TERMO DE REFERÊNCIA

1. **DESCRIÇÃO DO OBJETO** (Art. 18, §3º, I)

Contratação de conexão IP dedicada redundante com velocidade de 200Mbps com serviço Anti-DDoS, para fins de interligação do Datacenter da Secretaria de Informática do TJPA localizado no Edifício Sede de Belém/PA à Internet com solução para gerenciamento pró-ativo de falhas.

2. **FUNDAMENTAÇÃO** (Art. 18, §3º, II)

a) Motivação da contratação (Art. 18, §3º, II, a)

O TJPA possui apenas um circuito de internet dedicado à Internet, de velocidade de 200Mbps, instalado no Datacenter do Fórum Cível da capital, integrante do contrato 020/2013/TJPA. Por este único circuito, todas as unidades judiciárias e administrativas acessam à Internet, assim como o TJPA provê acesso aos sistemas jurisdicionais à sociedade, tais como Libra, PJe, mensagem eletrônica (e-mail), Portal Externo e outros. A indisponibilidade neste único circuito de internet, também torna todos os serviços inoperantes, gerando grandes prejuízos financeiros e à imagem do sistema judiciário do Estado. A infraestrutura de redes de comunicação de dados com a rede mundial de computadores é um recurso imprescindível para a disponibilização de serviços e informações em larga escala, para o público interno e externo do Poder Judiciário do Estado do Pará.

b) Objetivos a serem alcançados (Art. 18, §3º, II, b)

Com a crescente demanda por serviços e aumento do volume de informações transacionadas, a presente contratação visa implantar um circuito de Internet, de operadora distinta da atual prestadora do circuito principal, com a mesma capacidade do atual, que seja redundante e capaz de suportar toda a capacidade de tráfego do circuito principal, em caso de indisponibilidade do mesmo. A instalação ocorrerá em local distinto do circuito atual com objetivo de garantir a segurança física do circuito. Ao implantar o circuito redundante, haverá o balanceamento de carga do tráfego para otimizar o desempenho da rede.

c) Benefícios diretos e indiretos (Art. 18, §3º, II, c)

Quanto maior a demanda e criticidade de acesos aos serviços de Internet, há necessidade de garantir maior disponibilidade do acesso à rede mundial de computadores, fato que será garantido com a dualidade dos circuitos. Será implementado o protocolo BGP entre os circuitos de internet (principal e redundante) que garantirá a comutação automática dos acessos à Internet, mitigando o tempo de indisponibilidade, praticamente imperceptível ao usuário final, melhorando o grau de satisfação na prestação do serviço. O circuito será implantado por meio de fibra óptica, com topologia em anel redundante em dupla abordagem na entrada do Datacenter do Ed. Sede, onde o tráfego do prédio sairá prioritariamente pelo circuito instalado no local.

Será adicionado o serviço proativo de segurança Anti-DDoS no circuito de internet com objetivo de proteger a rede deste Tribunal contra ataques distribuídos, conforme descrito no ANEXO D – SERVIÇO ANTI-DDoS.

d) Alinhamento entre a contratação e o Planejamento Estratégico (Art. 18, §3º, II, d)

O macro desafio do Planejamento Estratégico do Poder Judiciário do Pará 2015/2020 intitula a “Melhoria da Infraestrutura e Governança de TIC”, explicitando a necessidade de garantir uma rede eficiente de transmissão e troca de dados, célere e confiável, entre as unidades judiciárias e administrativas da Justiça Paraense, em todos os níveis.

O Plano de Gestão da Presidência – Biênio 2015/2017 contempla a iniciativa estratégica 11.1 descrita como a “Modernização da Infraestrutura de TIC”, Ação 11.1.2 que diz respeito a “Melhorar os serviços de comunicação de dados”, a qual está inserida a Etapa 11.1.2.3 “Contratação e implantação dos circuitos de internet”.

e) Referência aos Estudos Preliminares da STIC (Art. 18, §3º, II, e)

Conforme documento dos Estudos Preliminares elaborados para esta contratação, anexado no processo PA-PRO-2016/02005 no sistema SIGADOC deste Tribunal, o TJPA não dispõe de infraestrutura própria dedicada de comunicação de dados para a troca de informações com a rede mundial de computadores. Por conseguinte, necessita contratar infraestrutura de comunicação junto a operadoras de telecomunicações para o atendimento das suas demandas.

A partir da massificação do uso de sistemas on-line, pesquisas, prestação de serviços e troca de mensagens eletrônicas, criou-se uma dependência no circuito de Internet. A conexão permite que o indivíduo interaja diretamente com as organizações externas, promovendo a desintermediação no acesso a um serviço, o qual pode ser obtido no momento que necessitar, devendo estar o máximo de tempo disponível, impactando diretamente na relação do TJPA com o seu público alvo: o cidadão.

A Internet tornou-se uma ferramenta fundamental, necessária e básica para a sobrevivência do ambiente corporativo, visto que as informações fornecidas e recebidas pelos sistemas on-line trafegam por este circuito de dados.

A necessidade de mantê-lo sempre disponível é mandatória para prestação dos serviços jurisdicionais, cujo os serviços agregados de segurança mitigam a probabilidade de indisponibilidade.

Em contrapartida, o cidadão está cada vez mais exigente e pouco tolerante a falhas e indisponibilidades. Com isso, a alta disponibilidade, segurança das informações trafegadas e o bom desempenho da arquitetura de TIC são vitais para muitos processos de negócio.

f) Relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados (Art. 18, §3º, II, f)

A abrangência do serviço compreende em 01 circuito de Internet redundante que será instalado no Datacenter do Ed. Sede do TJPA.

Id	Demanda Prevista	QTDE.	Quantidade a ser contratada
1	Circuito de Internet + Serviço Anti-DDoS	01	50% (2016) 50% (2017)

g) Análise de mercado de TIC com o levantamento de soluções disponíveis (Art. 18, §3º, II, g)

A solução de mercado que mais se assemelha à atual solução implantada no TJPA é a conexão via operadora de telefonia (Velox, NET, Virtua, GVT e outros). Porém, tais tipos de conexões são viabilizados por meio de comunicação compartilhada, não garantindo a velocidade real que é contratada, gerando insatisfação na qualidade do desempenho do serviço prestado. O tempo de reparo para uma eventual indisponibilidade é elevado ou inexistente, deixando o cliente ficar submetido ao tempo de reparo que a empresa informar, sem o poder de punições e multas pela não prestação do serviço.

No Estado do Pará, apenas 02 operadoras possuem capacidade técnica e comercializam circuitos de Internet dedicados à Internet, sendo a CLARO S/A e a TELEMAR NORTE LESTE S/A (OI). Como o TJPA já possui celebrado o contrato 020/2013/TJPA firmado com a empresa CLARO S/A, a opção é realizar a contratação com a empresa OI, assim garantindo a conectividade redundante com operadoras distintas. Os provedores de Internet existentes em Belém, local onde será instalado o circuito redundante, subcontratam uma das duas operadoras supracitadas e comercializam para o usuário final com valores superiores, comparado com a contratação direta junto a operadora. Este instrumento visa a contratação direta com a operadora, sem intermediários.

O serviço de segurança Anti-DDoS é um serviço contra ataques distribuídos, onde os atacantes originam tráfegos de diversos locais distintos (cidades, estados e países) com objetivo efetuarem milhares de requisições simultaneamente, até congestionar e paralisar o circuito de Internet pelo excesso de requisições. A única forma de evitar este tipo de ataque é o serviço Anti-DDoS que a operadora bloqueia pró-ativamente nos equipamentos de borda (backbone) os requisitantes indevidos.

O acesso à Internet será via cabo de fibra óptica, com dupla abordagem de entrada no Datacenter do ed. Sede, oferecendo sustentação ao AS – *Autonomous System* (Sistema Autônomo) do TJPA, sendo essa solução e meio de transmissão o mais avançado do mercado para garantir o melhor desempenho e disponibilidade da rede. Neste circuito será implementado o serviço de proteção de ataques distribuídos (DDoS - *Distributed Denial of Service*) por requisições originados em ambientes externos do Tribunal, tornando a infraestrutura segura e menos vulnerável a este tipo de ataque. O serviço proativo Anti-DDoS é um serviço contra ataques distribuídos, onde os atacantes originam tráfegos de diversos locais distintos (cidades, estados e países) com objetivo efetuarem milhares de requisições simultaneamente, até congestionar e paralisar o circuito de Internet pelo excesso de requisições. A única forma de evitar este tipo de ataque é o serviço proativo de segurança Anti-DDoS da operadora que bloqueia ativamente nos equipamentos de borda (*backbone*) os requisitantes indevidos.

