

# ESPECIFICAÇÕES TÉCNICA

LOTE 1

ADITAMENTO 2

## 1. OBJETO

- 1.1 Contratação de serviços para conectividade de tráfego à Internet com solução de proteção Anti DDoS, pelo período 36 (trinta e seis) meses, instalado na Usina Hidrelétrica de Itaipu.

## 2. DESCRITIVO DOS SERVIÇOS

### 2.1 Link de tráfego IP para internet com velocidade de 1 Gbps com suporte a BGP e bloco IP /29, com solução anti DDoS.

- 2.1.1 A CONTRATADA deverá fornecer e instalar um canal de comunicação Internet IP, com banda garantida de 1 Gbps com ligação à Rede Internet, com velocidade simétrica (upload e download) para uso exclusivo da ITAIPU na Usina Hidrelétrica Itaipu.
- 2.1.2 A CONTRATADA deve prover comunicação de dados IP versão 4 (IPv4) e IP versão 6 (IPv6) nativa, utilizando técnica de pilha-dupla (IPv4 e IPv6 simultaneamente) e com suporte a aplicações IP em conformidade com todos os padrões e recomendações relevantes da IETF (Internet Engineering Task Force)
- 2.1.3 O serviço oferecido pela CONTRATADA deverá suportar o transporte dos protocolos superiores ao nível 3 de forma transparente.
- 2.1.4 A banda fornecida pela CONTRATADA de 1 Gbps deve ser mantida durante 24 horas por dia, 7 dias por semana, incluindo sábados, domingos e feriados.
- 2.1.5 Caso a CONTRATADA venha a oferecer velocidades superiores à instalada, sem a solicitação da ITAIPU, não terá direito a qualquer espécie de remuneração adicional ou aditivo contratual, assumindo integralmente os custos dessa alteração.
- 2.1.6 A CONTRATADA deverá fornecer o roteador, sendo que a instalação, configuração, programação e manutenção do roteador são de responsabilidade da CONTRATADA (detalhe item 12).
- 2.1.7 A contratada será responsável pela infraestrutura e deverá instalar todo o meio físico necessário para o perfeito funcionamento dos serviços objeto desta contratação.
- 2.1.8 A CONTRATADA deverá viabilizar a mudança de endereço de forma a atender eventos da ITAIPU, mediante solicitação prévia de no mínimo 30 (trinta) dias.
- 2.1.9 A CONTRATADA deverá informar a ITAIPU com antecedência mínima de 48 (quarenta e oito) horas, eventuais interrupções programadas dos serviços, e estas ocorrerem em horário previamente combinado com os técnicos da ITAIPU, exceto em casos emergenciais devidamente comprovados.
- 2.1.10 Os sistemas autônomos da CONTRATADA e da CONTRATANTE trocarão informações de roteamento e alcançabilidade de redes IPv4 e IPv6 através do protocolo BGP-4, conforme as definições da RFC 4271 e suas respectivas erratas. Para esse fim, a CONTRATADA deverá:
- 2.1.10.1 Estabelecer e manter em funcionamento sessões BGP-4 em IPv4 e IPv6 com os roteadores da CONTRATANTE;
- 2.1.10.2 Fornecer à CONTRATANTE, mediante solicitação desta, tabelas de roteamento completas (full routing) ou parciais (partial routing) e rota padrão (default gateway);

- 2.1.10.3 Anunciar aos seus pares (peers) BGP nacionais e internacionais rotas para os prefixos CIDR IPv4 e IPv6 do Sistema Autônomo da CONTRATANTE, sem aplicar artifícios (tais como AS-prepend, manipulação de métricas etc.) que possam interferir na política de roteamento definida pela CONTRATANTE;
- 2.1.10.4 Usar endereços IPv4 e IPv6 roteáveis na Internet (ou seja, que não estejam listados na RFC 1918) nas interfaces de rede que interligam diretamente seus roteadores aos da CONTRATANTE.
- 2.1.11 O serviço oferecido pela CONTRATADA deverá possuir suporte a autenticação das sessões de BGP através de MD5 (Message-Digest Algorithm), para IPv4 e IPv6.
- 2.1.12 O roteamento destinado às redes divulgadas pela ITAIPU para a CONTRATADA deverá ser realizado pelo circuito contratado não utilizando outro AS como trânsito.
- 2.1.13 A CONTRATADA não poderá encaminhar aos roteadores da CONTRATANTE tráfego que não seja destinado às redes autorizadas por esta última.
- 2.1.14 A CONTRATADA não poderá aplicar nenhum tipo de filtro ou cache transparente que possam afetar o tráfego de dados da CONTRATANTE, a menos que tenha a prévia e expressa concordância desta última. A exceção é o serviço contra ataques DDOS (Distributed Denial of Service) que precisará ser realizado pela própria CONTRATADA com geração de relatórios mensais de detecção da ferramenta;
- 2.1.15 A CONTRATADA deverá fornecer uma chave de acesso (login) com permissão para acesso via ssh ou https a uma máquina looking-glass, situada na rede IP da CONTRATADA, em que tenha ativo o protocolo BGP4 com full-routing para consulta de no mínimo os seguintes itens:
  - 2.1.15.1 A visualização dos ASN percorridos até determinado endereço IP ou ASN - AS Path;
  - 2.1.15.2 A visualização das rotas com endereços de rede, máscara, gateway e tempo de vida/criação da rota;
  - 2.1.15.3 A visualização de um sumário com informações gerais relativas ao BGP como a versão da tabela de roteamento, última atualização da tabela, status e tempo de conexão dos neighbors;
  - 2.1.15.4 A execução de ping e trace-route até um determinado endereço IP;
  - 2.1.15.5 Verificar as ocorrências de flap e dampening.
- 2.1.16 A CONTRATADA deverá fornecer um bloco /29, de 8 (oito) endereços IP fixos e válidos na rede mundial de computadores para ITAIPU.
- 2.1.17 [A infraestrutura de conectividade contratada deverá ser totalmente disponibilizada através de fibras ópticas fim a fim, entre as dependências da CONTRATADA e a rede da CONTRATANTE, incluindo a última milha, não sendo aceito enlace de rádio ou outras tecnologias em qualquer parte da rede.](#)
- 2.2 **Link de tráfego IP para internet com velocidade de 1 Gbps (bloco IPv4 /29), com solução anti DDoS.**
  - 2.2.1 A CONTRATADA deverá fornecer e instalar um canal de comunicação Internet IP, com banda garantida de 1 Gbps com ligação à Rede Internet, com velocidade simétrica (upload e download), para uso exclusivo da ITAIPU na Usina Hidrelétrica Itaipu.
  - 2.2.2 A CONTRATADA deverá prover o serviço de Anti-DDoS neste canal de comunicação conforme premissas estabelecidas nesta especificação.

