ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. REQUISITOS DOOBJETO:

Contratação de empresa para prestação de serviços de acesso à internet, mediante ativação de circuito de comunicação de dados, com locação de equipamentos e suporte técnico e serviço de proteção contra-ataques distribuídos de negação de serviço (Distributed Denial of Service – DDoS), conforme as especificações e as condições estabelecidas neste documento, observado o quadro abaixo:

ITEM	DESCRIÇÃO	UN	QTDE.
I	Serviço mensal de acesso à *internet* de **1Gbps**, por meio de infraestrutura de fibra ópticae serviço de proteção contra-ataques distribuídos de negação de serviçode (Distributed Denial of Service – DDoS).	Mês	20
II	Serviço mensal de acesso à *internet* de **1Gbps**, por meio de infraestrutura de fibra óptica e serviço de proteção contra-ataques distribuídos de negação de serviço de (Distributed Denial of Service – DDoS).	Mês	20

1.1. **Características Gerais**:

1.1.1. Serão contratados dois serviços de acesso à internet de características idênticas, porém deverão ser providos por operadoras diferentes de telecomunicação.

1.1.2. Os serviços serão adquiridos em itens separados.

1.1.3. A empresa vencedora do primeiro item, não pode ser a vencedora do segundo item.

1.1.4. O CONTRANTE é um sistema autônomo (AS) e é proprietária de um bloco cidr/23 - 512 endereços IPs válidos e contíguos.

1.1.5. O serviço internet deverá ser disponibilizado em protocolo IP pela CONTRATADA com a utilização e publicação do bloco cidr/23 da CONTRATANTE.

1.1.6. A CONTRATANTE informará à CONTRATADA o ASN e o prefixo correspondente.

1.2. **Características de Independência da Infraestrutura de Comunicação:**

1.2.1. A operadora de telecomunicações vencedora do processo licitatório deverá dispor dos recursos necessários em seus roteadores backbone para prover o serviço de balanceamento de tráfego com a outra operadora atuante.

1.2.2. Dada a finalidade da contratação, a CONTRATADA deverá disponibilizar acesso à Internet em infraestrutura de comunicação ou backbone próprios, ou através de subcontratação de pelo menos 3 (três)

provedores distintos e que sejam Autonomous System (AS), sem prejuízo da velocidade contratada.

1.2.3. O acesso provido deve ser participante do backbone da contratada com conexão a outros provedores de acesso de abrangência nacional e internacional.

1.2.4. É permitida a subcontratação, salvo à última milha do circuito fornecido, ou seja, o enlace entre a CONTRATADA e o CONTRATANTE.

1.2.5. A CONTRATADA deverá fornecer o acesso exclusivamente através de fibra ótica instalada diretamente no CPD do CONTRATANTE.

1.2.6. A CONTRATADA deverá fornecer link único, não sendo aceito fornecimento de diversos links de menor velocidade com balanceamento entre eles.

1.3. **Especificações e características técnicas:**

1.3.1. A CONTRATADA deve considerar a velocidade definida como real, ou seja, deve entregar efetivamente velocidade de acesso na porta do roteador a **1Gbps**, no mínimo, retirando a porcentagem de overhead adicional da tecnologia a ser utilizada.

1.3.2. No decorrer da vigência do contrato de prestação de serviço poderá ocorrer, por solicitação do CONTRATANTE, aumento ou redução de velocidade de acesso, observando-se o limite de 25% (vinte e cinco por cento).

1.3.3. A CONTRATADA deve disponibilizar circuito dedicado durante 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, composto de um canal direto com a Internet de uso ilimitado, com conexões diretas do Brasil aos backbones da Internet (nacionais e internacionais).

1.3.4. A CONTRATADA deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos e recursos que forem necessários (roteadores, bastidores, meios de transmissão, cabeamento, dentre outros) para o provimento do serviço Internet para o CONTRATANTE.

1.3.5. Os equipamentos serão de propriedade da CONTRATADA que deverá ser responsável pelo suporte técnico e atualizações dos mesmos, cumprindo com os tempos de atendimento estabelecidos.

