nos dois sentidos, tanto de forma simultânea quanto alternada.

7.46.1.4. Ser capaz de gerar fluxos customizáveis em que o usuário configura o perfil de tráfego e a Classe de QoS de cada fluxo.

7.46.1.5. Ser capaz de realizar os testes em SCM com capacidade de até 1 Gbps, inclusive.

7.46.1.6. Ser utilizada nos testes de ativação de serviço, alteração da prestação de serviço e alteração de configuração de CPE.

7.47. A CONTRATADA deve acompanhar a recuperação de falha detectada na Rede IP Multisserviços até que seja normalizada a prestação dos serviços, mantendo a PRODESP informada sobre a evolução da recuperação, conforme disposto no Acordo Operacional.

7.48. A UPG deve interagir com o NOC da prestadora do SAI-BL e da prestadora do SSDWAN, sempre que necessário ou mediante solicitação da PRODESP, visando atuar em conjunto para resolver ou colaborar na solução de incidentes cuja causa raiz ou responsabilidade não for de imediato identificada, quando houver impasse entre as prestadoras quanto à responsabilidade pelo atendimento ou naqueles incidentes de maior complexidade técnica.

7.49. A equipe da UPG deve acompanhar a manutenção programada na rede de acesso da Rede IP Multisserviços até que seja normalizada a prestação dos serviços, mantendo a PRODESP informada sobre a execução da atividade de manutenção programada, conforme disposto no Acordo Operacional.

7.50. A unidade organizacional *Security Operation Center* (SOC) é incumbida da execução das atividades de monitoramento, detecção, reação e respostas a eventos de segurança em tempo real de ataques.

7.51. O SOC deve operar 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, sendo de responsabilidade da CONTRATADA a instalação, operação e manutenção dos recursos de infraestrutura necessários ao seu funcionamento em suas dependências.

DOS ACESSOS E REDE INTERNET BANDA LARGA (Lote 2)

7.52. O gerenciamento do Acesso e Rede Internet Banda Larga da CONTRATADA para a prestação do serviço SAI-BL, referido nesta seção do documento como Gerenciamento, consiste na execução das atividades compreendidas nas áreas funcionais da Gerência de Configuração, Gerência de Incidentes, Gerência de Desempenho e Gerência de Segurança.

7.53. O Gerenciamento tem como objetivo a continuidade da prestação dos serviços dentro dos parâmetros de desempenho técnico-operacional estabelecidos no Acordo de Nível de Serviço (SLA).

7.54. As atividades de Gerenciamento devem ser executadas de forma proativa e transparente para a prestação dos serviços, sem causar sua interrupção ou a degradação de sua qualidade.

Áreas Funcionais do Gerenciamento

7.55. A CONTRATADA deve ter implementado as áreas funcionais de gerenciamento de Configuração, Incidentes, Contabilidade, Desempenho e Segurança para os Acessos e Rede Internet Banda Larga da CONTRATADA.

Requisitos Operacionais para a Estrutura Organizacional do Gerenciamento

7.56. O NOC devem assegurar a alta disponibilidade dos recursos utilizados na prestação dos serviços, atuando com eficácia na identificação das causas de degradação e de interrupção da prestação dos serviços e na execução das ações para restaurar as condições de qualidade requisitadas para a prestação dos serviços.

7.57. O NOC deve atuar, com exclusividade, sobre os elementos gerenciados da Rede Internet e interconexões da CONTRATADA, e no CPE de acesso à Internet.

7.58. O NOC deve contar com equipe de técnicos especializados e operar em regime de 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, sendo de responsabilidade da CONTRATADA a instalação, operação e manutenção dos recursos de infraestrutura necessários ao seu funcionamento nas dependências da CONTRATADA.

7.59. A CONTRATADA deve atuar de forma preventiva, evitando a degradação ou a interrupção na prestação dos serviços ou minimizando seus efeitos, com base nas informações relativas ao CPE, apresentadas nas consoles de operação.

7.60. A CONTRATADA deve acompanhar a recuperação de falha detectada na Rede Internet e suas interconexões sob sua gestão até que seja normalizada a prestação dos serviços, mantendo a PRODESP informada sobre a evolução da recuperação, conforme disposto no Acordo Operacional.

7.61. O NOC da CONTRATADA deve interagir com o NOC/UPG da prestadora do SCM e STI e da prestadora do SSDWAN, sempre que necessário ou mediante solicitação da PRODESP, visando atuar em conjunto para resolver ou colaborar na solução de incidentes cuja causa raiz ou responsabilidade não for de imediato identificada, quando houver impasse entre as prestadoras quanto à responsabilidade pelo atendimento ou naqueles incidentes de maior complexidade técnica.

DA SOLUÇÃO SD-WAN (Lote 3)

7.62. O gerenciamento da solução SD-WAN e dos recursos de *hardware* e *software* a estes agregados para a prestação dos serviços, referido neste documento como Gerenciamento, consiste na execução das atividades compreendidas nas áreas funcionais da Gerência de Configuração, Gerência de Incidentes, Gerência de Desempenho e Gerência de Segurança.

7.63. As unidades organizacionais *Network Operation Center* (NOC) e Unidade Provedora de Gerenciamento (UPG), sob a coordenação da primeira, são incumbidas da execução das atividades compreendidas nas áreas funcionais da Gerência de Configuração, Gerência de Incidentes, Gerência de Desempenho e Gerência de Segurança.

7.64. A Administradora da Rede e Serviços deve ter acesso à todas as instâncias de gerenciamento implementadas no contrato, incluindo o acesso às instâncias de gerenciamento dos OES.

7.65. O Gerenciamento tem como objetivo a continuidade da prestação dos serviços dentro dos parâmetros de desempenho técnico-operacional estabelecidos no Acordo de Nível de Serviço (SLA).

7.66. As atividades de Gerenciamento devem ser executadas de forma proativa e transparente para a prestação dos serviços, sem causar sua interrupção ou a degradação de sua qualidade.

7.67. O Gerenciamento deve se apoiar na utilização de recursos de *hardware* e *software*, constituídos por plataformas de gerenciamento referidas neste documento como Sistemas Especialistas de Gerenciamento (SEG), que dá suporte à formação da base de dados de gerenciamento.

7.67.1. O SEG e todos os elementos por ele gerenciados devem estar com a data e hora sincronizada através de NTP (*Network Time Protocol*).

7.68. A base de dados de gerenciamento utilizada pelo NOC e pela UPG deve conter, dentre outras, as informações de configuração de cada elemento de rede, as informações dos elementos gerenciados, o histórico de alarmes, histórico de eventos, o histórico das ações executadas e o histórico dos indicadores de desempenho.

7.68.1. Deve ser praticada rotina de *backup* que possibilite recuperação rápida, segura e consistente dessas informações pelo período de 36 (trinta e seis) meses.

7.69. O sistema de gerenciamento deve disponibilizar aos usuários da Administradora da Rede e Serviços e a seu preposto:

7.69.1. Visibilidade da rede com as principais métricas de desempenho da rede, como perda, latência, instabilidade e disponibilidade.

7.69.2. Qualidade da Experiência do usuário (QoE) para aplicativos.

7.69.3. Consulta às políticas de encaminhamento e de segurança por OES, por grupo de usuários e por aplicação.

7.69.4. *Benchmarks* históricos com tendências da experiência do obtida pelo usuário em aplicações e na rede (enlaces utilizados para acesso às aplicações e indicadores de QoS).

7.69.5. Recomendações de melhorias para uma melhor experiência com os aplicativos.

7.69.6. Auxílio em análises de *troubleshooting*.

7.69.7. Identificação dos maiores consumidores e aplicações considerando o consumo de largura de banda.

7.69.8. Geração de relatórios de análises de redes.

7.70. A solução SD-WAN deve possuir gerência centralizada permitindo a monitoração do status e da utilização dos enlaces por tipo de aplicação, conforme o perfil de segurança estabelecido para a unidade.

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

7.72. A gerência centralizada SD-WAN deve ser hospedada em ambiente da CONTRATANTE e gerenciado pela CONTRATADA.

7.73. O sistema de gerência deve suportar o gerenciamento das contas de usuários, possibilitando a desativação de usuários inativos ou desligados dos órgãos.

7.74. O sistema de gerência centralizada SD-WAN deve permitir acesso concorrente dos usuários.

7.75. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria.

7.76. A console de Gerência deve informar o status *up/down/speed* das interfaces LAN e WAN dos dispositivos SD-WAN, classificadas por OES ou grupo de usuários.

7.77. A console de Gerência deve informar o status acessível/inacessível/*configuration sync*/ *tunnels* up/*tunnels down* de cada dispositivo SD-WAN.

7.78. Deve permitir que todos os alarmes e eventos sejam registrados na console de Gerência.

7.79. A Gerência SD-WAN deve enviar mensagens *syslog* referentes aos dispositivos SD-WAN para um servidor *syslog* externo da CONTRATANTE.

7.80. Monitorar as informações e acompanhar a utilização de todos os enlaces conectados aos dispositivos SD-WAN executando a gestão técnica, de segurança e de qualidade.

7.81. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do *health check* (perda de pacotes, *jitter* e latência) de cada enlace conectado aos dispositivos SD-WAN.

7.82. Deve possuir gerenciamento de toda a infraestrutura SD-WAN via interface WEB utilizando HTTPS.

7.83. A solução concentradora e de gerenciamento devem ser capazes de tratar o conjunto de acessos de cada Unidade de Governo de forma independente, com políticas específicas para cada uma.

7.84. Permitir upgrade de sistema operacional das unidades remotas de forma centralizada, via ferramenta de gerência.

7.85. Permitir a distribuição de configurações padrão a todos ou grupo de equipamentos instalados nas unidades remotas.

7.86. Deve permitir que todos os alarmes e eventos sejam registrados e visualizados na console de Gerência.

Gerenciamento OES

7.87. A solução SD-WAN deve permitir a criação de diferentes instâncias de gerenciamento centralizado por grupo de unidades ou OES.

7.87.1. Estas instâncias devem ser acessadas somente pelos usuários autorizados de cada uma das unidades para monitoração e configuração de políticas de segurança.

7.88. Para cada OES devem ser disponibilizados 4 acessos de monitoração ao sistema de gerenciamento centralizado.

7.89. Cada OES deve ter a sua instância de gerenciamento, permitindo a visualização somente das suas unidades (provedoras e clientes).

7.90. Para cada OES, a solução deve permitir acesso ao sistema de gerência tanto para monitoração, quanto para configuração/alteração de políticas de segurança somente por usuários autorizados.

