Resposta ao pedido de esclarecimento da **Empresa EMBRATEL CLARO – BRASIIL.**

PEDIDO ESCLARECIMENTO 01

Os itens 3.1 e 3.2 do TERMO DE REFERÊNCIA citam respectivamente que: "O link dedicado de no mínimo 300Mbps com a Internet deve ser entregue no 6º andar da sede do CN-SESI, localizada localizado no EAMN - Edifício Armando Monteiro Neto, Setor Bancário Norte, Quadra 01, Bloco I, Brasília – DF". "A fibra ótica que chegar no 6º andar da sede do CN-SESI deverá ser interligada com o switch, fornecido do CN-SESI, que fica localizado no 7º andar". Nestes 2 itens, não fica claro como a CONTRATANTE necessita que o serviço seja entregue, nem o local exato. O serviço normalmente é entregue em um único local, na maioria das vezes no switch da CONTRATANTE, que neste caso seria no sétimo andar, porém, a CONTRATANTE solicita outra entrega no 6º andar. Sendo assim, solicitamos maiores esclarecimento e detalhamento sobre onde o serviço será entregue e por qual motivo e necessidade a CONTRATANTE informa 2 locais de entrega, 1 no 6º andar e outro no 7º andar. Qual seria a necessidade?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o link precisa ser entregue no 6º andar da sede do CN-SESI que fica localizado no EAMN - Edifício Armando Monteiro Neto, Setor Bancário Norte, Quadra 01, Bloco I, Brasília – DF. Caso a PROPONENTE deseje saber o local exato, o termo de referência prevê no item 14.3 a solicitação de uma vistoria técnica.

PEDIDO ESCLARECIMENTO 02

Os itens 3.3 e 3.4 respectivamente do TERMO DE REFERÊNCIA citam que: "O link dedicado de no mínimo 300Mbps com a Internet deve ser entregue na sede do CNSESI com redundância através de 2 (duas) conexões distintas entre o ponto de presença da CONTRATADA e o CN-SESI". "A conexão que ficar como a de "backup" deverá suportar no mínimo 100% (cem por cento) da velocidade de no mínimo 300Mbps". Entendemos que a entrega do link de 300 Mbps através de um anel óptico, onde caso ocorra a indisponibilidade por um lado do anel óptico, o outro lado do anel assuma o tráfego, atenderia estes 2 itens do edital integralmente. Nosso entendimento está correto? Caso não esteja correto, solicitamos gentileza de esclarecer com mais detalhe, o que a CONTRATANTE necessitaria com este item.

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento está correto.

PEDIDO ESCLARECIMENTO 03

O item 3.11. do TERMO DE REFERÊNCIA cita que: "A CONTRATADA se responsabiliza pela substituição dos equipamentos em caso de defeitos (queima por descarga elétrica, superaquecimento, falha do equipamento). A substituição deverá ser feita em no máximo 2 (duas) horas após aberto o chamado". Para chegar-se a conclusão de que um equipamento queimou, faz-se necessário todo um trabalho de seccionalização do incidente. Por tratar-se de vários pontos que podem ser acometidos por falha até chegar aos equipamentos da unidade, solicitamos que este prazo seja de até 4h. Nossa solicitação será aceita?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que naturalmente a abertura do chamado para a substituição do equipamento se dará a partir do momento que for diagnosticada a necessidade de substituição. Portanto, o tempo mencionado pela PROPONENTE para chegar-se a conclusão não está contemplado no prazo máximo de 2 horas mencionado no item 3.11 do Termo de Referência. Sendo assim, esta solicitação não será aceita.

PEDIDO ESCLARECIMENTO 04

O item 3.19. do TERMO DE REFERÊNCIA cita que: "A taxa de transmissão deverá sempre estar disponível na totalidade do fluxo contratado e não deve incluir a taxa de overhead de protocolos até a camada 2 do modelo OSI". Porém, o overhead é inerente a tecnologia e pode chegar a consumir de 5 a 10% da banda, a depender do uso da CONTRATANTE, não podendo ser retirado ou suprimido, sendo assim, acatar o que é citado neste item, acarreta em oferecer um link maior que 300 Mbps. Além disso, sabendo que não existe link comercial com banda para atender 300 Mbps mais adição de banda para atender o overhead citado neste item, acaba por obrigar a empresa CONTRATADA a oferecer um link maior, que neste caso será de 400 Mbps. Este fato ocasiona a necessidade da CONTRATADA precificar um link de 400 Mbps, encarecendo a solução. Mediante ao exposto, solicitamos gentileza em aceitar que a entrega do link de 300 Mbps, objeto desta licitação, seja feita CONSIDERANDO o overhead inerente da tecnologia. Nossa solicitação será aceita?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que este item também atende ao princípio da isonomia, ou seja, todos os PROPONENTES terão a mesma condição de competição. Sendo assim, esta solicitação não será aceita.