- 2.2.3 A banda fornecida pela CONTRATADA de 1 Gbps deve ser mantida durante 24 horas por dia, 7 dias por semana, incluindo sábados, domingos e feriados.
- 2.2.4 A CONTRATADA deverá fornecer um bloco /29 de 8 (oito) endereços IP fixos e válidos na rede mundial de computadores.
- 2.2.5 Caso a CONTRATADA venha a oferecer velocidades superiores à instalada, sem a solicitação da ITAIPU, não terá direito a qualquer espécie de remuneração adicional ou aditivo contratual, assumindo integralmente os custos dessa alteração.
- 2.3 **Link de tráfego IP para internet com velocidade de 5 Mbps (bloco IPv4 /29), com solução anti DDoS.**
  - 2.3.1 A CONTRATADA deverá fornecer e instalar um canal de comunicação Internet IP, com banda garantida de 5 Mbps com ligação à Rede Internet, com velocidade simétrica (upload e download), para uso exclusivo da ITAIPU na Usina Hidrelétrica Itaipu.
  - 2.3.2 A CONTRATADA deverá prover o serviço de Anti-DDoS neste canal de comunicação conforme premissas estabelecidas nesta especificação.
  - 2.3.3 A banda fornecida pela CONTRATADA de 5 Mbps deve ser mantida durante 24 horas por dia, 7 dias por semana, incluindo sábados, domingos e feriados.
  - 2.3.4 A CONTRATADA deverá fornecer um bloco /29 de 8 (oito) endereços IP fixos e válidos na rede mundial de computadores.
  - 2.3.5 Caso a CONTRATADA venha a oferecer velocidades superiores à instalada, sem a solicitação da ITAIPU, não terá direito a qualquer espécie de remuneração adicional ou aditivo contratual, assumindo integralmente os custos dessa alteração.
- 2.4 **Link de tráfego IP para internet com velocidade de 20 Mbps (bloco IPv4 /29), com solução anti DDoS.**
  - 2.4.1 A CONTRATADA deverá fornecer e instalar um canal de comunicação Internet IP, com banda garantida de 20 Mbps com ligação à Rede Internet, com velocidade simétrica (upload e download), para uso exclusivo da ITAIPU na Usina Hidrelétrica Itaipu.
  - 2.4.2 A CONTRATADA deverá prover o serviço de Anti-DDoS neste canal de comunicação conforme premissas estabelecidas nesta especificação.
  - 2.4.3 A banda fornecida pela CONTRATADA de 20 Mbps deve ser mantida durante 24 horas por dia, 7 dias por semana, incluindo sábados, domingos e feriados.
  - 2.4.4 A CONTRATADA deverá fornecer um bloco /29 de 8 (oito) endereços IP fixos e válidos na rede mundial de computadores.
  - 2.4.5 Caso a CONTRATADA venha a oferecer velocidades superiores à instalada, sem a solicitação da ITAIPU, não terá direito a qualquer espécie de remuneração adicional ou aditivo contratual, assumindo integralmente os custos dessa alteração.
- 2.5 **Link de tráfego IP para internet com velocidade de 10 Mbps (bloco IPv4 /29), com solução anti DDoS.**
  - 2.5.1 A CONTRATADA deverá fornecer e instalar um canal de comunicação Internet IP, com banda garantida de 10 Mbps com ligação à Rede Internet, com velocidade simétrica (upload e download), para uso exclusivo da ITAIPU na Usina Hidrelétrica Itaipu.
  - 2.5.2 A CONTRATADA deverá prover o serviço de Anti-DDoS neste canal de comunicação

conforme premissas estabelecidas nesta especificação.

- 2.5.3 A banda fornecida pela CONTRATADA de 10 Mbps deve ser mantida durante 24 horas por dia, 7 dias por semana, incluindo sábados, domingos e feriados.
- 2.5.4 A CONTRATADA deverá fornecer um bloco /29 de 8 (oito) endereços IP fixos e válidos na rede mundial de computadores.
- 2.5.5 Caso a CONTRATADA venha a oferecer velocidades superiores à instalada, sem a solicitação da ITAIPU, não terá direito a qualquer espécie de remuneração adicional ou aditivo contratual, assumindo integralmente os custos dessa alteração.

### **3. LOCAL DE PRESTAÇÃO DOS SERVIÇOS**

- 3.1 Os equipamentos e links deverão ser instalados na ITAIPU no endereço, localizada na Av. Tancredo Neves, 6731, em Foz do Iguaçu, Paraná.
- 3.2 Dentro da Central Hidrelétrica da ITAIPU, o cabo óptico da CONTRATADA deverá ser instalado conforme a rota apresentada no mapa do ADENDO I.

### **4. INSTALAÇÃO**

- 4.1 Após a assinatura do contrato a ITAIPU emitirá a OIS - Ordem de Início de Serviço, que será o documento que autorizará o início dos trabalhos e será utilizado como referência de datas e o tempo será contado sempre em dias corridos.
- 4.2 A CONTRATADA deverá realizar os serviços de instalação dos links (fibra ótica e equipamentos) e das respectivas ativações, até o Data Center da ITAIPU, observado o prazo máximo de 60 (sessenta) dias corridos, contados da data estabelecida na Ordem de Início de Serviços, a ser emitida após a assinatura deste contrato. A CONTRATADA é responsável por pequenas obras de correção, caso necessário, nas caixas de passagens até os Data Centers da ITAIPU. Toda atividade deverá ser supervisionada pela equipe da ITAIPU.
- 4.3 Após a data de emissão da OIS, CONTRATADA deverá se reunir com os gestores da ITAIPU, no prazo máximo de até 10 (dez) dias úteis. A data da reunião deverá ser agendada em comum acordo com a ITAIPU. Nesta reunião a CONTRATADA deverá:
  - 4.3.1 Tratar do alinhamento e elaboração da programação das atividades e plano de trabalho, para alinhamento das metodologias, ferramentas e produtos que serão utilizados, emissão de autorizações de entrada e movimentações de material, passes de veículos e apresentação de documentos exigidos nesta especificação. A CONTRATADA e a ITAIPU, em comum acordo, deverão fazer um planejamento das atividades de instalação antes de iniciar a instalação propriamente dita.
  - 4.3.2 Após a data de emissão da OIS, em até cinco (05) dias úteis, a CONTRATADA deverá indicar o responsável técnico, representante preposto e seu eventual substituto para responder perante a ITAIPU até o término do contrato.
  - 4.3.3 Agendar vistorias técnicas de pré-instalação aos sites da ITAIPU para definição do posicionamento dos equipamentos, da instalação elétrica e demais requisitos necessários à instalação física dos equipamentos. Como produto dessas vistorias técnicas a CONTRATADA deverá elaborar um relatório detalhado, por local de instalação. Tal relatório deverá fazer parte do Plano de Instalação.
  - 4.3.4 Apresentar os parâmetros a serem utilizados pelo sistema que registrará os chamados descritos no item 6 desta especificação técnica. Os mesmos serão analisados pela ITAIPU para identificação das adequações necessárias a serem

realizadas pela CONTRATADA para que a mesma atenda a todas as exigências descritas nesta especificação técnica.

- 4.4 Caso após a realização desta primeira reunião existam questionamentos direcionados a ITAIPU e/ou a CONTRATADA, a mesma terá o prazo de até 05 (cinco) dias úteis contados a partir do dia seguinte a realização da reunião, para responder formalmente. A ITAIPU disponibilizara para a CONTRATADA o endereço de correio eletrônico para que seja o contato técnico a ser utilizado para o disposto no subitem 4.3 da especificação técnica.
- 4.5 Como produto da reunião descrita no subitem 4.3 desta Especificação, a CONTRATADA deverá encaminhar por meio eletrônico, em 5 (cinco) dias úteis após a realização da reunião e esclarecimento de possíveis dúvidas remanescentes da mesma, o Plano de Instalação.
- 4.6 O Plano de Instalação dos serviços fornecidos deverá conter de forma detalhada:
  - 4.6.1 Descrição dos circuitos que deverão ser instalados;
  - 4.6.2 Pré-requisitos para a instalação: deverão ser descritos todos os recursos e condições que deverão ser providos pela ITAIPU, necessários para que a CONTRATADA possa realizar os serviços de instalação;
  - 4.6.3 Relatórios das vistorias técnicas de pré-instalação;
  - 4.6.4 Visão geral da arquitetura da solução que será implantada;
  - 4.6.5 Descrição das etapas do processo de instalação, detalhando as opções de configuração adotadas;
  - 4.6.6 Descrição do funcionamento da solução Anti DDoS, incluindo manuais de utilização dos portais web para visibilidade e administração do serviço de proteção Anti DDoS;
  - 4.6.7 Cronograma de execução;
- 4.7 No prazo de até 5 (cinco) dias úteis, a partir do recebimento formal do Plano de Instalação, a ITAIPU deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido a CONTRATADA um novo prazo de até 5 (cinco) dias úteis para eventuais ajustes e reapresentação da documentação reprovada. A versão definitiva do Plano de Instalação será a versão aprovada pela Equipe Técnica da ITAIPU.