7.90.1. A configuração executada pelo OES deve ser restrita a alterações de políticas de segurança que não causem nenhum impacto nas configurações de rede, conectividade e disponibilidade do serviço SD-WAN prestado.

7.90.2. A solução SD-WAN deve possibilitar acesso exclusivamente ao gerenciamento das unidades previamente autorizadas para a alteração de políticas de segurança e aos itens necessários e autorizados pelo OES.

7.90.3. Demais itens de configuração devem ser desabilitados na gerência centralizada, conforme definição do perfil de usuário.

7.91. Cada unidade é responsável por gerenciar quais usuários terão o acesso que permite a configuração ou alteração de políticas segurança.

7.92. Estes usuários autorizados podem realizar alteração de configuração de políticas de segurança somente para as suas unidades, desde que estas alterações não impactem na conectividade e nas configurações de rede dos sites.

7.93. É responsabilidade de cada OES realizar estas alterações, quando necessário, sem impacto para a disponibilidade da solução, assim como gerenciar os usuários ativos, inativos e desligados.

7.94. As unidades que não forem gerenciadas em uma instância específica de um OES serão controladas por uma gerência centralizada comum a ser administrada pela Administradora de Rede e Serviços.

7.95. A solução deve permitir a criação de políticas de encaminhamento e de segurança distintas para cada uma das instâncias gerenciáveis.

Sistemas Especialistas de Gerenciamento (SEG)

7.96. O SEG deve efetuar a coleta e atualização das informações disponíveis de cada elemento gerenciado, dentro do intervalo máximo de 15 (quinze) minutos.

7.96.1. Os elementos gerenciados da solução SD-WAN são os dispositivos SD-WAN associados aos respectivos enlaces conectados à solução.

7.97. Cada dispositivo SD-WAN deve transmitir para o SEG, de imediato, os alarmes gerados em decorrência de alterações nas condições de operação dos elementos, como por exemplo, alterações do estado operacional dos links conectados (link *up/down*), alarmes de desempenho de violação de utilização de processador, alarmes de segurança, entre outros, de tal forma que o SEG tome conhecimento dos eventos mais significativos e consiga atuar de forma proativa que garanta o SLA contratado.

7.98. O SEG deve ser escalável, flexível e capaz de atender à expansão da quantidade de elementos gerenciados, decorrentes da ampliação da prestação dos serviços ao longo do período de vigência do Contrato.

7.99. É responsabilidade da CONTRATADA prover as plataformas de Gerenciamento do SEG.

7.100. É responsabilidade da CONTRATADA, sempre que houver reconfiguração ou substituição do elemento gerenciado, proceder, se necessário, com a remodelagem desse elemento nas plataformas de Gerenciamento do SEG, bem como comunicar de imediato à Administradora da Rede e Serviços para que ela possa também remodelar, se necessário, na sua plataforma de monitoramento.

Áreas Funcionais do Gerenciamento

7.101. A Gerência de Configuração é responsável por manter o controle quantitativo e qualitativo de cada um dos elementos gerenciados, por manter o controle da operação e da manutenção desses elementos e por manter o histórico das mudanças na estrutura física e lógica da solução SD-WAN e dos recursos agregados.

7.102. A Gerência de Configuração compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.102.1. Modelagem na plataforma de gerenciamento (SEG) dos elementos gerenciados e da conectividade entre eles.

7.102.2. Coleta de informações sobre a configuração dos dispositivos SD-WAN e atribuição dos valores iniciais aos parâmetros dos elementos gerenciados, conforme modelo da plataforma de gerenciamento.

7.102.3. Gestão da configuração dos elementos gerenciados e associados à prestação dos serviços, com a aplicação de métodos e processos para a identificação e registro das características físicas (estrutura de interconexão) e lógicas (relacionamento) dos elementos gerenciados, bem como das alterações dessas características (MAC – *Moves, Adds and Changes*).

7.102.4. Execução de teste funcional para verificar a alcançabilidade dos endereços IP de destinos configurados no dispositivo SD-WAN, do ID de modo a confirmar a conectividade inerente à prestação do serviço SD-WAN.

7.102.5. Coleta e geração de informações para a emissão de relatórios gerenciais.

7.102.6. Geração e envio de informações para os sistemas internos da CONTRATADA.

7.102.7. Acompanhamento da execução das ações coordenadas por essa gerência.

7.103. A Gerência de Incidentes é responsável pelo acompanhamento das ocorrências de alarmes, pela detecção de falha na solução SD-WAN e nos recursos agregados, pelo isolamento da falha e pelas decisões que devem ser tomadas para o restabelecimento da normalidade de funcionamento contínuo em casos de degradação, interrupção parcial ou interrupção total na prestação dos serviços.

7.104. A Gerência de Incidentes compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.104.1. Controle do nível de severidade de alarmes nos elementos gerenciados com funcionamento anormal, parcial ou fora de operação.

7.104.2. Análise e diagnóstico de incidentes, aplicação de técnicas de correlação de eventos e de testes funcionais nos elementos gerenciados para localização, identificação de causas e isolamento de falhas.

7.104.3. Comparação entre a configuração corrente do elemento gerenciado com as configurações armazenadas na base de dados de gerenciamento, para detecção de divergências que possam dar causa a falha.

7.104.4. Intervenção nos elementos gerenciados para ajustes em sua configuração com a finalidade de isolamento ou de solução de falha, inclusive efetuando, se for o caso, *roll-back* de configuração.

7.104.5. Acionamento das equipes de manutenção corretiva para solução de falhas e acompanhamento das ações para o restabelecimento da normalidade do funcionamento dos elementos que apresentarem falhas.

7.104.6. Execução de testes funcionais para verificação das condições normais de funcionamento dos recursos inerentes à prestação dos serviços, inclusive quanto à alcançabilidade dos endereços IP de destinos configurados no dispositivo SD-WAN, do ID de modo a confirmar a conectividade inerente à prestação da solução SD-WAN.

7.104.7. Registro e controle, em base de dados, das informações de falhas nos recursos inerentes à prestação dos serviços para permitir a emissão de relatórios gerenciais.

7.104.8. Geração e envio de informações de falhas para os sistemas internos da CONTRATADA.

7.104.9. Acompanhamento da execução das ações coordenadas por essa gerência.

7.105. Para a execução das funções da Gerência de Incidentes, deve ser utilizado um sistema de apoio para o Registro de Incidente que, dentre outras facilidades, permita a abertura de Registro de Incidente detectado pelo SEG ou comunicado pelo solicitante, o acompanhamento e o encerramento de comunicação associada ao Registro de Incidente, a consulta ao histórico dos incidentes para análise e solução de incidente e o escalonamento de Registro de Incidente para equipe especializada na resolução de falhas.

7.106. A Gerência de Desempenho é responsável pelo monitoramento dos indicadores de desempenho especificados no SLA, pela avaliação desses indicadores de desempenho, pela solução de deficiências de desempenho e planejamento de capacidade nominal dos recursos, conforme requisitos da prestação dos serviços.

7.107. A Gerência de Desempenho compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.107.1. Gestão dos limiares para os parâmetros de monitoramento dos elementos gerenciados, incluindo um intervalo de valores aceitável (*threshold*), um valor de alerta e um valor em que se remove a situação de alerta, tendo por base o atendimento aos indicadores definidos para a Qualidade dos Serviços (QoS) prestados por serviço.

7.107.2. Monitoramento contínuo e em tempo real dos elementos gerenciados para identificação de taxas crescentes de utilização, taxas crescentes de erro, atrasos de transmissão, dentre outras anormalidades, visando evitar a ocorrência de alarmes decorrentes de valores dos parâmetros fora dos limites estabelecidos (*thresholds*).

7.107.3. Análise das tendências do desempenho dos elementos gerenciados.

7.107.4. Gestão da capacidade nominal dos recursos inerentes à prestação dos serviços.

7.107.5. Análise dos parâmetros de configuração, dos valores limites dos parâmetros e do regime de coleta de informações dos elementos gerenciados.

7.107.6. Registro e controle, em base de dados, das informações de desempenho dos elementos gerenciados para a emissão de relatórios gerenciais.

7.107.7. Geração e envio de informações de desempenho para os sistemas internos da CONTRATADA.

7.107.8. Acompanhamento da execução das ações coordenadas por essa gerência.

7.108. A Gerência de Segurança é responsável pela segurança do transporte de informações através dos recursos utilizados para a prestação dos serviços, pela detecção de qualquer evento adverso, confirmado ou sob suspeita, de tentativa de violação dos recursos e pela geração de alarmes sempre que ocorra evento dessa natureza.

7.109. A Gerência de Segurança compreende, pelo menos, as funções relacionadas nos subitens que seguem:

7.109.1. Configuração de disparo de alarme de violação de segurança.

7.109.2. Controle de Permissão de Acesso (*Access Control*) aos recursos utilizados para a prestação dos serviços.

7.109.3. Controle da confidencialidade das informações transportadas (*confidentiality*).

7.109.4. Controle da integridade das informações transportadas (*integrity*).

7.109.5. Monitoramento e análise contínuos dos recursos associados à prestação dos serviços, incluindo a supervisão do status dos alarmes de violação de segurança, quanto aos riscos inerentes às tentativas de acesso não autorizado, aos ataques de negação de serviço (DoS), de uso ou acesso não autorizado ou de modificações nos recursos sem o conhecimento ou consentimento prévio do solicitante.

7.109.6. Bloqueio e desbloqueio de segurança de um endereço IP ou de um bloco de endereços IP, de origem ou de destino, no dispositivo SD-WAN, executado com a inclusão ou com a exclusão do endereço na lista de controle de acesso (ACL) do dispositivo SD-WAN.

7.109.7. Geração de registro de incidente de segurança, incluindo as tentativas de acesso negadas e os ataques bem-sucedidos, em base de dados, contendo informações de data e horário da ocorrência, endereço IP de origem da atividade, protocolo utilizado e portas envolvidas.

7.109.8. Análise dos registros de incidente de segurança para a emissão de relatórios gerenciais.

7.109.9. Geração e envio de informações de segurança para os sistemas internos da CONTRATADA.

7.109.10. Acompanhamento da execução das ações coordenadas por essa gerência.

Requisitos Operacionais para a Estrutura Organizacional do Gerenciamento

7.110. O NOC e a UPG devem assegurar a alta disponibilidade dos recursos utilizados na prestação dos serviços, atuando com eficácia na identificação das causas de degradação e de interrupção da prestação dos serviços e na execução das ações para restaurar as condições de qualidade requisitadas para a prestação dos serviços.