1.3.6. A CONTRATADA deverá permitir acesso a console dos roteadores, pelo CONTRATANTE, com permissão de escrita, através de usuário e senha específicos. Assim, a equipe técnica do CONTRATANTE poderá

colaborar na criação de configuração específica ao balanceamento de tráfego, caracterizados por ajustes de policiamento de tráfego e pesos na interface, com intuito de filtrar e balancear o roteamento de entrada a faixas específicas dedomínios da internet, ainda que toda a responsabilidade de configuração seja da CONTRATADA.

1.4. **Características dos roteadores:**

1.4.1. Os equipamentos a serem disponibilizados pela CONTRATADA para prover o serviço deverão ser instalados no CPD do CONTRATANTE.

1.4.2. Deverão ser “non-blocking”, com saída para a rede da contratada em porta ethernet 1000/Mbps – IEEE 802.3ab.

1.4.3. Os roteadores deverão também atender aos seguintes requisitos mínimos:

1.4.3.1. Suportar capacidade de filtros de pacotes (por protocolo, endereço IP de origem, endereço IP de destino, porta de UDP/TCP de origem, porta de UDP/TCP de destino);

1.4.3.2. Suportar classificação de tráfego de acordo com diversos critérios (interface, IP origem/destino, portas TCP/UDP, MAC e serviço), em cada interface física e lógica (sub- interface);

1.4.3.3. Suporte aos seguintes protocolos de conectividade à Internet: ATM, Fast Ethernet, MPLS, BGPv4, MBGP;

1.4.3.4. Deve possuir software de roteamento com suporte a compressão de dados;

1.4.3.5. Deverá suportar os protocolos de roteamento (RIPv1/v2, OSPFv3, IGRP, EIGRP, BGPv4, MBGP);

1.4.3.6. Deverá possuir processador interno com arquitetura RISC;

1.4.3.7. Suporte a NAT (RFC1631) e suporte a VLANS"s (IEEE 802.1Q) com roteamento entre elas;

1.4.3.8. Suportar RFC791 (Internet Protocol);

1.4.3.9. Possuir no mínimo capacidade de processamento de 820 mil pacotes por segundo (PPS).

1.4.3.10. O roteador deverá possuir, no mínimo, duas interfaces Fast Ethernet para configuração de rede LAN.

1.4.4. Todos os roteadores devem ser dimensionados para operar com carga máxima de CPU e memória de 80%, desde que satisfeita a condição de tráfego igual ou inferior à capacidade da porta WAN do roteador, calculada a média de no máximo 5 minutos. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou

memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para o CONTRATANTE.

1.4.4.1. A CONTRATADA terá um prazo 10 (dez) dias corridos para substituição ou atualização do equipamento, após notificação do CONTRATANTE em caso de problemas que limitem o funcionamento do equipamento.

1.4.4.2. A CONTRATADA terá um prazo 12 (doze) horas para substituição ou atualização do equipamento, após notificação do CONTRATANTE em caso de inoperatividade do equipamento.

1.4.4.3. O prazo de execução mencionado nos itens anteriores poderá ser prorrogado por igual período, a critério do CONTRATANTE, mediante justificativa da CONTRATADA.

1.4.4.4. Caso o problema não seja solucionado com atualização do equipamento, este deverá ser obrigatoriamente substituído por equipamento que atenda à demanda do serviço.

1.4.5. Todas as atualizações e correções (patches) de softwares, necessárias para o cumprimento dos requisitos exigidos neste documento de Referência, deverão ser realizadas sem ônus adicionais para o CONTRATANTE e sempre comunicadas previamente.

1.4.6. A CONTRATADA deverá habilitar nos roteadores o protocolo SNMP, disponibilizando nestes uma comunidade SNMP com acesso de leitura e permitir a solicitação de configuração de traps específicos pelo CONTRATANTE.