## 5. CONDIÇÕES DE ACEITAÇÃO DA INSTALAÇÃO

- 5.1 Após concluir a instalação dos links, a CONTRATADA deverá emitir o Termo de Aceite de Instalação do Serviço, conforme modelo apresentado no ADENDO II, anexando os testes de validação dos enlaces.
- 5.2 Os testes de validação da última milha devem incluir:
  - 5.2.1 RFC-2544: Deverá efetuar medições de *throughput*, *back-to-back*, perda de quadros e latência de acordo com RFC 2544; tamanho do quadro: definido por RFC ou configurável pelo usuário de um a dez tamanhos de quadro.
  - 5.2.2 Geração de tráfego e modelagem de até 16 fluxos Ethernet e IP, incluindo o monitoramento simultâneo de taxa de transferência, perda de quadros, *jitter* de pacotes, latência e quadros fora de sequência. Incluir a capacidade de gerar tráfego com frames de tamanho fixo, tamanhos de quadro aleatórios ou varredura de um tamanho de quadro mínimo para um máximo. Deve, além disso, permitir inundação de MAC da camada 2.

- 5.2.3 Testes de Perda de Inserção e Atenuação, realizados em conformidade com a norma EIA/TIA-526-7, com utilização de equipamento OTDR (Refletômetro óptico de domínio do tempo) capaz de realizar os testes de conformidades no mesmo padrão.
- 5.3 No primeiro dia útil subsequente a data de confirmação de recebimento do Termo de Aceite de Instalação do Serviço por parte da ITAIPU, o serviço entrará na FASE DE HOMOLOGAÇÃO, etapa na qual será submetido a avaliação técnica qualitativa pela ITAIPU durante o prazo de 5 (cinco) dias úteis. Ao final deste período, caso a ITAIPU não se manifeste formalmente em contrário, o serviço será considerado como ativo comercialmente, estando apto para faturamento a partir do primeiro dia útil após o término da FASE DE HOMOLOGAÇÃO.
  - 5.3.1 São condições para a assinatura do Termo de Aceite de Instalação do Serviço por parte da ITAIPU:
    - 5.3.1.1 A ITAIPU receber o comunicado da CONTRATADA informando da conclusão dos serviços de instalação, conforme descrito no subitem 5.2 desta especificação técnica.
    - 5.3.1.2 A ITAIPU concluir a avaliação técnica qualitativa conforme condições constantes nesta especificação técnica e constatar que não existem anormalidades ou foram sanados todos os problemas detectados.
- 5.4 Caso não sejam atendidos todos os critérios técnicos exigidos na especificação técnica será emitido LAUDO desfavorável pelo Gestor do Contrato. A ITAIPU devolverá o Termo de Aceite de Instalação enviado pela CONTRATADA, e o serviço NAO ESTARÁ apto para faturamento.
- 5.5 O prazo para a instalação do serviço, disposto no item 4, será suspenso no momento do recebimento do Termo de Aceite de Instalação do Serviço e será retomado no dia subsequente a emissão do LAUDO desfavorável, indicado no subitem 5.3.1.

## 6. REGISTRO E ATENDIMENTO DE OCORRÊNCIAS

- 6.1 No prazo máximo de 10 (dez) dias úteis, contados a partir do dia seguinte a assinatura da Ordem de Serviço (OIS), a CONTRATADA deverá apresentar a ITAIPU as informações sobre os canais de atendimento para abertura dos chamados;
- 6.2 A CONTRATADA deverá providenciar o registro de toda e qualquer solicitação de reparo, independentemente de sua natureza, cabendo a ITAIPU, o devido acompanhamento. A ITAIPU serão disponibilizados os seguintes canais de atendimento para abertura dos chamados:
  - 6.2.1 Website e telefone (0800); ou
  - 6.2.2 Website e Call Center; ou
  - 6.2.3 E-mail e telefone (0800); ou
  - 6.2.4 E-mail e Call Center.
- 6.3 Cada chamado deverá conter, no mínimo, o registro das informações abaixo:
  - 6.3.1 Número do registro/ocorrência (a ser fornecido pela CONTRATADA);
  - 6.3.2 Identificação do atendente;
  - 6.3.3 Identificação do solicitante;
  - 6.3.4 Data e hora de abertura do chamado/início da interrupção (considerando o fuso



horário de Brasília);

- 6.3.5 Descrição da ocorrência.
- 6.3.6 Designação do circuito.
- 6.4 No provimento deste serviço por meio de telefone (0800) a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e moveis.
- 6.5 Para os atendimentos por meio de telefone (0800) ou de Call Center, o tempo máximo de espera deverá ser de até 03 (três) minutos.
- 6.6 No provimento deste serviço por meio Website, deverá ser possível que a ITAIPU indique uma lista de produtos por meio de arquivo anexo ou diretamente na página, em um único registro. Neste caso, a data e hora do registro serão consideradas como horário da abertura do chamado para todos os produtos listados.
- 6.7 No caso da CONTRATADA optar pelo atendimento por e-mail, deverão informar as caixas postais para recebimento de correspondência. Deverá ser possível que a ITAIPU indique uma lista de circuitos através de arquivo anexo ou diretamente no corpo de e-mail, em um único registro. Neste caso, a data e hora do registro serão consideradas como início de interrupção para todos os circuitos listados.
  - 6.7.1 A CONTRATADA deverá garantir o perfeito funcionamento do sistema de correio, sem qualquer impedimento para o recebimento das mensagens, tais como falta de espaço na caixa postal ou interrupção no sistema de mensagens.
  - 6.7.2 As notificações de recebimento deverão ser recebidas nas caixas disponibilizadas para a ITAIPU em até 1 (um) minuto após o envio da mensagem origem.
  - 6.7.3 Considerando a descentralização do corpo técnico da ITAIPU, a CONTRADADA deve disponibilizar, no máximo, 10 (dez) caixas postais, conforme solicitação da ITAIPU.
- 6.8 Durante a prestação do serviço, poderão ser agendados, a critério da ITAIPU, testes periódicos para constatação do funcionamento dos meios independentes de acesso.
- 6.9 O horário de abertura de chamado será determinado conforme abaixo:
  - 6.9.1 Para chamados abertos pelos canais 0800 ou Call Center → o horário da abertura do chamado será a data e hora da ligação realizada pelo profissional da ITAIPU informando do problema ocorrido. Caso a atendente não possa informar o número de chamado neste momento, a mesma deverá, obrigatoriamente, informar um número de protocolo que registre a data e hora da ligação realizada.
  - 6.9.2 Para chamados abertos pelo canal Website → o horário da abertura do chamado será a data e hora do acesso ao Website para registro do problema ocorrido. No momento do registro, a página web deverá informar o número de chamado, caso isso não seja possível, a mesma deverá informar um número de protocolo que registre a data e hora do acesso realizado.
  - 6.9.3 Para chamados abertos por e-mail → o horário da abertura do chamado será a data e hora da notificação de recebimento da mensagem origem. Caso os profissionais da CONTRATADA, responsáveis pelo registro dos chamados realizados por e-mail, não possa informar o número de chamado, os mesmos deverão, obrigatoriamente, informar um número de protocolo que registre a data e hora recebimento da mensagem origem, por meio do envio de um e-mail de resposta a ITAIPU.
- 6.10 O horário de abertura do chamado demarcara o início da contagem do prazo de solução das ocorrências, independente do retorno da CONTRATADA. O horário de abertura de chamado será determinado conforme descrito no subitem 6.9 desta



especificação técnica.

- 6.11 O serviço de registro de chamados deverá ser disponibilizado de acordo com a modalidade de atendimento estabelecida no subitem 6.2 desta especificação técnica.
- 6.12 O serviço de registro de chamados deverá ser disponibilizado em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados.
- 6.13 Não deverá haver qualquer limitação para o número de solicitações de reparo.
- 6.14 Não deverá haver qualquer limitação para o número de técnicos da ITAIPU autorizados a abrir chamados técnicos.

