

PREGÃO ELETRÔNICO NACIONAL NF 1301-26

SERVIÇOS DE REDE DE COMUNICAÇÃO DE DADOS IP/MPLS E DE CONECTIVIDADE DE TRÁFEGO À INTERNET COM SOLUÇÃO DE PROTEÇÃO ANTI-DDOS, PARA A ITAIPU

ADITAMENTO 5

I) Em conformidade com o disposto no subitem 2.6.1 do Caderno de Bases e Condições (CBC) do Pregão Eletrônico Nacional NF 1301-26, a ITAIPU responde perguntas realizadas por empresas interessada nesta licitação:

PERGUNTA 1

“Prazo para Remanejamento de Circuitos

O Anexo I prevê que todos os links poderão sofrer mudança de endereço por solicitação da ITAIPU, devendo a CONTRATADA disponibilizar o circuito no novo endereço no prazo máximo de 30 (trinta) dias úteis, sem custos adicionais, desde que dentro do mesmo perímetro urbano. Entretanto, eventuais mudanças de endereço podem demandar atividades de engenharia, obtenção de autorizações, construção de facilidades de acesso, lançamento de infraestrutura e contratação de terceiros, fatores que podem impactar o prazo originalmente definido.

Dessa forma, solicitamos esclarecer:

Está correto o entendimento de que o prazo para remanejamento poderá ser ampliado para até 60 (sessenta) dias úteis, mediante comprovação da necessidade de implantação de nova infraestrutura ou outras condições técnicas indispensáveis à ativação do serviço?”

RESPOSTA

Entendimento correto, conforme já esclarecido no item II, alínea "b", do Aditamento 1. O prazo regular de 30 (trinta) dias úteis para a mudança de endereço de circuitos dentro do mesmo perímetro urbano poderá ser ampliado para até 60 (sessenta) dias úteis, desde que a CONTRATADA comprove a necessidade de implantação de nova infraestrutura ou de outras condições técnicas indispensáveis à ativação do serviço.

PERGUNTA 2

“Viabilidade Técnica para Atendimento em Novo Endereço

Considerando a previsão de alteração de endereço dos links ao longo da vigência contratual, observamos que o edital não contempla expressamente situações em que o novo local indicado pela ITAIPU não possua cobertura ou viabilidade técnica para atendimento pela CONTRATADA. Dessa forma, solicitamos esclarecer:

Está correto o entendimento de que a obrigação de atendimento estará condicionada à prévia análise de viabilidade técnica da CONTRATADA e que, inexistindo cobertura ou viabilidade técnica no novo endereço indicado, não serão aplicadas penalidades, multas, glosas ou quaisquer sanções à CONTRATADA?”

RESPOSTA

Entendimento correto, conforme já esclarecido no item II, alínea "b", do Aditamento 1. A obrigação de atendimento em novo endereço indicado pela ITAIPU está condicionada à prévia análise de viabilidade técnica da CONTRATADA. Caso o local não possua cobertura ou viabilidade técnica, não será aplicada à CONTRATADA nenhuma penalidade, multa, glosa ou sanção.

PERGUNTA 3

“Acesso aos Equipamentos de Borda (CPE)

Os itens 4.4.5 e 4.4.6 do Anexo I estabelecem requisitos relacionados aos equipamentos de borda fornecidos pela CONTRATADA, incluindo mecanismos de segurança e implementação de políticas definidas pela ITAIPU.

Considerando que o objeto contempla serviço gerenciado, cuja operação, administração e manutenção dos equipamentos são de responsabilidade da CONTRATADA, solicitamos esclarecer:

Está correto o entendimento de que não será exigido acesso administrativo da ITAIPU aos equipamentos CPE da CONTRATADA, podendo o atendimento aos requisitos editalícios ocorrer mediante disponibilização de informações, relatórios, registros ou acesso em modo somente leitura?”

RESPOSTA

Entendimento correto, conforme já esclarecido no item II, alínea "b", do Aditamento 1. Por se tratar de serviço gerenciado, cuja operação, administração e manutenção são de responsabilidade da CONTRATADA, não será exigido acesso administrativo da ITAIPU aos equipamentos CPE. Os requisitos editalícios serão atendidos mediante a disponibilização de informações, relatórios, registros ou acesso em modo somente leitura.

PERGUNTA 4

“Aplicabilidade dos Requisitos de Segurança e Mitigação de DDoS

Observamos que os itens 1.1.8 a 1.1.11 do Anexo I estabelecem exigências relacionadas à proteção contra ataques DoS/DDoS, detecção e mitigação de incidentes de segurança, monitoramento de eventos de segurança e gestão de vulnerabilidades.

Entretanto, o objeto do Lote 1 refere-se à contratação de serviços de Rede de Comunicação de Dados IP/MPLS, enquanto o Lote 2 contempla serviços de conectividade Internet com solução de proteção Anti-DDoS.

Dessa forma, solicitamos esclarecer:

Está correto o entendimento de que os requisitos constantes dos itens 1.1.8 a 1.1.11 constituem exigências exclusivas do Lote 2, não sendo aplicáveis ao fornecimento dos serviços do Lote 1 (Rede IP/MPLS)?”