1.5. **Abertura e Acompanhamento de Chamados:**

1.5.1. O CONTRATANTE poderá realizar a abertura de chamados técnicos e solicitações de serviços para reparo do serviço Internet. A abertura destes chamados poderá acontecer diretamente na Central de Atendimento;

1.5.2. A Central de Atendimento deverá ser acessada por um número único nacional não tarifado (0800) ou número fixo local, exclusivo para o CONTRATANTE ou corporativo com chave de acesso exclusiva, limitando o redirecionamento da ligação para área de abertura de chamados apenas 1 (uma) vez. O CONTRATANTE não poderá esperar por mais de 60 (sessenta) segundos em linha para ser atendida, conforme legislação brasileira;

1.5.3. A CONTRATADA não poderá condicionar a abertura do chamado ao fornecimento de informações, salvo a designação do circuito da

CONTRATANTE;

1.5.4. A CONTRATADA poderá disponibilizar, complementarmente, Portal de Atendimento em domínio público na internet para abertura de chamado, disponibilizando interface com campos para preenchimento da designação do circuito, para informações adicionais (com intuito de detalhar o problema enfrentado), e campo contendo o endereço de email do solicitante para recebimento do ticket de abertura do chamado.

1.5.5. A CONTRATADA deve fornecer número de protocolo após a abertura de chamado, considerando quaisquer das modalidades de abertura.

1.5.6. A Central de Atendimento deve estar à disposição do CONTRATANTE para recebimento de reclamações e solicitações de serviços no período de 24 horas por dia, 7 dias por semana, todos os dias do ano.

1.5.7. As informações relativas aos chamados deverão ser atualizadas automaticamente sempre que houver alguma alteração em sua situação. O tipo de informação acerca do chamado deve obedecer: a Identificação do chamado (Id), Identificação do circuito e acesso, data e hora da abertura, Tipo da Ocorrência (indisponibilidade e retardo e taxa de erro e taxa de perda); No fechamento do chamado: Identificação do chamado (Id), Data e hora do fechamento, Indicativo de procedência e improcedência; Em pendência: Identificação do chamado (Id), Data e hora de início, Data e Hora de fim.

1.5.8. Os registros dos chamados deverão conter todas as informações relativas ao chamado aberto, como tempo de início e fim de atendimento, identificação do elemento (equipamento, enlace ou serviço) afetado, nome, fone e e-mail do contato no CONTRATANTE que foi posicionado acerca do reparo e restabelecimento do serviço, descrição detalhada da resolução do chamado com um código associado e responsabilidades.

1.5.9. O acompanhamento on-line da resolução de chamados pela CONTRATANTE deverá ser feito através do sistema de atendimento.

1.6. **Monitoramento do Serviço:**

1.6.1. A CONTRATADA deve disponibilizar informações sobre os serviços de acesso à internet por meio de um portal de monitoramento, com acesso restrito ao CONTRATANTE, por meio de usuário e senha a ser fornecido, contendo estatísticas de desempenho e de disponibilidade do acesso para os últimos 6 (seis) meses, no mínimo.

1.6.2. O portal de monitoramento deve permitir que o CONTRATANTE realize consultas, bem como visualize relatórios com dados de desempenho dos

serviços contratados. Os relatórios devem disponibilizar, pelo menos, as seguintes informações:

1.6.2.1. Disponibilidade do serviço de internet;

1.6.2.2. Dados do tráfego do circuito contratado, com suas séries históricas, fornecendo subsídios para analisar o desempenho e as tendências de aproveitamento do link.

1.6.2.3. Informações da banda utilizada e do volume de tráfego.

1.6.2.4. Retardo da rede;

1.6.2.5. Perda de pacotes;

1.6.2.6. Acompanhamento dos Chamados contendo todas as informações relativas ao chamado como data/hora de abertura, data/hora conclusão, identificação do elemento (circuito ou equipamento), descrição detalhada do chamado.

1.7. **Serviço de proteção contra-ataques de negação de serviço (DistributedDenialof Service-DDoS):**

1.7.1. **Características Gerais:**

1.7.1.1. 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.

1.7.1.2. Suportar 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.

1.7.1.3. Prover informações de origem de ataque dos países, ranges de IP's e características do tipo de ataque.

1.7.1.4. Serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação

1.7.1.5. Capacidade 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:

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

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

1.7.1.5.3. Realizar autenticação de conexão TCP, quando do recebimento de pacotes syn;

1.7.1.5.4. Limitar o número de conexões TCP simultâneas de um mesmo host;

1.7.1.5.5. Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

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

1.7.1.5.7. Ataques denominados de "Comand-and-Control", Point ofSale Malware, Remote Access Trojans RAT's via feed atualizado diariamente;