## 7. SUPORTE TÉCNICO

- 7.1 A CONTRATADA deverá fornecer todos os recursos necessários para a solução de gestão, supervisão e análise, mantendo uma equipe de monitoramento em horário integral, 24 horas por dia, sete dias por semana (24x7), disponível em seu centro de monitoramento que deverá acompanhar os indicadores e realizar as intervenções necessárias.
- 7.2 A CONTRATADA deverá fornecer serviços de operação, manutenção e suporte técnico de forma ininterrupta 24x7 durante toda a vigência do Contrato.
- 7.3 O monitoramento deverá ser proativo para toda a solução contratada, com notificações de eventos para as áreas responsáveis da ITAIPU e abertura de tickets de atendimento para as equipes responsáveis da CONTRATADA. Essas notificações devem ser realizadas por e-mail, contato telefônico ou mensagens SMS de forma a garantir que os analistas tenham sido efetivamente contatados.
- 7.4 A CONTRATADA deverá disponibilizar sob regime contínuo (24x7) um número de telefone para atendimento e registro de chamados pertinentes a solicitações ou incidentes relacionados ao serviço contratado.
- 7.5 O início do atendimento deverá ocorrer imediatamente após a abertura do chamado, sendo que a sua conclusão não poderá exceder os tempos de solução definidos na tabela do subitem 7.10.8.
- 7.6 Sempre que os limiares forem alcançados, alarmes devem ser gerados para as equipes envolvidas e automaticamente criar um chamado através das ferramentas de Trouble Tickets.
- 7.7 Para os casos de manutenções programadas, estas deverão ser realizadas pela CONTRATADA, sempre com aviso prévio à ITAIPU, de no mínimo 3 (três) dias úteis, devendo ocorrer sempre fora do horário comercial praticado pela ITAIPU.
- 7.8 Interrupções programadas pela CONTRATADA para efeitos de manutenção preventiva e/ou corretiva dos serviços podem ocorrer, sem prejuízo no cálculo de disponibilidade dos serviços afetados. Os horários e tempos de paralisação serão acordados e comunicados.
- 7.9 Serviço de Suporte Técnico.
  - 7.9.1 O Serviço de Suporte Técnico é um serviço de assistência prestado por técnicos especializados da CONTRATADA, local ou remotamente, para a execução de tarefas de manutenção corretiva relacionadas ao objeto do contrato.
  - 7.9.2 O Serviço de Suporte Técnico deverá estar disponível 24 horas por dia, 7 dias por semana à disposição da ITAIPU, durante a vigência do contrato, sem custo para a ITAIPU.

- 7.9.3 Este serviço poderá ser solicitado pela ITAIPU por meio de Solicitação de Serviço por meio de documento e/ou canais de comunicação especificados no Plano de Trabalho e pelo(s) Representante(s) previamente definido(s).
- 7.10 Solicitação de serviço de suporte técnico
- 7.10.1 O Serviço de Suporte Técnico (local ou remoto) será formalizado pela ITAIPU por meio de e-mail, chamada telefônica ou mensagens de texto (SMS), ocasião em que será aberta uma Solicitação de Serviço, considerando para todos os efeitos a data e a hora em que é realizado o contato solicitando o serviço.
- 7.10.2 A abertura e registro da solicitação de serviço de suporte técnico por parte da CONTRATADA deverá ser imediata para todos os casos e em regime 24x7.
- 7.10.3 O eventual deslocamento dos técnicos da CONTRATADA para fornecer o serviço de suporte técnico, incluindo as despesas de viagem que possam ocorrer, será de responsabilidade exclusiva da CONTRATADA.
- 7.10.4 Durante a execução dos serviços nas sedes da ITAIPU, os técnicos designados pela CONTRATADA não poderão atender qualquer solicitação de serviço originada de fontes não especificadas pela ITAIPU.
- 7.10.5 Para efeitos de atendimento por parte da CONTRATADA, levando em consideração o grau de não disponibilidade do sistema como um todo que possa causar o problema ocorrido, as solicitações de serviços de suporte técnico serão classificadas, de acordo com sua criticidade, da seguinte forma:
- 7.10.5.1 NÍVEL CRÍTICO, consiste em situação de emergência grave, caracterizada por qualquer uma das seguintes situações:
- i. Subsistema completamente parado que impede o funcionamento normal da solução como um todo (sistema parado).
  - ii. Indisponibilidade total do sistema.
- 7.10.5.2 NÍVEL MÉDIO, consiste numa situação de emergência, caracterizada por:
- i. Subsistema principal com desempenho degradado.
  - ii. Unidade gravemente degradada em sua capacidade de operação.
  - iii. Componentes simples completamente parados.
- 7.10.5.3 NÍVEL NORMAL, caracterizado por:
- i. Defeito menor que não afeta a disponibilidade do equipamento de computação hospedado.
  - ii. Problema em algum componente redundante.
  - iii. Defeito intermitente, desde que não se enquadre em níveis críticos ou médio.
- 7.10.5.4 NÍVEL DE CONSULTA, caracterizado por:
- i. Qualquer tipo de consulta que a ITAIPU decida fazer à CONTRATADA referente aos equipamentos e/ou serviços por ela proporcionados.
- 7.10.6 Ao abrir uma solicitação de serviço, a ITAIPU informará o nível de criticidade, conforme descrito acima, e a CONTRATADA deverá responder através dos canais de comunicação especificados.
- 7.10.7 A ITAIPU reserva-se o direito de modificar o nível de criticidade da solicitação de serviço à medida que o problema evolui, comunicando à CONTRATADA.

- 7.10.8 A CONTRATADA deverá fornecer o serviço de suporte técnico solicitado de acordo com os níveis de criticidade estabelecidos pela ITAIPU e mencionados na tabela a seguir:

CRITICIDADE	DESCRIÇÃO	TEMPO MÁXIMO PARA INÍCIO DO ATENDIMENTO (1)	TEMPO MÁXIMO SOLUÇÃO DO PROBLEMA (2)
0	Crítico	Imediato	2h
1	Médio	2h	6h
2	Normal	4h	12h
3	Consulta	4h	24h

- 7.10.8.1 Entende-se como início do atendimento o período compreendido entre a abertura do chamado ou solicitação de Serviço de Suporte Técnico e a designação do profissional responsável para atender à solicitação.
- 7.10.8.2 Entende-se como solução do problema o tempo total utilizado para a efetiva solução do problema. Os detalhes das ações deverão constar no relatório técnico correspondente e deverão ser assinados por um representante da área gestora, atestando o cumprimento, ou não, dos prazos.
- 7.10.8.3 Nos níveis Crítico e Médio, as horas serão corridas e não úteis.
- 7.10.9 O fechamento da Solicitação de Serviço deverá ser aprovado pela ITAIPU.
- 7.10.10 Em caso de descumprimento dos prazos estabelecidos, serão aplicadas as penalidades previstas no Contrato.

## 8. RELATÓRIOS

- 8.1 Durante a vigência contratual, a CONTRATADA deverá apresentar, até o 8º (oitavo) dia útil de cada mês, um arquivo contendo o registro de todas as interrupções do serviço ocorridas no mês anterior. O mesmo deverá estar no formato XLS (para ambiente MS Windows) ou outro formato definido em comum acordo e deverá conter as seguintes informações de cada interrupção:
- 8.1.1 Identificação do chamado;
  - 8.1.2 Designação do circuito;
  - 8.1.3 Endereço de instalação do circuito;
  - 8.1.4 Data e hora de abertura do chamado/início da interrupção (considerando o fuso horário Brasília);
  - 8.1.5 Data e hora do fechamento do chamado/fim da interrupção (considerando o fuso horário Brasília);
  - 8.1.6 Duração da interrupção (em minutos);
  - 8.1.7 Tempo de responsabilidade da contratada;