A solução proposta visa garantir a padronização, segurança, disponibilidade e interoperabilidade de comunicação entre a rede do TJPA e a Internet.

Conforme o Item 1.2.2- Contratações Públicas Similares dos Estudos Preliminares, optou-se por contratar os serviços da operadora OI pela vantagem econômica, técnica e ser a única operadora de telecomunicações distinta do atual contrato que possui condições técnicas em ofertar o serviço demandado.

h) Natureza do objeto com a indicação dos elementos necessários para caracterizar o bem e/ou serviço a ser contratado (Art. 18, §3º, II, h)

Contratação de conexão IP dedicada redundante com velocidade de 200Mbps com serviço Anti-DDoS, para fins de interligação do Datacenter da Secretaria de Informática do TJPA localizado no Edifício Sede de Belém/PA à Internet com solução para gerenciamento pró-ativo de falhas.

i) Quanto ao parcelamento dos itens a serem contratados (Art. 18, §3º, II, i)

A solução proposta contratar de única empresa, não sendo possível que seja entregue por diferentes operadoras, portanto a definição do objeto deve resguardar a complexidade do mesmo, sem parcelamento do objeto.

j) Forma e critério de seleção do fornecedor com a indicação da modalidade e o tipo de licitação (Art. 18, §3º, II, j)

No Estado do Pará, apenas 02 operadoras possuem capacidade técnica e comercializam circuitos de internet dedicados à Internet com proteção contra ataques DDoS, sendo a CLARO S/A e a OI. Como o TJPA já possui celebrado o contrato 020/2013/TJPA firmado a empresa CLARO S/A, a opção é realizar a contratação com a empresa OI, pela contratação direta, por inexigibilidade.

k) Impacto ambiental decorrente da contratação (Art. 18, §3º, II, k)

Não haverá impacto ambiental, pois, trata-se de contratação cujo objeto é prestação de serviços de telecomunicações.

l) Conformidade técnica e legal do objeto com a indicação das normas técnicas e legais (Art. 18, §3º, II, l)

As normas e especificações técnicas estão descritas no ANEXO B – ESPECIFICAÇÃO TÉCNICA.

m) Obrigações contratuais da CONTRATADA (Art. 18, §3º, II, m)

A CONTRATADA deverá se responsabilizar pela operação e manutenção de toda rede;

A CONTRATADA deverá encarregar-se da aquisição dos equipamentos necessários à prestação do serviço e realizar todas as atividades necessárias para fornecer e entregar o objeto contratual.

Não será permitida a sublocação e a subcontratação de serviços em parte ou de modo global do objeto.

O TJPA poderá promover a alteração de localização do ponto contratado a qualquer momento, com a correspondente alteração contratual com a CONTRATADA, desde que haja viabilidade técnica.

Reparar ou substituir qualquer item do objeto contratual pertencente a CONTRATADA, sem ônus para o TJPA, visando atender a disponibilidade do serviço contratado.

Assumir inteira responsabilidade técnica e administrativa do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento.

Respeitar e obedecer às normas fixadas pela Administração do TJPA.

Assumir a responsabilidade pela boa execução e eficiência dos serviços prestados.

Prestar os serviços na forma ajustada, nos horários estabelecidos pelo TJPA, utilizando-se da melhor técnica recomendada para sua execução, exceto os serviços emergenciais.

Fazer-se representar, no local da prestação dos serviços, por preposto aceito pela Administração com a atribuição de coordenar e fiscalizar a execução dos serviços e o cumprimento das normas disciplinares, de segurança e legislação pertinentes.

Responsabilizar-se por qualquer dano ocorrido em decorrência da má realização dos serviços, desde que a responsabilidade lhe seja imputável.

Atender prontamente às chamadas e às determinações do representante da Administração do TJPA com vistas a corrigir defeitos observados na execução do serviço ou em operação.

Utilizar pessoal técnico devidamente identificado com crachás contendo nome, foto e cargo/função desempenhada nas dependências do TJPA.

O TJPA não aceitará, sob pena de nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, quaisquer que sejam independentemente de sua natureza.

O inadimplemento das obrigações da CONTRATADA, com referência aos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do contrato, não transfere à Administração do TJPA a responsabilidade por seu pagamento, nem poderá onerar o objeto deste Termo de Referência.

Serão de responsabilidade da CONTRATADA todas e quaisquer despesas decorrentes de sua atividade.

Responder, em relação aos seus empregados, por todas as despesas decorrentes da execução dos serviços, apresentando-os identificados com crachás da empresa, garantindo-lhes alimentação e transporte até o local dos serviços, porquanto não terão qualquer vínculo com o TJPA.

Responsabilizar-se pelos danos causados diretamente ao TJPA ou a terceiros, decorrentes de culpa ou dolo dos seus empregados ou preposto, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade à presença de fiscalização ou o acompanhamento dos serviços pelo TJPA.

Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos

serviços ou em conexão com eles, ainda que acontecido nas dependências do TJPA e no local que o circuito será instalado.

Assumir todos os encargos sobre demanda trabalhista, previdenciários, obrigações sociais previstas na legislação social e trabalhista em vigor, cível ou penal, relacionado a serviços, originariamente ou vinculados por prevenção, conexão ou contingência, além de assumir a responsabilidade pelos encargos fiscais e comerciais.

Quaisquer inadimplências referentes aos encargos estabelecidos nas condições anteriores não transferem a responsabilidade por seu pagamento o TJPA, nem poderão onerar o objeto do Termo de Referência, ou do contrato futuro, razão pela qual a CONTRATADA deverá renunciar expressamente, a qualquer vínculo de solidariedade, ativa ou passiva, para com o TJPA.

Não transferir, sob nenhum pretexto, no todo ou em parte qualquer responsabilidade constante do futuro contrato para terceiros, sejam engenheiros, projetistas, técnicos ou outros profissionais.

Dirimir quaisquer dúvidas existentes nos Projetos Executivos, quando da eventual execução das obras, perante o TJPA.

MUDANÇAS DE ENDEREÇO

No caso de mudanças de endereço em que estejam instalados equipamentos para prestação de serviços contratados, a CONTRATADA se compromete a fazer a mudança da instalação dos equipamentos para o novo endereço, dentro da mesma cidade ou município, no prazo de 45 (quarenta e cinco) dias consecutivos, a partir da expressa solicitação da mudança, desde que haja viabilidade técnica.

n) Obrigações contratuais da CONTRATANTE (Art. 18, §3º, II, m)

Alocar um Fiscal do Contrato, que será responsável pela avaliação do fornecimento e pelo atestado de cumprimento das obrigações do Contrato, consoante as disposições do artigo 67 da Lei n° 8.666/93.

Comunicar, por escrito, quaisquer instruções ou procedimentos sobre assuntos relacionados à execução do Contrato.

Notificar a CONTRATADA, por escrito, da aplicação de eventuais penalidades, nos termos do Contrato.

Permitir o livre trânsito dos funcionários da CONTRATADA, durante a execução dos serviços, pelas dependências do TJPA e correlato, desde que devidamente identificados através de crachás e uniformizados.

Prestar as informações e os esclarecimentos que sejam solicitados pelos empregados da CONTRATADA, sempre que necessário.

Tornar disponível as instalações e os equipamentos necessários à execução dos serviços, quando for o caso.

Autorizar por escrito o acesso de funcionários da CONTRATADA às dependências do TJPA e correlato em horários fora do expediente normal, desde que solicitado antecipadamente ou mediante justificativa fundamentada ou emergente.

Fiscalizar a prestação dos serviços, comunicando à CONTRATADA quaisquer fatos que necessitem sua imediata intervenção.

Responsabilizar-se pelas despesas com publicação necessárias a legitimação do Contrato e respectivos aditivos, se ocorrerem.

Solicitar o afastamento imediato do funcionário da CONTRATADA que se tornar inconveniente ou prejudicial à prestação do serviço contratado.

Dar à CONTRATADA as condições necessárias a regular execução do contrato.

Notificar a CONTRATADA por qualquer irregularidade na execução dos serviços.

Manter o controle da identificação dos empregados da CONTRATADA para acesso às dependências do TJPA e correlato.

3. DETALHAMENTO DO OBJETO (Art. 18, §3º, III)

Caberá a CONTRATADA todo o processo de planejamento, instalação, configuração e testes da solução que será interligada à infraestrutura de TIC da CONTRATANTE.

A instalação da solução deverá ser feita por profissionais devidamente qualificados e habilitados.

Todo o processo de instalação deverá ser documentado pela CONTRATADA sob a forma de relatório técnico, de modo que a Equipe Técnica da CONTRATANTE possa reproduzir a instalação e configuração da solução quando necessário.

A especificação técnica detalhada da solução está descrita no ANEXO B – ESPECIFICAÇÃO TÉCNICA.