7.111. A UPG deve atuar, com prioridade em relação ao NOC, sobre os dispositivos SD-WAN.

7.112. A UPG deve monitorar os seguintes recursos:

7.112.1. Infraestrutura da solução SD-WAN.

7.112.2. Dispositivos SD-WAN.

7.113. A UPG deve apresentar os relatórios referentes aos indicadores do Nível de Qualidade do Serviço de Comunicação Multimídia (NQSCM), conforme disposto no Acordo Operacional.

7.114. A CONTRATADA deve manter o SEG operacional e atualizado, propiciando condições necessárias para a execução do Gerenciamento pelo NOC e pela UPG.

7.115. O NOC deve contar com equipe de técnicos especializados e operar em regime de 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, sendo de responsabilidade da CONTRATADA a instalação, operação e manutenção dos recursos de infraestrutura necessários ao seu funcionamento nas dependências da CONTRATADA.

7.116. A UPG deve contar com equipe de técnicos especializados nas tecnologias utilizadas na solução SD-WAN e operar em regime de 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, nas dependências da PRODESP no município de Taboão da Serra – SP, para atendimento exclusivo à Rede Intragov.

7.117. A equipe técnica da UPG deve ser composta por um gerente, um coordenador e por atendentes, cuja qualificação profissional deve atender aos perfis que constam nos subitens que seguem:

7.117.1. Gerente – profissional com experiência em projetar, instalar, configurar e operar redes de telecomunicações de médio ou grande porte e com conhecimento de soluções de SD-WAN.

7.117.1.1. O Gerente deve permanecer na UPG com a frequência mínima de uma vez por semana, em dia combinado previamente com a ADMINISTRADORA, ou quando solicitado pelo Administrador da Rede, em horário comercial.

7.117.2. Coordenador – profissional com experiência em coordenação de equipe de atendimento de redes de telecomunicações e com certificação técnica para instalação, configuração e operação em redes que utilizem os dispositivos SD-WAN.

7.117.2.1. O Coordenador deve executar atividades exclusivas à UPG, comparecendo nesta unidade todos os dias úteis da semana, em horário comercial.

7.117.3. Atendente – profissional com certificação técnica para instalação, configuração e operação em redes de telecomunicações que utilizem os dispositivos SD-WAN.

7.117.3.1. A equipe de atendentes deve permanecer na PRODESP em regime de 24x7.

7.117.4. Técnico de segurança – profissional especializado em segurança com capacitação para configuração, monitoração e *troubleshooting* de todas as funcionalidades de segurança disponíveis na solução SD-WAN.

7.117.4.1. Este profissional deve ser capaz de identificar possíveis ameaças e tomar as ações necessárias preventivas.

7.117.4.2. Este profissional deve auxiliar a Administradora da Rede e Serviços que possuírem autorização de alterações de políticas de segurança, orientando nas configurações e monitorações necessárias para atender às necessidades reduzindo eventuais impactos de configurações não adequadas.

7.117.4.3. A equipe de técnicos de segurança deve permanecer na PRODESP em regime de 24x7.

7.118. Na ausência do Gerente ou do Coordenador, deve ser indicado, com no mínimo 5 (cinco) dias de antecedência, um substituto qualificado.

7.119. A equipe de atendentes da UPG deve ser dimensionada, a critério da CONTRATADA, para a execução de suas atribuições até o limite de 8 (oito) posições para consoles de operação a serem instaladas no ambiente cedido pela PRODESP.

7.120. A equipe da UPG deve acionar o NOC quando necessário de modo a escalar ou cooperar na solução de incidentes cuja complexidade requeira suporte especializado.

7.121. A equipe da UPG deve acionar o SOC quando necessário nos casos de incidentes relacionados à ataques na infraestrutura da solução SD-WAN.

7.122. A UPG deve interagir com o NOC/UPG da prestadora do SCM e STI e da prestadora do SSDWAN, sempre que necessário ou mediante solicitação da PRODESP, visando atuar em conjunto para resolver ou colaborar na solução de incidentes cuja causa raiz ou responsabilidade não for de imediato identificada, quando houver impasse entre as prestadoras quanto à responsabilidade pelo atendimento ou naqueles incidentes de maior complexidade técnica.

7.123. A equipe da UPG deve dispor de consoles de operação integrada ao SEG, em tempo real, instaladas, operadas e mantidas pela CONTRATADA, em quantidade suficiente para o desempenho de suas atividades de Gerenciamento.

7.124. A interligação das consoles de operação da UPG ao SEG deve ser feita através de um circuito digital redundante e dedicado com capacidade a ser definida pela CONTRATADA, de modo a garantir o desempenho e a disponibilidade mensal de 99,95% (noventa e nove por cento e noventa e cinco centésimos).

7.124.1. A CONTRATADA deve providenciar a ampliação da capacidade nominal do circuito digital sempre que a média móvel trimestral no horário comercial de utilização de qualquer um desses recursos ultrapassar 50% de sua capacidade nominal ou quando o valor do 95º Percentil mensal, no horário comercial, de qualquer um desses recursos atingir ou ultrapassar 90% da sua capacidade nominal, o que ocorrer primeiro.

7.124.2. A implantação da estrutura necessária para a interligação das consoles de operação da UPG ao SEG deve estar concluída no prazo de 90 (noventa) dias ou de 60 (sessenta) dias, respectivamente, a contar da data de assinatura do Contrato, conforme conste no Plano de Implantação.

7.124.3. Durante a vigência do Contrato, as ampliações necessárias na estrutura de interligação das consoles de operação da UPG ao SEG devem estar disponíveis no prazo de 60 (sessenta) dias a contar da data de ocorrência do evento que lhe der causa.

7.124.4. O não cumprimento dos prazos pode implicar na aplicação de penalidade por descumprimento contratual.

7.125. Além das consoles de operação, a CONTRATADA é responsável pelas licenças de *softwares*, pelos recursos de infraestrutura de rede local e comunicação e pelo fornecimento de bens de consumo, todos para a sua utilização, necessários ao funcionamento da UPG nas dependências da PRODESP.

7.126. A UPG deve ser implantada em área de acesso restrito, em condições adequadas de iluminação e climatização, cedida pela PRODESP para uso da CONTRATADA.

7.127. Para o funcionamento da UPG, a PRODESP é responsável pela cessão de área para instalação de até 8 (oito) consoles de operação, pelo mobiliário, pelo fornecimento de energia elétrica, pela guarda e integridade dos equipamentos instalados e pela permissão de acesso dos profissionais credenciados à área de acesso restrito.

7.128. Para a execução das funções da Gerência de Desempenho e da Gerência de Incidentes, pela equipe da UPG, as informações relativas ao dispositivo SD-WAN devem ser agrupadas e apresentadas na console de operação, através de interface gráfica, sob visão topológica de cada uma das instâncias de gerenciamento, apresentando o dispositivo SD-WAN, os enlaces conectados ao dispositivo, e sob visão geográfica da solução SD-WAN por localidade, apresentando os dispositivos SD-WAN instalados em cada localidade.

7.129. As informações relativas ao dispositivo SD-WAN que devem ser apresentadas nas consoles de operação são as que constam nos subitens que seguem:

7.129.1. Status do dispositivo SD-WAN e de suas interfaces.

7.129.2. Alarmes e eventos ocorridos no dispositivo SD-WAN, com informações de data e hora de cada ocorrência.

7.129.3. Tráfego em curso, por interface do dispositivo SD-WAN.

7.130. O sistema de gerenciamento deve monitorar e informar o status UP/DOWN/SPEED das interfaces LAN e WAN dos dispositivos SD-WAN.

7.131. A CONTRATADA deve atuar de forma preventiva, evitando a degradação ou a interrupção na prestação dos serviços ou minimizando seus efeitos, com base nas informações relativas ao dispositivo SD-WAN.

7.132. A equipe da UPG deve acompanhar a manutenção programada na solução SD-WAN até que seja normalizada a prestação dos serviços, mantendo a PRODESP informada sobre a execução da atividade de manutenção programada, conforme disposto no Acordo Operacional.

7.133. A unidade organizacional *Security Operation Center* (SOC) é incumbida da execução das atividades de monitoramento, detecção, reação e respostas a eventos de segurança em tempo real de ataques.

7.134. O SOC deve operar 24 (vinte e quatro) horas por dia nos 7 (sete) dias de todas as semanas do ano, sendo de responsabilidade da CONTRATADA a instalação, operação e manutenção dos recursos de infraestrutura necessários ao seu funcionamento em suas dependências.

VIII. MONITORAMENTO

DA REDE IP MULTISSERVIÇOS E DE SEUS RECURSOS AGREGADOS (Lote 1)

8.1. O monitoramento da Rede IP Multisserviços e dos recursos de *hardware* e *software* a esta agregados para a prestação dos serviços, referido neste documento como Monitoramento, consiste na execução de atividades pela PRODESP com a finalidade de verificar se o nível de qualidade dos serviços prestados atende aos parâmetros de desempenho técnico-operacional estabelecidos no SLA.

8.2. O Monitoramento deve ser feito de forma transparente à prestação dos serviços, ou seja, sem causar interrupção ou degradação de sua qualidade, compreendendo também o acompanhamento da execução das ações operacionais preventivas e corretivas por parte da CONTRATADA.

8.3. A PRODESP irá monitorar, de forma on-line, os CPE da rede de acesso da Rede IP Multisserviços, bem como os roteadores da borda BGP do AS GESP utilizados para a prestação do Serviço de Trânsito Internet, fazendo uso do Sistema de Gerência de Infraestrutura de Rede da PRODESP (GIR).

8.3.1. A CONTRATADA deve configurar uma VPN com uso de endereço IP fornecido pela PRODESP para que todos os CPE da rede de acesso da Rede IP Multisserviços sejam acessíveis pelo GIR.

8.3.2. A CONTRATADA deve fornecer as informações das MIB do CPE da rede de acesso da Rede IP Multisserviços, configurando a comunidade (*community*) no CPE na modalidade somente leitura (*read only*).

8.3.2.1. O valor da comunidade a ser configurada será definido pela PRODESP.

8.3.3. A CONTRATADA deve permitir coletas de informações disponíveis na MIB dos CPE da Rede de Acesso da Rede IP Multisserviços pelas plataformas de gerenciamento da própria PRODESP e/ou de outras que venham a ser autorizadas pela PRODESP, dentro do intervalo máximo de 15 (quinze) minutos, com a utilização do Protocolo SNMP (*Simple Network Management Protocol*) versão v2c e v3.

