ANEXO I

TERMO DE REFERÊNCIA

CONTRATAÇÃO DE PRESTAÇÃO DO SERVIÇO DE COMUNICAÇÃO MULTIMÍDIA, DO SERVIÇO DE ACESSO À INTERNET E DO SERVIÇO DE TRÂNSITO INTERNET, PARA O ACORDO DE NÍVEIS DE SERVIÇOS (SLA), PARA O GERENCIAMENTO DA REDE IP MULTISSERVIÇOS E DE RECURSOS AGREGADOS, PARA O MONITORAMENTO DA REDE IP MULTISSERVIÇOS E DE RECURSOS AGREGADOS E PARA O FORNECIMENTO DE INFORMAÇÕES RELATIVAS À PRESTAÇÃO DOS SERVIÇOS.

PREÂMBULO

CONTEÚDO DO ANEXO I

ANEXO I – TERMO DE REFERÊNCIA: fornece as especificações técnicas mínimas necessárias às quais o produto ou serviço ofertado pela proponente deverá obrigatoriamente atender.

ÍNDICE

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de prestação do serviço de comunicação multimídia, do serviço de acesso à internet e do serviço de trânsito internet, para o acordo de níveis de serviços (sla), para o gerenciamento da rede IP multisserviços e de recursos agregados, para o monitoramento da rede IP multisserviços e de recursos agregados e para o fornecimento de informações relativas à prestação dos serviços.

2. DESCRIÇÃO DA SOLUÇÃO

2.1. 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, pelos Órgãos/Entidades Signatários, denominados OES, que integram ou vierem a integrar a Rede Intragov, referidos como solicitantes, e pelas Unidades indicadas.

2.2. 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.

2.2.1. 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.

2.3. A PRODESP exerce as funções de administração da Rede Intragov, sendo neste caso referida como Administradora da Rede.

2.4. Os serviços a serem prestados são o Serviço de Comunicação Multimídia (SCM), o Serviço de Acesso à Internet (SAI) e o Serviço de Trânsito Internet (STI).

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

2.4.2. O Serviço de Acesso à Internet e o Serviço de Trânsito Internet devem ser prestados com a agregação de recursos à Rede IP Multisserviços.

2.5. 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.

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

2.6. 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:

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

2.6.2. 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;

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

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

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

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

2.8. Os serviços devem ser prestados em conformidade com as especificações técnicas e operacionais que constam dos capítulos II – Descrição do Serviço de Comunicação Multimídia, III – Descrição do Serviço de Acesso à Internet e IV – Descrição do Serviço de Trânsito Internet, deste documento.

2.9. Os serviços devem ser prestados em conformidade com os parâmetros associados às especificações técnicas e operacionais que constam do capítulo 6 - Acordo de Níveis de Serviços (SLA), deste documento.

2.10. A Rede IP Multisserviços e os recursos a ela agregados devem ser gerenciados em conformidade com as especificações técnicas e operacionais que constam do capítulo 7 – Gerenciamento da Rede IP Multisserviços e de Recursos Agregados, deste documento.

2.11. A Rede IP Multisserviços e os recursos a ela agregados são objeto de monitoramento, por parte da Administradora da Rede, em conformidade com as especificações técnicas e operacionais que constam do capítulo 8 – Monitoramento da Rede IP Multisserviços e de Recursos Agregados, deste documento.

2.12. 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 9 – Fornecimento de Informações, deste documento.

2.13. O Acordo Operacional, firmado entre a CONTRATADA e a PRODESP nos termos da Cláusula III do 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, e dos sistemas internos da CONTRATADA.

2.14. A CONTRATADA deve atender às 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.

Relacionamento entre a CONTRATADA, OES e Administradora da Rede

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

2.16. O SAOG será utilizado para suporte aos seguintes processos:

2.16.1. Atendimento a Solicitações de Serviços;

2.16.2. Registro de Incidentes;

2.16.3. Gestão do Faturamento;

2.16.4. Gestão de Qualidade;

2.16.5. Gestão de Conectividade na Rede.

2.16.6. Monitoramento da Rede;

2.16.7. Desempenho dos ID.

2.17. As informações relativas aos processos de Atendimento a Solicitações de Serviços, Registro de Incidentes, Gestão do Faturamento e Gestão de Conectividade na Rede devem ser as mesmas, tanto para o SAOG quanto para os sistemas internos da CONTRATADA.

2.17.1. O detalhamento dos processos que devem ser integrados entre os sistemas internos da CONTRATADA e o SAOG, caso a

CONTRATADA faça essa opção, encontra-se no Acordo Operacional.

2.18. Caso seja realizada a integração com os sistemas internos da CONTRATADA, as informações oriundas dos sistemas internos da CONTRATADA devem ser fornecidas para o SAOG de forma automática. Eventuais falhas nessa comunicação não eximem a CONTRATADA do cumprimento dos SLAs pertinentes, dado que o SAOG é a ferramenta oficial para gestão do serviço, sendo a CONTRATADA usuária compulsória desse sistema.

2.19. Caso seja realizada a integração com os sistemas internos da CONTRATADA, o SAOG enviará informações relativas à prestação dos serviços para os sistemas internos da CONTRATADA de forma automática, não havendo responsabilidade pela validação e sincronização dessas informações nos sistemas da CONTRATADA.

2.20. Cabe à Administradora da Rede a apuração dos indicadores de SLA previstos no Contrato, com base nas informações do SAOG.

2.21. No processo de Atendimento a Solicitações de Serviços, definido no Acordo Operacional, as informações referentes aos endereços utilizados nas Solicitações emitidas pelo SAOG devem seguir o padrão do Código de Endereçamento Postal (CEP) dos Correios.

2.21.1. Os endereços das Unidades (UP ou UC) que não constarem no cadastro dos Correios serão definidos pela Administradora da Rede.

2.22. Caso seja realizada a integração com os sistemas internos da CONTRATADA, para que haja a troca de forma automática das informações, a CONTRATADA deve instalar, operar e manter, roteadores e circuito digital com capacidade nominal de 8 Mbps (oito megabits por segundo), dedicado, ponto a ponto, com redundância, com indisponibilidade mensal de, no máximo, 30 (trinta) minutos, com a finalidade de interligar diretamente seus sistemas internos ao SAOG, localizado na PRODESP em Taboão da Serra – SP.

2.22.1. A CONTRATADA deve providenciar a ampliação do circuito digital sempre que a sua média móvel trimestral de utilização, no horário comercial, 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.

2.22.2. Durante a vigência do Contrato, as ampliações e as readequações nos roteadores e no circuito digital devem estar disponíveis no prazo de 60 (sessenta) dias a contar da data de ocorrência do evento que lhe der causa, conforme critérios dispostos acima.

2.23. A troca de mensagens entre o SAOG e os sistemas internos da CONTRATADA deve se basear no padrão JMS (Java Message Service), no protocolo de comunicação SOAP (Simple Object Access Protocol) e no protocolo de rede HTTP (Hypertext Transfer Protocol), para o transporte de informação em XML (Extensible Markup Language), atendendo à formatação e validação do XSD (XML Schema Definition).

2.24. Os arquivos XSD referentes a cada fila dos processos necessários à integração serão fornecidos à CONTRATADA após a solicitação formal pela integração entre os sistemas.

2.24.1. Os procedimentos descritos no Acordo Operacional não caracterizam, para fins de integração, especificação de requisitos para a análise e o desenvolvimento desta integração, devendo a CONTRATADA apenas utilizá-los como referência para a interpretação dos arquivos XSD.

3. DESCRIÇÃO DO SERVIÇO DE COMUNICAÇÃO MULTIMÍDIA

Prestação do Serviço de Comunicação Multimídia

3.1. 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.

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

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

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

3.2. 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).

3.3. A prestação do SCM deve ser feita em protocolo IPdesde 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 UC quanto UP, através da Rede IP Multisserviços.

3.4. O SCM deve ser prestado com isolamento de tráfego IP entre as redes locais das Unidades (UC ou UP) 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.

3.4.1. Não existe limite para inclusão de VPN na Rede IP Multisserviços.

3.5. 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).

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

3.7. 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.

3.7.1. 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.

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

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

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

3.8. 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.

3.9. 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.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

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

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

3.12. 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.

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

3.14. 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.

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

3.15.1. Entende-se por full-mesh o modelo do tipo multiponto-multiponto em que qualquer Unidade (UC ou UP) associada à VPN tem conectividade com qualquer outra Unidade (UC ou UP) da mesma VPN.

3.15.2. Entende-se por hub-spoke o modelo do tipo multiponto-ponto em que qualquer UC associada à VPN só possui conectividade com a UP da mesma VPN.

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

3.17. 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*) e a variações de retardo da rede (*jitter*) 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 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.

3.18. 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 < = 70 ms (terrestre) Latência < = 370 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 < = 80 ms *Jitter* < = 30 ms Perda de pacotes < = 0,1 %
MISSÃO CRÍTICA	Latência < = 100 ms Latência < = 400 ms (somente para sinalização de voz por satélite) Perda de pacotes < = 0,5 %
SUPORTE À NEGÓCIO	Latência < = 150 ms Perda de pacotes < = 1,0 %
PADRÃO	Latência < = 300 ms (terrestre) Latência < = 600 ms (satélite) Perda de pacotes < = 2,0 %

3.18.1. Entende-se por latência o período de tempo, expresso em milissegundos, para transportar um pacote IP entre a porta LAN de um CPE de origem e a porta LAN do CPE de destino na Rede IP Multisserviços.

3.18.2. 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 a porta LAN do CPE de origem e a porta LAN do CPE de destino.

3.18.3. Entende-se por perda de pacotes, expresso em percentagem, a quantidade de pacotes IP não recebidos na porta LAN do CPE de destino em relação ao total de pacotes enviados pela porta LAN do CPE de origem.

3.18.4. Os valores dos parâmetros de QoS que constam na tabela se referem à medida realizada em um único sentido na comunicação fim a fim entre duas Unidades.

Configuração das Redes Virtuais Privadas (VPN)

3.19. 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.

3.20. Uma Unidade pode estar associada a apenas uma VPN ou a mais de uma VPN, nesse último caso a Unidade pode se interligar ao backbone da Rede IP Multisserviços por um ou mais SCM.

3.20.1. A conectividade IP entre as atuais VPN da Rede IP Multisserviços é apresentada na tabela a seguir, podendo sofrer alterações durante o período de vigência do Contrato:

VPN	UP participantes
INTRAGOV	PRODESP FAZENDA
FAZENDA	FAZENDA PRODESP
CEETPS	CEETPS PRODESP FAZENDA
METROPOLITANO	METROPOLITANO PRODESP FAZENDA
CPTM	CPTM PRODESP FAZENDA

Requisitos Operacionais e Técnicos da Rede IP Multisserviços

3.21. 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 (UC ou UP).

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

3.22.1. 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 (UC ou UP).

3.22.2. Um conjunto mínimo de informações configuradas nos CPE deve ser padronizada, conforme estabelecido no Acordo Operacional.

3.23. 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.

3.23.1. 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.

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

3.23.3. O backbone da Rede IP Multisserviços deve ser autorredundante, sendo cada PE interligado a pelo menos dois outros PE.