3.1 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a)

Principais Papéis (Art. 18, § 3º, III, a,1)

A execução do(s) serviço(s) contratado(s) pressupõe a existência dos seguintes papéis e responsabilidades:

a) Patrocinador da Contratação: é o titular da área demandante, responsável por representar os interesses deste Tribunal no contexto desta contratação, pela aprovação da necessidade e, por fim, pela negociação das ações necessárias para que os objetivos sejam alcançados.

b) Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato.

c) Fiscal Demandante do Contrato: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução.

d) Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução.

e) Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

f) Preposto: funcionário representante da Contratada, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

Dinâmica da Execução (Art. 18, § 3º, III, a, 2)

A execução do objeto contratado(s) será realizada da seguinte forma:

a) Instalação do circuito: em até 45 (quarenta e cinco) dias corridos após a assinatura do contrato.

b) Configuração do circuito com BGP e AS: em até 15 (quinze) dias após a instalação do circuito.

c) Implantação do serviço proativo de segurança Anti-DDoS: será aplicado em até 15 (quinze) dias após a configuração do circuito com BGP e AS.

d) O recebimento definitivo do serviço dar-se-á após a conferência e aceitação do serviço com as especificações do objeto e cumprimento dos itens citados acima, sendo o prazo máximo total de até 75 (setenta e cinco) dias, prazos acumulados dos itens “a”, “b” e “c”.

Instrumentos de Solicitação do(s) Equipamento(s) e Serviço(s) (Art. 18, § 3º, III, a, 3)

Serão utilizados os seguintes instrumentos formais de solicitação do(s) serviço(s):

a) Comunicação por mensagem eletrônica (e-mail) e abertura de chamado via central 0800 para solicitação dos serviços.

Níveis de Serviços Exigidos (NSE) (Art. 18, § 3º, III, a, 4)

Serão utilizadas as seguintes formas de acompanhamento dos prazos:

a) Sistema interno de acompanhamento de chamados (CA SDM).

b) Deverá fornecer atendimento on-site, com substituição do equipamento defeituoso.

c) A Central de Assistência Técnica da CONTRATADA deverá permitir comunicação de inoperância através de telefone franqueado (ex: serviço 0800), com atendimento em língua portuguesa, e portal de monitoramento via web.

d) A Central de Assistência Técnica da CONTRATADA deverá estar à disposição da CONTRATANTE para recebimento de reclamações e esclarecimento de dúvidas e eventuais problemas no período de 24 horas por dia, 7 dias por semana, todos os dias do ano.

e) As reclamações feitas através da Central de Assistência Técnica da CONTRATADA deverão ser atendidas em no máximo 24h corridas depois de registrada.

f) Os serviços de atendimento técnico que necessitarem ser executados nas dependências da CONTRATANTE serão agendados com um funcionário da CONTRATANTE. Em caso de impedimento ao acesso de técnicos no local da ocorrência, que seja de responsabilidade da CONTRATANTE, o cômputo do período de indisponibilidade não considerará o período de tempo em que o técnico da CONTRATADA permanecer impedido de realizar a manutenção.

g) O início do atendimento deverá ser contado a partir da solicitação feita pela CONTRATANTE a Central de Serviços da CONTRATADA.

h) Entende-se por finalização do atendimento o momento a partir do qual o serviço estiver disponível e em perfeitas condições de funcionamento atendendo ao que está especificado como condições mínimas de uso.

i) Quando da solicitação de atendimento, via telefone ou e-mail, a CONTRATANTE fornecerá a CONTRATADA, as seguintes informações, para fins de abertura de chamado técnico:

   i) Código de identificação do cliente fornecido pela CONTRATADA

   ii) Descrição da anormalidade observada

   iii) Nome e telefones do responsável pela abertura do chamado

j) A CONTRATADA deverá fornecer no momento da abertura do chamado, um número de protocolo para acompanhamento do atendimento.

k) A CONTRATADA apresentará um relatório mensal de chamada para cada atendimento feito, tenha sido na sede da CONTRATANTE ou nas instalações da CONTRATADA, contendo data, hora de chamada, início e término do atendimento, identificação do solicitante, identificação do funcionário que atendeu o problema, identificação do problema e as medidas corretivas tomadas, esse relatório poderá ser apresentado em mídia impressa ou digital ou via web.

l) A CONTRATADA deverá apresentar, por ocasião da assinatura do contrato, todos os procedimentos e informações necessárias ao acionamento do seu serviço de suporte e solução de problemas.

m) A CONTRATADA não será responsável pela solução de problemas internos, a partir da rede interna da CONTRATANTE.

n) A CONTRATADA deverá garantir os seguintes índices de desempenho usados como referência para Garantia de Nível de Serviço do Circuito de Internet:

   i) Latência média: ≤ 180 ms para pacotes de 512Bytes
   ii) Perda de pacotes média: ≤ 1 %
   iii) Disponibilidade mensal do circuito: ≥ 99,35 %
   iv) Tempo máximo de reparo: Até 06 (seis) horas a contar a partir da abertura do chamado técnico na Central de Assistência Técnica da CONTRATADA.

o) Esses valores deverão estar disponíveis para consulta pela CONTRATANTE na página web da CONTRATADA no regime 24X7. Em caso de descumprimento desses valores ao longo de 7 (sete) dias, a CONTRATANTE terá o direto ao crédito automático de 01 (um) dia de serviço (equivalente a 1/30 do preço do valor mensal pago a CONTRATADA).

p) A CONTRATADA também deverá dispor de relatórios contendo as informações sobre o desempenho do núcleo da sua rede (rede da CONTRATADA) na forma de página web.

q) A realização de testes, ajustes e manutenção necessários à prestação do serviço devem ser agendadas e devidamente comunicados à CONTRATANTE com antecedência mínima de 03 (três) dias úteis.

r) Para o serviço de segurança Anti-DDoS, deverá seguir o seguinte SLA.

   a. Prazo para entrega de relatórios mensais: Até 5 (cinco) dias úteis.

   b. Prazo para entrega de relatórios de incidente (após mitigação do ataque): Até 2 (dois) dias úteis.

   c. Requisição de adição/retirada de rede monitorada, modificação na lista de contatos autorizados do cliente, relatórios de dados do tráfego do cliente monitorado em um período especifico: Até 2 (duas) horas.

   d. Requisição da lista de redes monitoradas, alertas e mitigações, informações sobre ataques recebidos, lista de contatos autorizados pelo cliente: Até 8 (oito) horas.

   e. Mitigação de incidentes deve seguir o seguinte quadro:

Sequência de Incidentes	**SLA**	
Início do ataque	Tempo de detecção	15 minutos
Detecção do ataque		
Tentativa de contato com o TJPA		
Solicitação de autorização de mitigação	Tempo de autorização	*
Início de mitigação	Tempo de início de mitigação	15 minutos

*O tempo de autorização depende exclusivamente do TJPA

Monitoramento da Execução (Art. 18, § 3º, III, a, 5)

Serão utilizadas as seguintes formas de comunicação e acompanhamento da execução:

a) Além da reunião de alinhamento, deverão ser realizadas, caso necessárias, outras reuniões presenciais ou não entre o Gestor do Contrato e o Preposto da Contratada;

b) Poderão ser realizados, alternativamente e a critério do Gestor do Contrato, o controle e o acompanhamento mediante o uso de mensagens eletrônicas. Nesse caso, o Fiscal Técnico ou Gestor do Contrato deverá apresentar descritivo contendo situações merecedoras de avaliação por parte da Contratada.

Qualidade e Recebimento do(s) produto(s) (Art. 18, § 3º, III, a, 6)

Instalação física: Deverá ser implantado cabos de fibra óptica, com dupla abordagem e topologia em anel.

Configuração do circuito com BGP e AS: Deverá ser configurado o protocolo BGP para divulgação do plano de endereçamento IP obtido pelo sistema autônomo (AS) do TJPA

Implantação do serviço proativo de segurança Anti-DDoS: Será implantado nos roteadores de borda da Internet, dentro da operadora, que deverá emitir um relatório e/ou informação que o serviço foi implantado.

Recebimento definitivo do serviço: Após as configurações de balanceamento, será realizado a simulação com testes de comutação automática, tornando o circuito principal inoperante para atestar se o circuito redundante assume todo o tráfego da rede, e vice-versa. Haverá recebimento definitivo do serviço após os testes de balanceamento, comprovação do uso máximo da banda contratada (download e upload) e simulação de testes de ataques DDoS que dar-se-á após a conferência e aceitação do serviço entregue, para fins de confirmação com as especificações do objeto.