1.7.1.5.8. Ataques à camada de aplicação, incluindo protocolos HTTP e DNS Volumetricos;

1.7.1.5.9. Bloqueio de query de DNS, resposta de query de DNS baseado em domínio pré-cadastrado para autenticação e checagem de flag de recursão DNS;

1.7.1.5.10. DNS BlackList; RegEx para registros específicos ou "flags de recursão. Possuir mecanismos de quando bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente;

1.7.1.5.11. Autenticação em query DNS por requisição em TCP;

1.7.1.5.12. Autenticação em JavaScript e Redirect para HTTP;

1.7.1.5.13. Adicionar expressão regular de "payload" em black-list;

1.7.1.5.14. Prevenir que hosts válidos sejam adicionados a black-list por engano.

1.7.1.5.15. Capacidade de interagir automaticamente ou manualmente com solução "on-premisse" (appliance) localizado in-site no datacenter do cliente; No caso, o appliance quando detectar um ataque DDoS pode automaticamente ou manualmente (conforme SLA) requisitar mitigação na nuvem, para apenas o tráfego atacado, e não todo o tráfego do datacenter.

1.7.1.5.16. A sinalização entre datacenter e nuvem deve ser capaz de ocorrer em qualquer protocolo protegido (TCP/UDP/ICMP/DNS/HTTP), podendo ser ativada por qualquer uma das contra-medidas acima.

1.7.1.5.17. Manter lista dinâmica de endereços IP bloqueados,

retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro.

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

1.7.1.5.19. 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.

1.7.1.5.20. A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e quantidade ilimitada de eventos de ataque ao longo da vigência contratual;

1.8. **Características da Infraestrutura de Suporte Anti-DDoS:**

1.8.1.1. Possuir no mínimo 2 Centros Operacionais de Segurança (ou SOC – *Security Operations Center*) localizados 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.

1.8.1.2. Possuir3centros de limpeza nacional, cada um com capacidade de mitigação de 60Gbps e 3 centros de limpeza internacionais com capacidade de mitigação de 500Gbps.

1.8.1.3. Evitar saturação da banda de Internet em caso de ataques de negação de serviço (DistributedDenialof Service – DDoS) com capacidade de mitigar 10 Gbps.

1.8.1.4. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como *Remote Triggered Black Hole*.

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

1.8.1.6. O bloqueio de ataques DOS e DDOS não são realizados por

ACLs em roteadores de borda.

1.8.1.7. A mitigação de ataques DDOS é iniciada em até 15 minutos da emissão do alerta.

1.8.1.8. Deve disponibilizar um portal onde a contratante tem acesso online aos tipos de ataques sofridos e o tamanho destes ataques categorizados por severidade (Ex: baixo, Médio, Alto).

1.8.1.9. A mitigação dos ataques é realizada dentro do Brasil, sem encaminhamento do tráfego para limpeza fora do território brasileiro.

1.8.1.10. Em momentos de ataques DOS e DDOS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de tuneis GRE (GenericRoutingEncapsulation), configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante e/ou utilização da técnica VRF Clean (Virtual RoutingandForwarding) via BGP Full;

1.9. **Requisitos de projeto e de implementação do serviço de Anti-DDoS:**

1.9.1. A CONTRATADA deverá fornecer o conjunto de manuais técnicos oficiais, elaborados pelo fabricante de cada equipamento, contendo todas as informações sobre o produto como instruções para instalação, configuração, operação e gerenciamento. Os manuais técnicos do fabricante devem estar escritos em português ou inglês e podem ser fornecidos em mídia eletrônica (CD-ROM ou DVD).

1.9.2. A CONTRATADA deverá planejar a execução do projeto de implantação. Deverá ser elaborada uma documentação completa onde deverá constar dentre outras informações: mapa da rede, mapa do perímetro, telas de instalação/configuração do produto, outras informações relevantes para administração do ambiente.

1.9.3. O “Plano de Implantação” deverá contemplar, no mínimo:

1.9.3.1. Cronograma de instalação, configuração, testes e ativação e;

1.9.3.2. Detalhamento dos testes a serem realizados quando concluídas as instalações e configurações dos equipamentos. Deverá ser apresentado um documento ao final da realização dos testes com dados informativos que comprovem o bom funcionamento dos componentes pertinentes à solução.