- 8.1.8 Causa da interrupção, classificada como segue:
  - 8.1.8.1 Responsabilidade do cliente;
  - 8.1.8.2 Problema no meio físico de acesso;
  - 8.1.8.3 Problema de rede da operadora;
  - 8.1.8.4 Problema de equipamento de rede da operadora;
  - 8.1.8.5 Problema de equipamento de acesso da operadora;
  - 8.1.8.6 Problema no serviço de proteção Anti DDoS: Bloqueio de tráfego legítimo;
  - 8.1.8.7 Problema no serviço de proteção Anti DDoS: Não bloqueio de tráfego malicioso;
  - 8.1.8.8 Problema no serviço de proteção Anti DDoS: Indisponibilidade das ferramentas de visibilidade e administração do serviço anti DDoS, explicitadas no item 13 desta especificação técnica.
  - 8.1.8.9 Outros (a detalhar no campo “Descrição detalhada da causa da interrupção”)
- 8.1.9 Descrição detalhada da causa da interrupção.
- 8.2 Durante a vigência contratual, a CONTRATADA deverá apresentar, até o 8º (oitavo) dia útil de cada mês, um arquivo contendo o registro de todas as ocorrências do serviço anti DDoS. O mesmo deverá estar no formato XLS (para ambiente MS Windows) ou outro formato definido em comum acordo e deverá conter as seguintes informações de cada interrupção:
  - 8.2.1 Identificação da ocorrência;
  - 8.2.2 Designação do circuito;
  - 8.2.3 Endereço de instalação do circuito;
  - 8.2.4 Data e hora da identificação do ataque (considerando o fuso horário de Brasília)
  - 8.2.5 Data e hora de notificação do ataque feita pela CONTRATADA a ITAIPU, conforme subitem 13.16 da especificação técnica;
  - 8.2.6 Data e hora da solicitação da mitigação do ataque pela ITAIPU (considerando o fuso horário de Brasília);
  - 8.2.7 O tipo e o alvo do ataque;
  - 8.2.8 A ocorrência foi mitigada de forma automática ou mediante autorização da ITAIPU;
  - 8.2.9 Data e hora do início da mitigação do ataque pela CONTRATADA (considerando o fuso horário de Brasília);
- 8.3 Em até 5 (cinco) dias úteis após o recebimento do arquivo citado no subitem 8.2, a ITAIPU deverá informar a CONTRATADA se o material encaminhado está de acordo ou solicitar as correções necessárias.

## 9. DISPONIBILIDADE MENSAL DO SERVIÇO

- 9.1 O Índice de Disponibilidade Mensal do Serviço (IDMS), objeto desta contratação, deverá ser de 99,40% (noventa e nove vírgula quarenta por cento).
- 9.2 O Índice de Disponibilidade Mensal do Serviço (IDMS), para as FERRAMENTAS DE VISIBILIDADE E ADMINISTRAÇÃO DO SERVIÇO ANTI DDoS, explicitadas no item 13, deverá ser de 99,40% (noventa e nove vírgula quarenta por cento).
- 9.3 O Índice de Disponibilidade Mensal do Serviço (IDMS) apurado será calculado pela

seguinte fórmula:

$$\text{IDMS apurado (\%)} = (1 - (\text{tempo de interrupção registrado no mês} / \text{tempo total})) \times 100$$

- 9.3.1 A ITAIPU aplicará um desconto correspondente ao minuto de interrupção (serviço não disponível) quando o objetivo de disponibilidade for inferior a 99,40%.
- 9.3.2 Deverá ser entendido como “tempo de interrupção registrado no mês” a soma de todos os tempos (em minutos) entre a(s) formalização(ões) do(s) registro(s) do(s) chamado(s) e a completa solução do(s) problema(s) com o respectivo fechamento entre a ITAIPU e a CONTRATADA, desde que não seja constatada responsabilidade da ITAIPU. A ITAIPU fará a formalização do registro de chamado nas seguintes situações:
  - 9.3.2.1 A impossibilidade de trafegar dados, voz ou vídeo através dos circuitos contratados, causada pelo acesso, porta, ou problemas internos da rede da CONTRATADA;
  - 9.3.2.2 O não atendimento a qualquer um dos indicadores técnicos descritos nesta especificação técnica.
- 9.3.3 Deverá ser entendido como “Tempo Total Mensal” do serviço:
  - 9.3.3.1 A quantidade de dias da prestação do serviço, expresso em minutos, considerando-se o mês comercial nos meses da ativação e da desativação do circuito.
  - 9.3.3.2 43.200 minutos para os demais meses.
- 9.3.4 Ocorrências que se repitam num período de menos de três horas serão consideradas problemas intermitentes, sendo considerado o tempo decorrido entre a primeira e a última ocorrência para efeito de cálculo do tempo de interrupção.
- 9.3.5 Não serão computadas no cálculo do IDMS, 2 (duas) interrupções anuais do serviço, agendadas, em comum acordo, com antecedência mínima de 15 (quinze) dias corridos, ou outro período concedido pela ITAIPU, sendo de no máximo 4 (quatro) horas de duração.
- 9.3.6 Falhas na infraestrutura, sob responsabilidade da ITAIPU, que comprometam a disponibilidade do Serviço contratado, não acarretarão ônus à CONTRATADA.
- 9.4 A CONTRATADA deve garantir uma vazão mínima de 95% (noventa e cinco por cento) da velocidade contratada, considerando para este cálculo a carga de todos os protocolos utilizados pela ITAIPU, independente de falhas em rotas alternativas. O não atendimento a este item será entendido como indisponibilidade do circuito.
- 9.5 A CONTRATADA deverá apresentar entre o primeiro e o quinto dia útil do mês subsequente à realização dos serviços o Relatório de Disponibilidade por enlace contratado e apresentação da planilha Prévia de Faturamento para aprovação do gestor da ITAIPU. Na Planilha Prévia de Faturamento deverá constar em caso de valores inferiores a 99,4% de disponibilidade em algum enlace, o início da falha será marcado pelo aviso/registro da ITAIPU para a CONTRATADA. O término do período será efetivado pelo retorno/aviso da CONTRATADA, somado a confirmação pela ITAIPU, que o problema foi solucionado. O tempo também será considerado quando a CONTRATADA comunicar à ITAIPU, o que ocorrer primeiro. O valor será descontado do respectivo enlace. O abatimento corresponde ao serviço não entregue. O referido abatimento não exime a CONTRATADA das Penalidades previstas no contrato.
- 9.6 **TOLERÂNCIAS DE DEGRADAÇÃO DO DESEMPENHO DO SERVIÇO**
  - 9.6.1 Perdas de Pacote

- 9.6.1.1 O tráfego poderá apresentar o máximo de 1% (um por cento) de perda de pacote. O índice de perda de pacote será computado através de pacotes ICMP do tipo echo-request e echo-reply ou timestamp-request e timestamp-reply que trafegarão entre o roteador de conexão da ITAIPU e o roteador de borda da CONTRATADA. Será utilizada uma taxa de amostragem superior a 100 (cem) pacotes de até 1500 (mil e quinhentos) bytes a cada 10 (dez) minutos. A perda será considerada superior a este índice, quando a quantidade de pacotes sem retorno em duas amostragens consecutivas exceder 1% (um por cento). O não atendimento a este item será entendido como indisponibilidade do circuito.
- 9.6.1.2 Não serão consideradas para a amostragem de perda de pacotes as perdas causadas pelo descarte de pacotes ofensivos, como os vindos de um ataque de negação de serviço (DoS), ou as perdas causadas pelo congestionamento no circuito contratado.
- 9.6.2 Latência
- 9.6.2.1 A CONTRATADA deverá garantir em seu serviço uma latência média inferior a 25 ms (RTT - Round Trip Time) entre o roteador de conexão da ITAIPU até o roteador de borda da CONTRATADA. Este índice será computado através de pacotes ICMP do tipo echo-request e echo-reply ou timestamp-request e timestamp-reply que trafegarão entre o roteador de conexão da ITAIPU e o roteador de borda da CONTRATADA. Será utilizada uma taxa de amostragem superior a 100 (cem) pacotes de até 1500 (mil e quinhentos) bytes a cada 10 (dez) minutos. A latência será considerada superior à 25 ms quando duas amostragens consecutivas acusarem latência média maior que 25 ms. O não atendimento a este item será entendido como indisponibilidade do circuito.
- 9.6.2.2 Não serão consideradas para a amostragem de latência média, as variações de latência causadas por pacotes ofensivos, como os vindos de um ataque de negação de serviço (DoS), ou a variações de latência causadas pelo congestionamento no circuito contratado.
- 9.7 **INTERRUPÇÃO DE SERVIÇOS**
- 9.7.1 As interrupções programadas pela ITAIPU para efeitos de manutenção preventiva e/ou corretiva dos serviços poderão ocorrer, sem prejuízo no cálculo de disponibilidade dos serviços afetados. Os horários e tempos de paralisação serão acordados e comunicados pelos gestores da ITAIPU.