8.3.4. A CONTRATADA deve permitir o acesso às informações de configuração e do status dos componentes dos CPE, através de protocolo SSH (*Security Shell*), com privilégios somente de leitura.

8.3.5. A CONTRATADA deve fornecer a informação de endereço IP que identifica cada um dos elementos da Rede IP Multisserviços utilizados no percurso (*hops*), desde a interface WAN do CPE de origem até a interface WAN do CPE de destino, quando da execução do comando de determinação de rota (*traceroute*).

8.3.6. A CONTRATADA deve fornecer as informações de configuração, de estado e do desempenho dos recursos associados à prestação do Serviço de Trânsito Internet (STI), para acesso de forma on-line na modalidade somente leitura (*read only*).

8.3.7. A CONTRATADA deve coletar as informações das MIB dos roteadores da Borda BGP do AS GESP associados à prestação do Serviço de Trânsito Internet (STI), através da comunidade (*community*) a ser definida pela PRODESP, na modalidade somente leitura (*read only*), disponibilizando estas informações nas consoles do SEG.

8.3.8. A CONTRATADA deve coletar as informações disponíveis na MIB dos roteadores da Borda BGP do AS GESP, dentro do intervalo máximo de 15 (quinze) minutos, com a utilização do Protocolo SNMP (*Simple Network Management Protocol*) versão v2c e v3.

8.4. A PRODESP irá monitorar, de forma on-line, os CPE da rede de acesso da Rede IP Multisserviços, os roteadores da borda BGP do AS GESP e os equipamentos de terminação dos circuitos digitais utilizados para a prestação do Serviço de Trânsito Internet, através de consoles do SEG.

8.5. As consoles para a execução do Monitoramento devem estar disponíveis e com acesso às informações durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, em tempo real e agrupadas através de interface gráfica, sob visão topológica da Rede Intragov, durante todo o período de vigência do Contrato.

8.6. A CONTRATADA deve prover inicialmente 4 (quatro) consoles do SEG, instaladas para suportar as atividades de Monitoramento realizadas pela PRODESP.

8.7. A CONTRATADA deve realizar treinamento prático referente à utilização das consoles do SEG, contemplando todas as funcionalidades especificadas neste capítulo, em 3 (três) turmas de até 8 (oito) pessoas, atendendo ao disposto no documento Plano de Transição.

8.8. A PRODESP executará testes funcionais para verificação das condições normais do funcionamento dos recursos utilizados na prestação dos serviços, procederá à abertura de Registro de Incidente sempre que detectar falhas nos elementos de rede monitorados e gerará informações para a emissão de relatórios de monitoramento dos níveis de qualidade da prestação dos serviços, não eximindo a CONTRATADA de suas responsabilidades de gerenciamento e controle sobre os serviços contratados.

Monitoramento de desempenho e qualidade de rede

8.9. A CONTRATADA deve prover nas consoles do SEG informações para monitoramento de desempenho e de qualidade operacional da rede contendo, no mínimo, as seguintes informações dos CPE:

8.9.1. Ocupação dos enlaces.

8.9.2. Latência, variação da latência (*jitter*) e perda de pacotes.

8.9.3. Tráfego por porta/protocolo.

8.9.4. Tráfego por endereço IP de origem e/ou destino.

8.9.5. Tráfego por classe de serviço (CoS).

8.10. A medição dos parâmetros de QoS (latência, *jitter* e perda de pacotes) deve ser executada de forma automática e periódica pelos CPE dos SCM ativos.

8.11. O sistema de monitoramento deve obter as informações de forma automática e periódica nos equipamentos de rede.

8.12. A solução deve permitir a coleta de dados, o processamento e a geração de relatórios personalizáveis, com gráficos e tabelas que permitam a avaliação do estado operacional da rede e do perfil de tráfego.

8.13. A solução deve contemplar a geração de alarmes automáticos disparados pela extrapolação de limiares configurados previamente.

8.14. A CONTRATADA deve disponibilizar, em regime de 24x7, durante toda a vigência do Contrato, os parâmetros essenciais de disponibilidade e desempenho, incluindo, no mínimo, UP/DOWN das interfaces, ocupação, latência, *jitter*, perda de pacotes, CPU e memória dos equipamentos, bem como a configuração dos equipamentos.

8.15. Os limiares para a geração automática de alarmes devem ser validados com a Administradora da Rede e Serviços, podendo sofrer adequações que venham a ser necessárias.

8.16. A CONTRATADA deve entregar, quando solicitado, relatórios para efeito de *capacity planning*, identificando os SCM com saturação e os SCM com baixo nível de ocupação.

8.16.1. Os relatórios devem conter informações do tráfego por protocolo/aplicação e por classe de QoS, bem como o comportamento do tráfego ao longo do tempo, considerando *baselines* e linhas de tendência.

8.16.2. Os critérios adotados para a classificação dos SCM com baixo e alto nível de ocupação devem ser acordados previamente com a Administradora da Rede e Serviços.

8.17. A CONTRATADA deve disponibilizar as informações no ritmo de 20% ao ano dos SCM ativos.

Dos Acessos e rede internet banda larga (Lote 2)

8.18. O monitoramento do Acesso e Rede Internet Banda Larga da CONTRATADA para a prestação do serviço SAI-BL e SAI-BLI, referido nesta seção do documento como Monitoramento, consiste na execução das atividades pela PRODESP com a finalidade de verificar se o nível de qualidade dos serviços prestados atende aos parâmetros de desempenho técnico-operacional estabelecidos no SLA.

8.19. A CONTRATADA deve disponibilizar um portal web de monitoramento com informações essenciais de disponibilidade e utilização atualizadas do serviço de cada acesso à Internet (enlace e CPE) contratado.

8.19.1. Os parâmetros essenciais de disponibilidade e desempenho incluem, no mínimo, UP/DOWN das interfaces, ocupação (upload e download), CPU e memória dos equipamentos.

8.20. O Monitoramento deve ser feito de forma transparente à prestação dos serviços, ou seja, sem causar interrupção ou degradação de sua qualidade, compreendendo também o acompanhamento da execução das ações operacionais preventivas e corretivas por parte da CONTRATADA.

8.21. O portal de Monitoramento deve estar disponível e com acesso às informações durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, em tempo real e agrupadas através de interface gráfica, sob visão topológica dos acessos à Internet, durante todo o período de vigência do Contrato.

8.22. As credenciais do portal (usuário e senha) devem ser informadas à PRODESP, bem como para os OES contratantes do serviço.

8.23. A CONTRATADA deve disponibilizar manual prático referente às informações do portal de monitoramento, contemplando todas as funcionalidades especificadas neste capítulo.

8.24. A PRODESP ou o OES contratante executará testes funcionais ou com a ferramenta disponibilizada pela Entidade de Suporte à Aferição da Qualidade – ESAQ, definida pelo Regulamento de Qualidade dos Serviços de Telecomunicações – RQUAL (Resolução nº 717, de 23 de dezembro de 2019, da ANATEL), para verificação das condições normais do funcionamento dos recursos utilizados na prestação dos serviços, procederá à abertura de Registro de Incidente sempre que detectar falhas nos elementos de rede monitorados e gerará informações para a emissão de relatórios de monitoramento dos níveis de qualidade da prestação dos serviços, não eximindo a CONTRATADA de suas responsabilidades de gerenciamento e controle sobre os serviços contratados.

Da solução de SD-WAN (Lote 3)

8.25. O monitoramento da solução SD-WAN e dos recursos de *hardware* e *software* a esta agregados para a prestação dos serviços, referido neste documento como Monitoramento, consiste na execução de atividades pela PRODESP com a finalidade de verificar se o nível de qualidade dos serviços prestados atende aos parâmetros de desempenho técnico-operacional estabelecidos no SLA.

8.26. A CONTRATADA deve manter atualizadas as versões de software/firmware dos dispositivos SD-WAN envolvidos na solução, efetuando o monitoramento dos parâmetros e indicadores necessários para o perfeito funcionamento da solução, de forma a mitigar os riscos de segurança e ocorrência de falhas.

8.27. O Monitoramento deve ser feito de forma transparente à prestação dos serviços, ou seja, sem causar interrupção ou degradação de sua qualidade, compreendendo também o acompanhamento da execução das ações operacionais preventivas e corretivas por parte da CONTRATADA.

8.28. A PRODESP irá monitorar, de forma on-line, os dispositivos SD-WAN fazendo uso do Sistema de Gerência de Infraestrutura de Rede da PRODESP (GIR).

8.28.1. A CONTRATADA deve configurar uma VPN com uso de endereço IP fornecido pela PRODESP para que todos os dispositivos SD-WAN sejam acessíveis pelo GIR.

8.28.2. A CONTRATADA deve fornecer as informações das MIB do dispositivo SD-WAN, configurando a comunidade (*community*) no dispositivo na modalidade somente leitura (*read only*).

8.28.3. O valor da comunidade a ser configurada será definido pela PRODESP.

8.28.4. A CONTRATADA deve permitir coletas de informações disponíveis na MIB dos dispositivos SD-WAN pelas plataformas de gerenciamento da própria PRODESP e/ou de outras que venham a ser autorizadas pela PRODESP, dentro do intervalo máximo de 15 (quinze) minutos, com a utilização do Protocolo SNMP (*Simple Network Management Protocol*) versão v2c e v3.

8.28.5. A CONTRATADA deve permitir o acesso às informações de configuração e do status dos dispositivos SD-WAN, através de protocolo SSH (*Security Shell*), com privilégios somente de leitura.

8.29. A PRODESP irá monitorar, de forma on-line, os dispositivos SD-WAN, através de consoles do SEG.

8.30. O monitoramento de toda a solução SD-WAN, de dispositivos SD-WAN e Links de Acessos será realizado pela CONTRATADA do SSDWAN no período de 24 x 7 x 365, sendo esta responsável pela abertura de chamados para o atendimento de incidentes pelas CONTRATADAS dos serviços: SCM, STI, SAI-BL e SAI-BLI.

8.30.1. A atuação deve ser proativa e/ou reativa, com o intuito de evitar que os links estejam indisponíveis simultaneamente.

8.30.2. Deve manter um controle contendo designações, endereços IP e quaisquer dados relevantes para o devido atendimento.

8.30.3. Deve manter um backup de configuração de todos os dispositivos SD-WAN com número de revisão que permita a visibilidade nas alterações.

8.31. As consoles para a execução do Monitoramento devem estar disponíveis e com acesso às informações durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, em tempo real e agrupadas através de interface gráfica, sob visão topológica da solução SD-WAN, durante todo o período de vigência do Contrato.