Forma de Pagamento (Art. 18, § 3º, III, a, 7)

O pagamento do(s) produto(s) e serviço(s) ocorrerá da seguinte maneira:

a) O pagamento ocorrerá em parcela única e será efetuado em até 40 (quarenta) dias, contados da apresentação da nota fiscal ao TJPA;

Transferência de Conhecimento (Art. 18, § 3º, III, a, 8)

Apesar do objeto não contemplar algum repasse de conhecimento, faz-se necessário um repasse *in-loco* nas dependências da CONTRATANTE, sem ônus, sobre a ferramenta de monitoramento do circuito, com previsão máxima de 4 (quatro) horas de repasse e uso da ferramenta.

Direitos de Propriedade Intelectual (Art. 18, § 3º, III, a, 9)

Em conformidade com o Art. 111 da Lei nº 8.666/1993, devem ser preservados os direitos autorais e intelectuais dos produtos gerados durante a vigência do Contrato. No entanto, isto não se aplica ao objeto em questão.

Qualificação Técnica dos Profissionais (Art. 18, § 3º, III, a, 10)

a) Apresentação de, no mínimo, um atestado de capacidade técnica emitido por pessoa jurídica de direito público ou privado, comprovando que a CONTRATADA fornece/forneceu serviços compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.

b) A CONTRATADA deverá apresentar o Termo de Autorização de SCM – Serviço de Comunicação Multimídia expedido pela ANATEL, ou extratos do Termo de Autorização outorgado pela ANATEL, os quais deverão ter sido publicados no Diário Oficial da União.

c) Declaração da CONTRATADA de que atenderá às exigências mínimas relativas à implantação das instalações, equipamentos e pessoal técnico especializado, essencial para o cumprimento do objeto da licitação.

d) A CONTRATADA deverá comprovar através de Atestado de Capacidade Técnica emitida por pessoa jurídica de direito público ou privado, ou Anotação de Responsabilidade Técnica ART com Certidão de Acervo Técnico - CAT expedidos pelo CREA de qualquer unidade da federação, que presta serviço similar em pontos e tecnologia conforme o objeto desta licitação.

e) A CONTRATADA deverá comprovar através de declaração e/ou anotação de Responsabilidade Técnica expedida pelo CREA de qualquer unidade da federação, de que a participante possui infraestrutura técnica e operacional mínima, própria ou terceirizada, no Estado do Pará, considerando-se como tal a existência de equipe técnica especializada, instalações físicas e equipamentos apropriados para o perfeito atendimento e manutenção dos serviços ofertados, comprovando que o proponente executou, ou está executando, serviço com características idênticas ou semelhantes às do objeto do presente termo de referência.

Penalidades (Art. 18, § 3º, III, a, 11)

Caso haja interrupções não programadas nos serviços, A CONTRATADA fica sujeita a descontos na fatura mensal acrescidos de multa pecuniária, regidos a partir das cláusulas a seguir:

Considera-se paralisação programada pela CONTRATADA a interrupção para manutenção preventiva e/ou substituição dos equipamentos e meios utilizados no provimento do(s) Acesso(s) (objeto deste Contrato), desde que devidamente informados a CONTRATANTE com a antecedência mínima de 5 (cinco) dias úteis.

A CONTRATADA concederá descontos no valor mensal por interrupção no funcionamento do(s) acesso(s) e pagará multa, cujas causas não sejam atribuídas a CONTRATANTE, observadas as demais condições estabelecidas no contrato.

Para efeito de descontos, o tempo de interrupção deverá ser considerado entre o início da interrupção registrada no Centro de Atendimento da CONTRATADA ou a partir da comunicação de interrupção, feita pela CONTRATANTE, e a sua total recuperação.

Para efeito de desconto, o período mínimo a ser considerado é de 30 (trinta) minutos consecutivos, adotando-se como início da contagem o tempo e o horário da ocorrência do fato que proporcionou a CONTRATANTE o direito de receber o desconto.

Os períodos adicionais serão considerados como períodos inteiros de 30 (trinta) minutos.

O valor do desconto e da multa será aplicado no mês imediatamente subsequente ao mês no qual ocorreram os fatos que originaram os descontos, tendo como base o valor vigente do(s) acesso(s) do mês da ocorrência da interrupção.

Quando os valores de disponibilidade do Serviço estabelecidos pela CONTRATADA não forem atendidos, será concedido ao cliente um desconto por interrupção e uma multa também será cobrada sendo calculada a partir da seguinte equação.

1) $VD = \frac{VM}{1440} \times N$	Onde: VD = Valor do desconto; VM = Valor mensal do circuito (em R$); n = Quantidade de períodos de 30 (trinta) minutos. 1440 = 1 dia de utilização, em minutos (24 x 60)
2) M = VD x 0.5	Onde: M = Valor da multa a ser paga por indisponibilidade VD = Valor do desconto (calculado na 1ª equação)
3) VDT = VD + M	Onde: VDT = Valor do desconto total a ser concedido VD = Valor do desconto por indisponibilidade (eq. 1) M = Multa (eq. 2)

No caso da inoperância de um circuito ser reincidente num período de 03 (três horas) contados a partir do restabelecimento do mesmo, considerar-se-á como tempo de indisponibilidade do circuito, o início da primeira interrupção até o final da última (restabelecimento total do circuito).

Os descontos e as multas serão calculados por indisponibilidade do circuito.

Nas interrupções da prestação de um ou mais dos serviços (*links* de dados, portal de monitoramento ou proteção Anti-DDoS) contratados, excetuadas as seguintes situações:

i) Caso fortuito ou de força maior.

ii) Operação inadequada, falha ou mau funcionamento de equipamentos não mantidos pela CONTRATADA.

iii) Falha de equipamento da CONTRATADA, ocasionada pelo TJPA.

iv) Falha na infraestrutura física do TJPA.

v) Em casos de manutenções preventivas, testes e ajustes necessários à prestação do serviço licitado.

vi) Impedimento, por qualquer motivo, do acesso de pessoal técnico da CONTRATADA às dependências do TJPA, onde estejam localizados os equipamentos de propriedade da CONTRATADA e/ou por ela mantidos.

vii) Interrupção devido aos efeitos de interferências solares nos acessos satélites.

Proposta de modelos (Templates) (Art. 18, § 3º, V)

A CONTRATA deverá orientar sua proposta conforme o modelo proposto no ANEXO E - MODELO DE PROPOSTA.

ANEXO A – LISTA DE LOCALIDADES

ITEM	SITE	ENDEREÇO	MUNICÍPIO	VELOCIDADE
1	Ed. Lauro Sodré (Prédio Sede)	Av. Almirante Barroso,3089. CEP: 66.613-710. Bairro: Souza	Belém	200Mbps

ANEXO B – ESPECIFICAÇÃO TÉCNICA

1. CONEXÃO DE IPv4 DEDICADO COM A INTERNET

1.1 Fornecimento de serviço para inclusão da CONTRATANTE ao *Backbone* de Internet da CONTRATADA, tornando a CONTRATANTE, nó da Rede Mundial de Computadores.

1.2 A instalação do ponto de acesso físico na CONTRATANTE será feita no seguinte endereço: Av. Almirante Barroso, 3089, bairro Souza, em Belém-PA, CEP 66.613-710, na sala do Datacenter da Secretaria de Informática.

1.3 A taxa de transmissão do circuito é de 200 (duzentos) Mbps de banda simétrica garantida, 24h por dia, 7 dias por semana.

1.4 A conexão deverá ligar a CONTRATANTE ao Ponto de Presença (PoP) do Backbone da CONTRATADA em Belém-PA, sem passar por nenhuma rede IP intermediária, a não ser aquela comumente chamada de “enlace”, tipicamente com máscara 255.255.255.252.

1.5 O acesso ao PoP da CONTRATADA deverá ser realizado através do protocolo: ETHERNET, por meios não estatísticos, onde não haja compartilhamento de banda desde o equipamento roteador até a porta de entrada do backbone da CONTRATADA. Os links e as portas de acesso ao centro de roteamento da CONTRATADA deverão ser exclusivos e dedicados, não podendo haver compartilhamento com outros usuários.

1.6 A conexão deve usar meio físico redundante, ou seja, devem existir pelo menos duas conexões físicas entre a rede da CONTRATANTE e o PoP da CONTRATADA, também conhecido como dupla abordagem.

1.7 Cada conexão física estabelecida deve usar encaminhamento distinto das demais conexões físicas estabelecidas a fim de evitar queda simultânea.

1.8 Cada conexão física estabelecida deve usar um canal único (não agregado) que garanta isoladamente 100% (cem por cento) da banda contratada para chegar ao PoP da CONTRATADA.

1.9 A interface de conexão entre o roteador da CONTRATADA instalado no CONTRATANTE e a rede interna da CONTRATANTE deve usar a tecnologia Gigabit Ethernet.