RESPOSTA

Entendimento correto, conforme já esclarecido nas respostas às Perguntas 4 e 5 e no item II, alínea "b", do Aditamento 1. Os requisitos de proteção contra ataques DoS/DDoS, detecção e mitigação de incidentes, monitoramento de eventos de segurança e gestão de vulnerabilidades, previstos nos itens 1.1.8 a 1.1.11 do Anexo I, constituem exigências exclusivas do Lote 2, voltado à conectividade Internet. Esses requisitos não se aplicam ao Lote 1, de Rede IP/MPLS, cuja arquitetura fechada para interconexão corporativa privada apresenta menor superfície de exposição a riscos volumétricos.

PERGUNTA 5

“Os itens 1.2.7 do Lote 1 e 4.7.7 do Lote 2 dos Anexos I (Especificações Técnicas) estabelecem que a CONTRATADA deverá disponibilizar portal web de gerenciamento acessível à ITAIPU, contendo visualização em tempo real do estado dos enlaces, indicadores de desempenho, estatísticas de tráfego, registros de eventos/falhas, histórico de incidentes e informações de inventário/topologia. Adicionalmente, os itens 1.2.10/1.2.11 do Lote 1 e 4.7.10/4.7.11 do Lote 2 exigem que o acesso ocorra via Internet pública sob protocolo HTTPS com certificação digital (padrão X509), efetuando o registro em log de histórico de todos os acessos realizados, com autenticação de usuário, data e hora. Sabe-se que, no padrão de mercado de Tecnologia da Informação e Telecomunicações, a melhor prática de arquitetura para operações de NOC/SOC consiste na utilização de ecossistemas especializados e integrados via API, dividindo as funções em: Plataforma de ITSM / Gestão de Incidentes e Chamados (ex: Zendesk): Voltada para a abertura proativa de chamados, controle de prazos de MTTR, acompanhamento do ciclo de vida dos incidentes, gestão de mudanças, relatórios de SLA e aprovação formal do fechamento de chamados pela ITAIPU.

Plataforma de Monitoramento e Telemetria (ex: Zabbix / Grafana): Voltada para a coleta contínua SNMPv3/NetFlow, dashboards em tempo real de latência, perda de pacotes, disponibilidade e mapas de topologia de rede. Para garantir a máxima performance, segurança

e usabilidade, a Proponente pretende ofertar uma solução integrada onde ambas as plataformas (Zendesk e Zabbix/Grafana) estarão interconectadas por API/Webhooks (gerando chamados automáticos ao detectar falhas), operando em ambiente em nuvem/web seguro sob HTTPS com certificado digital (X509), com autenticação individualizada e registro de logs auditáveis de acesso de todos os usuários da ITAIPU mantidos por no mínimo 6 (seis) meses. As plataformas serão disponibilizadas mediante links/portais com acesso direto e/ou redirecionamento cruzado entre as ferramentas.

Diante do exposto, está correto o entendimento de que a disponibilização da solução de gerenciamento composta por plataformas especializadas e integradas (por exemplo, Zendesk para a Gestão de Incidentes/ITSM e Zabbix/Grafana para o Monitoramento/Telemetria em tempo real), disponibilizadas sob protocolo seguro HTTPS (X509), com acessos autenticados, registros individuais de logs de auditoria de acessos em ambas as plataformas e integração automática via API, atende integralmente às exigências dos itens 1.2.7 a 1.2.11 do Lote 1 e 4.7.7 a 4.7.11 do Lote 2 do Anexo I do Edital?"

RESPOSTA

Entendimento correto, com ressalvas. Conforme esclarecido no Aditamento 3, será admitida solução composta por plataformas distintas, dedicadas ao monitoramento e telemetria da infraestrutura e à gestão de incidentes, requisições e serviços, desde que integradas entre si por meio de APIs, webhooks ou mecanismos equivalentes e que, consideradas em seu conjunto, atendam integralmente a todas as funcionalidades previstas nas alíneas "a" a "e" dos subitens 1.2.7 e 4.7.7, permitindo à ITAIPU a rastreabilidade dos eventos, incidentes e respectivas tratativas.

Cada plataforma que compuser a solução deverá observar, individualmente, os requisitos de acesso via Internet pública mediante protocolo HTTPS com certificação digital (padrão X509), autenticação individualizada de usuários, registro em log de todos os acessos realizados, com identificação do usuário, data e hora, e recuperação do registro de histórico, e período de armazenamento dos relatórios de 6 (seis) meses.

O prazo de 60 (sessenta) dias para disponibilização e a condição de pagamento previstos nos subitens 1.2.8 e 4.7.8 aplicam-se à totalidade das plataformas que compõem a solução.

As ferramentas citadas pela proponente foram consideradas apenas como exemplo. O atendimento aos requisitos será verificado na execução contratual.

II) Permanecem inalteradas as condições contidas no CBC do Pregão Eletrônico Nacional NF 1301-26.

Emitido por: Divisão de Suporte Técnico	Data de emissão: 09 de outubro de 2026
---	--