8.32. A CONTRATADA deve prover inicialmente 6 (seis) consoles do SEG, instaladas para suportar as atividades de Monitoramento realizadas pela PRODESP.

8.33. A CONTRATADA deve realizar treinamento prático referente à utilização das consoles do SEG, contemplando todas as funcionalidades especificadas neste capítulo, bem como a funcionalidade de monitoramento do SD-WAN deste documento, em 3 (três) turmas de até 8 (oito) pessoas, atendendo ao disposto no documento Plano de Implantação.

8.34. A PRODESP executará testes funcionais para verificação das condições normais do funcionamento dos recursos utilizados na prestação dos serviços SD-WAN, procederá à abertura de Registro de Incidente sempre que detectar falhas nos dispositivos SD-WAN monitorados e gerará informações para a emissão de relatórios de monitoramento dos níveis de qualidade da prestação dos serviços, não eximindo a CONTRATADA de suas responsabilidades de gerenciamento e controle sobre os serviços contratados.

8.35. Deve monitorar o status (UP / DOWN) e a performance de todos os dispositivos SD-WAN (CPU / Memória / Tráfego / Degradação).

8.36. Os dispositivos SD-WAN instalados devem suportar o protocolo SNMP nas versões 2, para checagem de status, e TRAP para envio e notificação de alarmes, minimamente informando consumo de CPU e memória e dados relacionados as interfaces (status, erros e tráfego em ambas as direções).

8.37. A CONTRATADA deve manter uma equipe exclusiva, dimensionada de acordo com o fluxo de chamados, disponível 24x7 para atendimento à CONTRATANTE.

Monitoramento de desempenho e qualidade de rede

8.38. A CONTRATADA deve prover nas consoles do SEG informações para monitoramento de desempenho e de qualidade operacional.

8.39. O sistema de gerenciamento centralizado da solução SD-WAN deve fornecer visualização de informações on-line (com pollings a cada 5 minutos e de forma gráfica) da rede que deve apresentar, no mínimo, os seguintes itens para cada um dos dispositivos SD-WAN monitorados:

8.39.1. Topologia da rede, incluindo os equipamentos da rede de acesso e seus links, com visualização do estado operacional de todos os elementos da rede, atualizados automaticamente.

8.39.2. Alarmes e eventos ocorridos na rede com informações de data e hora de ocorrência e identificação dos recursos afetados.

8.39.3. Consumo de banda dos links (entrada e saída) com os valores instantâneos, médios e de pico durante todo o contrato, separados por semana e dia, com diferenciação de dias úteis e horário comercial.

8.39.4. Consumo de banda por classe de serviço com os valores instantâneos, médios e de pico durante todo o contrato, separados por semana e dia, com diferenciação de dias úteis e horário comercial.

8.39.5. Utilização de memória e CPU dos equipamentos da rede de acesso.

8.39.6. Estratificação de tráfego (entrada e saída) classificado por endereçamento (IP de origem e de destino), portas (de origem e de destino), serviço, protocolos, classes de serviço de todos os links e respectivos volumes, permitindo a agregação e/ou junção de tipos diferentes de tráfego e a sumarização dos dados coletados.

8.39.7. Retardo dos links com valores instantâneos, médios e de pico.

8.39.8. Inventário dos equipamentos e links da rede contendo, no mínimo, as seguintes informações: enlace, com código de identificação, tecnologia e nível de serviço; dispositivo/roteador, com fabricante, modelo, configuração lógica e física (placas, interfaces, memória, slots e demais) e endereçamento lógico, com IPs e máscaras.

8.40. A visualização das informações deve se referir a um dispositivo SD-WAN ou a um grupo de dispositivos de um OES, de acordo com a segregação em instâncias de gerenciamento por grupo de usuários.

8.41. O sistema de monitoramento deve obter as informações de forma automática e periódica nos dispositivos SD-WAN.

8.42. A solução deve permitir a coleta de dados, o processamento e a geração de relatórios personalizáveis, com gráficos e tabelas que permitam a avaliação do estado operacional da rede e do perfil de tráfego considerando os diferentes tipos de enlaces (MPLS e banda larga).

8.43. A CONTRATADA deve disponibilizar, em regime de 24x7, durante toda a vigência do Contrato, os parâmetros essenciais de disponibilidade e desempenho, incluindo, no mínimo, UP/DOWN das interfaces, ocupação, latência, *jitter*, perda de pacotes, CPU e memória dos dispositivos SD-WAN, bem como a configuração deles.

Monitoramento de tráfego de rede

8.44. A CONTRATADA deve disponibilizar solução capaz de monitorar e identificar o tráfego no nível de aplicação (camadas 4-7 do modelo OSI), bem como deve ser capaz de possibilitar a tomada de ações sobre fluxos de tráfego específicos que possam ameaçar a segurança da rede ou congestionar as conexões, prejudicando o desempenho das demais aplicações.

8.45. A CONTRATADA deve prover à PRODESP acesso à solução nas consoles do SEG.

8.46. A console de monitoramento deve permitir a visão das informações de todos os enlaces monitorados pela solução SD-WAN de forma centralizada.

8.47. A identificação do tráfego deve ocorrer por meio de recurso de inspeção profunda de pacote (*deep packet inspection*) e de assinaturas de perfil de tráfego característico de cada aplicação, sempre atualizadas com a última versão disponível no fabricante.

8.48. O monitoramento e identificação do tráfego devem ocorrer em tempo real e não devem impactar negativamente no fluxo e no desempenho das aplicações.

8.49. A CONTRATADA deve fornecer acesso ao Monitoramento do Serviço de Segurança para disponibilizar relatórios e informações do tráfego monitorado, bem como visualizar os eventos e alertas, contendo informações como Tipo do(s) ataque(s), Horário de início e fim, volume de tráfego bloqueado e não bloqueado; IP(s) de destino(s); os maiores alvos de ataques; os maiores ofensores (IP de origem), dentre outros.

8.50. A CONTRATADA deve utilizar equipamentos e *softwares* que suportem nativamente o monitoramento de tráfego que use o protocolo IPv6, permitindo sua ativação imediata quando solicitado pelo OES ou pela Administradora da Rede e Serviços.

8.51. A solução SD-WAN deve monitorar o tráfego com resolução de, no mínimo, 1 (um) minuto, armazenando o conjunto de amostras com essa resolução por, no mínimo, 2 (duas) horas.

8.51.1. Decorrido o prazo de 2 (duas) horas, a solução pode realizar agregação dos dados, devendo manter disponível via console de monitoramento, no mínimo, o valor médio diário (resolução de um dia) pelo prazo de 1 (um) ano.

8.52. A solução SD-WAN deve permitir a geração de relatórios personalizáveis, utilizando as informações coletadas, com gráficos e tabelas que permitam a avaliação do estado operacional da rede, assim como apresentar a classificação do tráfego por aplicação, pela sua origem ou pela combinação origem/aplicação.

8.52.1. A solução deve permitir a exportação de relatórios, gráficos e logs para os formatos PDF, HTML, CSV e XML, aplicáveis a cada caso.

8.52.2. A solução deve suportar o agendamento de envio de relatórios por e-mail.

8.53. A solução SD-WAN deve contemplar a geração de alarmes automáticos, com pelo menos três níveis de criticidade, disparados pela extrapolação de limiares previamente configurados em políticas de encaminhamento ou de segurança, permitindo identificar comportamentos anômalos de tráfego.

8.53.1. O sistema deve ser capaz de enviar alertas automáticos de alarme por e-mail, SNMP *traps* ou mensagens *syslog* destinados a IP informado pela Administradora da Rede e Serviços, quando solicitado.

8.54. A solução deve permitir, além do monitoramento, a tomada de ações para realizar o gerenciamento ativo do fluxo de tráfego de aplicações que, eventualmente, possam comprometer a operação da rede, incluindo, no mínimo, os seguintes recursos:

8.54.1. Definição de políticas de tráfego.

8.54.2. Garantia de banda mínima por aplicação.

8.54.3. Controle de banda máxima por aplicação.

8.54.4. Controle de tráfego por segmentos de rede.

8.54.5. Policiamento de tráfego, com descarte de pacotes.

8.54.6. Priorização de pacotes.

8.55. A solução deve suportar a criação de políticas de tráfego por grupos ou categorias de aplicações.

8.56. A solução deve permitir a definição de políticas de encaminhamento tráfego globais e por OES.

8.57. A solução deve suportar a criação de políticas de segurança baseadas em horários e dias da semana.

8.58. A solução deve disponibilizar relatórios de tráfego customizáveis, gerados automaticamente e sob demanda, por interface gerenciada pelo dispositivo SD-WAN, contemplando, no mínimo:

8.58.1. Tráfego por protocolo/aplicação, bem como o comportamento do tráfego ao longo do tempo.

8.58.2. Tráfego por host ou IP específico.

8.58.3. Quantidade de conexões ativas.

8.58.4. Protocolos/aplicações mais ativos.

8.58.5. IP de origem/destino mais ativos.

8.58.6. Banda total por protocolo ou aplicação.

8.58.7. Domínios HTTP/HTTPS mais acessados.

8.59. A solução SD-WAN deve permitir a geração de relatórios de tráfego em tempo real e em escala de longo prazo, com janela temporal definida pelo usuário.

8.60. A solução SD-WAN deve permitir agendar a exportação automática e periódica dos logs de tráfego para um servidor FTP ou SCP da Administradora da Rede e Serviços, quando solicitado.

8.61. A CONTRATADA deve apresentar documentação técnica da solução SD-WAN e como será implantada, com a finalidade de demonstrar a conformidade com as especificações técnicas requeridas para esta solução, no prazo estabelecido no Plano de Implantação.

8.61.1. Cabe à Administradora da Rede e Serviços efetuar a análise da documentação e solicitar eventual revisão.

8.62. A implantação, testes e aceitação da solução SD-WAN ocorrerão atendendo ao disposto no Plano de Implantação.

IX. FORNECIMENTO DE INFORMAÇÕES (Lotes 1, 2 e 3)

9.1. A CONTRATADA deve fornecer as informações relativas à prestação dos serviços especificados, para fins de acompanhamento e execução dos procedimentos definidos nesta Especificação Técnica e em seus anexos.

9.2. Para fins do Monitoramento e para a execução dos procedimentos definidos no Acordo Operacional a CONTRATADA deve fornecer as informações conforme disposto no capítulo anterior.

9.3. Para fins de análise quanto ao cumprimento do SLA a CONTRATADA deve fornecer informações sobre os níveis de qualidade dos serviços prestados na forma de relatórios gerenciais, emitidos conforme disposto no Acordo Operacional.