3.24. Devido ao alto grau de complexidade das redes locais da UP PRODESP em Taboão da Serra/SP e da UP SEFAZ em São Paulo/SP, devem ser instalados PE do backbone da Rede IP Multisserviços nos respectivos sites dessas UP, com dupla abordagem na interligação com os outros PoP do backbone e com exclusividade de uso por essas UP,

sendo a interligação do PE ao CPE do SCM dessas duas UP realizada com cabo interno.

3.24.1. 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.

3.25. 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.

3.26. Deve ser atribuído a cada SCM e ao backbone da Rede IP Multisserviços um código de identificação (ID) a ser utilizado para se referir ao SCM nos procedimentos estabelecidos no Acordo Operacional.

3.27. A Rede IP Multisserviços deve ser dimensionada para a prestação do SCM na modalidade multicast para até 8.000 hosts multicast.

3.28. Atender, no mínimo, por VPN, à quantidade de 10 sessões multicast simultâneas.

3.29. 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, conforme recomendações das RFC 791 (Internet Protocol Version 4 Specification), RFC 6890 (Special-Use IP Address Registries), RFC 2460 (Internet Protocol Version 6 Specification), RFC 4291 (Internet Protocol Version 6 Addressing Architecture) e definições complementares da IANA (Internet Assigned Numbers Authority).

3.29.1. 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.

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

3.29.3. A Rede IP Multisserviços deve dar suporte para o roteamento e para o transporte de pacotes IP gerados pela Unidade (UC ou UP) na versão IPv6, sob demanda, para até 100% da Rede IP Multisserviços.

3.29.4. A Rede IP Multisserviços deve dar suporte para o roteamento e para o transporte de pacotes IPv6, gerados pela Unidade (UC ou UP), de forma nativa, em que o CPE da unidade de origem recebe o pacote IPv6 da rede local e o encaminha sem encapsulamento IPv4, através do backbone, até o CPE de destino, o qual o encaminha para a rede local.

3.29.5. Os PE da Rede IP Multisserviços devem dar suporte ao serviço de VPN IP MPLS para SCM em IPv6 por meio da solução 6VPE, de acordo com a RFC 4659 (BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN).

3.29.6. Quando justificado pela Administradora da Rede, a Rede IP Multisserviços deve dar suporte para o roteamento e para o transporte de pacotes IP gerados pela Unidade (UC ou UP) 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 unidade de origem e o CPE da unidade de destino é feita através de uma conexão fim a fim em IPv6 ou em IPv4.

3.29.7. A Rede IP Multisserviços deve ser suportada por serviços de rede habilitados para IPv6, necessários para a plena operação da rede, tais como gerenciamento, monitoramento e segurança.

3.30. 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.

3.31. 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.

3.32. 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.

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

3.34. 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), RFC 2212 (Specification of Guaranteed Quality of Service), RFC 2474 (Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers), RFC 2475 (An Architecture for Differentiated Services), RFC 3270 (Multi-Protocol Label Switching Support of Differentiated Services), RFC 3564 (Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering), RFC 3754 (IP Multicast in Differentiated Services Networks).

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

3.36. 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), 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).

3.37. A Rede IP Multisserviços deve fazer uso do protocolo IGMPv3 (Internet Group Management Protocol versão 3), definido pela RFC 3376, 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.

3.38. A Rede IP Multisserviços deve fazer uso do protocolo MLDv2 (Multicast Listener Discovery versão 2), definido pela RFC 3810, 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.

3.39. A Rede IP Multisserviços deve fazer uso do protocolo PIM-SM (Protocol Independent Multicast - Sparse Mode), definido pela RFC 4601 para criar e otimizar o roteamento dos pacotes IP (v4 e v6) entre os hosts multicast participantes de uma mesma sessão multicast.

3.40. 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.

3.41. 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.

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

3.41.2. O SCM com redundância é constituído por dois conjuntos CPE/enlace implantados com dupla abordagem, em que cada conjunto é construído com recursos de transmissão distintos e conectado a um PE distinto do backbone da Rede IP Multisserviços.

3.42. 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.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

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

3.44. 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.

3.45. Em casos previamente aprovados pela Administradora da Rede, 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.

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

3.45.2. 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.

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

3.46. O CPE do SCM de uma Unidade (UC ou UP) deve suportar a funcionalidade DHCP relay, devendo a CONTRATADA realizar sua configuração sempre que solicitado pela Administradora da Rede ou pelo OES.

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

3.47.1. 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.

3.47.2. 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.

3.48. 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.

3.48.1. 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.

3.49. 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**

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

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

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

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

3.49.5. 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).

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

3.51. 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.

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

3.53. 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 ou 40 Gbps, até o limite de oito interfaces.

3.54. 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.

3.55. 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 (UC ou UP).

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

3.57. 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.

3.58. O CPE deve permitir a coleta de informações gerenciais de sua Management Information Base (MIB) 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 protocolo de terminal virtual Telnet (Teletype Network) ou SSH (Security Shell), com privilégios de leitura para a Administradora da Rede.

3.59. O SCM de uma Unidade (UC ou UP) 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 e 40 Gbps.

3.59.1. A Rede IP Multisserviços deve dar suporte à quantidade máxima de 18.000 SCM ativos para Unidades (UC ou UP), com capacidade nominal dentre os valores acima.

3.59.2. Além das quantidades apresentadas na tabela acima, a Rede IP Multisserviços deve dar suporte à quantidade máxima de 2.000 SCM ativos para Unidades Cliente, cujos serviços devem ser prestados a título gratuito e com capacidade dentre os valores definidos na Cláusula Social do Contrato.

3.59.3. Como alternativa para o cumprimento do compromisso da Cláusula Social, será facultado à Contratada oferecer o provimento do serviço de acesso à Internet banda larga empresarial prestado ao mercado pela Contratada. A velocidade garantida de download do serviço de internet banda larga ofertado deve ser igual ou superior à capacidade nominal do SCM solicitado pela UC. A velocidade garantida de upload do serviço de internet banda larga deve corresponder a, no mínimo, 50% da velocidade garantida de download. Não poderão ser aplicáveis franquias de dados que, se excedidas, resultem em bloqueio ou redução das taxas de upload e download. O serviço deve ser prestado com o uso de endereçamento IP fixo. A Contratada não poderá restringir nenhum tipo de aplicação que envolva a UC ou bloquear qualquer porta de servidor, salvo por solicitação da PRODESP. Essa oferta alternativa deverá ser submetida à aprovação prévia da PRODESP que, para tanto, consultará a UC quanto à conveniência de sua adoção.

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

3.61. Ao definir a capacidade nominal do SCM de uma Unidade (UC ou UP), 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.

3.61.1. 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.

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

3.63. 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).

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

3.65. 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 e Padrão, em SCM com capacidade nominal instalada de até 4 Mbps, restrito a um salto por enlace.

3.66. A transmissão no enlace via satélite pode ser feita no modo assimétrico, desde que sejam garantidas taxa de transmissão de 50% (cinquenta 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).

Infraestrutura para a Prestação do Serviço de Comunicação Multimídia

3.67. 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.

3.67.1. Cabe ao OES prover recursos mínimos de segurança lógica do perímetro de suas unidades, com a ativação de firewalls.

3.68. 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.

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

3.68.1.1. Cabos, fibras ópticas e demais meios de transmissão;

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

3.68.1.3. 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.

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

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

3.68.4. 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.

3.68.5. 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.

3.69. 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.

3.70. 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.

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

3.71. O OES deve fornecer as tomadas elétricas adequadas, na quantidade a ser definida pela CONTRATADA, condições ambientais, espaço e guarda apropriados para a instalação dos equipamentos da CONTRATADA.

3.72. 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

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

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

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

3.75.1. Otimização dos protocolos TCP, DNS, HTTP e FTP;

3.75.2. 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.

3.75.3. 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.

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

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

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

3.78.1. Embarcado no sistema operacional do CPE (em software);

3.78.2. Um módulo de aceleração WAN adicionado ao CPE;

3.78.3. Um equipamento (appliance) dedicado externo ao CPE.

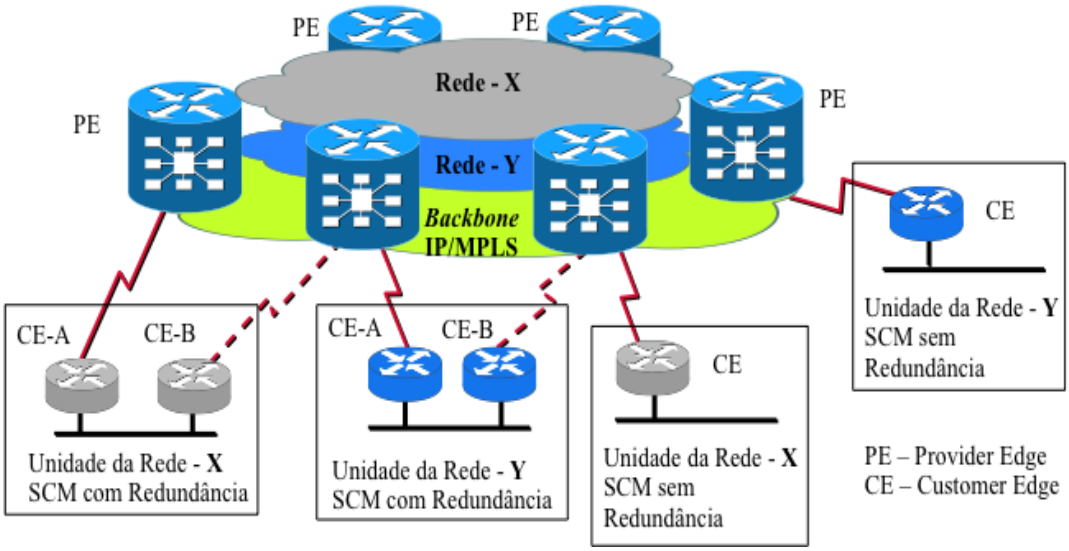
3.79. O elemento concentrador da solução de aceleração de tráfego deve ser instalado nas dependências da CONTRATADA.

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

3.81. 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.

Topologia da Rede IP Multisserviços

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



4. DESCRIÇÃO DO SERVIÇO DE ACESSO À INTERNET

Prestação do Serviço de Acesso à Internet

4.1. O Serviço de Acesso à Internet é prestado à Unidade (UC ou UP) que o tenha contratado e consiste na oferta de acesso à Internet, associado a funcionalidades, para a Unidade (UC ou UP) a que for prestado o Serviço de Comunicação Multimídia com a utilização de endereço IPv4 ou IPv6, ambos do plano de endereçamento do Governo do Estado de São Paulo.

4.1.1. A prestação do Serviço de Acesso à Internet à Unidade (UC ou UP) pressupõe a prestação do SCM para essa Unidade.

4.2. A prestação do Serviço de Acesso à Internet deve ser feita através de uma Unidade Provedora de Internet (UPI) dotada de recursos técnicos para executar as funções de controle dos endereços IP (v4 e v6) a partir dos quais o acesso à Internet pode ser feito, tradução dos endereços IP privados para endereços IP públicos, resolução de nomes, controle de acesso a conteúdos, bloqueio de tentativas indevidas de acesso à Internet oriundas das Unidades (UP e UC) e bloqueio de tentativas de intrusão às Unidades (UP e UC) provenientes da Internet.

4.3. 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).