1.9.3.3. Eventuais desconformidades entre os procedimentos executados e os documentos fornecidos serão comunicados à CONTRATADA para que providencie os ajustes necessários.

1.9.4. A “Documentação Técnica da Solução” deverá contemplar, no mínimo, o projeto executivo contendo o conjunto dos elementos necessários e suficientes à implantação dos equipamentos ou execução dos serviços, inclusive desenhos das topologias físicas e lógicas, condições de alimentação, aterramento e ambientação (iluminação, temperatura, umidade, etc.) e especificações físicas, elétricas, operacionais e suas limitações.

2. EXECUÇÃO DOS SERVIÇOS:

2.1. A CONTRATADA deverá entregar os serviços de acesso à internet totalmente operacional, com a totalidade da banda de comunicação contratada e os níveis de serviços exigidos, em até 60 (sessenta) dias corridos, após a emissão da Ordem de Fornecimento.

2.2. Todo o processo de instalação e implantação dos serviços será acompanhado e supervisionado por unidade técnica do CONTRATANTE, à qual a CONTRATADA deverá se reportar antes de qualquer ação e decisão referente à implantação da solução em tela.

2.3. Todos os custos com realização de canalização, entradas, tubulações, entre outros, compreendendo todo o percurso de infraestrutura de cabeamento, desde os centros de roteamento das contratadas até o equipamento roteador a ser instalado no CPD do CONTRATANTE, deverão ser realizados sem ônus adicional ao CONTRATANTE.

2.4. A tecnologia de acesso a ser implantada no CPD do CONTRATANTE deverá utilizar materiais não susceptíveis a propagação de fogo, sobretudo aqueles para uso interno.

2.5. Após a conclusão da presente etapa de instalação dos serviços, a CONTRATADA deverá apresentar como condição para recebimento provisório do objeto documentação técnica da solução (as-built), contendo: topologia física e lógica da rede, descrição de equipamentos e circuitos de comunicação de dados, descrição dos níveis mínimos de serviços contratados, dados para acesso ao portal de monitoramento dos serviços e dados para abertura de chamados de suporte técnico.

2.6. Uma vez recebido o objeto, a CONTRATADA deverá encaminhar mensalmente CONTRATANTE, para fins de atestação e pagamento, fatura e relatório de prestação dos serviços, contendo:

2.6.1. Nota fiscal dos serviços com período de faturamento;

2.6.2. Aferição dos Níveis Mínimos de Serviço (NMS) para o período faturado,

incluindo indisponibilidades de serviço, detalhados por dia, período e causas, bem como cálculo dos índices IDM, PET e PDP, de acordo com as condições apresentados no item níveis mínimos de serviço (NMS).

2.6.3. Relação dos chamados de suporte técnico abertos e fechados, com identificação do chamado, problema relatado e solução adotada, no período faturado.

2.7. **Níveis Mínimos de Serviço:**

2.7.1. Os serviços de acesso à internet deverão estar operacionais em um regime 24x7 (24 horas por dia, 7 dias por semana).

2.7.2. O Limiar de qualidade (LQIDM) para o Índice de Disponibilidade Mensal (IDM) é de 99,5% (noventa e nove e meio por cento).

2.7.3. O Índice de Disponibilidade Mensal (IDM) deverá ser calculado mensalmente por meio da seguinte fórmula: **IDM = [(Tm – Ti)** / **Tm], onde**:

2.7.3.1. **IDM** é o Índice de Disponibilidade Mensal do serviço;

2.7.3.2. **Tm** é o tempo total mensal de operação, em minutos, no mês de faturamento;

2.7.3.3. **Ti** é o somatório dos períodos de indisponibilidade do serviço, em minutos, no mês de faturamento.

2.7.4. No caso de inoperância reincidente num período inferior a 3 (três) horas, contado a partir do restabelecimento do serviço Internet da última inoperância, considerar-se-á como tempo de indisponibilidade do serviço o início da primeira inoperância até o final da última inoperância, quando o serviço estiver totalmente operacional.

