**CHAMAMENTO PÚBLICO Nº 37/2025**

**PERGUNTAS E RESPOSTAS 3**

|  |  |
| --- | --- |
| **Processo nº 03127/2024 - SC nº 226333** | **Tipo: Menor Preço Global** |
| **Abertura: 24/04/2025** | **Horário: 10h** |
| **Local: SBN, Quadra 1, Bloco C, Edifício Roberto Simonsen, 2º andar, CEP 70040-903 Brasília (DF). Fone: (61) 3317-9891 – E-mail:** [**processodeselecao@cni.com.br**](mailto:processodeselecao@cni.com.br) | |

**QUESTIONAMENTO 01**

Considerando as características técnicas e comuns a toda a prestação de serviço de Internet Dedicada, entendemos que na fatura poderão constar valores para os serviços de Circuito, CPE, Anti-DDoS e Gerência desde que o valor final de cada site seja exatamente àquele acordado no final do certame.

Nosso entendimento está correto?

**Resposta:** O entendimento está correto.

**QUESTIONAMENTO 02**

Entendemos que a solução de proteção contra-ataques de negação de serviços deve ser disponibilizada no backbone da CONTRATADA, não sendo permitida a subcontratação da mesma, ou seja, para que a integridade dos dados e informações trafegadas não sejam comprometidas, não será permitido que a CONTRATADA realize o redirecionamento do tráfego para infraestruturas de terceiros para que estes realizem a mitigação dos ataques e não será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.  
Nosso entendimento está correto? Caso o entendimento esteja correto, as licitantes deverão comprovar que possuem infraestrutura própria de proteção contra-ataques de negação de serviços?

**Resposta:** O entendimento está correto. Esse item será comprovado na implantação do serviço por localidade, e caso não seja atendido, não será considerada realizada a implantação.

**QUESTIONAMENTO 03**

A conexão ao ASN proporciona rotas redundantes, otimizando a resiliência da rede e permitindo redirecionamento automático de tráfego em caso de falhas. Isso melhora a eficiência do roteamento, reduz a latência e é crucial para aplicações de baixa latência, como voz e vídeo em tempo real. Além disso, facilita políticas de segurança e controle de tráfego, como mitigação de ataques DDoS, e permite escalabilidade eficiente da rede, incorporando novos PoPs sem reconfigurações complexas. A implementação de QoS garante prioridade ao tráfego crítico, mantendo a qualidade dos serviços, e a integração com outros ISPs e CDNs melhora a conectividade global e a experiência do usuário.

Sabe-se que compartilhamento de um Autonomous System Number (ASN) entre empresas de um mesmo grupo econômico é uma prática amplamente reconhecida no setor de telecomunicações, especialmente por razões técnicas, econômicas e operacionais. Essa prática é comum entre grandes empresas que possuem estruturas de rede integradas e visam otimizar a gestão de seus recursos de conectividade.

Primeiramente, é importante esclarecer que o ASN é um identificador único atribuído a uma entidade autônoma de roteamento na Internet, usado para estabelecer políticas de tráfego e comunicação entre redes. Sua função está ligada à gestão eficiente de blocos de endereços IP e à integração de redes sob uma única lógica operacional. Nesse contexto, o compartilhamento de um ASN por diferentes empresas do mesmo grupo não apenas é tecnicamente viável, como também recomendado em diversos casos, visto que garante economia de escala, racionalização de recursos e consistência na gestão de tráfego de dados.

No Brasil, essa prática encontra respaldo em normativas regulatórias e padrões internacionais de governança da Internet. A ANATEL, por meio de regulamentações como o Regulamento de Numeração (Resolução nº 709/2019) e o Regulamento do Serviço de Comunicação Multimídia (Resolução nº 614/2013), incentiva o uso racional e eficiente de recursos de telecomunicações, incluindo infraestrutura compartilhada dentro de grupos econômicos. Complementarmente, as diretrizes do LACNIC (entidade responsável pela administração de ASNs na América Latina) permitem o uso compartilhado de um mesmo ASN por diferentes unidades de uma organização, desde que todas estejam sob a administração de uma entidade centralizada.

Cabe ressaltar que esse modelo de compartilhamento é comum em grandes grupos de telecomunicações no Brasil e no mundo, também adotem estratégias similares para gerir suas operações. O uso centralizado de ASNs é especialmente vantajoso em um cenário em que as redes precisam suportar um tráfego crescente de dados e oferecer alta disponibilidade e resiliência.