4.3.1. Os indicadores de desempenho técnico-operacional do Acordo de Níveis de Serviços devem ser atendidos ainda que a Unidade Provedora Internet esteja sob a ocorrência de tentativas indevidas de acesso à Internet, oriundas das Unidades (UP e UC), ou de tentativas de intrusão às Unidades (UP e UC) provenientes da Internet.

4.4. O Serviço de Acesso à Internet 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.

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

4.5. A tradução dos endereços IP privados aptos de cada Unidade deve ser executada para um endereço IP público da CONTRATADA (NAT), de uso exclusivo e permanente vinculado a cada Unidade a que for prestado o Serviço de Acesso à Internet.

4.5.1. Em caso de recebimento de notificação judicial sobre o uso indevido da Internet através de endereço IP público do SAI, 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, anexando cópia da respectiva notificação.

4.6. Quando a Unidade fizer o uso de endereço IPv6, a UPI deverá encaminhar o tráfego para o AS GESP.

4.7. A função de resolução de nomes do Serviço de Acesso à Internet deve ser executada por servidores de DNS que suportem FQDN (Fully Qualified Domain Name) e o encaminhamento de pesquisas de nomes (DNS forward queries), provenientes de servidores DNS das Unidades.

4.7.1. Os servidores de DNS devem ser dedicados e atender aos requisitos de extensão para resolução de nomes DNSSEC (Domain Name System Security Extensions), definido pelas RFC 4033, RFC 4034 e RFC 4035, de modo a garantir a autenticidade e a integridade das respostas na interação com os demais servidores de DNS.

4.8. A função de controle de acesso a conteúdos do Serviço de Acesso à Internet deve ser configurada na estrutura da UPI através da implantação de filtros com base em um perfil único.

4.8.1. A configuração dos filtros de controle de acesso a conteúdos na UPI deve ser feita pela CONTRATADA de acordo com as informações fornecidas pela Administradora da Rede, conforme previsto no Plano de Transição.

4.8.2. Alterações na configuração dos filtros de controle de acesso a conteúdos na UPI devem ser feitas pela CONTRATADA em conformidade com as informações fornecidas pela Administradora da Rede ao longo do período de vigência do Contrato.

4.9. A função de bloqueio de tentativas indevidas de acesso à Internet oriundas das Unidades (UP e UC) compreende a utilização de mecanismos de segurança que efetuem a filtragem de pacotes na camada de rede, no conceito de inspeção stateful, permitam o acesso controlado das redes internas à Internet, sendo este controle implantado por meio de regras baseadas em controle de aplicações, permitam a implantação de regras específicas para tratamento de exceções (white lists) de endereços IP e URL, gerem alarme em caso de potencial violação da segurança e registrem, em log, as informações pertinentes.

4.10. A função de bloqueio de tentativas de intrusão às Unidades (UC e UP) provenientes da Internet deve ser feita com a utilização de mecanismos de segurança para a detecção de atividades suspeitas, a geração de alarme em caso de potencial violação da segurança e o registro, em log, das informações pertinentes, de modo a dar proteção às redes internas contra acessos não autorizados originados na Internet.

4.11. A UPI deve participar de todas as VPN da Rede IP Multisserviços em que participam Unidades que tenham contratado a prestação do Serviço de Acesso à Internet, para as quais deve ser configurada rota default para a UPI.

4.12. Na prestação do Serviço de Acesso à Internet deve ser feito roteamento direto do tráfego destinado aos sites das Unidades participantes do AS GESP pelo backbone da Rede IP Multisserviços, de modo a otimizar o tráfego entre a VPN AS GESP e as demais VPN.

4.13. A UPI deve suportar o tráfego de voz sobre IP.

Infraestrutura para a Prestação do Serviço de Acesso à Internet

4.14. A UPI deve ser instalada, operada e mantida pela CONTRATADA em suas dependências.

4.15. A operação da UPI é monitorada pela Administradora da Rede.

4.16. A UPI deve ser dotada de mecanismo para o controle dos endereços IP (v4 e v6) a partir dos quais o acesso à Internet pode ser feito, de servidores de resolução de nomes (DNS), de servidores de filtros de conteúdo, de servidores de firewall, de servidores de IDS/IPS e de roteadores e ser interconectada à Internet, ao backbone da Rede IP Multisserviços e à VPN AS GESP da Rede IP Multisserviços.

4.17. Todos os componentes de hardware e de software da estrutura da UPI devem ser duplicados de forma que, no caso de falha do elemento principal, o elemento secundário tenha capacidade suficiente para atendimento pleno a toda a carga de processamento.

4.18. Caso o licenciamento do software da estrutura da UPI seja condicionado à quantidade de usuários, a CONTRATADA deve considerar quantidade ilimitada de usuários.

4.19. A estimativa para o dimensionamento inicial dos componentes da estrutura da UPI deve considerar os requisitos de volume de processamento que constam na tabela a seguir, referente a valores de sua utilização na HMM em dias úteis.

PARÂMETROS	VALORES
Número de domínios acessados	100.000
Número de requisições por segundo	50.000
Número de sessões concorrentes	1.500.000

4.20. O filtro de conteúdo da estrutura da UPI deve ser dimensionado levando em consideração que o Serviço de Acesso à Internet é prestado com múltiplos perfis de acesso à conteúdos.

4.21. A estrutura da UPI deve ser interconectada à Internet através de 2 (dois) PoP do AS da CONTRATADA.

4.22. Para fins de log, a estrutura da UPI deve ser dimensionada para atender a um volume de 600.000.000 (seiscentos milhões) de requisições por dia.

4.23. Cada uma das conexões da UPI à Internet deve ter banda útil inicial de 10 Gbps.

4.24. A estrutura da UPI deve ser interligada a dois PE do backbone da Rede IP Multisserviços, através de conexões, locais ou remotas, com banda útil inicialmente definida em 20 Gbps, adequada à vazão do tráfego das Unidades que contratam a prestação do Serviço de Acesso à Internet.

4.25. A estrutura da UPI deve ser interligada a dois PE do backbone da Rede IP Multisserviços, através de conexões, locais ou remotas, com banda útil inicialmente definida em 2 Gbps, adequada à vazão do tráfego entre a UPI e a VPN AS GESP.

4.26. A implantação da estrutura da UPI ou sua adequação deve estar concluída no prazo de 60 (noventa) dias ou de 30 (sessenta) dias, respectivamente, a contar da data de assinatura do Contrato, conforme conste no Plano de Transição.

4.27. A estrutura da UPI deve ser ampliada a fim de acompanhar o crescimento da utilização do serviço ao longo do período de execução contratual.

4.28. A CONTRATADA deve providenciar a ampliação da estrutura da UPI 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.

4.29. Durante a vigência do Contrato, as ampliações dos recursos da estrutura da UPI devem estar disponíveis no prazo de 30 (sessenta) dias a contar da data de ocorrência do evento que lhe der causa, conforme critérios dispostos acima.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

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

Requisitos Operacionais para a Prestação do Serviço de Acesso à Internet

4.31. A UPI 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.

4.32. Deve ser atribuído aos recursos da estrutura da UPI e suas conexões códigos de identificação (ID) a ser utilizado para se referir a esses elementos nos procedimentos estabelecidos no Acordo Operacional.

4.33. A estrutura da UPI e suas conexões devem ser gerenciadas pela CONTRATADA para a prestação do serviço e para o planejamento da capacidade nominal desses recursos.

4.34. A CONTRATADA é responsável pela operação e manutenção, corretiva ou preventiva, de todos os recursos da estrutura da UPI e de suas conexões.

4.35. Na prestação do Serviço de Acesso à Internet todos os acessos realizados e todos os bloqueios executados devem ser registrados em log contendo as informações relacionadas nos subitens que seguem.

4.35.1. Os registros gerados pelo servidor de DNS devem conter, dentre outras, as seguintes informações: data-hora do acesso, endereço de origem (IPv4 e IPv6), endereço de destino (IPv4 e IPv6), URL, e o tipo de apontamento gerado.

4.35.2. Os registros gerados pelo servidor de filtro de conteúdo devem conter, dentre outras, as seguintes informações: data-hora do acesso, endereço de origem (IPv4 e IPv6), endereço de destino (IPv4 e IPv6), URL, porta de destino, categoria e a ação tomada.

4.35.3. Os registros gerados pelo servidor de firewall devem conter, dentre outras, as seguintes informações: data e hora do acesso,

endereço de origem (IPv4 e IPv6), endereço de destino (IPv4 e IPv6), porta de origem, porta de destino, protocolo e o tipo de ação tomada.

4.35.4. Os registros gerados pelo servidor de IDS/IPS devem conter, dentre outras, as seguintes informações: data-hora do acesso, assinatura, endereço de origem (IPv4 e IPv6), endereço de destino (IPv4 e IPv6), porta de origem, porta de destino, protocolo, URL e o tipo de status do evento.

4.36. A CONTRATADA deve gerar relatórios gerenciais da prestação do Serviço de Acesso à Internet, de modo a permitir a análise do histórico e do desempenho da estrutura da UPI e fornecê-los à Administradora da Rede, atendendo às especificações, quanto à forma, conteúdo e periodicidade, definidas no Acordo Operacional.

4.37. A CONTRATADA deve gerar relatórios de utilização do Serviço de Acesso à Internet destinada às Unidades a que o serviço é prestado, atendendo às especificações, quanto à forma, conteúdo e periodicidade, definidas no Acordo Operacional.

5. DESCRIÇÃO DO SERVIÇO DE TRÂNSITO INTERNET

Prestação do Serviço de Trânsito Internet

5.1. O Serviço de Trânsito Internet é prestado à Unidade (UC ou UP) 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.

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

5.1.2. Quando justificado pela Administradora da Rede, 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.

5.2. 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).

5.3. 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.

5.4. 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).

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

5.5. 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.

5.6. 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.

5.6.1. Cada um dos AS (AS1 e AS2) deve ter estrutura dualizada de Roteadores BGP, implantada em endereços distintos ou em um mesmo endereço, para fins de conexão com o AS GESP.

5.6.2. 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

5.7. A banda útil inicial de Trânsito Internet para o AS GESP deve ser de 100 Gbps, simétrica, distribuída dinamicamente entre o AS1 e o AS2.

5.8. 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.

5.9. A implantação da estrutura do AS GESP ou sua adequação deve estar concluída no prazo de 60 (sessenta) dias ou de 30 (trinta) dias, respectivamente, a contar da data de assinatura do Contrato, conforme conste no Plano de Transição.

5.10. 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.

5.11. Durante a vigência do Contrato, as ampliações dos recursos da estrutura do AS GESP devem estar disponíveis no prazo de 30 (trinta) dias a contar da data de ocorrência do evento que lhe der causa, conforme critérios no item anterior.

5.12. 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.

5.13. 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 PRODESP do AS GESP, PoP SEFAZ do AS GESP e PoP FDE do AS GESP.

5.14. A localização dos três pontos de presença do AS GESP corresponde a ambientes indicados, respectivamente, nos endereços PoP PRODESP do AS GESP na Rua Agueda Gonçalves, n° 240, Taboão da Serra – SP, PoP SEFAZ do AS GESP na Secretaria da Fazenda, na Av. Rangel Pestana, n° 300, São Paulo – SP, e no PoP FDE do AS GESP na Av.São Luís, 99 , São Paulo – SP.