PEDIDO ESCLARECIMENTO 05

O item 4.4. do TERMO DE REFERÊNCIA cita que: "A CONTRATADA deverá realizar quaisquer adequações necessárias a instalação dos circuitos de acesso nos locais especificados pela CONTRATANTE em seus sites, tais como dutos, caixas de passagem, sistema proteção contra descargas entre outros". Além deste item, os subitens do item 4.4 ratificam. Porém, o entendimento é que toda a infraestrutura citada neste item, fica nas dependências da CONTRATANTE e que não cabe a CONTRATADA intervir, nem efetuar qualquer tipo de obra na infraestrutura interna da CONTRATANTE. Cabe a CONTRATADA responsabilidade no que estiver externo ao endereço da edificação, como comummente ocorre em licitações semelhantes. Sendo assim, solicitamos que o que consta neste item seja de responsabilidade da CONTRATANTE e não CONTRATADA. Nossa solicitação será aceita?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto, pois conforme estabelece o item 4.4 e 4.4.3 do Termo de Referência, quaisquer eventuais adequações e adaptações ficarão a cargo da CONTRATADA. Para evitar que estas eventuais adequações e adaptações não estejam contempladas em sua planilha de formação de preços, o Termo de Referência prevê no item 14.3 que para confecção da proposta, a PROPONENTE poderá solicitar uma vistoria técnica para melhor dimensionamento da proposta. Sendo assim, esta solicitação não será aceita.

PEDIDO ESCLARECIMENTO 06

O item 6.4.2. do TERMO DE REFERÊNCIA cita que para testes de performance será utilizado: "Testes de ICMP para os hosts google-public-dns-a.google.com (atualmente IPv4 8.8.8.8), b.ntp.br (atualmente IPv4 200.189.40.8) portal.office.com (atualmente IPv4 13.107.9.156)". Porém, os endereços de destinos informados não são garantidos pela CONTRATADA e eles poderão estar indisponíveis, com lentidão ou outro problema de performance que não está na responsabilidade ou alcance da CONTRATADA, sendo assim, entendemos que o teste de performance ideal, de forma a garantir o link de internet de responsabilidade da CONTRATADA é aquele realizado do roteador de borda até a porta WAN do roteador CPE que fica no endereço da CONTRATANTE. A CONTRATADA não poderá ser penalizado por algo que não é responsável. Nosso entendimento está correto? Solicitamos que este texto seja alterado para adequação ao que foi justificado. Nossa solicitação será atendida?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto. Esclarecemos ainda que levaremos em consideração que a CONTRATADA não terá responsabilidade sobre os endereços utilizados durante os testes. No entanto, levando em consideração o alto porte tecnológico das empresas Google e Microsoft será mantido os endereços para testes. Além disto, a forma de medição sugerida no questionamento atestaria apenas a conexão da CONTRATANTE com a CONTRATADA e não a conexão da CONTRATANTE com a internet, que é o objetivo dessa contratação. A forma de medição especificada no edital define 3 hosts de Entidades diferentes, que contam com diversas camadas de redundâncias, e, portanto, a probabilidade das 3 localizações estarem indisponíveis simultaneamente é muito improvável.

PEDIDO ESCLARECIMENTO 07

O item 7.4. do TERMO DE REFERÊNCIA cita que: "Também poderá ser entendido como Período de Interrupção 1/3 (um terço) do tempo em minutos entre a abertura de um chamado e seu fechamento, decorrentes da identificação de Degradação de Qualidade (DQ) e a completa solução do problema, através dos serviços de gerenciamento de rede da CONTRATANTE ou CONTRATADA". Não entendemos o que cliente quer dizer com: "Também poderá ser entendido como Período de Interrupção 1/3 (um terço) do tempo em minutos entre a abertura de um chamado e seu fechamento...", pois 1/3 de tempo entre a abertura e o encerramento já é a interrupção. Sendo assim, poderiam esclarecer melhor que diz este item? Poderiam dar um exemplo prático desta situação, principalmente informando em que momento o 1/3 tempo está inserido?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o item 7.4 do Termo de Referência trata da Degradação da Qualidade (DQ) e não do Período de Interrupção (PI) em si.

Neste sentido, esclarecemos que: **para os chamados abertos visando a correção da Degradação de Qualidade (DQ),** 1/3 (um terço) do tempo entre a abertura deste chamado e o seu fechamento poderá ser entendido como Período de Interrupção, pois este item (7.4) é claro quando diz que: são para chamados decorrentes da identificação de Degradação de Qualidade (DQ) e a completa solução do problema.