Entendemos que para garantir a robustez e a confiabilidade da infraestrutura de rede, poderá ser considerado empresas incorporadas ou do mesmo grupo econômico que estejam conectadas ao Sistema Autônomo (ASN) da licitante.

Nosso entendimento está correto?

**Resposta:** O entendimento está correto.

**QUESTIONAMENTO 04**

Para melhor esclarecimento, solicitamos as informações e quantitativos mínimos de Access Points solicitados, não há informações mínimas referente ao quantitativo e especificações de atendimento dos Access Points.

Solicitamos essas informações para melhor dimensionamento da proposta.

Nossa solicitação será aceita?

**Resposta:** Conforme esclarecimento nº2, desconsiderar os itens 5.6 e 5.7. do chamamento público.

**QUESTIONAMENTO 05**

Entendemos que os lances serão enviados considerando o valor global para 60 meses. Nosso entendimento está correto?

**Resposta:** O entendimento está correto.

3.3.13.1.7. A CONTRATADA deve possuir pelo menos um centro de limpeza nacional com capacidade mínima de mitigação de 1Gbps e um centro de limpeza internacional com capacidade mínima de mitigação de 30Gbps

Sugerimos que o item acima seja revisado, para uma melhor condição técnica visando a garantia dos serviços para a CNI. A capacidade de mitigação solicitada no item acima é muito pequena comparada à banda dos links. Nossa sugestão é que o centro de mitigação nacional seja capaz de absorver no mínimo 100G de ataques.

**Resposta:** Sugestões não acatada, pois entendemos que poderá ter limitação de participantes no chamamento.

3.3.13.1.8. A CONTRATADA deve mitigar ataques por 3 horas

Sugerimos que o item acima seja revisado, para uma melhor condição técnica visando a garantia dos serviços para a CNI. A mitigação deverá ser mantida enquanto o ataque se mostrar presente. Isto visa que os serviços da CNI sejam mantidos ativos e com o menor impacto possível.

**Resposta:** Sugestão acatada. Ver Errata nº1 abaixo.

3.3.13.1.13. Em momentos de ataques DoS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma da contratada e o CPE do contratante

Solicitamos que o item acima seja flexibilizado, permitindo o retorno de tráfego limpo de outras formas além do túnel GRE, como internet direct dentre outras. Nosso pedido será acatado?

**Resposta:** Sugestão acatada. Ver Errata nº2 abaixo.

**QUESTIONAMENTO 06**

Referente ao modelo de proposta de preços.

Entendemos que o valor Mensal/Unitário (R$), corresponde ao valor mensal do link adicionado ao valor do ddos correspondente multiplicados pela quantidade de links requeridos. Estamos corretos no entendimento?

**Resposta:** O entendimento está parcialmente correto. O “Valor Mensal/Unitário (R$)” corresponde ao valor mensal do link com todos os custos operacionais (não só DDoS) e impostos inclusos, multiplicado pela quantidade solicitada na mesma linha da tabela informada na clausula “DA PROPOSTA DE PREÇO”.

**QUESTIONAMENTO 07**

Entendemos dos itens: 3.5 e do 3.5.1, que se trata apenas de fornecimento de link dedicado de 200 Mbps para conexão à infraestrutura de comunicação as nuvens Microsoft Azure e Google Cloud, não sendo obrigado a contratada fornecer nem roteador no site do cliente e nem o serviço de cloud. Estamos corretos no entendimento?

**Resposta: O entendimento está correto.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ERRATA 1**

NO ITEM 3.3.13.1.8 do Termo de referência **onde se lê:**

A CONTRATADA deve mitigar ataques por 3 horas

**Deve-se ler:** A mitigação deverá ser mantida pela CONTRATADA enquanto o ataque se mostrar presente. Isto visa que os serviços das CONTRATANTES sejam mantidos ativos e com o menor impacto possível.

**ERRATA 2**

NO ITEM 3.3.13.1.13 do Termo de referência **onde se lê:**

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

**Deve-se ler:** Em momentos de ataques DoS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation) ou através de outras técnicas de tunelamento, configurado entre a plataforma da contratada e o CPE do contratante.

**Para todos os efeitos este documento passa a integrar o Chamamento em referência.**

Brasília, 17/04/2025

**Comissão Permanente de Contratação e Alienação - CPCA**