5.14.1. A CONTRATADA deverá efetuar *site survey* para verificar as limitações físicas da área disponível nos ambientes para a instalação de no máximo 3 (três) *racks* padrão 19", devendo se ajustar às condições e exigências de cada PoP.

5.15. 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.

5.16. A Borda BGP do AS GESP deve ser localizada nos PoP PRODESP do AS GESP, PoP SEFAZ do AS GESP e PoP FDE do AS GESP.

5.17. 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:

5.17.1. Equipamentos do PoP PRODESP do AS GESP:

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

Conexão em âmbito local (LAN)	24 (*) (**)	10 Gbps
Ampliação de capacidade ou redundância	2 (*)	100 Gbps

(*) Portas devem estar distribuídas em dois módulos distintos e independentes.
(**) 12 portas SFP 1000 Base-T e 12 portas SFP 1000 Base-SX

5.17.2. Equipamentos do PoP SEFAZ do AS GESP:

Finalidade	Quantidade de Portas	Capacidade de cada Porta
Interligação ao PoP PRODESP e ao PoP FDE do AS GESP	2 (*)	100 Gbps
Interligação a um dos roteadores BGP do AS2	1	100 Gbps
Interligação ao PoP SEFAZ do *backbone* da Rede IP Multisserviços	1	100 Gbps
Conexão local com roteador BGP redundante	1	100 Gbps
Conexão de âmbito local (LAN)	24 (*) (**)	10 Gbps
Ampliação de capacidade ou redundância	2 (*)	100 Gbps

(*) Portas devem estar distribuídas em dois módulos distintos e independentes.
(**) 12 portas SFP 1000 Base-T e 12 portas SFP 1000 Base-SX

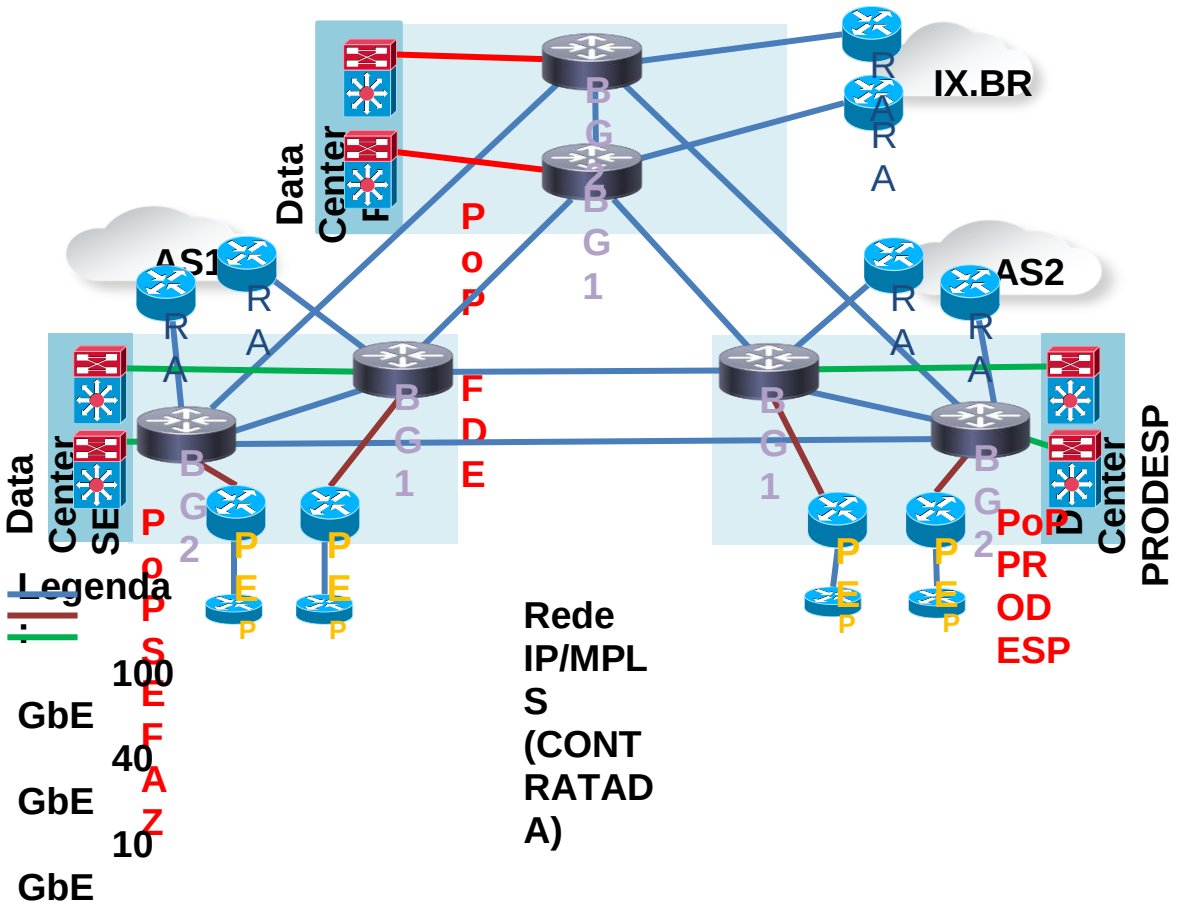
5.17.3. Equipamento do POP FDE do AS GESP:

Finalidade	Quantidade de Portas	Capacidade de cada Porta

Interligação ao PoP PRODESP e ao PoP SEFAZ do AS GESP	2 (*)	100 Gbps
Interligação ao *switch* do IX.br	2 (*)	100 Gbps
Conexão local com roteador BGP redundante	1	100 Gbps
Conexão de âmbito local (LAN)	24 (*) (**)	10 Gbps
Ampliação de capacidade ou redundância	2 (*)	100 Gbps

(*) Portas devem estar distribuídas em dois módulos distintos e independentes.
(**) 12 portas SFP 1000 Base-T e 12 portas SFP 1000 Base-SX.

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



5.19. 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:

5.19.1. Dar suporte aos protocolos IPv4 e IPv6;

5.19.2. 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;

5.19.3. 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;

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

5.19.5. 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 94/188 Gbps (half duplex / full duplex);

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

5.19.7. 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 (priorização de tráfego), IEEE 802.1Q (VLAN) e IEEE 802.1X (controle de acesso por porta);

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

5.19.9. Ter 4 (quatro) Gigabytes de memória RAM;

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

5.19.11. Ter dimensões padronizadas para montagem em armário (rack) de 19”;

5.19.12. 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;

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

5.20. 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.

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

5.20.1.1. 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.

5.20.1.2. 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.

5.20.2. 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.

5.20.3. Cada equipamento terminal deve ser interligado pela CONTRATADA a uma porta do Roteador BGP nos PoP PRODESP do AS GESP, PoP SEFAZ do AS GESP e PoP FDE do AS GESP, destinadas a essa finalidade.

5.20.4. 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.

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

5.21.1. A UP PRODESP deve ser interligada em âmbito local aos dois Roteadores BGP do PoP PRODESP do AS GESP;

5.21.2. A UP SEFAZ deve ser interligada em âmbito local aos dois Roteadores BGP do PoP SEFAZ do AS GESP;

5.21.3. A UP FDE (Secretaria da Educação) deve ser interligada em âmbito local aos dois Roteadores BGP do PoP FDE do AS GESP;

5.21.4. Cada um dos Roteadores BGP do PoP PRODESP 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;

5.21.5. Cada um dos Roteadores BGP do PoP SEFAZ 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.

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

5.22.1. O PoP PRODESP 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.

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

5.22.2. O PoP SEFAZ 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.

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

5.22.3. 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.

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

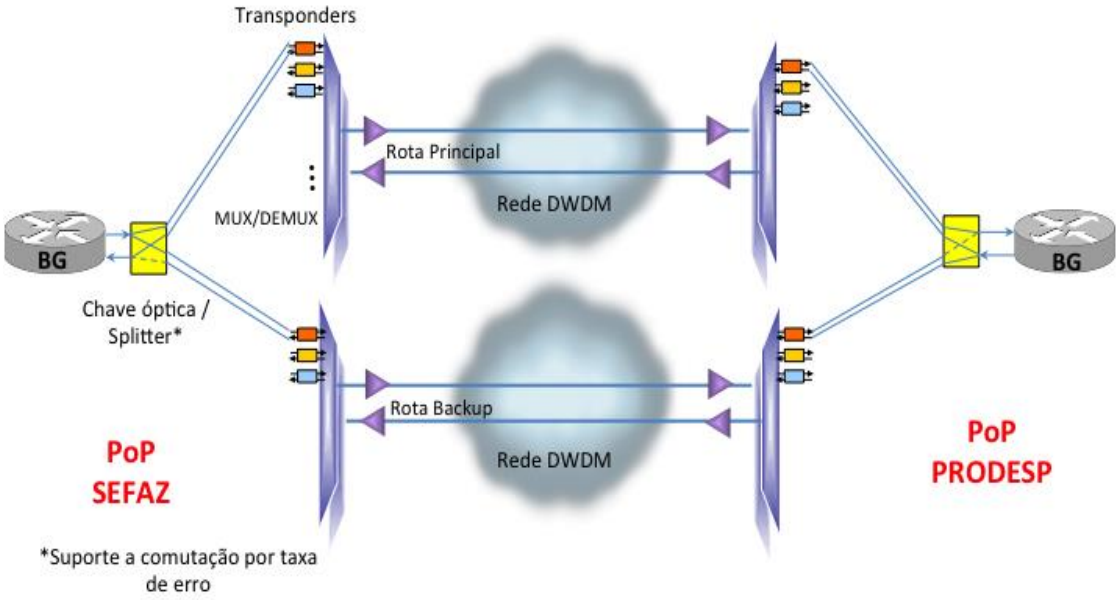
5.22.5. Os circuitos digitais devem ser transparentes a códigos e a protocolos, configurados na modalidade ponto a ponto permanente e de uso exclusivo para a prestação do Serviço de Trânsito Internet.

5.22.6. O PoP FDE 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 na Av. João Dias, 3.163, São Paulo - SP.

5.23. Para o provimento dos circuitos digitais dedicados ponto a ponto em dupla abordagem, a solução deve contemplar a proteção de circuito através de equipamentos distintos, tais como multiplexadores, demultiplexadores, amplificadores ópticos e transponders utilizados em soluções DWDM.

5.24. 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 poderá passar pelo terceiro PoP (técnica também conhecida como bypass).

5.25. 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:



5.26. 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.

Requisitos Operacionais para a Prestação do Serviço de Trânsito Internet

5.27. 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.

5.28. Deve ser atribuído a cada porta do Roteador 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.

5.29. Os Roteadores BGP dos PoP do AS GESP devem ser instalados e configurados pela CONTRATADA e operados pela PRODESP com assistência da CONTRATADA durante o período inicial de 30 (trinta) dias

da operação, sendo de responsabilidade da CONTRATADA a manutenção dos equipamentos.

5.29.1. Nesse período a CONTRATADA deve manter um especialista com qualificação técnica em BGP na PRODESP em horário comercial, 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.

5.29.2. 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.

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

5.30. 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.

5.30.1. O suporte técnico deve ser dado por especialista certificado, através de atendimento telefônico em horário comercial, sem limitação de chamadas, e de atendimento in loco, caso necessário, em horário comercial no próximo dia útil após a solicitação feita pela PRODESP.