Pela prestadora do SCM E STI (Lote 1)

9.4. Para fins de análise quanto ao desempenho das Unidades (UP e UC), a CONTRATADA deve fornecer as informações sobre os níveis de ocupação de banda de todos os ID ativos na Planta da Rede Intragov, através de relatórios gerenciais de utilização de capacidade, base mensal, semestral e anual, cujas especificações, forma, conteúdo e periodicidade de envio se encontram dispostos no Acordo Operacional.

Pela prestadora do SAI-BL e SAI-BLI (Lote 2)

9.5. Para fins de gestão da prestação do Serviço de Acesso à Internet Banda Larga (SAI-BL) e do Serviço de Acesso à Internet Banda Larga Itinerante (SAI-BLI), os registros dos logs devem ser gerados e permanecerem disponíveis durante 15 (quinze) dias corridos, para acesso on-line no portal de monitoramento para a PRODESP, e devem ser mantidos pela CONTRATADA em meio magnético que assegure a integridade, confidencialidade e autenticidade das informações armazenadas, pelo prazo de 1 (um) ano a contar da sua geração.

9.6. Para fins de gestão da prestação do Serviço de Acesso à Internet Banda Larga (SAI-BL) e do Serviço de Acesso à Internet Banda Larga Itinerante (SAI-BLI), os registros dos logs gerados devem ser entregues pela CONTRATADA, no prazo de 48 (quarenta e oito) horas a contar de sua solicitação pela PRODESP, em local e na forma especificados no Acordo Operacional.

9.7. Para fins de análise quanto ao desempenho das Unidades (UP e UC), a CONTRATADA deve fornecer as informações sobre a disponibilidade, do sistema de gerenciamento centralizado e dos dispositivos SD-WAN, utilização de banda por enlace, incidentes abertos devido à falha ou degradação do SCM, STI e SAI-BL conectados aos dispositivos SD-WAN e incidentes de segurança de acordo com os níveis de serviço previstos no SLA.

9.7.1. As informações devem ser providas através de relatórios gerenciais, base mensal, semestral e anual, cujas especificações, forma, conteúdo e periodicidade de envio se encontram dispostos no Acordo Operacional.

X. DO PAGAMENTO

10.1. A CONTRATADA deverá disponibilizar, mensalmente, o espelho da fatura detalhando os serviços realizados referente ao mês anterior, por meio eletrônico, em 10 (dez) dias úteis antes do faturamento para conferência e atesto

10.2. O pagamento referente aos serviços realizados será efetuado mensalmente em 60 (sessenta) parcelas, em até 30 (trinta) dias, após protocolização e aceitação pela PRODESP da Nota Fiscal Eletrônica/Fatura correspondente, a quantidade devidamente atestada pela comissão competente.

10.2.1. Na ocorrência de rejeição da(s) Nota(s) Fiscal(is), motivada por erro ou incorreções, o prazo para pagamento passará a ser contado a partir da data da sua reapresentação.

XI. DA VIGÊNCIA DO CONTRATO

11.1. O contrato terá vigência de 60 (sessenta meses), não sendo prorrogável, não sendo prorrogável na forma do art. 75, da Lei nº 13.303/2026.

XII. GLOSSÁRIO

12.1. Os termos empregados neste documento, no plural ou no singular, mas neles não expressamente definidos, devem ser interpretados de acordo com as definições apresentadas a seguir.

ACL (*Access Control List*)	Lista de controle de acesso que é configurada em equipamentos de comunicação de dados tais como roteadores, contendo regras de permissão e bloqueio de tráfego, baseadas em informações contidas no cabeçalho dos pacotes, tais como endereços de origem e de destino, protocolo utilizado e número de porta.
Amplificador óptico	Dispositivo que amplifica sinais ópticos diretamente, sem necessidade de conversão de sinal óptico para elétrico.

Anycast	É uma metodologia de endereçamento e roteamento de rede em que um único endereço IP de destino é compartilhado por dispositivos (geralmente servidores) em vários locais. Os roteadores direcionam os pacotes endereçados a este destino para o local mais próximo do remetente.
API (*Application Programming Interface*)	Conjunto de rotinas e padrões estabelecidos por um *software* para a utilização das suas funcionalidades por aplicativos que não pretendem envolver-se em detalhes da implementação do *software*, mas apenas usar seus serviços.
AS (*Autonomous System*)	Sigla utilizada para definir um Sistema Autônomo na Internet, sendo constituído de roteadores locais e de linhas de comunicação, funcionando sob uma mesma administração técnica e mediante procedimentos próprios de roteamento interno.
AS GESP	Sistema Autônomo do Governo do Estado de São Paulo. Acrônimo definido no escopo deste documento.
Backbone	Espinha dorsal de uma rede constituída por nós de comutação interligando pontos, formando uma grande via por onde trafegam informações. Sua estrutura é constituída basicamente por equipamentos de grande capacidade de processamento de sinais, interligados por circuitos de alta capacidade.
Banda	Em telecomunicações, se refere à capacidade de transmissão de informação de um circuito ou uma rede, expressa em bits/s (bits por segundo).
BGP-4 (*Border Gateway Protocol version* 4)	Protocolo de roteamento utilizado na Internet global para a troca de informações de roteamento dentro de um AS ou entre AS distintos. Tal troca de informações se dá no contexto de sessões BGP-4, estabelecidas entre pares de roteadores localizados em diferentes AS.
Borda do AS GESP	Recursos necessários para implantar o roteamento BGP do AS GESP, incluindo as interfaces de conexão com a Internet, com a Rede IP Multisserviços e com as redes de âmbito local.
Botnet	Conjunto de computadores, usualmente espalhados pela Internet, contaminados com algum código malicioso que permite o seu controle remoto.
Broadcast/Multicast Storm Control	Mecanismo de controle de mensagens *Broadcast/Multicast Storm* que ocorre em processo de *loop*, quando uma mensagem gera uma resposta que por sua vez gera uma nova mensagem, criando-se assim um efeito de enxurrada de mensagens.
Capacidade nominal do SCM	Correspondente a um dos valores de capacidade padrão de mercado, expressa em múltiplos de bits/s (bits por segundo).

Banda útil	É a banda que está trafegando no circuito.
CIDR (*Classless Inter-Domain Routing*)	Roteamento entre domínios, constituídos por blocos de endereços IP, sem respeitar as classes definidas no protocolo IP versão 4 (IPv4), utilizando máscaras de rede de tamanho variável que permitem flexibilidade na criação de blocos de endereços.
Circuito	Enlace para transmissão de sinal entre dois pontos com equipamento de terminação em cada ponta.
Classe de Serviço	Método utilizado para segregar o tráfego possibilitando tratamento diferenciado de modo a compatibilizá-lo com os requisitos das aplicações.
Clean pipe	Tipo de serviço de transporte de dados em que o tráfego é previamente analisado e filtrado pelo prestador do serviço, entregando ao cliente final apenas tráfego isento de ameaças cibernéticas.
Conectividade IP	Atributo de conexão lógica entre hosts de uma rede de comunicações, utilizando o protocolo IP.
CoS (*Class of Service*)	Classes de Serviço. Parâmetro associado aos quadros Ethernet (camada 2) com o objetivo de priorização no encaminhamento de quadros associados a determinados serviços.
CPE (*Customer Premises Equipment*)	Equipamentos instalados nas dependências do cliente para permitir a conexão física e lógica da rede local (LAN) com a rede de telecomunicações.
CPE SD-WAN	Tipo de CPE que incorpora funcionalidades de SD-WAN.
CSV (*Comma-Separated Values*)	Formato de arquivo texto usualmente suportado por planilhas eletrônicas.
DHCP (*Dynamic Host Configuration Protocol*)	Protocolo que permite que equipamento conectado à rede IP receba endereço IP e máscara de rede, automaticamente através de um servidor, e, opcionalmente, informações adicionais de configuração do protocolo IP, tais como *gateway* padrão e IP do servidor DNS.
DHCP *Relay Agent*	Host que atua na rede local como uma extensão do servidor DHCP instalado em rede remota.
DNS (*Domain Name System*)	Serviço hierárquico da Internet que realiza a tradução de nomes de domínios para endereços IP.
DNSSEC (*Domain Name System Security Extensions*)	Padrão internacional que estende a tecnologia DNS, reduzindo o risco de manipulação de dados e domínios forjados.

DoS / DDoS (*Denial of Service / Distributed Denial of Service*)	Ataque por Negação de Serviço / Ataque Distribuído por Negação de Serviço. São ataques que visam provocar uma sobrecarga na utilização dos meios de comunicação de dados ou em recursos computacionais de forma que o desempenho desses recursos seja degradado.
Download	Expressa a capacidade da rede para transferência de dados no sentido da rede de telecomunicações para a Unidade CONTRATANTE por segundo (popularmente conhecida como velocidade).
DPI (*Deep Packet Inspection*)	Técnica disponível em equipamentos de rede que analisa informação contida no *payload* dos pacotes.
DSCP (*Differentiated Service Code Point*)	Modelo de marcação de pacotes com base em códigos, os quais serão utilizados para a priorização de tráfego e proporcionar qualidade de serviço em redes IP.
Dual Stack ou Pilha Dupla	São dispositivos com interfaces de rede que podem originar e receber pacotes IPv4 e IPv6.
DWDM (*Dense Wavelength Division Multiplexing*)	Multiplexação Densa por Comprimento de Onda Tecnologia que permite trafegar muitos canais de alta velocidade, como, por exemplo, 2,5 Gbps, em um único par de fibras ópticas.
ESAQ (Entidade de Suporte à Aferição da Qualidade)	Entidade que suporta o processo de aferição dos indicadores de qualidade das redes de Telecomunicações no Brasil.
Enlace	Meio de transmissão de sinal de um circuito.
Ethernet	Padrão usado para a conexão física de redes locais (LAN Ethernet) ou de longa distância (Metro Ethernet), que descreve protocolo, cabeamento, topologia, mecanismos de acesso ao meio de transmissão e envio/recepção de quadros da camada de enlace do modelo OSI.
FC (Fator de Capacidade)	Acrônimo definido no escopo deste documento.
Filtro de conteúdo	Função de controle de acesso a conteúdos da Internet com seleção de pacotes na camada de rede.
Firewall	Dispositivo de segurança que limita o acesso de terceiros a determinada rede ligada à Internet, com diversos tipos de mecanismos de controle por *software* e *hardware*.
Flow Control	Controle de fluxo definido pela IEEE 802.3x, que consiste em gestão específica de filas.
FQDN (*Fully Qualified Domain Name*)	Nome de um domínio que especifica a sua exata localização na hierarquia do Sistema de Nomes Domínios (DNS) da Internet.