1.10 A CONTRATADA deve estar preparada para usar meio físico metálico ou ótico no roteador da CONTRATADA instalado no CONTRATANTE e a rede interna da CONTRATANTE, sem ônus de qualquer natureza ao CONTRATANTE.

1.11 Cada conexão física ao PoP da CONTRATADA deve usar um meio terrestre com taxa média de erros de bits igual ou menor a 10^{-9} (fibra ótica ou melhor).

1.12 Todos os equipamentos, cabos e elementos de suporte usados nas vias públicas em cada uma das conexões físicas entre o CONTRATANTE e o PoP da CONTRATADA devem ser isolados para garantir que não haja ponto único de falha no meio do caminho;

1.13 A CONTRATADA deve fazer o monitoramento das conexões físicas entregues no prédio Sede da CONTRATANTE com o propósito de detectar imediatamente a indisponibilidade de qualquer uma das conexões físicas estabelecidas e iniciar o processo de recuperação da conexão falhada, de tal forma que seja possível evitar a falha completa de todas as conexões físicas. A CONTRATADA deve informar a CONTRANTANTE sobre recuperações desta natureza para mantê-la ciente de eventual falha completa das conexões físicas;

1.14 A CONTRATADA deve fornecer, em regime de comodato, os equipamentos necessários para a ativação do serviço, inclusive o roteador e é responsável pela instalação, configuração e manutenção destes;

1.15 A CONTRATADA deve franquear a CONTRATANTE o acesso SSH ou Telnet permanente ao equipamento roteador instalado no CONTRATANTE com permissão de leitura de configuração e monitoramento completo do equipamento com o propósito de garantir a conformidade da configuração, da capacidade do equipamento e dos enlaces para o serviço contratado

1.16 À CONTRATADA, caberá o fornecimento, instalação, suporte e manutenção dos equipamentos roteadores, conforme especificação constante no **ANEXO C** deste documento, ficando a guarda e a administração das rotas e as políticas de segurança desses ativos a cargo da CONTRATANTE, sendo que o gerenciamento, a configuração física e do circuito de enlace ficará sob a responsabilidade da CONTRATADA.

1.17 Em situações emergenciais que venham a ocorrer fora do horário de expediente regular do TJPA (8h às 14h), a CONTRATADA deverá responsabilizar-se pela administração de rotas e políticas de segurança, desde que demandada pela CONTRATANTE através do serviço de suporte técnico fornecido.

1.18 A CONTRATADA deve ser capaz de prover trânsito IP internacional para o Sistema Autônomo (AS) da CONTRATANTE, com suporte ao protocolo BGP-4.

1.19 A CONTRATADA deverá estar preparada para fornecer conectividade IPv6, conforme plano de migração da CONTRATANTE, obedecendo prazos acordados previamente entre as partes e sem ônus de qualquer natureza, sem qualquer tradução de endereçamento de rede – Network Address Translation (NAT).

1.20 A CONTRATADA deverá oferecer todos os meios para utilização do protocolo BGP (*Border Gateway Protocol*) a qualquer momento, quando solicitado, sem ônus de qualquer natureza a CONTRATANTE, obedecendo ao prazo máximo de 5 (cinco) dias corridos para entrega deste serviço.

1.21 Admitir latência de rede de até 40 ms (quarenta milisegundos), sendo que latência consiste no tempo médio de trânsito (ida e volta – *round-trip delay*) de um pacote ICMP de 512 (quinhentos e doze) Bytes entre o roteador de borda da CONTRATADA e o roteador de borda instalado no site do TJPA. Para medir esta latência a qualquer momento, deve-se calcular a média do tempo de ida e volta de 600 pacotes ICMP tipo “echo” com tamanho de 512 (quinhentos e doze) Bytes enviados em intervalos de 1 (um) minuto.

1.22 A taxa de perda de pacotes será determinada pela porcentagem dos pacotes que foram enviados pelo centro de monitoramento da CONTRATADA para o equipamento instalado no site do TJPA e não retornarem para o centro de monitoramento da CONTRATADA. De cada 1000 (mil) pacotes, a perda máxima permitida é de 1% (um por cento).

1.23 A taxa de erros máxima admitida é deve ser igual ou inferior a inferior a 10^-9 (dez elevado a menos nove, equivalente a 0,0000001%).

1.24 A Disponibilidade do Serviço é o índice que mede o percentual de tempo que o circuito de Internet esteve operacional para transmissão e recepção (condições normais de funcionamento e operação) deve ser 99,9% mensal.

1.25 A conexão IP deve ter a variação do atraso de pacote IP (IP Packet Delay Variation – IPDV) média, também chamado de Jitter, definido pela RFC3393, de no máximo 20 ms (vinte milisegundos) entre o roteador de borda instalado na rede da CONTRATANTE e o roteador de borda da rede da CONTRATADA, quando o enlace não estiver saturado. Para medir o IPDV médio de forma simplificada, deve-se calcular o valor médio do módulo da diferença dos tempos de ida e volta (RTT - Round Trip Time) divididos por 2 (dois) de uma sequência de 1000 pacotes ICMP tipo “echo” com tamanho mínimo de 512 (quinhentos e doze) bytes enviados em intervalos de 1 (um) minuto.

1.26 A CONTRATADA deve realizar troca de tráfego IP nacional com pelo menos 2 (dois) provedores de acesso à Internet nacionais. Estes provedores devem estar designados na ANATEL como Grupo Detentor de Poder Mercado Significativo. Para cada conexão de troca de tráfego, a CONTRATADA deve manter circuito nacional exclusivo, usando caminhos físicos diferentes. Qualquer um destes circuitos deve ter capacidade de sobra suficiente para atender o serviço de acesso à Internet contratado com 100% (cem por cento) de banda garantida.

1.27 A CONTRATADA deve possuir em sua rede um mecanismo de proteção contra ataques de negação de serviço distribuído (Distributed Denial of Service – DDoS), com propriedade de evitar a saturação da banda de Internet e a indisponibilidade do serviço durante os momentos de ataque à rede do CONTRATANTE.

1.28 A CONTRATADA deve configurar acessos de leitura para uma comunidade SNMP que suporte no mínimo a RFC1213 (MIB-II) no roteador instalado dentro da CONTRATANTE;

1.29 A CONTRATADA deve configurar o roteador instalado dentro da CONTRATANTE para enviar notificações do tipo SNMP TRAP para o servidor de gerência da CONTRATANTE, a ser informado no momento da ativação do serviço. No mínimo, devem ser enviados SNMP TRAP nos seguintes casos: mudança de estado de interfaces, taxa média de uso da memória acima de 80% e taxa média de uso médio de CPU acima de 80%, considerando o último minuto de uso;

1.30 A CONTRATADA deve configurar coleta de fluxos de tráfego IPFIX ou Netflow v9 ou equivalente no roteador instalado dentro da CONTRATANTE. Os fluxos coletados devem ser exportados e enviados para servidor de gerência da CONTRATANTE, a ser informado no momento da ativação do serviço;

1.31 A CONTRATADA deve configurar o envio de mensagens do tipo Syslog no roteador instalado dentro da CONTRATANTE. Os parâmetros facilidade, severidade e servidor de log serão informados pela CONTRATANTE no momento da ativação do serviço.

2. ACORDO DE NÍVEL DE SERVIÇO-ANS (*Service Level Agreement* – SLA)

2.1 O serviço será considerado indisponível a contar do início de uma interrupção registrada na Central de Assistência Técnica (Call Center) da CONTRATADA até o total restabelecimento do circuito às condições normais de operação e a respectiva informação e certificação do TJPA.

2.2 A disponibilidade do serviço será calculada por cada ponto de acesso à rede, para um período de 1 (um) mês, através da seguinte equação:

$D = \frac{T_0 - T_i}{T_0} \times 100$	Onde: D = disponibilidade; T_o = período de operação (1 mês), em minutos; T_i = tempo total de indisponibilidade do ponto de acesso, ocorrida no período de operação (1 mês), em minutos.

2.3 No cálculo de disponibilidade, não serão consideradas as interrupções programadas, de urgência e aquelas que não sejam de responsabilidade da CONTRATADA.

2.4 As manutenções programadas que haja necessidade de interrupção do circuito, devem ocorrer, obrigatoriamente, entre às 20h e 06h do dia seguinte. Caso não haja interrupção do circuito para realizar uma manutenção (preventiva e/ou corretiva), poderá ser realizado em qualquer momento. Em ambos os casos, a CONTRATADA deverá acordar o dia/hora, previamente, com a CONTRATANTE.