5.30.2. 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.

5.31. 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 e AS2, 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.

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

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

5.34. 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.

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

5.34.2. 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.

5.35. 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

5.36. 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.

5.37. 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:

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

5.37.2. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

5.37.3. Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

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

5.37.5. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

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

5.38. A solução deve implementar múltiplas técnicas de detecção de ataques, incluindo análise de mal 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.

5.39. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

5.40. 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.

5.41. 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.

5.42. 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 baseline (linha de base) para cada entidade monitorada, de forma que possa aprender e relatar dinamicamente eventuais mudanças nos comportamentos de tráfego.

5.43. 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.

5.43.1. Por solicitação da Administradora da Rede 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.

5.44. Caso sejam utilizados dois AS próprios na prestação do Serviço de Trânsito Internet, a solução de monitoramento, detecção e mitigação de ataques deve ser implementada internamente aos AS da CONTRATADA.

5.44.1. Caso seja utilizado um AS próprio e um AS de terceiro, a solução de monitoramento, detecção e mitigação de ataques deve ser implementada internamente ao AS próprio e quanto ao AS de terceiro, internamente a este AS ou de forma dedicada no PoP do AS GESP.

5.45. Deve ser implementada solução dedicada de monitoramento, detecção e mitigação de ataques no PoP FDE do AS GESP de modo a detectar os ataques provenientes das conexões ao IX.br.

5.46. 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.

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

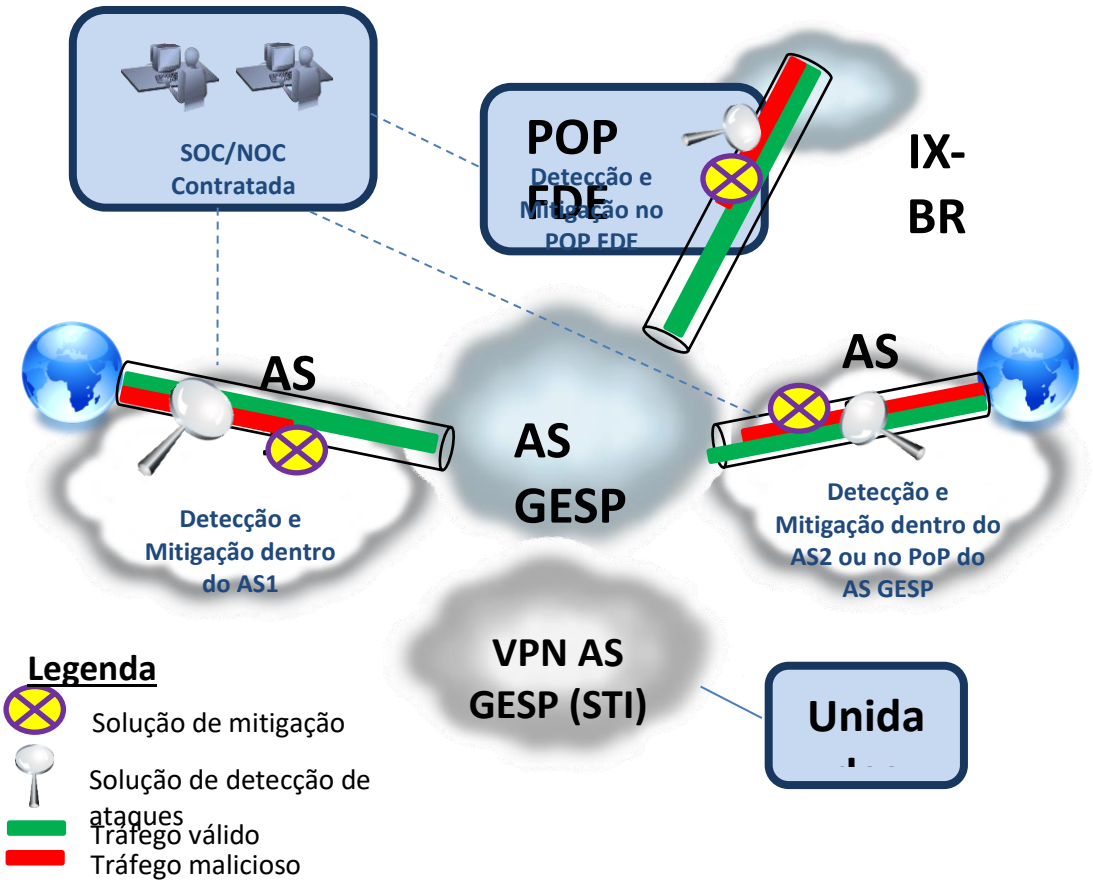
5.47. A figura a seguir demonstra a solução de monitoramento, detecção e mitigação de ataques, na qual o AS GESP somente recebe tráfego válido proveniente da Internet, através das seguintes opções de detecção e mitigação:

5.47.1. Solução a ser implementada no AS próprio;

5.47.2. Solução a ser implementada no AS de terceiro ou de forma dedicada no AS GESP;

5.47.3. Solução dedicada a ser implementada no PoP FDE do AS GESP para proteção das conexões ao IX.br.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br



5.48. A solução de monitoramento, detecção e mitigação de ataques provida através dos AS próprios ou de um AS próprio e um AS de terceiro deve suportar ataques de até 200 Gbps, entregando um canal limpo de 100 Gbps (clean pipe) para o AS GESP, inclusive no caso de tráfego com pacotes de 64 bytes.

5.48.1. A capacidade de mitigação de ataques deve ser escalável, correspondendo a, pelo menos, 4 (quatro) vezes a capacidade nominal das conexões do AS GESP, sempre garantindo a entrega de canal limpo com a banda útil dessas conexões.

5.49. No caso de AS de terceiro com a solução de monitoramento, detecção e mitigação de ataques implementada de forma dedicada no PoP do AS GESP, a solução deve suportar inicialmente ataques de 100 Gbps, entregando um canal limpo equivalente a banda útil da conexão do AS GESP com o AS de terceiro.

5.49.1. A capacidade de mitigação de ataques deve ser escalável, sempre garantindo a entrega de canal limpo equivalente a banda útil da conexão do AS GESP com o AS de terceiro.

5.50. A solução de monitoramento, detecção e mitigação dedicada a ser implementada no PoP FDE do AS GESP deve suportar inicialmente a capacidade de mitigação de ataques de 100 Gbps, entregando um canal limpo equivalente a banda útil das conexões do AS GESP com o IX.br.

5.50.1. A capacidade de mitigação de ataques deve ser escalável, sempre garantindo a entrega de canal limpo equivalente a banda útil das conexões do AS GESP com o IX.br.

5.51. 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.

5.52. 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 Remote Triggered Black Hole, conforme detalhado na RFC 5635.

5.52.1. 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, 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.

5.52.2. A proposta de contramedidas a serem tomadas pela CONTRATADA deve ser previamente submetida à validação por parte da Administradora da Rede.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

5.53. 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).

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

5.55. 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 0800, 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.

5.56. 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.

5.57. 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.

5.57.1. 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.

5.58. 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).

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

5.60. A implantação e ativação das soluções de monitoramento, detecção e mitigação de ataques deve estar concluída no prazo de 120 (cento e vinte) dias a contar da data de assinatura do Contrato.

5.61. 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.

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

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

5.62.2. 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.

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

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

5.65. 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.

5.66. 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.

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

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

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

5.67.2. 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.

6. ACORDO DE NÍVEIS DE SERVIÇOS (SLA)

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 irá apurar mensalmente os indicadores do SLA utilizando informações de seus sistemas e de informações recebidas da CONTRATADA.

6.7. A notificação para aplicação de penalidades é feita com base nos resultados da apuração mensal dos indicadores que constam nos relatórios emitidos pelo SAOG.

6.8. As ocorrências relacionadas no processo de gestão da qualidade, descrito no Acordo Operacional, podem ser consideradas como excludentes de responsabilidade da CONTRATADA na apuração do SLA, desde que sejam por ela comprovadas e recebam a anuência prévia da Administradora da Rede.

6.9. Para fins das disposições deste acordo, entende-se por “incidente” qualquer ocorrência que, devido à falha na entrega ou na prestação dos serviços, afete a conectividade entre duas Unidades, desde a interface LAN do CPE de uma Unidade até a interface LAN do CPE de outra Unidade, seja por interrupção ou degradação da comunicação, ou qualquer ocorrência na prestação do Serviço de Acesso à Internet ou do Serviço de Trânsito Internet que, devido à falha nos recursos agregados à Rede IP Multisserviços, afete a prestação desses serviços.

6.10. Em caso de mais de 2 (dois) incidentes associados a um mesmo ID, ocorridos em período móvel trimestral, a CONTRATADA deve entregar ao respectivo OES e à Administradora da Rede um relatório de análise de causa raiz com propostas de solução.

6.11. 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.

6.12. 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).

6.13. Sempre que a CONTRATADA julgar que a responsabilidade por um incidente recai sobre a Unidade (UC ou UP), cabe à CONTRATADA o ônus da prova, devendo apresentar testes comprobatórios e relatórios específicos.

Frequência de Registros de Incidente por ID

6.14. A Frequência de Registro de Incidentes por ID corresponde ao número total de registros abertos de forma proativa ou de forma reativa, por mês.

6.15. A apuração do indicador deve ser feita com base nas informações de abertura de registro de incidentes.

6.16. 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	2	Registros

Frequência de Registros de Incidente do SCM

6.17. 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.

6.18. A apuração do indicador deve ser feita com base nas informações de abertura de registro de incidentes.

6.19. 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

6.20. O prazo para Solução de Incidente, cuja causa é de responsabilidade da CONTRATADA, corresponde ao valor máximo admissível do PTI relativo aos serviços SCM, SAI e STI ou aos recursos da UPI, do AS GESP e do backbone IP-MPLS.

6.21. O prazo para Solução de Incidentes é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Solução de Incidentes em Serviços ou em recursos	240	Minutos

6.22. O prazo para Solução de Incidente no SCM para um ID deve ser multiplicado pelo fator de 1,5 (um e meio) quando a Unidade estiver localizada na área rural do município, conforme definido no plano diretor vigente.

Indisponibilidade de Serviço

6.23. 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.

6.24. A apuração da Indisponibilidade de Serviço deve considerar os incidentes cuja causa é de responsabilidade da CONTRATADA.

6.25. 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 dos Serviços SCM, SAI, STI por Unidade

6.26. A Indisponibilidade do SCM, por Unidade, se desdobra em Indisponibilidade do SCM com redundância e Indisponibilidade do SCM sem redundância.

6.27. 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

6.28. 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;

6.29. 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.

6.30. 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.

6.31. A Indisponibilidade do SAI corresponde ao período de tempo total no mês, por Unidade, em que não há oferta de acesso à Internet com as funcionalidades da estrutura da UPI, para a Unidade que contratou o SAI.

6.32. A Indisponibilidade do SAI decorrente da interrupção na prestação do SCM para a Unidade não deve ser considerada na apuração da Indisponibilidade do SAI para o ID a que for prestado o SAI e o SCM.

6.33. A Indisponibilidade do STI corresponde ao período de tempo total no mês, por Unidade, em que não há oferta de acesso à Internet para a Unidade que contratou o STI.