## 10. REQUISITOS TÉCNICOS

- 10.1 Preferencialmente deverão ser disponibilizados, no mínimo, 2 (dois) meios independentes de acesso aos endereços descritos na especificação técnica. Estes meios deverão utilizar caminhos / rotas diferentes através de fibra óptica. A ITAIPU, a qualquer momento poderá auditar a comprovação da solução apresentada, por vistorias e testes, acordados com a CONTRATADA.
- 10.1.1 Serão considerados caminhos diferentes caso a distância entre os cabos seja de no mínimo 3 (três) metros durante todo o percurso entre a CONTRATADA e a caixa de entrada localizada nas dependências da ITAIPU, salvo distância necessária para aproximação e manobras dos cabos. A critério da CONTRATADA, e desde que não afete o índice de disponibilidade exigido, será permitida a utilização de caixa já existente antes da entrada no prédio da ITAIPU.
- 10.2 Para o provisionamento dos serviços a CONTRATADA deve:
- 10.2.1 Possuir registro de AS nos organismos internacionais de registro, tais como ARIN e

RADB.

- 10.2.2 Garantir que os circuitos contratados serão exclusivamente dedicados para o tráfego da ITAIPU.

## 11. REQUISITOS DO ROTEADOR/CPE

- 11.1 A Contratada deverá fornecer um roteador/CPE para prover o link, com as características mínimas a seguir descritas:
- 11.1.1 O roteador deverá ser fornecido pela CONTRATADA com todos os acessórios e programas necessários à sua instalação, operação e monitoração proativa.
  - 11.1.2 Deve ser fornecido equipamento para permitir a conexão do Link de acesso à Internet ao ambiente LAN da ITAIPU. Este equipamento deve operar em 110/220V.
  - 11.1.3 O roteador deverá ser instalado com todos os acessórios necessários em um rack 19” e ocupar no máximo 2 UR (duas unidades de rack).
  - 11.1.4 Ser dimensionado, fornecido, instalado, configurado, mantido, gerenciado e operado pela CONTRATADA, garantindo-se o desempenho e os níveis de serviços contratados.
- 11.2 As características do equipamento devem ser totalmente compatíveis com os serviços especificados e atender completamente aos níveis de serviços pretendidos nesta especificação técnica;
- 11.3 A versão do sistema operacional dos equipamentos deve ser a versão estável (final) mais atual, na data de entrega;
- 11.4 A atualização do sistema operacional deverá ser efetivada sempre que houver lançamento de novas versões com atualizações críticas, que agreguem melhorias ou correções aos serviços contratados;
- 11.5 Deverá implementar interface modo texto baseada em SSHv2 para acesso remoto ao equipamento;
- 11.6 Deverá possuir fonte de alimentação com chaveamento automático de tensão de entrada 110/220 VAC a 60 Hz;
- 11.7 Devem permitir a criação de usuários, em base localizada no próprio roteador, com permissão de acesso ao equipamento do tipo “somente leitura”, bem como a execução de comandos visualização de informações e configuração, bem como a comandos de troubleshooting - ping (simples e avançado), traceroute, telnet e SSH. O acesso a que se refere este item deve ser permitido via SSH e HTTPS. Não deve haver restrições aos comandos.

## 11.8 INTERFACES EQUIPAMENTO CPE:

- 11.8.1 A(s) interface(s) de interligação do(s) circuito(s) da CONTRATADA aos equipamentos da ITAIPU, deverá(ão) ser no mínimo Gigabit Ethernet, exceto para os links com velocidades maiores ou igual a 1Gbps, que deverá ser utilizado interface de no mínimo de 10GBASE-SR (IEEE 802.3ae);
- 11.8.1 acesso físico interno (conexão entre o equipamento de comunicação de dados da CONTRATADA instalado nas dependências da CONTRATANTE e a rede desta), deverá



ser formado por 2 (dois) ou mais enlaces Tenggabit Ethernet 10GBASE-SR (IEEE 802.3ae), agregados via LACP - Link Aggregation Control Protocol (IEEE 802.3ad). A exclusivo critério da CONTRATANTE, é permitido o uso de tecnologias alternativas, tais como Gigabit Ethernet 1000BASE-SX (IEEE 802.3z), 10 Gigabit Ethernet 10GBASE-SR (IEEE 802.3ae), agregação via EtherChannel, etc.

11.8.2 WAN: Número suficiente de interfaces para conexão com os enlaces WAN fornecidos (Links de acesso da Contratante).

11.9 A CONTRATADA deverá fornecer equipamentos homologados pela ANATEL.

## 12. REQUISITOS DE CAPACIDADE

12.1 A CONTRATADA deverá obrigatoriamente comprovar ser um AS (Autonomous System).

12.2 A CONTRATADA deverá operar um Sistema Autônomo (AS) devidamente registrado no Núcleo de Informação e Coordenação do PontoBR (NIC.br) do Comitê Gestor da Internet no Brasil (CGI.br). O serviço de consulta WHOIS em whois.registro.br deve comprovar que o número do sistema autônomo (ASN) está associado ao CNPJ da CONTRATADA ou à empresa com vínculo societário comprovado.

12.3 A CONTRATADA deverá possuir conexão direta de trânsito ou peering (no máximo 1 (um) AS hop), com ao menos 3 (três) backbones Internet com AS distintos em capacidade iguais ou superiores à banda máxima (velocidade) solicitada nesta especificação.

12.4 A CONTRATADA deverá possuir, no mínimo, 2 (dois) peering internacionais (que não seja via satélite), com América Latina e Estados Unidos.

12.5 A CONTRATADA deve possuir conexão direta de trânsito, com no mínimo 2 (dois) backbones Internet com AS distintos, sendo no mínimo 1 (um) deles Internacional e o outro de abrangência nacional, para IPv4 e IPv6.

12.6 A CONTRATADA deve possuir um peering/CDN com Google, Microsoft e Meta.

## 13. REQUISITOS DE SEGURANÇA DO SERVIÇO ANTI DDOS

13.1 A solução deve implementar mecanismos capazes de detectar ataques que façam o uso não autorizado de recursos de rede, automaticamente, tanto para IPv4 e IPv6, para no mínimo:

13.1.1 Ataques de inundação ou volumétricos, incluindo:

13.1.1.1 SYN Flood;

13.1.1.2 UDP Flood;

13.1.1.3 TCP Flood;

13.1.1.4 ICMP Flood.

13.1.2 Ataques à pilha TCP, incluindo:

13.1.2.1 Mau uso das flags TCP;

13.1.2.2 Ataques de RST e FIN;

13.1.2.3 TCP idle Resets.

13.1.3 Ataques que utilizam fragmentação de pacotes (IP, TCP e UDP).

13.1.4 Ataques de botnets.

- 13.2 A solução deve implementar mecanismos capazes de mitigar quaisquer ataques que façam o uso não autorizado de recursos de rede, automaticamente, tanto para IPv4 e IPv6, para no mínimo:
  - 13.2.1 Ataques de inundação ou volumétricos, incluindo:
    - 13.2.1.1 SYN Flood;
    - 13.2.1.2 UDP Flood;
    - 13.2.1.3 TCP Flood;
    - 13.2.1.4 ICMP Flood.
  - 13.2.2 Ataques à pilha TCP, incluindo:
    - 13.2.2.1 Mau uso das flags TCP;
    - 13.2.2.2 Ataques de RST e FIN;
    - 13.2.2.3 TCP idle Resets.
  - 13.2.3 Ataques que utilizam fragmentação de pacotes (IP, TCP e UDP);
  - 13.2.4 Ataques de botnets e worms;
  - 13.2.5 Ataques que utilizam falsificação de endereços IP de origem (IP spoofing);
  - 13.2.6 Ataques à camada de aplicação, incluindo os protocolos HTTP e DNS, para no mínimo:
    - 13.2.6.1 HTTP URL Get/Post Flood;
    - 13.2.6.2 SIP Invite Flood;
    - 13.2.6.3 DNS Flood;
    - 13.2.6.4 DNS, NTP e SNMP Reflection/Amplification;
    - 13.2.6.5 Slowloris e Pyloris.
- 13.3 A solução deve implementar mecanismo de mitigação baseado no desvio de tráfego sob suspeita para um Centro de Mitigação na infraestrutura da CONTRATADA.
  - 13.3.1 No Centro de Mitigação o tráfego será inspecionado e tratado de forma que o tráfego malicioso seja bloqueado e o tráfego legítimo seja devolvido para a rede para ser roteado até seu destino;
  - 13.3.2 A mitigação de ataques deverá 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 na infraestrutura da CONTRATADA, de forma transparente para a ITAIPU;
  - 13.3.3 Deverá ser possível desviar para o Centro de Mitigação somente o tráfego para o(s) IP(s) sob suspeita de ataque;
  - 13.3.4 O sistema implantado na rede da CONTRATADA deverá atuar sobre o tráfego somente em momentos de ataque, estando completamente “off-line” em situações normais.
- 13.4 A solução deve suportar a detecção e mitigação automática de ataques, utilizando múltiplas técnicas para mitigação e contramedidas, para no mínimo:
  - 13.4.1 White lists;
  - 13.4.2 Black lists;