2.7.5. Além do Índice de Disponibilidade Mensal (IDM), deverá ser aferida métrica correspondente ao Percentual de Pacotes com Erros de Transmissão (PET), que, uma vez superada, deverá ser considerada como período de indisponibilidade do serviço:

2.7.5.1. A métrica Percentual de Pacotes com Erros de Transmissão (PET) se refere à relação existente entre a quantidade de pacotes transmitidos/recebidos com erro e quantidade de pacotes transmitidos/recebidos, em cada acesso contratado;

2.7.5.2. Para medição desse percentual, em todos os períodos do dia, a contratada deverá realizar aferições do percentual de pacotes com erros para cada enlace integrante do acesso contratado, através da

monitoração das interfaces WAN contratadas. As aferições deverão ser feitas em cada interface, por sentido de tráfego (inbound/outbound), apresentadas em valores referentes a cada intervalo de 5 (cinco) minutos, sendo o limite aceitável de erros de até 1,0% (um por cento) do total de pacotes trafegados em cada interface e sentido;

2.7.5.3. Para cada valor da taxa de erros por pacotes acima do limite permitido no subitem anterior, deverá ser computado período de indisponibilidade de 5 (cinco) minutos na fórmula do IDM.

2.7.6. Além dos dois indicadores anteriores, deverá ser aferida métrica correspondente ao Percentual de Descarte de Pacotes (PDP), que, uma vez superada, deverá ser considerada como período de indisponibilidade de serviço:

2.7.6.1. A métrica Percentual de Descarte de Pacotes (PDP) se refere à relação existente entre a quantidade de pacotes transmitidos/recebidos descartada para cada pacote transmitido/recebido, em cada acesso contratado;

2.7.6.2. Em todos os períodos do dia, a contratada deverá realizar aferições do percentual de descarte de pacotes para cada enlace integrante do acesso contratado, através da monitoração das interfaces dos roteadores de acesso e do backbone participante do enlace. As aferições serão feitas em cada interface, por sentido (inbound/outbound), apresentadas em valores referentes a cada intervalo de 5 (cinco) minutos, sendo o limite aceitável de descartes de até 1,0% (um por cento) do total de pacotes trafegados em cada interface e sentido;

2.7.7. Serão desconsiderados os valores que ultrapassem este limite quando a contratada comprovar a utilização superior a 80% (oitenta por cento) da velocidade do respectivo enlace no mesmo intervalo;

2.7.8. Sempre que o percentual de descarte de pacotes for superior ao limite máximo permitido, será computado período de indisponibilidade de 5 (cinco) minutos na fórmula do IDM.

2.8. Sempre que duas aferições de PET e PDP estiverem acima do limite máximo permitido, desde que elas ocorram em uma mesma porta de comunicação e durantes os mesmos intervalos de tempo de um mesmo dia, somente deverá ser computado o período de indisponibilidade associada a uma delas.

2.9. Indisponibilidades serão consideradas quando ocorrer qualquer tipo de

problema nos equipamentos, links de comunicação ou backbone da contratada, que impeça a transmissão ou recepção de pacotes nos serviços de acesso à Internet ou impactem no seu desempenho, mesmo que parcialmente (como por exemplo, não acessar sites internacionais).

2.10. Os períodos de manutenção, inclusive os de ordem preventiva, provocadas pela CONTRATADA serão considerados como indisponibilidade.

2.11. A violação de qualquer nível de serviço só poderá ser desconsiderada pelo CONTRATANTE quando for decorrente de falha em algum equipamento de propriedade do CONTRATANTE, decorrente de procedimentos operacionais por parte do CONTRATANTE, por qualquer equipamento da contratada que não possa ser corrigida por inacessibilidade causada pelo CONTRATANTE ou eventuais interrupções programadas, desde que previamente autorizadas pelo CONTRATANTE.

2.12. A CONTRATADA deverá calcular o total de desconto a ser aplicado no valor total mensal do serviço, o qual será considerado como glosa, de acordo com a seguinte fórmula:

2.12.1. **Vd = Cm * (1 - IDM), onde:**

2.12.1.1. Vd é o valor do desconto;

2.12.1.2. Cm é o custo mensal dos serviços prestados;

2.12.1.3. DM é o índice de disponibilidade mensal dos serviços, calculado no item 2.7– Níveis Mínimos de Serviço, observadas as aferições de PET e PDP;.