6.34. A Indisponibilidade do STI decorrente de interrupção na prestação do SCM para a Unidade não deve ser considerada na apuração da Indisponibilidade do STI para o ID a que for prestado o STI e o SCM.

6.35. 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.

6.36. A Indisponibilidade do SAI é expressa em horas através da seguinte fórmula:

Indisponibilidade do SAI (horas) = ISAI / 60

Em que:

ISAI – período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do Serviço SAI, por Unidade, no mês, de responsabilidade da CONTRATADA, sem considerar aqueles decorrentes de interrupção na prestação do SCM, no caso das Unidades que contratam o SAI e o SCM.

6.37. A Indisponibilidade do STI é expressa em horas através da seguinte fórmula:

Indisponibilidade do STI (horas) = ISTI / 60

Em que:

ISTI – período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do Serviço STI, por Unidade, no mês, de responsabilidade da CONTRATADA, sem considerar aqueles decorrentes de interrupção na prestação do SCM, no caso das Unidades que contratam o STI e o SCM.

6.38. 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 do SAI e STI, por Unidade		

Indisponibilidade de recursos da UPI, do AS GESP ou do *backbone* IP-MPLS

6.39. A indisponibilidade de recursos da UPI, do AS GESP ou do backbone IP-MPLS 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.

6.40. A apuração da indisponibilidade de recursos da UPI, do AS GESP ou do backbone IP-MPLS deve considerar os incidentes cuja causa é de responsabilidade da CONTRATADA.

6.41. Para o cálculo da indisponibilidade de recursos da UPI, do AS GESP ou do backbone IP-MPLS, deve ser considerado o PTI referente ao incidente associado ao ID do recurso, de cada Registro de Incidente fechado no mês calendário.

6.42. A indisponibilidade de recursos da UPI é expressa em horas através da seguinte fórmula:

Indisponibilidade de recursos da UPI (horas) = IUPI / 60

Em que:

IUPI – período de tempo total, expresso em minutos, correspondente à soma dos PTI de interrupção na prestação do SAI simultaneamente para todas as Unidades que a contrataram, no mês, de responsabilidade da CONTRATADA.

6.43. 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.

6.44. 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.

6.45. A indisponibilidade de recursos da UPI, do AS GESP ou do backbone IP-MPLS, por mês, é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade da UPI	0,5	Hora
Indisponibilidade do AS GESP		
Indisponibilidade do *backbone* IP-MPLS		

6.46. Para fins de aplicação de sanção, a indisponibilidade de recursos da UPI, do AS GESP ou do backbone IP-MPLS prevalece, respectivamente, em relação à Indisponibilidade do SAI, do STI ou do SCM, por Unidade.

6.47. Os eventuais registros de incidentes abertos para cada Unidade, associados à interrupção da prestação de um serviço cuja causa é a mesma falha identificada através do registro de incidente aberto para o recurso correlacionado a este serviço, devem ser desconsiderados na apuração do SLA.

Nível da Qualidade do SCM

6.48. 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.

6.49. 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.

6.50. O valor mínimo do Nível da Qualidade do Serviço de Comunicação Multimídia é o que consta na tabela abaixo:

INDICADOR	VALOR	UNIDADE
Nível de Qualidade do SCM	93	%

6.51. 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.

6.52. A quantidade de ID da amostra consta no Acordo Operacional.

6.53. 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.

6.54. Deverão 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.

6.55. 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

6.56. A latência corresponde ao período de tempo expresso em milissegundos para transportar um pacote IP entre a porta LAN de um CPE de origem e a porta LAN do CPE de destino na Rede IP Multisserviços, sendo para o seu cálculo adotada a seguinte fórmula:

L = (RTT/2)

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

6.57. O jitter ou variação do atraso, expresso em milissegundos, corresponde à variação máxima de retardo entre pacotes IP de um fluxo de pacotes IP transportados pela Rede IP Multisserviços entre a porta LAN do CPE de origem e a porta LAN do 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)
Dn-1 - atraso total do “enésimo menos 1” pacote (em milissegundos - ms)

6.58. 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 à acessos em que ocorre a prestação de serviços que demandam essa Classe de Serviço.

Perda de Pacotes

6.59. A perda de pacotes, expresso em porcentagem, corresponde à quantidade de pacotes IP não recebidos na porta LAN do CPE de destino em relação ao total de pacotes IP enviados pela porta LAN do 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

6.60. O prazo para atendimento à Solicitação de Ativação de Serviços corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data do envio dos resultados dos testes de ativação do ID realizados por ela, desde que tenha sido dado o aceite pelo OES.

6.61. 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.

6.62. 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

6.63. Se a ativação dos serviços ocorrer em até 45 (quarenta e cinco) dias corridos em Área Urbana ou em até 68 (sessenta e oito) dias corridos em Área Rural, a CONTRATADA fará jus ao dobro do valor de remuneração eventual de ativação de serviços em até 90/135 dias, desde que no momento da solicitação o OES contratante concorde com a bonificação referente ao menor prazo.

Prazo para atendimento à Solicitação de Alteração da Prestação de Serviços

6.64. 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 do recebimento da solicitação pela CONTRATADA e a data do aceite pelo OES.

6.65. A apuração do indicador deve ser feita com base nas informações do protocolo da Solicitação na CONTRATADA e no aceite pelo órgão, via SAOG.

6.66. 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

6.67. Se a alteração da capacidade nominal do SCM ocorrer em até 45 (quarenta e cinco) dias corridos em Área Urbana ou em até 68 (sessenta e oito) dias corridos em Área Rural, a CONTRATADA fará jus ao dobro do valor de remuneração eventual de alteração da prestação de serviços em até 90/135 dias, desde que no momento da solicitação o OES concorde com a bonificação referente ao menor prazo.

Prazo para Atendimento a Solicitação de Alteração de Padrão de SCM

6.68. 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 do recebimento da solicitação pela CONTRATADA e a data do aceite pelo OES.

6.69. A apuração do indicador deve ser feita com base nas informações do protocolo na CONTRATADA e no aceite da solicitação no SAOG.

6.70. O atendimento, pela CONTRATADA, à Solicitação de Alteração de Padrão de SCM deve ser realizado no prazo máximo descrito na tabela a seguir:

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

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
De com redundância para sem redundância em área Urbana ou Rural	30	Dias corridos

6.71. Se a alteração de padrão do SCM, de sem redundância para com redundância, ocorrer em até 45 (quarenta e cinco) dias corridos em Área Urbana ou em até 68 (sessenta e oito) dias corridos em Área Rural, a CONTRATADA fará jus ao dobro do valor de remuneração eventual de alteração de padrão de SCM em até 90/135 dias, desde que no momento da solicitação o OES contratante concorde com a bonificação referente ao menor prazo.

6.72. 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

6.73. O prazo para atendimento a uma Solicitação de Alteração de Configuração de CPE corresponde ao período de tempo, expresso em horas, entre o momento do recebimento da solicitação pela CONTRATADA e o aceite pelo OES.

6.74. Entre as atividades previstas neste indicador estão a configuração de Classes de Serviço (CoS) e marcação de pacotes e a configuração de DHCP relay, entre outras alterações lógicas no CPE.

6.75. A apuração do indicador deve ser feita com base nas informações do protocolo na CONTRATADA e no aceite da solicitação no SAOG.

6.76. 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.

6.77. O atendimento, pela CONTRATADA, à Solicitação de Alteração de Configuração de CPE para UC ou UP deve ser realizado no prazo máximo descrito na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Configuração de CPE	2	Dias

Prazo para atendimento à Solicitação de Alteração de Localização Física de CPE

6.78. O prazo para atendimento à Solicitação de Alteração de Localização Física de CPE corresponde ao período de tempo, expresso em dias corridos, entre a data do recebimento da solicitação pela CONTRATADA e a data do envio dos resultados dos testes realizados por ela, desde que tenha havido aceite.

6.79. 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.

6.80. O prazo para a aprovação de GMUD não deve ser considerado para efeito de cálculo do indicador.

6.81. O prazo para atendimento à Solicitação de Alteração de Localização Física de CPE é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Localização Física de CPE em UC	15	Dias corridos
Prazo para Alteração de Localização Física de CPE em UP	30	Dias corridos

6.82. O valor do indicador “prazo para Alteração de Localização Física de CPE em UC” e o valor do indicador “prazo para Alteração de Localização Física de CPE em UP” devem ser multiplicados pelo fator de 1,5 (um e meio) quando o endereço da Unidade para instalação do ID estiver localizado na área rural do município, conforme definido no plano diretor vigente.

Prazo para atendimento à Solicitação de Alteração de Dados Cadastrais

6.83. 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.

6.84. 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

6.85. 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.

6.86. 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

6.87. 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.

6.88. 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.

6.89. 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 atendimento à Solicitação de Bloqueio ou Desbloqueio de Endereços IP

6.90. O prazo para atendimento à Solicitação de Bloqueio ou à Solicitação de Desbloqueio de Endereços IP, no SCM de UP ou UC, corresponde ao período de tempo, expresso em minutos, entre a data e o horário do recebimento da solicitação pela CONTRATADA e a data e o horário da execução do bloqueio ou desbloqueio, desde que tenha havido aceite.

6.91. Fica a critério do OES agendar uma data e horário para a execução do bloqueio ou do desbloqueio, sendo neste caso, descontado o período de tempo, expresso em minutos, entre a data e o horário de início de execução, indicados na solicitação onde constar o agendamento pelo OES, e a data e o horário de fim de execução informados pela CONTRATADA, desde que tenha ocorrido o aceite.

6.92. O prazo para atendimento à Solicitação de Bloqueio e Desbloqueio de Endereços IP é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Bloqueio ou Desbloqueio de Endereços IP	60	Minutos

Prazo para atendimento à Solicitação de Alteração de Configuração da Estrutura da UPI

6.93. O prazo para atendimento à Solicitação de Alteração de Configuração da Estrutura da UPI corresponde ao período de tempo, expresso em horas, entre a data e o horário do recebimento da solicitação pela CONTRATADA e a data e o horário da execução da alteração da configuração da estrutura da UPI, desde que tenha havido aceite.

6.94. O prazo para atendimento à Solicitação de Alteração de Configuração da Estrutura da UPI é o que consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Alteração de Configuração da Estrutura da UPI	4	Horas

Prazo para Reação e Mitigação de Ataques

6.95. 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.

6.96. O indicador deve ser medido, por evento, entre o início da ocorrência dos ataques e o início da efetiva mitigação dos mesmos pela CONTRATADA.

6.97. Para fins de apuração do indicador, o evento de ataques deve ser classificado como Ataque ao AS GESP ou Ataque ao OES.

6.98. 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).

6.99. 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.

6.100. 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 Ataques ao OES.