- 13.4.3 Limitação de taxa;
- 13.4.4 Técnicas desafio-resposta;
- 13.4.5 Descarte de pacotes mal-formados;
- 13.4.6 Bloqueio por localização geográfica (país) de endereços IP;
- 13.4.7 Técnicas de mitigação de ataques aos protocolos HTTP e DNS;
- 13.4.8 Manter uma lista dinâmica de endereços IP bloqueados.
- 13.5 Os endereços IP que não enviarem mais requisições maliciosas deverão ser removidos da lista de IPs bloqueados, após um período de tempo considerado seguro pela CONTRATADA;
- 13.6 Qualquer sistema colocado in-line no site da ITAIPU, caso a CONTRATADA ofereça, deverá ter obrigatoriamente comunicação com algum Centro de Mitigação implantado na rede da CONTRATADA, de forma a coordenar a limpeza automaticamente;
- 13.6.1 A solução deve implementar mecanismos capazes de detectar e mitigar ataques baseados em modo aprendizagem, através de anomalias estatísticas e desequilíbrio de volume de tráfego, que permite utilização de perfil de tráfego (baseline) tanto de longo quanto de curto prazo, para ataques volumétricos.
- 13.7 A solução deverá ser fornecer proteção para Flash Crowd, ou seja, quando ocorre o crescimento do volume de tráfego legítimo acima do esperado (perfil de tráfego/baseline), a solução deverá ser capaz de diferenciar o tráfego legítimo do malicioso, bloqueando apenas o tráfego proveniente de ataques;
- 13.8 A solução deverá ser capaz de detectar e mitigar os ataques destinados a qualquer endereçamento IP, tanto para IPv4 e IPv6, sob administração da ITAIPU;
- 13.9 Nos procedimentos de mitigação de ataques fica proibido o encaminhamento do tráfego para análise e limpeza fora do território brasileiro, exceto se o tráfego de origem for proveniente do exterior, caso em que será permitido o encaminhamento do mesmo para um centro de mitigação fora do território nacional disponibilizado pela CONTRATADA;
- 13.10 A CONTRATADA deverá possuir ao menos 1 (um) Centro de Mitigação em território nacional com capacidade de detecção e/ou mitigação de ataques e que seja capaz de tratar, sem gargalos, o tráfego de ataques demandado;
- 13.11 A solução deve possuir capacidade de analisar a reputação de endereços IP, possuindo base própria de informações, gerada durante a filtragem dos ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP;
- 13.12 Não será aceito bloqueio de ataques DoS e DDoS por ACLs em roteadores de borda da CONTRATADA, exceto mediante solicitação da ITAIPU;
- 13.13 As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques e devem ser mantidas atualizadas durante toda a vigência do contrato;
- 13.14 A solução deverá suportar funções de análise dos pacotes tratados com visualização estilo “wireshark” e download em formato pcap.
- 13.15 **FERRAMENTAS DE VISIBILIDADE E ADMINISTRAÇÃO DO SERVIÇO ANTI DDoS**
- 13.15.1 A CONTRATADA deverá fornecer acesso à ferramenta através de um navegador padrão para disponibilizar relatórios e informações do tráfego monitorado, bem como visualizar os eventos e alertas de segurança contendo, no mínimo, as

seguintes informações:

- 13.15.1.1 Informações sobre o tipo do(s) ataque(s);
- 13.15.1.2 Horário de início e fim;
- 13.15.1.3 Volume de tráfego bloqueado e não bloqueado;
- 13.15.1.4 IP(s) de destino(s);
- 13.15.1.5 Os maiores alvos de ataques;
- 13.15.1.6 Os maiores ofensores (IP de origem);
- 13.15.1.7 Os maiores ofensores por geolocalização (país);
- 13.15.1.8 Percentual das origens do(s) ataque(s) por geolocalização (país);
- 13.15.2 A CONTRATADA deverá fornecer acesso à ferramenta através de navegador padrão que permita à ITAIPU customizar em tempo real as configurações e regras, para no mínimo:
  - 13.15.2.1 Detecção e mitigação automática baseada em limiares de pps (pacotes por segundo) e bps (bits por segundo);
  - 13.15.2.2 Bloqueio e limitação de taxa para um IP ou range de IP's de destino.

#### **13.16 MODALIDADE DE ATENDIMENTO E PRAZOS DO SERVIÇO ANTI DDOS**

- 13.16.1 A CONTRATADA deverá realizar a detecção de ataques, de forma automática e proativa para, no mínimo, os ataques listados no subitem do item 13.1, e deverá notificar a ITAIPU por telefone e correio eletrônico em até 20 (vinte) minutos a partir do início do ataque, informando o tipo e o(s) alvo(s) do ataque.
  - 13.16.1.1 Após notificação da suspeita de ataque por parte da CONTRATADA, a ITAIPU poderá solicitar a mitigação do ataque. A CONTRATADA terá até 10 (dez) minutos para iniciar a mitigação após solicitação da ITAIPU.
  - 13.16.1.2 A ITAIPU poderá optar pela mitigação automática previamente configurada dos ataques detectados e, neste caso, a detecção e a mitigação deverão ocorrer em até 10 (dez) minutos a partir do início do ataque.
  - 13.16.1.3 A ITAIPU poderá alterar a qualquer momento o modo de mitigação para um determinado tipo e alvo do ataque: mitigação mediante autorização da ITAIPU (subitem 13.16.1.1) ou mitigação automática (subitem 13.16.1.2).
- 13.16.2 Caso a ITAIPU identifique a existência de tráfego malicioso, a CONTRATADA deverá realizar a mitigação de ataques em até 15 (quinze) minutos após a solicitação formal da ITAIPU através dos canais especificados no item 13.16.4.
  - 13.16.2.1 A ITAIPU poderá solicitar a mitigação do tráfego destinado a um IP específico, conjunto de IP's ou range de IP's.
  - 13.16.2.2 A ITAIPU poderá solicitar regras de mitigações específicas de acordo com as técnicas listadas no item 13.4.
- 13.16.3 Não haverá limitação na quantidade de mitigações de ataques e no volume de tráfego bloqueado durante o período de vigência contratual, seja através de detecção proativa (item 13.16.1) ou reativa (item 13.16.2);
- 13.16.4 A CONTRATADA deverá disponibilizar um Centro Operacional de Segurança (ou SOC - Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com operação de atendimento conforme definido no item 6 da especificação técnica;

- 13.16.5 As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
- 13.16.6 Caso seja constatado que o tráfego de DDoS não tenha sido bloqueado na rede da CONTRATADA após o tempo definido de acordo com os itens 13.16.1 e 13.16.2, o tempo de duração do ataque não bloqueado será contabilizado como indisponibilidade do serviço;
- 13.16.7 Caso seja constatado que o tráfego legítimo tenha sido bloqueado indevidamente por mal funcionamento da solução da CONTRATADA, o tempo de duração do bloqueio indevido será contabilizado como indisponibilidade do serviço.