2.5 São consideradas paralisações programadas da CONTRATADA a interrupção para manutenção preventiva ou para substituição dos equipamentos e meios utilizados no provimento do serviço, desde que devidamente informados com antecedência mínima de 5 (cinco) dias úteis, não podendo ultrapassar os seguintes limites do circuito:

a) Tempo máximo da interrupção: Deverá ser respeitado o limite estabelecido no contrato.

b) Frequência máxima de 1 (uma) ocorrência em cada 30 (trinta) dias, não acumulativo.

c) Quando for necessária ação da CONTRATADA nas dependências do TJPA, deverá ser solicitado prévio acesso ao preposto do contrato ou quem ele designar.

d) Quando o prazo mínimo de 5 (cinco) dias úteis de comunicação não for atendido, ou não houver a informação registrada, a interrupção incidirá no cômputo do cálculo de indisponibilidade do serviço.

2.6 Considera-se paralisação de URGÊNCIA pela CONTRATADA a interrupção para manutenção preventiva ou para substituição dos equipamentos e meios utilizados no provimento do serviço que comprovadamente comprometam o seu funcionamento mediante índices de degradação do circuito (banda passante, tempo de resposta e taxa de erro). Devendo, entretanto, ser comunicado ao TJPA até 2 (duas) horas antes do início do atendimento através de relatório, para ciência do corpo técnico do TJPA. Caso contrário, a interrupção incidirá no cômputo do cálculo de indisponibilidade do serviço a ser aplicado pelo TJPA.

2.7 Considera-se paralisação como não sendo responsabilidade da CONTRATADA os eventos relacionados à ocorrência de caso fortuito ou força maior (entende-se como caso fortuito ou força maior como sendo qualquer ocorrência que não seja proveniente de qualquer ação humana, tais como: descargas atmosféricas, tremores de terra, maremotos, enchentes, etc.) ou que venham a ser causados por qualquer ação do próprio TJPA, bem como falhas nos ativos de rede de sua propriedade.

3. INFRAESTRUTURA FÍSICA DE ACESSO

3.1 Os serviços relativos à especificação, ao projeto, à instalação, à operação e à manutenção da estrutura de comunicação concernente as estações e links terrestres até a interface que permita integração com a rede local do TJPA serão de responsabilidade da CONTRATADA.

3.2 Todos os materiais necessários e equipamentos para a instalação dos dispositivos, como cabos, conectores, braçadeiras, parafusos de fixação, anilhas de identificação e móveis eventualmente indisponíveis nas edificações como armários de comunicações (racks), deverão ser fornecidos pela CONTRATADA, bem como eventuais obras civis necessárias a instalação dos equipamentos e infraestrutura necessária para lançamento de cabos de acesso externo ao ambiente da CONTRATANTE, sem ônus à CONTRATANTE.

3.3 Os materiais a serem utilizados na instalação deverão ser de qualidade e propriedades físicas que melhor se adaptem às condições de cada localidade e de acordo com os melhores princípios, práticas de engenharia e Normas Técnicas da ABNT.

3.4 O TJPA será responsável em cada edificação pela infraestrutura interna das salas onde ficarão os equipamentos de terminação da CONTRATADA tal como especificado a seguir: energia elétrica comercial, climatização, unidades de fornecimento ininterrupto de energia (no-break), cabeamento para conexão das terminações à rede interna de dados, bem como switches e servidores de acesso e armários de comunicação (racks).

3.5 Os equipamentos fornecidos pela CONTRATADA ficarão sob guarda do TJPA, que deverá se responsabilizar pela integridade dos mesmos.

3.6 Para instalação de equipamentos externos, a infraestrutura é de responsabilidade da CONTRATADA.

3.7 Caberá ao TJPA o fornecimento do ponto de derivação de sua rede elétrica que deverá ser utilizada pela CONTRATADA para providenciar, em tempo hábil derivação para alimentar o seu quadro de energia e rede elétrica separada e exclusiva para seus equipamentos, 110 V (fase, neutro e terra) ou 220 V (fase, terra ou fase, neutro e terra) dependendo da tensão do equipamento.

3.8 Uma vez verificada a desconformidade do serviço entregue, a CONTRATADA terá o prazo de 15 (quinze) dias corridos para que sejam efetuados os devidos ajustes.

4. GARANTIA E ASSISTÊNCIA TÉCNICA

4.1 A CONTRATADA deverá possuir ponto de presença, na cidade de Belém-PA, onde se localiza o ponto principal da rede.

4.2 Considera-se como “ponto de presença”, no mínimo, a existência de equipe de técnicos especializados na manutenção dos circuitos ofertados.

4.3 A Central de Assistência Técnica da CONTRATADA deverá estar à disposição da CONTRATANTE para recebimento de reclamações e esclarecimento de dúvidas e eventuais problemas no período de 24 horas por dia, 7 dias por semana, todos os dias do ano.

4.4 A Central de Assistência Técnica da CONTRATADA deverá permitir comunicação de inoperância através de telefone franqueado (ex: serviço 0800), com atendimento em língua portuguesa, e portal de monitoramento via web.

4.5 As reclamações feitas através da Central de Assistência Técnica da CONTRATADA deverão ser atendidas em no máximo 24h corridas depois de registrada, excetuando a inoperância total.

4.6 Os serviços de atendimento técnico que necessitarem ser executados nas dependências da CONTRATANTE serão agendados com um funcionário da CONTRATANTE. Em caso de impedimento ao acesso de técnicos no local da ocorrência, que seja de responsabilidade da CONTRATANTE, o cômputo do período de indisponibilidade não considerará o período de tempo em que o técnico da CONTRATADA permanecer impedido de realizar a manutenção.

4.7 O início do atendimento deverá ser contado a partir da solicitação feita pela CONTRATANTE a Central de Serviços da CONTRATADA.

4.8 Entende-se por finalização do atendimento o momento a partir do qual o serviço estiver disponível e em perfeitas condições de funcionamento atendendo ao que está especificado como condições mínimas de uso.

4.9 Quando da solicitação de atendimento, via telefone ou e-mail, a CONTRATANTE fornecerá a CONTRATADA, as seguintes informações, para fins de abertura de chamado técnico:

a) Código de identificação do cliente fornecido pela CONTRATADA
b) Descrição da anormalidade observada
c) Nome e telefones do responsável pela abertura do chamado

4.10 A CONTRATADA deverá fornecer no momento da abertura do chamado, um número de protocolo para acompanhamento do atendimento.

4.11 A CONTRATADA deverá apresentar, por ocasião da assinatura do contrato, todos os procedimentos e informações necessárias ao acionamento do seu serviço de suporte e solução de problemas.

4.12 A CONTRATADA não será responsável pela solução de problemas internos, a partir da rede interna da CONTRATANTE.

4.13 Esses valores deverão estar disponíveis para consulta pela CONTRATANTE na página web da CONTRATADA no regime 24X7. Em caso de descumprimento desses valores ao longo de 30 (trinta) dias, a CONTRATANTE terá o direto ao crédito automático de 01 (um) dia de serviço (equivalente a 1/30 do preço do valor mensal pago a CONTRATADA).

4.14 A CONTRATADA também deverá dispor de relatórios contendo as informações sobre o desempenho do núcleo da sua rede (rede da CONTRATADA) na forma de página web.

4.15 A realização de testes, ajustes e manutenção necessários à prestação do serviço devem ser agendadas e devidamente comunicados à CONTRATANTE com antecedência mínima de 05 (cinco) dias úteis.

ANEXO C - EQUIPAMENTO ROTEADOR

O equipamento possui as seguintes características:

1 PORTAS

1.1 Possuir, no mínimo, 2 (dois) slots para a inserção de módulos.

1.2 Possuir 2 (duas) interfaces Ethernet 1000BaseT.

1.3 Possuir 2 (duas) interfaces Ethernet 1000BaseSX.

1.4 Possuir capacidade de associação das portas 1000Base-T e 1000Base-SX, no mínimo, em grupo de 4 (quatro) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad (link aggregation).

1.5 Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.

1.6 Implementar VLANs por porta.

1.7 Implementar VLANs compatíveis com o padrão IEEE 802.1q (VLAN tagging).

2 CABOS FANOUTS ÓPTICOS

2.1 Deverão ser fornecidos cabos fanouts ópticos compatíveis com as interfaces de fibra óptica que compõem os dispositivos adquiridos e em quantidade suficiente para a conexão dessas interfaces.

2.2 Devem ser fornecidos todos os cabos e acessórios necessários para que a conexão WAN seja estabelecida com o ponto de presença da operadora

3 FONTE DE ALIMENTAÇÃO

3.1 Possuir fonte de alimentação interna AC bivolt redundante, com seleção automática de tensão (na faixa de 100 a 240 V) e frequência (50/60 Hz);

3.2 Possuir cabo de alimentação para a fonte com, no mínimo, 1,80 m (um metro e oitenta centímetros) de comprimento, tripolar, atendendo o padrão ABNT.