Exemplo: caso a velocidade média de download ou upload inferior 70% (setenta por cento) do contratado, poderemos considerar 1/3 (um terço) do tempo compreendido entre a abertura do chamado para a solução da Degradação de Qualidade (DQ) e o seu fechamento poderá ser entendido como Período de Interrupção.

PEDIDO ESCLARECIMENTO 08

O item 7.3.1.5. do TERMO DE REFERÊNCIA cita que não é considerado falha a: "Latência bidirecional máxima superior a 150 ms (cem e cinquenta milissegundos)", porém, o item 7.4.1.3. cita que a degradação será considerada com: "Latência bidirecional média superior a 120 ms (cento e vinte milissegundos)". Aqui entendemos uma duplicidade de informação, pois se não é considerado falha com 150 ms, não poderá ser considerado degração com 120ms, sendo assim, entendo que para o item 7.4.1.3 deverá considerar também a latência de 150 ms. Nosso entendimento está correto?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto, pois o subitem 7.3.1 do Termo de Referência estabelece o que **são** consideradas Falhas (F). Portanto, seus subtitens apenas descrevem o **que será considerado**.

PEDIDO ESCLARECIMENTO 09

O item 8.1. do TERMO DE REFERÊNCIA cita que: "Após a assinatura do contrato, a CONTRATADA terá até 30 (trinta) dias úteis para a ativação do link", porém, devido a necessidade importação de equipamentos, contrução de acesso e demais itens inerentes a ativação, solicitamos que o prazo de ativação após a assinatura do CONTRATO seja de 60 (sessenta) dias úteis. Nossa solicitação será aceita?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o item 5.1 do Edital e 8.1 do Termo de Referência, estabelecem que após a assinatura do contrato, a CONTRATADA terá até 60 (sessenta) dias úteis para a ativação do link.

PEDIDO ESCLARECIMENTO 10

O item 9.4.3. do TERMO DE REFERÊNCIA cita que a CONTRATADA deverá disponibilizar ferramenta que informe o Status operacional (up/down) do link. Entendemos que a abertura automática de chamado assim que for percebido a indisponibilidade do link, como a inserção de informação no chamado da normalização da indisponibilidade pelo técnico, será o suficiente para atendimento a este item. Nosso entendimento está correto?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto. O que se pretende conforme estabelecido no item 9.4 do Termo de Referência, é a disponibilização de ao menos um portal para que CONTRATANTE tenha acesso as informações contidas nos subitens 9.4.1 ao 9.4.7.

PEDIDO ESCLARECIMENTO 11

Para o serviço de ANTIDDOS, nós temos algumas sugestões de melhorias para que resguarde o SESI de uma eventual entrega de um serviço que não atenda integralmente essa necessidade.

 # SUGESTÃO PARA A SOLUÇÃO DE ANTIDDOS:

O item 1.1 do TERMO DE REFERÊNCIA cita que o objeto da licitação trata-se de 1 link de acesso a internet simétrico (mesma velocidade de download e upload), mais o serviço de anti DDOS, porém, avaliando todo o edital, não há especificação técnica do serviço ANTI-DDOS. O serviço ANTI-DDOS pode variar muito, de acordo com as funcionalidades e especificações solicitadas pela CONTRATANTE. Esta variação altera de forma substancial o valor do serviço ANTI-DDOS, sendo necessário e de fundamental importância que esta definição seja estabelecida pela CONTRATANTE. Da forma como está, NÃO HÁ COMO PRECIFICAR, além disso, abre margem para uma prestação de serviço inferior e muitas vezes nem sendo serviço ANTI-DDOS. Para ser considerado um serviço ANTI-DDOS, faz-se necessário, no mínimo a definição da banda de mitigação e demais características abaixo. Sendo assim, solicitamos que a CONTRATANTE defina as especificações técnicas do serviço ANTI-DDOS semelhante ao que segue abaixo:

- **Cliente deve informar a banda de mitigação para o ANTI-DDOS. Para esta licitação sugerimos uma banda para mitigação de 500 Mbps Nacional e 5 Gbps Internacional. Cliente deverá inserir este item no TERMO DE REFERÊNCIA.**