FR (Fator de Redundância)	Acrônimo definido no escopo deste documento.
FS (Fator de Serviço)	Acrônimo definido no escopo deste documento.
FTP (*File Transfer Protocol*)	Protocolo de Transferência de Arquivos Protocolo da camada de aplicação que permite a transferência de arquivos. Está definido na RFC 959 do IETF.
Full routing	Característica em que todas as tabelas de roteamento são trocadas entre dois roteadores BGP.
GIR (Gerência de Infraestrutura de Rede)	Sistema mantido pela PRODESP. Acrônimo definido no escopo deste documento.
GMUD (Gerência de Mudanças)	Procedimento para a realização de intervenções (alterações, instalações ou reconfigurações) em sistemas ou em ambientes de telecomunicações ou processamento de dados.
GRE (*Generic Routing Encapsulation*)	Protocolo de tunelamento que permite o encapsulamento de vários outros protocolos sobre camada IP. Definido pelas RFCs 1701, 1702, 2784, 2890.
H.323	Padrão da família H.32x de recomendações ITU-T (*International Telecommunications Union – Telecommunication Standardization Sector*), que trata de "Sistemas Audiovisuais e Multimídia", com o objetivo de especificar sistemas de comunicação multimídia em redes baseadas em pacotes.
Horário Comercial	Neste documento o horário comercial se refere ao período de segunda-feira a sexta-feira das 8:00 as 18:00.
HMM (Hora de Maior Movimento)	Hora em que a utilização de um recurso é máxima ao longo de um dia.
Host	Qualquer computador, desde computador pessoal a supercomputador, dentre outros equipamentos como roteadores, conectado a uma rede.
Hot swap	Processo que permite a substituição de módulos em um equipamento, sem a necessidade do seu desligamento.
HTTP (*Hypertext Transfer Protocol*)	Protocolo de Transferência de Hipertexto É um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, em especial na Internet.
HTTPS (*HyperText Transfer Protocol Secure*)	Implementação do protocolo HTTP sobre uma camada adicional de segurança de forma que os sejam transmitidos por meio de uma conexão criptografada e com verificação de autenticidade do servidor e do cliente.

ICMP (*Internet Control Message Protocol*)	Protocolo que permite enviar mensagens relativas aos erros nas transmissões de pacotes IP, de volta à máquina de origem, bem como oferece recursos para localização de falhas no caminho de transmissão entre origem e destino.
ICMPv6 (*Internet Control Message Protocol Version 6*)	É uma versão atualizada do protocolo ICMPv4 para ser utilizada em conjunto com o IPv6, sendo parte substancial de sua arquitetura. Sua implementação, portanto, é obrigatória em todos os nós da rede que utilizam IPv6 para se comunicar.
ID (*Identifier*)	Código de identificação atribuído como referência a um elemento de rede utilizado para a prestação de serviços.
IDS (*Intrusion Detection System*)	Sistema de detecção de intrusão, instalado em um servidor com o objetivo de analisar o comportamento do tráfego com a Internet de forma individual, a fim de alertar e identificar ataques e tentativas de acessos indevidos ou mal-intencionados, tendo por base um conjunto de regras previamente estabelecido pelo administrador da rede.
IGMP (*Snooping Internet Group Management Protocol*)	É a função que permite que os switches encaminhem corretamente os pacotes de *multicast*, quando necessário, para o próximo *switch* no caminho de rede.
Informações Multimídia	Sinais de áudio, vídeo, dados, voz e outros sons, imagens, textos e outras informações de qualquer natureza.
Inspeção (*stateful*)	Mecanismo de análise de tráfego de pacotes em uma rede de telecomunicações, utilizada em sistemas de firewall e de controle de conteúdo, baseada no estado da transmissão de pacotes.
Integridade	Garantia de transporte de informações em rede de telecomunicações sem adulteração ou manipulação por terceiros.
Internet	Coleção de redes locais interligadas em âmbito internacional para troca de informações diversas baseada no protocolo IP.
Interoperabilidade	Permite a troca de informações entre as aplicações que estiverem sendo processadas nos computadores, de forma que possam ser utilizadas para se atingir objetivos comuns, tais como trabalho cooperativo, integridade, segurança dos dados e independência de equipamentos.
IP (*Internet Protocol*)	Protocolo responsável pelo roteamento de informações entre os diversos dispositivos de uma rede privada ou de uma rede pública, como a Internet.

IPFIX (*Internet Protocol Flow Information Export*)	Protocolo especificado pelo IETF para a exportação de informações de monitoramento de fluxo de pacotes IP. Está definido na RFC 5101 do IETF.
IP privado	Conjunto de endereços do protocolo IP definido pela RFC 1918, não divulgados na Internet.
IP público	Conjunto de endereços do protocolo IP definido pela RFC 1918, divulgados na Internet.
IPS (*Intrusion Prevention System*)	Sistema que busca prevenir tentativas de intrusão em uma rede, observando o comportamento do tráfego e o comparando com um conjunto de regras previamente estabelecido pelo administrador da rede, que, percebida a tentativa de intrusão, bloqueia o tráfego do invasor e emite alerta ao administrador da rede relativo ao evento.
IP *Spoofing*	Envio de pacotes IP com o endereço de origem adulterado para ocultar o verdadeiro remetente dos pacotes, sendo geralmente utilizado para ações maliciosas.
ITU-T *(International Telecommunications Union – Telecommunication Standardization)*	Sector - Grupo de padronização de telecomunicações da União Internacional de Telecomunicações (UIT), agência da ONU (Organização das Nações Unidas) especializada em Tecnologia da Informação e Comunicação.
Jumbo Frames	Quadros Ethernet com mais de 1.518 bytes de tamanho. Quadro Ethernet é de 1500 a 9000 MTU, a definição de tamanho de quadro para quadros jumbo frames é específica do fornecedor porque os quadros jumbo não fazem parte do padrão IEEE. O tamanho de quadro jumbo mais comumente usado é 9.018 bytes. Jumbo frames podem ser usados para todas as interfaces Gigabit e 10 Gigabit Ethernet que são suportadas em seu sistema de armazenamento.
LAN (*Local Area Network*)	Rede privada de comunicações digitais que interliga, em alta velocidade, terminais e computadores dentro de uma área específica, tal como um edifício ou um complexo industrial.
Link Aggregation	Método utilizado para agregação de portas Ethernet do CPE, padronizado pelo IEEE (padrão 802.3ad), visando constituir porta com capacidade correspondente à soma das capacidades das portas Ethernet agregadas.
Log	Termo utilizado para descrever o processo de registro de eventos relevantes em uma rede de telecomunicações ou em um sistema computacional, que pode ser utilizado para restabelecer o estado original da rede ou do sistema ou para que o administrador conheça o seu comportamento no passado, bem como para auditoria e diagnóstico de falhas.

Manipulação de URL (*Uniform Resource Locator*)	O ataque por manipulação de URL é usado por alguns hackers para fazer o servidor transmitir páginas às quais ele não teria autorização de acesso. Na prática, o usuário só tem acesso a links que são fornecidos pela página do site.
Mecanismo de QoS	Técnica para aplicação de regras de condicionamento da entrada do tráfego IP em rede de telecomunicações, através da classificação e da marcação do tráfego oriundo da rede local interligada à rede de telecomunicações.
Mesh	Malha de infraestrutura física capaz de prover mais de uma rota para o transporte de dados entre a origem e o destino.
MIB (*Management Information Base*)	Coleção estruturada de informações de um elemento gerenciado de uma rede de telecomunicações, organizadas em grupo e necessárias para o gerenciamento e o monitoramento (padronizadas MIB-II) dessa rede.
MPLS (*Multi Protocol Label Switching)*	Tecnologia de encaminhamento de pacotes de dados.
MTU (*Maximum Transmission Unit)*	É o quadro ou pacote de maior tamanho — em *bytes* ou octetos (*bytes* de oito *bits*) que pode ser transmitido através de um *link* de dados. É mais usado em referência ao tamanho do pacote em uma rede *ethernet* usando o protocolo da Internet (IP).
Multicast	É um método ou técnica de transmissão de um pacote de dados para múltiplos destinos ao mesmo tempo.
Multilink	Técnica de agregação de circuitos para constituir circuito de maior capacidade.
Multiplexador	Dispositivo capaz de agregar dois ou mais sinais de informação num único sinal de saída.
NAT (*Network Address Translation*)	Técnica que consiste em reescrever os endereços IP de origem de pacotes que passam por roteador ou firewall, para que um computador de uma rede interna tenha acesso a uma rede pública, e vice-versa.
NDP (Neighbor Discovery Protocol)	É o protocolo de descoberta de vizinhança foi desenvolvido sob a finalidade de resolver os problemas de interação entre nós vizinhos em uma rede. Para isso ele atua sobre dois aspectos primordiais na comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes
Next hop	Parâmetro utilizado em roteamento de redes com a finalidade de informar ao roteador o próximo salto no caminho percorrido pelo pacote de dados entre a origem e o destino a ser alcançado.

NOC (*Network Operations Center*)	Local em que se centraliza a gerência de uma rede de telecomunicações, pública ou privada, de modo que, através de plataformas de sistemas de gerenciamento que monitoram os elementos gerenciados, os operadores podem saber, em tempo real, a situação de cada elemento da rede e tomar as decisões para restabelecer suas condições normais de funcionamento em caso de ocorrências de falhas.
NQSCM	Nível da Qualidade do SCM Acrônimo definido no escopo deste documento.
NTP (*Network Time Security*)	O NTP é um protocolo para sincronização dos relógios dos computadores baseado no protocolo UDP sob a porta 123. É utilizado para sincronização do relógio de um conjunto de computadores e dispositivos em redes de dados com latência variável.
OES	Órgãos/Entidades Signatários Acrônimo definido no escopo deste documento.
OSI (*Open Systems Interconnection*)	Modelo conceitual de protocolo com sete camadas, definido pela ISO (*International Organization for Standardization*), para a compreensão e o projeto de redes de computadores. Trata-se de uma padronização internacional para facilitar a comunicação entre computadores e sistemas de diferentes fabricantes.
OSPFv3 (*Open Shortest Path First version* 2)	Protocolo de roteamento dinâmico que utiliza métricas que levam em consideração os custos das conexões entre os roteadores e o estado dessas conexões para a definição da melhor rota entre dois nós quaisquer de uma rede IPV4 e IPv6.
P (*Provider*)	Roteador do *backbone* da Rede IP Multisserviços que comuta IP/MPLS entre os PE, sem necessidade de sinalização das VPN.
Pacote IP	Informação encapsulada para transmissão na rede através do protocolo IP.
Partial routing	Característica em que parte das tabelas de roteamento da Internet é trocada entre dois roteadores BGP.
PBS	Preço Básico do Serviço Acrônimo definido no escopo deste documento.
PDF (*Portable Document Format*)	Formato de arquivo do tipo documento.
PE (*Provider Edge*)	Roteador de borda do *backbone* da Rede IP Multisserviços que mantém e divulga as informações das tabelas de rotas das VPN vinculadas, para encaminhamento do tráfego IP oriundo dos CPE associados a cada VPN.