6.101. O valor máximo admitido para este indicador consta na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Prazo para Reação e Mitigação de Ataques ao OES, por evento	30	Minutos
Prazo para Reação e Mitigação de Ataques ao AS GESP, por evento		

Indisponibilidade do SCM quando da Alteração/Adequação do Serviço

6.102. A Indisponibilidade do SCM quando da Alteração/Adequação do Serviço é o que consta na tabela seguir:

INDICADOR	VALOR	UNIDADE
Indisponibilidade do SCM quando da Alteração/Adequação do Serviço	2	Horas

Prazo para entrega de relatórios

6.103. 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

6.104. Os indicadores do SLA se encontram agrupados na tabela a seguir:

INDICADOR	VALOR	UNIDADE
Frequência de Registros de Incidente por ID	2	Registros
Frequência de Registros de Incidente do SCM	5	%
Prazo para Solução de Incidentes em Serviços ou em recursos da UPI, do AS GESP ou do *backbone* IP-MPLS	240	Minutos
Indisponibilidade do SCM sem redundância	8	Horas
Indisponibilidade do SCM com redundância	0,5	Hora
Indisponibilidade do SAI e STI, por Unidade	0,5	Hora
Indisponibilidade de recursos da UPI, do AS GESP ou do *backbone* IP-MPLS	0,5	Hora
Nível de 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 acesso	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 de Padrão de SCM de com redundância para sem redundância em Área Urbana ou Rural	30	Dias corridos
Prazo para Alteração da Configuração de CPE	4	Horas
Prazo para Alteração de Localização Física de CPE em UC	15	Dias corridos
Prazo para Alteração de Localização Física de CPE em UP	30	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 Bloqueio ou Desbloqueio de Endereços IP	60	Minutos
Prazo para Alteração de Configuração da Estrutura da UPI	4	Horas
Prazo para Reação e Mitigação de Ataques ao OES, por evento	30	Minutos
Prazo para Reação e Mitigação de Ataques ao AS GESP, por evento	30	Minutos
Indisponibilidade do SCM quando da Alteração/Adequação do Serviço	2	Horas

Prazo para entrega de relatórios em meio eletrônico	15	Dias corridos

7. GERENCIAMENTO DA REDE IP MULTISSERVIÇOS E DE RECURSOS AGREGADOS

7.1. O gerenciamento da Rede IP Multisserviços e dos recursos de hardware e software a esta 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.

7.2. 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 Sistema Especialista de Gerenciamento (SEG), que dá suporte à formação da base de dados de gerenciamento.

7.6. A base de dados de gerenciamento deve ser única, compartilhada pelo NOC e pela UPG, e 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.

Sistema Especialista de Gerenciamento (SEG)

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) da rede de acesso.

7.7.2. Os elementos gerenciados das estruturas agregadas à Rede IP Multisserviços para a prestação do Serviço de Acesso à Internet (SAI) e do Serviço de Trânsito Internet (STI) são os equipamentos de terminação dos circuitos digitais, roteadores, servidores da UPI, portas Internet e dispositivos da solução de monitoramento, detecção e mitigação de ataques instalados na UPI e 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 para que ela possa também remodelar, se necessário, na sua plataforma de monitoramento.

Áreas Funcionais do Gerenciamento

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

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

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;

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

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.

Requisitos Operacionais para a Estrutura Organizacional do Gerenciamento

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 Acesso à Internet e 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 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 SAI;

7.26.2. Infraestrutura do STI;

7.26.3. Dispositivos de aceleração WAN;

7.26.4. 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. 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;

7.31.2. 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. 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. 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.

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

7.33. A equipe de técnicos da UPG deve ser constituída por empregados da CONTRATADA, não sendo admitida a subcontratação para o desempenho de suas atribuições.

7.34. A equipe de atendentes da UPG deve ser dimensionada, a critério da CONTRATADA, para a execução de suas atribuições até o limite de 6 (seis) posições para consoles de operação a serem instaladas no ambiente cedido pela PRODESP.

7.35. 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.

7.36. A equipe da UPG deve acionar o SOC quando necessário nos casos de incidentes relacionados à ataques na infraestrutura do SAI e STI.

7.37. 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.

7.38. A interligação dos 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).

7.38.1. 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.

7.38.2. A implantação ou a adequação da estrutura necessária para a interligação dos 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.

7.38.3. Durante a vigência do Contrato, as ampliações necessárias na estrutura de interligação dos 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.

7.38.4. O não cumprimento dos prazos pode implicar na aplicação de penalidade por descumprimento contratual.

7.39. Além dos 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.

7.40. A UPG deve ser implantada em área de acesso restrito, em condições adequadas de iluminação e climatização, cedida pela PRODESP para uso da CONTRATADA.

7.41. 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.

7.42. 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 no 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.

7.43. As informações relativas ao CPE que devem ser apresentadas nos consoles de operação são as que constam nos subitens que seguem:

7.43.1. Roteamento da VPN configurada no PE associado ao CPE;

7.43.2. Status do CPE da rede de acesso e de suas interfaces;

7.43.3. Alarmes e eventos ocorridos no CPE da rede de acesso, com informações de data e hora de cada ocorrência;

7.43.4. Tráfego em curso, por interface do CPE da rede de acesso.

7.44. As informações relativas ao recurso de aceleração WAN que devem ser apresentadas nos consoles de operação são as que constam nos subitens que seguem:

7.44.1. Alarmes associados ao equipamento de aceleração WAN;

7.44.2. Medidas de desempenho de recursos computacionais tais como CPU e memória;

7.44.3. Medições da eficiência do processo de aceleração.

7.45. As informações relativas a funcionalidade de monitoramento, detecção e mitigação de ataques que devem ser apresentadas nos consoles de operação são os alarmes associados aos dispositivos da solução instalados nos PoP do AS GESP.

7.46. A equipe da UPG 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 nos consoles de operação.

7.47. A equipe da UPG deve utilizar software 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.

7.48. A equipe da UPG 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.

7.49. A equipe da UPG deve acompanhar a parada 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 preventiva, 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 da semana, sendo de responsabilidade da CONTRATADA a instalação, operação e manutenção dos recursos de infraestrutura necessários ao seu funcionamento em suas dependências.

8. MONITORAMENTO DA REDE IP MULTISSERVIÇOS E DE RECURSOS AGREGADOS

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 de terminal virtual Telnet (Teletype Network) ou 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 Acesso à Internet (SAI) e dos circuitos digitais 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 nos 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, os equipamentos de terminação dos circuitos digitais utilizados para a prestação do Serviço de Trânsito Internet e os equipamentos e circuitos da UPI utilizados para a prestação do Serviço de Acesso à Internet, através de consoles do SEG.

8.5. Os 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 deverá prover inicialmente 4 (quatro) consoles do SEG instalados para suportar as atividade de Monitoramento realizadas pela PRODESP.

8.7. A CONTRATADA deve realizar treinamento referente à utilização dos consoles SEG, contemplando todas as funcionalidades especificadas neste capítulo, 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 nos consoles do SEG informações para monitoramento de desempenho e de qualidade operacional da rede contendo, no mínimo, as seguintes informações:

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. Para obter essas informações o sistema de monitoramento deve utilizar recursos de protocolos e funcionalidades como SNMP, Cisco NetFlow (ou similar), Cisco IP SLA (ou similar), sFlow, IPFIX, RMON ou, porventura, outros disponíveis nos equipamentos.

8.11. A solução deve permitir a coleta de dados, o processamento e a geração de relatórios personalizáveis, com gráficos e tabelas que

Rua Agueda Gonçalves, 240 - Taboão da Serra - SP - CEP 06760-900 - Tel: (11) 2845-6000 (PABX)
Correspondência: Caixa Postal 04 - Taboão da Serra - SP - CEP 06754-970
www.prodesp.sp.gov.br - prodesp@prodesp.sp.gov.br

permitam a avaliação do estado operacional da rede e do perfil de tráfego.

8.12. A solução deve contemplar a geração de alarmes automáticos disparados pela extrapolação de limiares configurados previamente.

8.13. A CONTRATADA deve monitorar, em regime de 24x7, parâmetros essenciais de disponibilidade e desempenho, incluindo, no mínimo, UP/DOWN dos equipamentos e interfaces, ocupação, latência, descarte de pacotes, CPU e memória dos equipamentos.

8.14. Os limiares para a geração automática de alarmes devem ser validados com a Administradora da Rede, podendo sofrer adequações que venham a ser necessárias.

8.15. Mensalmente, a CONTRATADA deve entregar relatórios com análise do período para efeito de capacity planning, identificando os links com saturação, que necessitam de aumento de capacidade, e os links com baixo nível de ocupação, que podem ser candidatos à redução de capacidade. Os relatórios devem conter também análise do tráfego por protocolo/aplicação e por classe de QoS. As análises devem avaliar o comportamento do tráfego ao longo do tempo, considerando baselines e linhas de tendência, contendo as recomendações pertinentes a cada link que demandar adequação. Os critérios adotados para a classificação dos enlaces com baixo e alto nível de ocupação devem ser acordados previamente com a Administradora da Rede.

8.16. A CONTRATADA deve apresentar projeto executivo com a finalidade de demonstrar a conformidade com as especificações técnicas requeridas para esta solução.

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

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

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

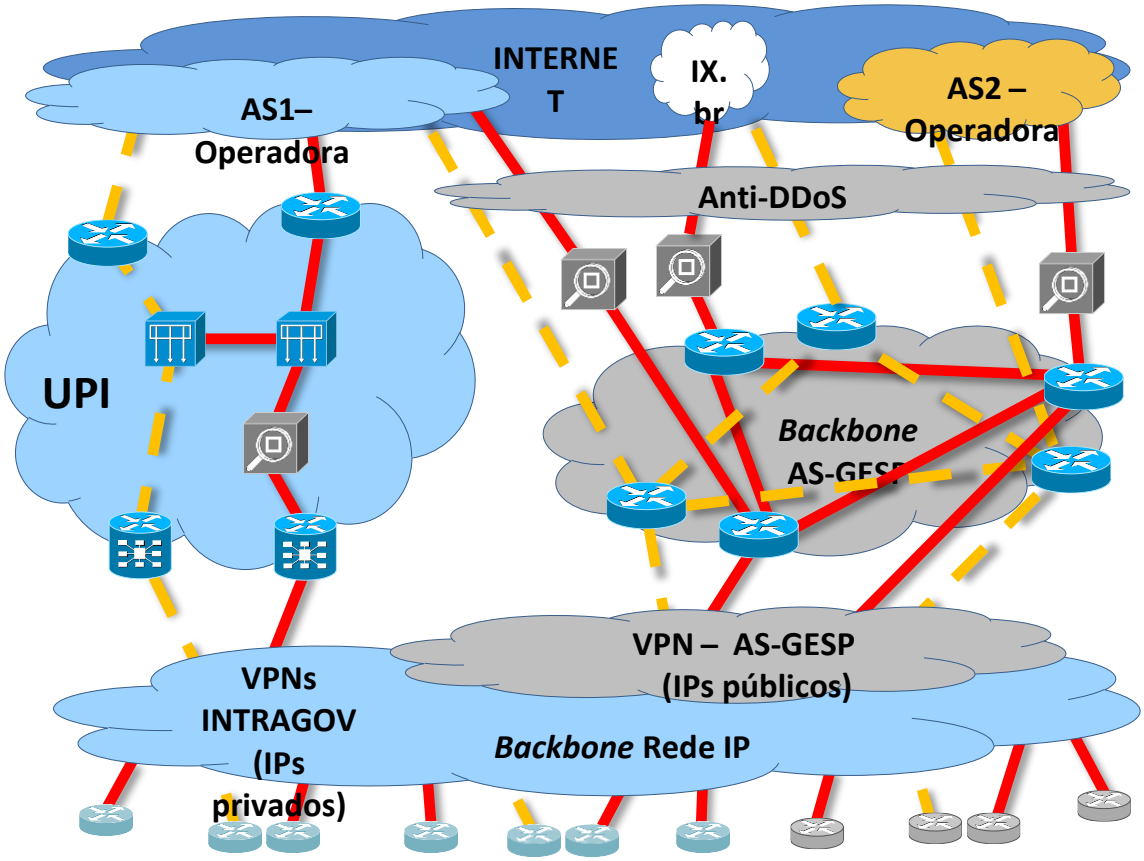
8.18.1. Os testes podem ser realizados tanto para fins de aceite da implantação da solução como para verificação do atendimento aos requisitos no decorrer da vigência do Contrato.