4 DIMENSÕES

4.1 Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários para montagem.

5 INDICAÇÃO DE FUNCIONAMENTO

5.1 Possuir LED (*Light-Emitting Diode*) para a indicação do status das portas e atividade de encaminhamento de pacotes.

6 GERENCIAMENTO

6.1 Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de *traps*.

6.2 Implementar pelo menos os seguintes níveis de segurança para SNMPv3:

i. Sem autenticação e sem privacidade (*noAuthNoPriv*).
ii. Com autenticação e sem privacidade (*authNoPriv*).
iii. Com autenticação e com privacidade (*authPriv*) baseada nos algoritmos de autenticação HMAC-MD5 ou HMAC-SHA e algoritmo de criptografia DES 56-bit.

6.3 Suportar SNMP sobre IPv6.

6.4 Possuir suporte a MIB (*Management Information Base*) II, conforme RFC 1213.

6.5 Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

6.6 Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.

6.7 Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.

6.8 Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes.

6.9 Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.

6.10 Permitir o controle da geração de *traps* por porta, possibilitando restringir a geração de *traps* a portas específicas.

6.11 Permitir o gerenciamento via CLI (*Command Line Interface*) e Web, utilizando os protocolos SSH e HTTPS.

6.12 Implementar nativamente 2 (dois) grupos RMON (Alarms e Events), conforme RFC 1757.

6.13 O equipamento deve suportar a configuração com um único endereço IP para gerência e administração (*Single IP Management* – SIM), para uso dos protocolos: SNMP, NTP, HTTPS, SSHv2, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede.

6.14 Possibilidade de criação de versões de configuração e suporte à função de *rollback* da configuração para versões anteriores.

7 FACILIDADES GERAIS

7.1 Implementar o protocolo Telnet para acesso à interface de linha de comando (CLI).

7.2 Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface ethernet e serial.

7.3 Ser configurável e gerenciável via GUI (*Graphical User Interface*), CLI, SNMP, Telnet, SSHv2, FTP, HTTP e HTTPS com, no mínimo, 5 (cinco) sessões simultâneas e independentes.

7.4 Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.

7.5 Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (*Secure Copy*) utilizando um cliente padrão ou SFTP (*Secure FTP*).

7.6 Suportar protocolo SSHv2, para gerenciamento remoto, implementando pelo menos o algoritmo de criptografia de dados 3DES.

7.7 Permitir que a sua configuração seja feita através de terminal assíncrono.

7.8 Permitir a gravação de log externo (*syslog*), possibilita definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.

7.9 Permitir o armazenamento da configuração em memória não volátil, possibilitando que após o restabelecimento de uma falha de alimentação elétrica volte a operar com a mesma configuração anterior a falha.

7.10 Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.

7.11 Suportar o espelhamento da totalidade do tráfego de uma porta (*Port Mirroring*), de um grupo de portas e de VLANs para um endereço IP. Sendo possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

7.12 Deve suportar IPv6.

7.13 Implementar NAT (*Network Address Translation*).

7.14 Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando, no mínimo, as seguintes informações:

i. IP de origem/destino;
ii. Parâmetro "*protocol type*" do cabeçalho IP;
iii. Porta TCP/UDP de origem/ destino;
iv. *Interface* de entrada do tráfego.

7.15 Deve ser possível especificar o uso da funcionalidade do item anterior somente para o tráfego de entrada, saída ou também para ambos os sentidos de forma simultânea em uma determinada interface do roteador.

7.16 A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado.

7.17 Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA – *Service Level Agreement*). Sendo suportadas, no mínimo, as seguintes operações de teste:

v. ICMP *echo*;
vi. TCP *connect* (em qualquer porta TCP do intervalo 1 - 50000 que o administrador especifique).
vii. UDP *echo* (em qualquer porta UDP do intervalo 1 - 50000 que o administrador especifique).
viii. O equipamento deve suportar pelo menos 5 (cinco) destas operações de teste simultaneamente.

7.18 Deverá ser fornecido um conjunto de manuais técnicos, para cada equipamento desta especificação, contendo todas as informações sobre o produto com as instruções para instalação, configuração, operação e gerenciamento, em conformidade com as funcionalidades e características descritas.

7.19 A solução de gerência de rede da CONTRATADA deverá atuar de forma pró-ativa, antecipando-se aos problemas na rede e garantindo os níveis de serviços estabelecidos deste Termo de Referência, realizando abertura automática, acompanhamento e fechamento de chamados técnicos (trouble tickets) relacionados com indisponibilidade e desempenho nos serviços de rede, gerenciamento da rede e segurança, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.

8 PROTOCOLOS ADICIONAIS

8.1 Implementar o protocolo NTPv3 (*Network Time Protocol*, versão 3), sendo suportada autenticação entre peers NTP, conforme definições da RFC 1305.

8.2 Implementar DHCP (*Dynamic Host Configuration Protocol*) Relay e DHCP Server.

8.3 Implementar o protocolo VRRP (*Virtual Router Redundancy Protocol* – RFC 2338) ou mecanismo similar de redundância de gateway, suportando mecanismo de autenticação MD5 entre os peers VRRP.

9 PROTOCOLOS DE ROTEAMENTO

9.1 Implementar roteamento estático.

9.2 Implementar roteamento dinâmico – RIPv2 *Cryptographic Authentication* (RFC 4822).

9.3 Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101, 3137, 3623 e 2370).

9.4 Implementar protocolo de roteamento BGPv4(RFC 4271, 3065, 4456, 1997, 1965, 1966, 4897, 2858 e 2385).

9.5 Permitir o roteamento nível 3 (três) entre VLANs.

9.6 Implementar, no mínimo, 100 (cem) grupos VRRP ou mecanismo similar de redundância de gateway simultaneamente.

9.7 Permitir a virtualização das tabelas de roteamento camada 3 (três).

9.8 Permitir que as tabelas virtuais sejam completamente segmentadas.

9.9 Suporte ao protocolo de tunelamento GRE (*General Routing Encapsulation* - RFC 2784), contemplando, no mínimo, os seguintes recursos:

i. Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica, definida pelo administrador do equipamento;
ii. Operação em modo multiponto (*multipoint GRE*);
iii. Possibilidade de configuração de *Keepalive* nos túneis;
iv. Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.

9.10 Implementar roteamento baseado em origem, com possibilidade de definição do próximo salto (Next Hop) camada 3 (três), baseado em uma condição de origem.

10 ROTEAMENTO IPv6

10.1 Suportar e implementar roteamento estático para IPv6.

10.2 Implementar roteamento dinâmico RIPng.

10.3 Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.

10.4 Implementar protocolo de roteamento *Multiprotocol* BGP com suporte a IPv6.

11 CARACTERÍSTICAS DE DESEMPENHO

11.1 Implementar, no mínimo, 4000 (quatro mil) Vlans simultaneamente.

11.2 Implementar, no mínimo, 4000 (quatro mil) interfaces vlans simultaneamente, para roteamento nível 3 (três) entre as Vlans configuradas.

11.3 Possuir *backplane* de, no mínimo, 5 (cinco) Gbps.

11.4 Suportar pelo menos 1 (um) Gbps de *throughput* com todas as funcionalidades de roteamento e segurança ativas simultaneamente.

11.5 Possuir uma taxa de comutação de pacotes de no mínimo 8 (oito) milhões pacotes por segundo (Mpps).

12 CARACTERÍSTICAS DE SEGURANÇA

12.1 Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.

12.2 Implementar filtragem de pacotes (ACL - *Access Control List*), para IPv4 e IPv6.

12.3 Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.

12.4 Proteger a interface de comando do equipamento através de senha.

12.5 Implementar o protocolo SSH V2 para acesso a CLI.

12.6 Permitir a criação de listas de acesso (ACL) baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP, sendo possível definir os endereços IP de origem das sessões Telnet e SSH.

12.7 Permitir a inserção de um certificado digital da PKI (*Public Key Infrastructure*) para autenticação do protocolo SSH e túneis IPSEC.

12.8 Implementar mecanismos de AAA (*Authentication, Authorization e Accounting*) com garantia de entrega.

12.9 Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso, incluindo os pacotes referentes a senhas.

12.10 Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede.

13 PROTOCOLOS DE NÍVEL DE ENLACE

14.1 Implementar padrão IEEE 802.1q (*Vlan Frame Tagging*).

14.2 Implementar padrão IEEE 802.1p (*Class of Service*) para cada porta.

14.3 Implementar o protocolo de negociação *Link Aggregation Control Protocol* (LACP – IEEE 802.3ad).

14 MULTICAST

15.1 Implementar mecanismo de controle de multicast através de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).

15.2 Implementar roteamento multicast PIM (*Protocol Independent Multicast*) nos modos sparse mode (RFC 2362) e dense mode, devendo ser suportada, por interface, a operação simultânea nos modos sparse mode e dense mode.