4. Características Gerais para o ANTI-DDOS abaixo que sugerimos constar no TERMO DE REFERÊNCIA:

4.1 Capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

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

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

4.4 Serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação

4.5 Capacidade de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes:

4.5.1 Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP
4.5.2 Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets
4.5.3 Realizar autenticação de conexão TCP, quando do recebimento de pacotes syn
4.5.4 Limitar o número de conexões TCP simultâneas de um mesmo host
4.5.5 Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP
4.5.6 Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing)
4.5.7 Ataques denominados de "Comand-and-Control", Point of Sale Malware, Remote Access Trojans RAT's via feed atualizado diariamente
4.5.8 Ataques à camada de aplicação, incluindo protocolos HTTP e DNS Volumetricos
4.5.9 Bloqueio de query de DNS, resposta de query de DNS baseado em domínio pré-cadastrado para autenticação e checagem de flag de recursão DNS
4.5.10 DNS BlackList; RegEx para registros específicos ou "flags de recursão. Possuir mecanismos de quando bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente
4.5.11 Autenticação em query DNS por requisição em TCP
4.5.12 Autenticação em JavaScript e Redirect para HTTP
4.5.13 Adicionar expressão regular de "payload" em black-list
4.5.14 Prevenir que hosts válidos sejam adicionados a black-list por engano

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

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

4.8 Manter lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro

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

4.10 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

4.11 Características da Infraestrutura de Suporte Anti-DDoS

4.11.1 Possuir Centro Operacional de Segurança (ou SOC – Security Operations Center) 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
4.11.2 Possuir 2 centros de limpeza nacional cada um com capacidade de mitigação de 10Gbps e 3 centros de limpeza internacional com capacidade de mitigação de 30Gbps
4.11.3 Evitar saturação da banda de Internet em caso de ataques de negação de serviço (Distributed Denial of Service – DDoS) com capacidade de mitigar 10 Gbps.
4.11.4 Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole,
4.11.5 As funcionalidades de monitoramento, detecção e mitigação de ataques são mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual
4.11.6 O bloqueio de ataques DOS e DDOS não são realizados por ACLs em roteadores de borda.
4.11.7 A mitigação de ataques DDOS é iniciada em até 15 minutos da emissão do alerta
4.11.8 Deve disponibilizar um portal onde a contratante tem acesso online aos tipos de ataques sofridos e o tamanho destes ataques categorizados por severidade (Ex: baixo, Médio, Alto)
4.11.9 A mitigação dos ataques é realizada dentro do Brasil, sem encaminhamento do tráfego para limpeza fora do território brasileiro
4.11.10 Em momentos de ataques DOS e DDOS, todo trafego limpo é reinjetado na infraestrutura da contratante através de túneis VPN Clean, configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante

4.12 REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

4.12.1 A CONTRATADA deverá fornecer o conjunto de manuais técnicos oficiais, elaborados pelo fabricante de cada equipamento, contendo todas as informações sobre o produto como instruções para instalação, configuração, operação e gerenciamento. Os manuais técnicos do fabricante devem estar escritos em português ou inglês e podem ser fornecidos em mídia eletrônica (CD-ROM ou DVD).
4.12.2 A CONTRATADA deverá planejar a execução do projeto de implantação. Deverá ser elaborada uma documentação completa onde deverá constar dentre outras informações: mapa da rede, mapa do perímetro, telas de instalação/configuração do produto, outras informações relevantes para administração do ambiente.
4.12.3 O “Plano de Implantação” deverá contemplar, no mínimo:
4.12.4 Cronograma de instalação, configuração, testes e ativação e;
4.12.5 Detalhamento dos testes a serem realizados quando concluídas as instalações e configurações dos equipamentos. Deverá ser apresentado um documento ao final da realização dos testes com dados informativos que comprovem o bom funcionamento dos componentes pertinentes à solução.
4.12.6 Eventuais desconformidades entre os procedimentos executados e os documentos fornecidos serão comunicados à CONTRATADA para que providencie os ajustes necessários.
4.12.7 A “Documentação Técnica da Solução” deverá contemplar, no mínimo, o projeto executivo contendo o conjunto dos elementos necessários e suficientes à implantação dos equipamentos ou

execução dos serviços, inclusive desenhos das topologias físicas e lógicas, condições de alimentação, aterramento e ambientação (iluminação, temperatura, umidade, etc.) e especificações físicas, elétricas, operacionais e suas limitações.

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que apenas necessitamos que a CONTRATADA forneça a serviço de proteção do link contra ataques de negação de serviço, evitando ocorrências de indisponibilidade. O detalhamento do ataque como os que sugerido pela PROPONENTE não faz parte da nossa estratégia e ações que visam a proteção. Sendo assim, agradecemos a sugestão, mas não a acataremos.

***Resposta enviada no e-mail** [redacted]@embratel.com.br

Brasília, 09 de setembro de 2021.

Comissão de Licitação Serviço Social da Indústria – Conselho Nacional