#### 14. MEDIÇÃO DOS SERVIÇOS

- 14.1 Os serviços serão recebidos provisoriamente por responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações técnicas.
- 14.2 Os serviços poderão ser rejeitados, no todo ou em parte, quando for executado em desacordo com os procedimentos descritos na especificação técnica ou constatado utilização de material, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo responsável pela fiscalização do contrato, à custa da CONTRATADA, sem prejuízo da aplicação de penalidades.
- 14.3 Os serviços serão recebidos definitivamente no prazo de até 5 dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do serviço executado e materiais empregados.
- 14.4 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.
- 14.5 pagamento das faturas mensais estará sujeito à glosa quando não houver cumprimento dos níveis de serviço exigidos ou quaisquer outras que impliquem em glosas previstas.
- 14.6 A ITAIPU aplicará um desconto correspondente ao minuto de interrupção (serviço não disponível) quando o objetivo de disponibilidade for inferior a 99,4%, calculado conforme a seguinte fórmula:

$$D = P \times I / 43200$$

- 14.6.1 D = Valor do desconto em reais (R\$) relativo à falha no acesso - circuito dedicado indisponível/baixa performance.
- 14.6.2 I = Quantidade de minutos indisponíveis/baixa performance.
- 14.6.3 P = Preço mensal em reais (R\$) dos serviços contemplados no(s) Lote(s) 1 e/ou no 2.
- 14.7 Para efeito de contagem de tempo, o início da falha será marcado pelo aviso/registro da ITAIPU para a CONTRATADA. O término do período será efetivado pelo retorno/aviso da CONTRATADA, somado a confirmação pela ITAIPU, que o problema foi solucionado. O tempo também será considerado quando a CONTRATADA comunicar à ITAIPU, o que ocorrer primeiro.

#### 15. HORÁRIO DE TRABALHO

- 15.1 Para os trabalhos a serem desenvolvidos na estrutura interna da ITAIPU, a

CONTRATADA deverá observar o horário praticado na Central Hidrelétrica de ITAIPU, compreendido de segunda a sexta-feira, das 7h30 às 17h30, exceto feriados e dias não trabalhados, conforme o calendário da ITAIPU.

- 15.2 As Horas extras executadas por exclusiva necessidade da CONTRATADA, para recuperação de prazos contratuais, poderá ser executada com prévia autorização da Itaipu, sem nenhum adicional.
- 15.3 Todas as atividades que necessitem que o ambiente contratado seja desativado, em parte ou no todo, deverão ser realizadas depois do término da jornada diária de trabalho. Neste caso, a CONTRATADA deverá obter previamente a autorização de execução deste serviço junto a ITAIPU. Esta programação de serviço deverá ser feita no prazo mínimo de 2 (dois) dias úteis, salvo em casos de indisponibilidade dos recursos envolvidos, onde o atendimento deve ser imediato e respeitando o SLA contratado.
- 15.4 Todo o transporte de materiais e todo e qualquer deslocamento de empregados da Contratada será de total responsabilidade da Contratada.
- 15.5 O acesso de empregado da contratada estará restrito ao local onde serão realizados os serviços e sempre terão o acompanhamento de um empregado da Itaipu previamente designado para tal.

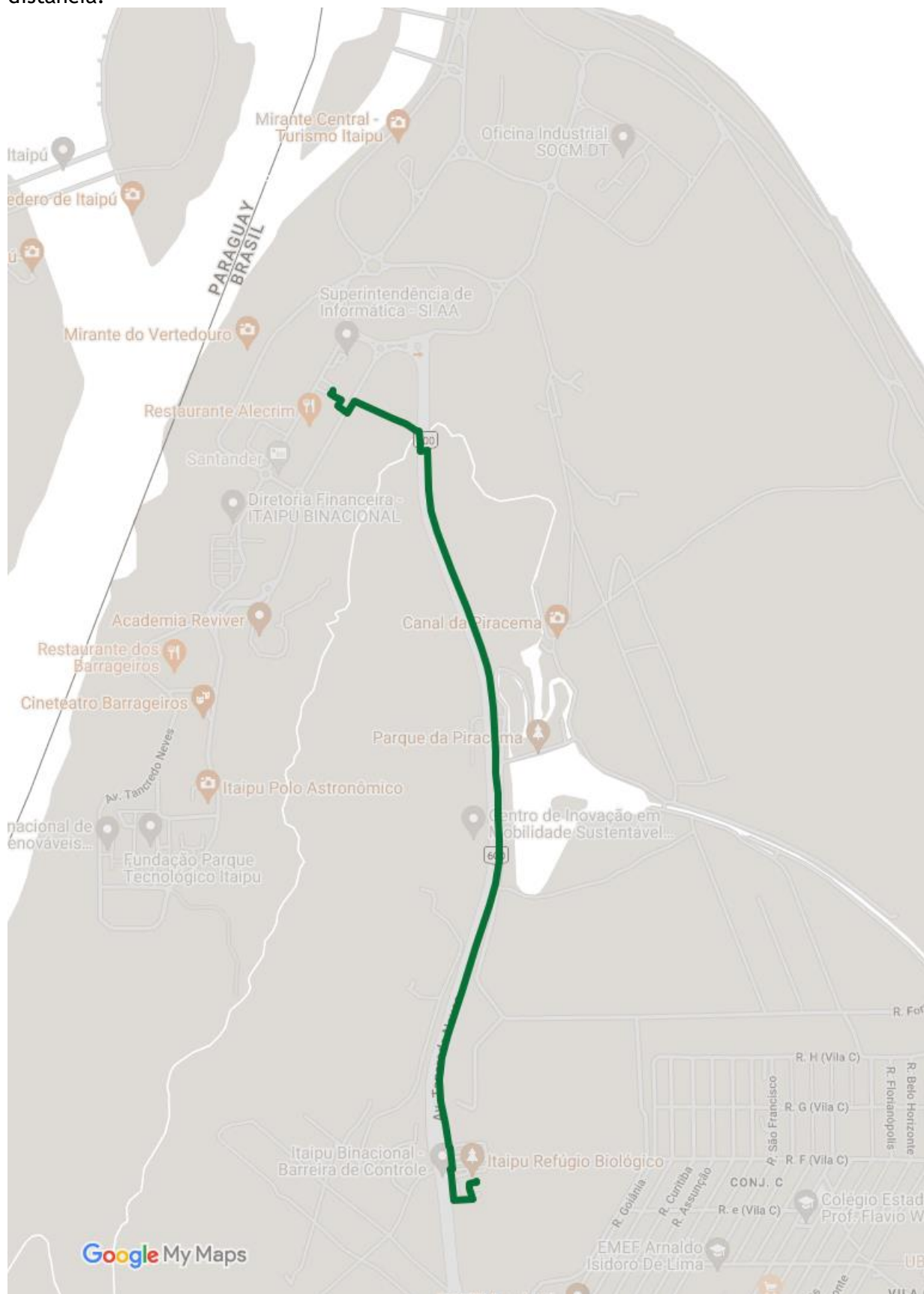
## **16.ADENOS**

ADENDO I - ROTA DO CABO ÓPTICO NA ITAIPU

ADENDO II - TERMO DE ACEITE

## ADENDO I - ROTA DO CABO ÓPTICO NA ITAIPU

Trajetória apresentada pela linha em verde, representando aproximadamente 4 Km de distância.





## ADENDO II - MODELO DE TERMO DE ACEITE

### TERMO DE ACEITE

À ITAIPU Binacional

Referente ao circuito: <inserir a designação do circuito>

Informamos que concluímos a instalação do circuito abaixo identificado

Designação do circuito:	
Tipo de solicitação:	(   ) Instalação   (   ) Alteração de velocidade
Velocidade do circuito:	
Disponibilidade do circuito:	
Endereço completo:	
Data da Ativação:	

Iniciaremos a execução e o faturamento dos serviços entregues no endereço formalizado neste Termo, a partir da data de início indicada abaixo.

Atenciosamente

De acordo

---

Responsável da Contratada

---

Responsável da ITAIPU

Data da instalação: \_\_\_\_/\_\_\_\_/\_\_\_\_

Data de início do serviço: \_\_\_\_/\_\_\_\_/\_\_\_\_

**OBSERVAÇÃO: ESTE DOCUMENTO DEVE SER EMITIDO EM PAPEL TIMBRADO QUE IDENTIFIQUE O EMISSOR.**