15 QUALIDADE DE SERVIÇO (QoS)

16.1 Possuir a facilidade de priorização de tráfego através do protocolo IEEE P802.1p.

16.2 Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação as demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego real-time (voz e vídeo).

16.3 Classificação e reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

16.4 Classificação, marcação e remarcação baseadas em CoS (*Class of Service* - nivel 2) e DSCP (*Differentiated Services Code Point* - nivel 3), conforme definições do IETF (*Internet Engineering Task Force*).

16.5 Suportar funcionalidades de QoS (Quality of Service) de Traffic Shaping e Traffic Policing.

16.6 Suporte à especificação de banda por classe de serviço.

16.7 Suporte à configuração de ações para os pacotes que excederem a especificação, como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP e descarte do pacote.

16.8 Suporte aos mecanismos de QoS WRR (*Weighted Round Robin*) e WRED (*Weighted Random Early Detection*).

16.9 Implementar LFI (*Link Fragmentation e Interleaving*), tanto em interfaces seriais com encapsulamento Frame Relay, quanto em interfaces seriais configuradas com encapsulamento PPP (Point to Point Protocol).

16.10 Implementar RTP (*Real-Time Transport Protocol*) e a compressão do cabeçalho dos pacotes RTP (IP RTP Header Compression).

16.11 Implementar priorização nível 2 IEEE 802.1p e priorização nível 3 dos tipos IP Precedence e DSCP (*Differentiated Services Code Point*).

16.12 O equipamento (roteador) deve suportar o mapeamento das prioridades nível 2 (IEEE 802.1p) em prioridades nível 3 (*IP Precedence e DSCP*) e vice-versa.

16.13 Implementar política de enfileiramento nas linhas seriais (priorização de tráfego por tipo de protocolo trafegado).

16.14 Devem ser suportadas pelo menos as seguintes técnicas de enfileiramento: Priority Queuing, Custom Queuing, Weighted Fair Queuing, Class-Based Weighted Fair Queuing e Low Latency Queuing;

16.15 Implementar RSVP (*Resource Reservation Protocol*).

16 INTERNET PROTOCOL VERSÃO 6 (IPV6)

17.1 Suporte total e nativo ao protocolo IPv6.

17.2 Suporte à configuração de endereços IPv6 para gerenciamento.

17.3 Suporte a consultas de DNS com resolução de nomes em endereços IPv6.

17.4 Implementar ICMPv6 com as seguintes funcionalidades:

i. ICMP request
ii. ICMP Reply
iii. ICMP Neighbor Discovery Protocol (NDP)
iv. ICMP MTU Discovery

17.5 Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, SNMP, SYSLOG e DNS sobre IPv6.

17.6 Implementar mecanismo de Dual Stack (IPv4 e IPv6) para permitir migração de IPv4 para IPv6;

17 GARANTIA E INTERLIGAÇÃO DOS EQUIPAMENTOS

18.1 Os equipamentos (roteadores) instalados na CONTRATANTE pela CONTRATADA terão garantia total de peças e serviços durante a vigência do contrato, com atendimento on-site 24X7, com solução total do problema em até 3 (três) horas a partir da abertura do chamado.

18.2 A CONTRATADA garantirá a substituição, em até 2 (duas) horas a partir da abertura do chamado, do equipamento defeituoso por outro de primeiro uso, da mesma marca e especificações descritas neste Termo de Referência.

18.3 Todos os cabos e adaptadores necessários para interligar os roteadores instalados na CONTRATANTE a CONTRATADA serão de responsabilidade desta.

ANEXO D – SERVIÇO ANTI-DDoS

1. Requisitos de segurança do serviço Anti-DDoS

1.1 A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviços para o circuito de Internet evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS e DDOS de acordo considerando os requisitos mínimos a seguir:

1.1.1 Serviços deverão ter pró-atividade para solução e prevenção de incidentes e ataques.

1.1.2 Monitorar disponibilidade e performance de todos os circuitos de dados existentes nesse termo de referência em regime 24x7 utilizando profissionais de forma dedicada.

1.1.3 Tomar todas as providências necessárias para recompor a disponibilidade do circuito em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada.

1.1.4 A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações históricas e preditiva própria, gerada a partir de outros ataques rechaçados ou bem-sucedidos, e devem estar interligadas com os principais centros mundiais de avaliação de reputação de endereços IP.

1.1.5 A CONTRATADA deve ter gerência pró-ativa para solução e prevenção de incidentes e ataques. A filtragem de pacotes deve sempre ser baseada nos endereços IPs de origem do ataque e os filtros devem ser aplicado em toda a rede da CONTRATADA.

1.1.6 A solução ofertada não poderá afetar a visibilidade do endereço de origem das requisições, mantendo o tráfego legítimo livre de qualquer modificação.

1.1.7 A proteção deverá operar sem exigir o desligamento de qualquer outro circuito de acesso da CONTRATADA, independente de quantos ou quais sejam os demais fornecedores.

1.1.8 O ataque deve ser mitigado na estrutura da contratada, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pela CONTRATADA continuem disponíveis aos seus usuários.

1.1.9 A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como lista de liberação (*White Lists)*, lista de bloqueios *(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.

1.1.10 A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:

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

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

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

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

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

1.1.11 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.

1.1.12 A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico.

1.1.13 O serviço deve suportar a mitigação de ataques que utilizam técnicas de *spoofing* utilizando algoritmos de desafio-resposta, como SYN Cookies e TCP SYN *authentication*.

1.1.14 A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.

1.1.15 A CONTRATADA deve fornecer centro de limpeza nacional cada um com capacidade de mitigação de 1GB e centro de limpeza internacional com capacidade de mitigação de 10GB para mitigar os ataques nos circuitos da CONTRATANTE. No caso da utilização de soluções baseadas em centros de limpeza de dados com redirecionamento do tráfego de entrada, o serviço deve ser capaz de entregar, no mínimo, 80% (oitenta por cento) de tráfego limpo a CONTRATADA.

1.1.16 Caso sejam utilizadas soluções baseadas em centros de limpeza de dados com redirecionamento do tráfego de entrada, será exigido que a contratada possua ao menos três centros de mitigação em três continentes distintos. O CONTRATANTE efetuará os ajustes de MTU ou MSS, nos seus dispositivos de rede, necessários ao correto fluxo de dados nos túneis GRE.

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

1.1.18 A contratada deve mitigar ataques por, no mínimo, 3 horas ou tempo superior, se necessário. 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*.

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

1.1.20 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.

1.1.21 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.

1.1.22 Em momentos de ataques DOS e DDOS, todo trafego limpo deve ser reinjetado na infraestrutura da contratante através de túneis GRE (*Generic Routing Encapsulation*), configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante.

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

1.1.24 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

1.1.25 Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.

1.1.26 A contratada deve possuir um contrato de 15 minutos para iniciar a mitigação de ataques de DDOS

1.1.27 A CONTRATADA deverá disponibilizar uma Solução de Monitoração de acompanhamento contra ataques DDoS, que contemple:

a) Quadro Sinóptico para visualização da ocupação de banda do link Internet e níveis de severidade dos ataques.

b) Os alertas deverão fornecer, no mínimo, as seguintes funcionalidades:

- Visualização de informações on-line, de forma gráfica da banda consumida no ataque;

- Acompanhamento do nível de importância do ataque, o percentual do nível de severidade do ataque, o consumo de banda do ataque e tipo do ataque e classificação.

- Origem de ataques com identificação do endereço IP e porta de origem

- Destino de ataques, com identificação do endereço IP e porta de destino.

- Protocolo de transporte do alerta.

- Cada alerta deverá ter um número de identificação que facilite sua consulta.

- Informar a data de início e fim do acompanhamento do alerta

- Volume de ataques sumarizados por hora, dia, semana e mês.

- Relatório por tipos de ataques.

c) O Portal de monitoração da CONTRATADA deverá possuir uma interface única para acesso às suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços.

d) O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, um administrador de rede da CONTRATANTE.

ANEXO E - MODELO DE PROPOSTA

Os valores informados devem incluir todos os custos e despesas tais como: tributos incidentes, taxa de administração, serviços, encargos sociais, trabalhistas e outros necessários ao cumprimento integral do OBJETO deste termo aditivo e seus anexos.

Empresa:

Endereço completo:

Telefone/Fax/E-mail:

Banco/Agência/Conta Corrente

Valor do circuito (A)	Valor do serviço Anti-DDoS (B)	Taxa única de Instalação (C)	Valor Global anual [(A+B)x12] + C

Valor Global anual: R$

Validade da proposta:

Prazo de conclusão dos serviços:

Local e data

_____
Assinatura do representante legal