PIM-SM (*Protocol Independent Multicast - Sparse Mode*)	Protocolo de roteamento *multicast* projetado para distribuição em grande escala para receptores esparsos.
Plataforma IP-MPLS (*Multiprotocol Label Switching*)	Infraestrutura de *backbone* provida em tecnologia IP MPLS, em que o protocolo de roteamento é baseado em pacotes rotulados, onde cada rótulo representa um índice na tabela de roteamento do próximo roteador, definido na RFC 3031.
PNG (*Portable Network Graphics*)	Formato de arquivo do tipo imagem.
Ponto de Presença do *Backbone* (PoP)	Local de instalação de um ou mais elementos do *backbone* da Rede IP Multisserviços, denominados P (*Provider*) ou PE (*Provider Edge*).
PoP (*Point of Presence ou Ponto de Presença*)	É um ponto de acesso de determinado local para qualquer outro ponto, por meio da Internet. Provedor de Internet (*Internet Services Provider* – ISP) ou provedor de serviços online mantém um (ou vários) pontos de presença na rede.
Port Security	Técnica utilizada para controlar (permitindo ou rejeitando) a conexão de equipamentos à porta de um determinado dispositivo de rede de telecomunicações.
Porta LAN	Interface física de equipamento, do tipo roteador, que permite a conexão com uma rede local.
Protocolo	Descrição formal de formatos de mensagem e de regras que dois equipamentos devem obedecer ao trocar mensagem entre si, podendo incluir sincronização, sequenciamento e verificação de erros nessa troca de mensagem.
PSCM	Preço do Serviço de Comunicação Multimídia.
PSTI	Preço do Serviço de Transito Internet.
PTI	Período de Tratamento do Incidente. Acrônimo definido no escopo deste documento.
QoS (*Quality of Service*)	Designação para as características técnicas de desempenho de uma rede de telecomunicações, associadas à classe de serviço, capaz de propiciar tratamento diferenciado para diferentes aplicações.
Rack	Estrutura fechada, do tipo gabinete, para acondicionamento de equipamentos com padrão de fixação de 19 polegadas e para a instalação da terminação de cabeamento em uma rede local, composto por acessórios de fixação, régua de alimentação elétrica, portas de acesso com tranca e elementos para ventilação interna.

Rede de Telecomunicações	Conjunto operacional contínuo de circuitos e equipamentos, que executam as funções de transmissão, comutação, multiplexação ou quaisquer outras indispensáveis à operação de serviço de telecomunicações, incluindo os sistemas de gerenciamento para a sua operação.
Rede Intragov	Rede de telecomunicações privativa para a prestação de serviços que atendam às necessidades de comunicação dos órgãos da Administração Pública Estadual e outras entidades de interesse do governo estadual.
RFC (*Request for Comments*)	Documentos produzidos pelo IETF (*Internet Engineering Task Force*) descrevendo protocolos, procedimentos operacionais, tecnologias e inovações aplicáveis à Internet.
Roteador BGP	Equipamento que opera na camada 3 do modelo OSI de referência e que utiliza o protocolo BGP para comunicação com outros roteadores.
RTP (*Real Time Protocol*)	Protocolo para transporte de dados de aplicações de tempo real, como, por exemplo, voz sobre IP, definido pelo IETF na RFC 3550.
SAI (Serviço de Acesso Internet)	Acrônimo definido no escopo deste documento.
SAOG (Sistema de Apoio Operacional e de Gestão)	Sistema mantido pela PRODESP, utilizado pelos OES e pela Administradora da Rede e Serviços para solicitação de serviços junto à CONTRATADA, abertura e acompanhamento de incidentes relacionados aos serviços previstos em Contrato, monitoramento dos ID da Rede IP Multisserviços, entre outras funcionalidades.
SCM (Serviço de Comunicação Multimídia)	Acrônimo definido no escopo deste documento.
SCP (*Secure Copy Protocol)*	É um protocolo para transferir seguramente arquivos entre um local e um host remoto ou entre dois hosts remotos.
SD-WAN (*Software-Defined* WAN)	Tecnologia que gerencia de forma automática, a partir de políticas pré-configuradas, o encaminhamento de tráfego em redes WAN híbridas, em que há dois ou mais diferentes acessos à WAN numa Unidade.
SEG (Sistemas Especialistas de Gerenciamento)	Conjunto de sistemas de gerenciamento de redes da CONTRATADA, instalados e operados no NOC.
Sessão *multicast*	Conexão lógica entre *hosts multicast* estabelecida na Rede IP Multisserviços.

SIP (*Session Initiation Protocol*)	Protocolo utilizado para estabelecer, modificar e finalizar sessões entre dois ou mais pontos em uma Rede IP, definido pelo IETF na RFC 3261.
SLA (*Service Level Agreement*)	O SLA, Acordo de Nível de Serviço, é um contrato entre um Prestador de Serviços e um cliente, estabelecendo valores mensuráveis relacionados aos serviços prestados.
SNMP (*Simple Network Management Protocol*)	Protocolo desenvolvido para permitir o gerenciamento de elementos da rede (ex. servidores, roteadores, *switches*, impressoras, etc.). Protocolo da camada de aplicação (camada 7 no modelo OSI).
SOC (*Security Operations Center*)	Local que concentra os recursos e atividades de gerenciamento de segurança de uma rede de dados WAN.
Spanning Tree	Técnica utilizada para prevenir os congestionamentos, broadcast e outros efeitos colaterais indesejados das ligações em *loop*, padronizado na especificação IEEE 802.1d.
SSH (*Secure Socket Shell*)	*Secure Shell* é um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura.
STI (Serviço de Trânsito Internet)	Acrônimo definido no escopo deste documento.
SVA (Serviço de Valor Adicionado)	São aplicações que utilizam a rede de telecomunicações ou que sequer usam a rede, mas são cobrados por meio da fatura enviada pelas prestadoras aos consumidores. Os SVA não são serviços de telecomunicações.
TCP (*Transmission Control Protocol*)	Protocolo utilizado para transmissão de informação em rede de telecomunicações com garantia de entrega.
TCP/IP (*Transmission Control Protocol/Internet Protocol*)	Este termo se refere à utilização do protocolo TCP em uma rede de telecomunicações que adota roteamento IP.
Throughput	Característica técnica de um equipamento que traduz sua capacidade de vazão de tráfego de informações, expressa em múltiplos de bit por segundo.
Traffic shaping	Utilizado para definir a prática de priorização do tráfego de dados, através do condicionamento do débito de redes, a fim de otimizar o uso da largura de banda disponível.
Traffic policing	É o processo de monitoramento do tráfego de rede para a conformidade com um contrato de tráfego e a tomada de medidas para fazer cumprir esse contrato.

Trânsito Internet	Serviço oferecido por um AS, que consiste em prover a outro AS acesso aos demais AS presentes na Internet.
Transponder	Numa rede DWDM é um elemento que envia e recebe sinais através da fibra óptica, podendo realizar funções como conversão do comprimento de onda do sinal, regeneração 3R (potência, forma e relógio), bem como encapsulamento do sinal cliente.
TTA	Total de acessos da rede Acrônimo definido no escopo deste documento.
TTF	Total de acessos da rede com resultados fora dos limites em pelo menos um dos parâmetros de QoS. Acrônimo definido no escopo deste documento.
Tunelamento	Denominação do processo para o estabelecimento de um caminho lógico (túnel), através da utilização de um protocolo, que visa o encaminhamento de pacotes IP recebidos no início do túnel, onde são encapsulados e transmitidos até o final do túnel, onde são desencapsulados e encaminhados para o seu destino.
UC (Unidade Cliente)	Acrônimo definido no escopo deste documento.
Unicast	É uma forma de envio de informações direcionadas para somente um único destino. Na transmissão *Unicast*, uma conexão de rede ponto a ponto é implementada entre o remetente e cada receptor.
UP (Unidade Provedora)	Acrônimo definido no escopo deste documento.
UPG (Unidade Provedora de Gerenciamento)	Acrônimo definido no escopo deste documento.
Upload	Expressa a capacidade da rede para transferência de dados no sentido da Unidade CONTRATANTE para a rede de telecomunicações por segundo (popularmente conhecida como velocidade).
URL (*Uniform Resource Locator*)	Endereço de um recurso, do tipo arquivo ou aplicação, na Internet, formado por um protocolo, pela denominação do recurso, pelo domínio e por nomes de diretórios, subdiretórios e arquivos, e pelo número da porta lógica.
uRPF (*unicast Reverse Path Forwarding*)	Recurso disponível em roteadores e utilizado para proteção contra tráfego com IP de origem forjado.

UTM (*Unified Threat Management*)	Dispositivo com uma abordagem à segurança da informação em que fornece múltiplas funções de segurança.
VPN (*Virtual Private Network*)	É uma rede de comunicações privada construída sobre uma rede de comunicações pública. O tráfego de dados é levado pela rede pública utilizando protocolos padrões.
VRE (Valor da Remuneração Eventual)	Acrônimo definido no escopo deste documento.
VRRP (*Virtual Router Redundant Protocol*)	Protocolo utilizado para aumentar a disponibilidade de um gateway default através da definição de um roteador virtual que representa dois ou mais roteadores que atuam em grupo (um principal e os demais *backups*), sendo que somente um dos roteadores detém o papel de principal.
WAN (*Wide Area Network*)	Rede de telecomunicações com abrangência em uma grande área geográfica. Tipicamente é criada e mantida por provedores de telecomunicações.
Worm	Código computacional malicioso. Geralmente se propaga por conta própria pelas redes de computadores, contaminando outros dispositivos.
WRED (*Weighted Random Early Detection)*	Algoritmo de gerenciamento de filas utilizado em redes de dados.
XML (*eXtensible Markup Language*)	Recomendação da W3C (www.w3.org) de linguagem de formatação para descrição de dados.