Monitoramento na UPI e no AS-GESP

8.19. A CONTRATADA deve ativar solução capaz de monitorar e identificar o tráfego no nível de aplicação (camada 7 do modelo OSI), bem como deve ser capaz de tomar ações sobre fluxos de tráfego específicos que possam ameaçar a segurança da rede ou congestionar as conexões, prejudicando o desempenho de todas as demais aplicações.

8.20. A CONTRATADA deve prover à PRODESP acesso à solução nos consoles do SEG.

8.21. A CONTRATADA deve ativar a funcionalidade, no mínimo, em todos os enlaces principais (ativos) da infraestrutura da UPI e do AS-GESP, conforme ilustrado na figura a seguir.



	Acesso principal: • **AS-GESP: 100 Gbps por enlace** • **UPI: 20 Gbps por enlace**
	Acesso redundante: mesmas capacidades dos enlaces primários
	Ambiente da Operadora
	Ambiente de Governo
	Contingência de Operadora para a Internet
	Ponto de troca de tráfego metropolitano
	Roteadores da rede de acesso
	Roteadores de borda
	Estrutura composta por filtros de conteúdo, firewalls, IDS/IPS e DNS
	Solução de monitoramento na UPI e no AS-GESP

8.22. A identificação do tráfego deve ocorrer por meio de recurso de inspeção profunda de pacote (deep packet inspection) e de assinatura de perfil de tráfego característico de cada aplicação.

8.23. A solução deve ser capaz de identificar o tráfego das aplicações mais usuais como aplicações corporativas, rede sociais, P2P, streaming de vídeo, streaming de áudio, jogos populares, VPN, Proxy Web e outros serviços para navegação anônima, navegação web, serviços na nuvem, identificando a aplicação específica, no mínimo, nos seguintes casos: YouTube, Vimeo, Netflix, Facebook, Instagram, Twitter, WhatsApp, Telegram, Skype, Spotify, Deezer, iTunes, FaceTime, Vevo, Office 365 (SharePoint, Excel, PowerPoint, Word, Outlook) e TOR.

8.24. O monitoramento e identificação do tráfego devem ocorrer em tempo real e não devem impactar negativamente o fluxo e o desempenho das aplicações.

8.25. De forma a assegurar a confidencialidade das comunicações, a solução não deve realizar a descriptografia de tráfego nem fornecer acesso ao conteúdo trafegado, mesmo para conexões não criptografadas. A identificação deve se restringir ao nível de aplicação e à identificação dos endereços IP de origem e de destino e não deve fornecer acesso ao conteúdo trafegado.

8.26. A solução não deve caracterizar ponto de falha para o tráfego na UPI e no AS-GESP. Os equipamentos devem possuir recurso de bypass automático do tráfego em caso de falta de energia.

8.27. O sistema deve permitir a geração de relatórios personalizáveis, utilizando as informações coletadas, com gráficos e tabelas que permitam a avaliação do estado operacional da rede. Deve apresentar a classificação do tráfego por aplicação, pela sua origem ou pela dupla origem/aplicação.

8.28. O sistema deve contemplar a geração de alarmes automáticos disparados pela extrapolação de limiares previamente configurados, permitindo identificar comportamentos anômalos de tráfego.

8.29. 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:

8.29.1. Definição de políticas de tráfego;

8.29.2. Garantia de banda mínima para aplicações críticas;

8.29.3. Controle de banda máxima por aplicação;

8.29.4. Policiamento de tráfego, com descarte de pacotes;

8.29.5. Priorização de pacotes.

8.30. A solução deve permitir a definição de políticas de tráfego globais e por OES.

8.31. Mensalmente, a CONTRATADA deve entregar relatórios com análise do período para efeito de capacity planning. Os relatórios devem conter também análise do tráfego por protocolo/aplicação e por classe de QoS (priorização de pacotes). As análises devem avaliar o comportamento do tráfego ao longo do tempo, considerando baselines e linhas de tendência, contendo as recomendações pertinentes.

8.32. A CONTRATADA deve apresentar projeto executivo com a finalidade de demonstrar a conformidade com as especificações técnicas requeridas para esta solução.

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

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

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

8.33.2. Os testes 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.

9. FORNECIMENTO DE INFORMAÇÕES

9.1. A CONTRATADA deve fornecer as informações relativas à prestação dos serviços especificados, para fins de acompanhamento e execução dos procedimentos definidos neste Contrato e seus anexos.

9.2. A CONTRATADA deve fornecer, mediante solicitações ad hoc da PRODESP, informações de IP accounting, conforme disciplinado no Acordo Operacional.

9.3. 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.

9.4. Para fins de gestão da prestação do Serviço de Acesso à Internet (SAI), os registros dos logs devem ser gerados, permanecerem disponíveis, durante 15 (quinze) dias corridos, para acesso on-line nos consoles do SEG instaladas na PRODESP e serem mantidos, pela CONTRATADA, em meio magnético que assegure a integridade, confidencialidade e autenticidade das informações armazenadas, pelo prazo de 3 (três) anos a contar da sua geração.

9.5. Para fins de gestão da prestação do Serviço de Acesso à Internet (SAI), 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.

9.6. Para fins de gestão da prestação dos serviços as informações eletrônicas relativas ao faturamento dos serviços devem ser depositadas no SAOG ou transmitidas dos sistemas internos da CONTRATADA para o SAOG, até o quinto dia após o encerramento do período do faturamento, no formato especificado no Acordo Operacional.

9.7. 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.

9.8. 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.

10. GLOSSÁRIO

10.1. 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.
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.
Autorredundante	Característica que define o processo automático de transferência das tarefas entre elementos quando da falha de um deles, reduzindo o risco de inatividade ou de interrupção desta tarefa.
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.
Black Lists	Listas de endereços proibidos para recebimento ou envio de mensagens eletrônicas, aplicadas em ferramenta que disciplina o tráfego de mensagens, atendendo a critérios de segurança.
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 do SCM	Capacidade de transporte de informação do serviço SCM ao *backbone* da Rede IP Multisserviços, expressa em múltiplos de bits/s (bits por segundo).
Capacidade nominal	Capacidade do SCM correspondente a um dos valores padrão de mercado, expressa em múltiplos de bits/s (bits por segundo).
Banda útil	Banda associada a cada classe de serviço, expressa em múltiplos de bits/s (bits por segundo).
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.
CSV (*Comma-Separated Values*)	Formato de arquivo texto usualmente suportado por planilhas eletrônicas.
DHCP (*Dynamic Host Configuration Protocol*)	Protocolo que permite que equipamento conectado a 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	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.
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.

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.
Endereço MAC (*Media Access Control*)	Endereço físico da interface de um dispositivo de rede, utilizado para transporte na camada 2 (Enlace) do Modelo OSI.
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.
GIP (Gestão Integrada de Processos)	Sistema mantido pela PRODESP. Acrônimo definido no escopo deste documento.

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, sem garantia de qualidade de serviço (QoS), para codificação e decodificação de fluxos de dados de áudio e vídeo, garantindo interoperabilidade entre produtos de diversos fabricantes.
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.
Hostname	Nome dado ao host, que serve para identificá-lo na rede com mais facilidade do que através de seu endereço IP.
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.

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.
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 loopback	Endereço do protocolo IP atribuído a uma interface virtual do roteador.
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.
Isolamento lógico	Técnica que permite o isolamento entre redes virtuais de telecomunicações que compartilham recursos físicos, de forma a manter a confidencialidade e a integridade das informações em cada rede virtual, quando do transporte de informações.
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.
JMS *(Java Message Service)*	Interface que suporta protocolos de comunicação baseados em mensagens, inclusive XML.
Jumbo Frames	Quadros Ethernet com mais de 1.518 bytes.
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.

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.
Middleware	Programa de computador que faz a mediação entre outros programas, executando serviços de identificação, autenticação, autorização, gerência da entrega de mensagens, dentre outros.
MOS (*Mean Opinion Score*)	Pontuação de 1 a 5, definida pelo ITU-T na recomendação P.800, para representar a qualidade da transmissão de um sinal de voz. Valores maiores representam melhor qualidade de transmissão.
MPLS (*Multi Protocol Label Switching)*	Tecnologia de encaminhamento de pacotes de dados.
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.
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.
OAM	*Operations Administration and Maintenance* Conjunto de atividades, processos e ferramentas envolvidos na administração, operação e manutenção de uma rede de telecomunicações.
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.
OSPFv2 (*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.
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.
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.
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*)	Ponto de Presença
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.
Projeto físico	Projeto que documenta e detalha o ambiente físico (infraestrutura) de implantação de recurso de rede de telecomunicações ou a ela agregado.
Projeto lógico	Projeto que documenta e detalha o ambiente lógico (configuração) de conectividade de recurso de rede de telecomunicações ou a ela agregado.
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.
PSAI	Preço do Serviço de Acesso à Internet.
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.
RTSP (*Real Time Streaming Protocol*)	Protocolo de rede para controle da transmissão de conteúdo multimídia, definido pelo IETF na RFC 2326. Oferece funcionalidades para controlar o fluxo de dados transportados pelo protocolo RTP.
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 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.
SEG (Sistema Especialista 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).
SOAP *(Simple Object Access Protocol)*	Protocolo utilizado para troca de informações estruturadas baseadas em XML que utiliza como protocolo de transporte o HTTP. É utilizado como protocolo para implementação de *Web Services*.
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.
STI (Serviço de Trânsito Internet)	Acrônimo definido no escopo deste documento.
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.
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.
UP (Unidade Provedora)	Acrônimo definido no escopo deste documento.
UPG (Unidade Provedora de Gerenciamento)	Acrônimo definido no escopo deste documento.
UPI (Unidade Provedora de Internet)	Acrônimo definido no escopo deste documento.
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.
VoIP (*Voice over Internet Protocol)*	Voz sobre IP é uma tecnologia que permite que uma conversação de voz seja transportada sobre uma rede de dados IP.

VPN (*Virtual Private Network*)	Rede virtual privada que propicia o tráfego de informações de forma segura, através do uso da técnica de tunelamento com ou sem criptografia.
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 e realiza o roteamento a cada momento.
WAN (*Wide Area Network*)	Rede de telecomunicações com abrangência em uma grande área geográfica. Tipicamente é criada e mantida por provedores de telecomunicações.
White lists	Listas de endereços permitidos para recebimento ou envio de mensagens eletrônicas, aplicadas em ferramenta que disciplina o tráfego de mensagens, atendendo a critérios de segurança.
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.
XSD *(XML Schema Definition)*	Arquivo XML utilizado para definição de regras de validação ("esquemas") de um outro arquivo em formato XML.