



Proc. Nº

0554/2025

FOLHA DE RESPOSTA

Fl. Nº 01

Rubrica

SETOR DE TI (CPD)

Esclarecimentos – Pregão Eletrônico 044/2025

Questionamento 1: O item relativo ao prazo de reparo de duas horas mencionado no Termo de Referência é inviável de ser cumprido pelos técnicos responsáveis por realizar os reparos no endereço especificado. Essa atividade requer várias etapas, como a identificação do incidente, a tentativa de reparo remoto, o acionamento da equipe de campo, o deslocamento do técnico e, finalmente, a efetiva reparação. Outro ponto a ser observado é a disponibilidade do link, no Termo de Referência é solicitado uma disponibilidade de 95,00%. Segundo a regulamentação da ANATEL, para essa porcentagem de disponibilidade o prazo de reparo equivalente é de 8 (oito) horas. Portanto solicitamos que o prazo de reparo seja ampliado para 8 (oito) horas, em conformidade com o padrão estabelecido pela ANATEL, para garantir uma ampla participação de interessados neste certame. Nossa solicitação será acatada?

Resposta

O item 9.1.6 “O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.”, foi definido visto que o serviço de acesso a internet para cada unidade tem por objetivo atender as necessidades de comunicação da respectiva unidade para execução das atividades locais. Uma paralisação prolongada afetará diretamente estas atividades, principalmente se envolverem atendimento público, diferentemente de utilização para ambiente doméstico, que é mais flexível. Entretanto, havendo regulamentação da ANATEL, poderá ser considerado o prazo de 8 (oito) horas.

Questionamento 2: Notamos que o Termo de Referência exige que o fornecimento do serviço de internet banda larga seja realizado exclusivamente por meio de infraestrutura em fibra óptica, com justificativa fundamentada no Estudo Técnico Preliminar. Contudo, considerando o princípio da isonomia previsto no art. 5º, inciso I, da Lei nº 14.133/2021, que assegura igualdade de condições a todos os concorrentes, solicitamos a gentileza de avaliar a possibilidade de ampliar o escopo das tecnologias admitidas, ao menos de forma complementar e devidamente justificada, em localidades onde a infraestrutura óptica não esteja disponível, desde que seja assegurado o cumprimento de todos os parâmetros de desempenho, qualidade e estabilidade definidos no edital. Tal medida permitiria ampliar a competitividade do certame, sem comprometer a finalidade pública da contratação, viabilizando a participação de uma maior gama de fornecedores, garantindo assim a plena execução do objeto. Dessa forma, sugerimos que o edital preveja a possibilidade de uso de tecnologia diversa da fibra óptica, de maneira subsidiária, apenas para os casos onde for comprovada a indisponibilidade técnica ou operacional da referida infraestrutura, mantendo-se os critérios técnicos de qualidade exigidos pela Administração. Nossa solicitação será acolhida?

Resposta

O objeto primariamente definido (lote 01, item 01.a “LINK DE INTERNET PADRÃO GPON / FTTH COM IP FIXO 1 Gbps”) já pressupõem o uso de fibra óptica (FO) para o estabelecimento do enlace físico da rede a ser estabelecida. A quase totalidade dos 91 pontos levantados se encontram no perímetro urbano, e conseqüentemente são atendidos pela infraestrutura física construída pela concessionária de energia elétrica, que é utilizada pelas concessionárias de telecomunicações para o lançamento das suas respectivas redes de FO. Entretanto, considerando que as concessionárias de telecomunicações ainda não atenderam 100% dos pontos possíveis na área urbana do município, e somado a isto, há pontos que estão além do perímetro urbano estabelecido, excepcionalmente poderá ser considerado o uso de outras tecnologias para complementar o link, desde que se mantenha os outros parâmetros estabelecidos.

Questionamento 3: Em atenção ao Edital, foi observado que dentre as exigências técnicas previstas para o fornecimento de serviço de internet banda larga, constam requisitos relacionados à disponibilização de NOC (Network Operations Center) e SOC (Security Operations Center). Contudo, cumpre destacar que tais estruturas são

PREFEITURA MUNICIPAL DE SÃO JOAQUIM DA BARRA

ESTADO DE SÃO PAULO

Praça Prof. Ivo Vannuchi S/N – Fone PABX (16) 3810-9000 – FAX (16) 3810-2056



Proc. Nº

0554/2025

FOLHA DE RESPOSTA

Fl. Nº 02

Rubrica

características de serviços de maior complexidade e criticidade, como links dedicados, redes MPLS, rede SD-WAN, etc., onde há, de fato, a necessidade de gerenciamento ativo da rede e da segurança com recursos avançados e dedicados. Por sua natureza, o serviço de internet banda larga possui um escopo técnico distinto, sendo ofertado sob regime de acesso compartilhado, com gerenciamento padrão, sem a aplicação de ferramentas ou políticas específicas de segurança e monitoramento de rede que justifiquem a presença de NOC e SOC dedicados. Dessa forma, considerando o princípio da razoabilidade e o adequado dimensionamento técnico da contratação em relação à natureza do objeto, solicitamos a gentileza de reavaliar a obrigatoriedade dos requisitos de NOC e SOC para o serviço de banda larga; Tal ajuste contribuirá para uma maior adequação técnica da contratação, sem comprometer a qualidade dos serviços prestados. Nossa solicitação será acatada?

Resposta

O objeto primariamente definido (lote 01, item 01.a “LINK DE INTERNET PADRÃO GPON / FTTH COM IP FIXO 1 Gbps”), mesmo sendo GPON (Gigabit Passive Optical Network, ou Rede Óptica Passiva com Capacidade de conexão em Gigabits) / FTTH (Fiber To The Home), nas características mínimas solicitadas é exigido “Disponibilização de um endereço IP padrão IPv4 Classe C e/ou padrão IPv6 Global Unicast Address (GUA), roteável, para permitir o acesso direto via Internet de dispositivos instalados no local pela CONTRATANTE;”. Um IP roteável permite que possamos redirecionar as conexões com os equipamentos internos diretamente (relógios de ponto, DVR, câmeras de monitoramento, etc) sem a interferência de CGNAT. Na realidade cada conexão se comporta como um link dedicado, com todas as vantagens e desvantagens incluídas.

A justificativa para a disponibilização de um Network Operations Center (NOC) e um Security Operations Center (SOC) para atender 91 links de internet padrão GPON/FTTH, com IPs roteáveis (IPv4 Classe C e/ou IPv6 Global Unicast Address - GUA), em unidades de atendimento público com serviços à municipalidade, é ainda mais robusta e crítica. Aqui estão os pontos-chave, com ênfase no contexto de serviços públicos:

- **Justificativa para o NOC (Network Operations Center) em Serviços Públicos**

O NOC é vital para assegurar a continuidade e a qualidade dos serviços públicos digitais, que são essenciais para o funcionamento da municipalidade e para o atendimento ao cidadão.

- 1) **Garantia da Disponibilidade dos Serviços Essenciais:**

- Impacto Direto no Cidadão: Cada um dos 91 links interliga uma unidade de atendimento público. A falha de um único link pode paralisar serviços como emissão de documentos, agendamentos médicos, registro de ocorrências, ou acesso a programas sociais. O NOC minimiza essa interrupção.
- Serviços Críticos: Pense em unidades de saúde, escolas, delegacias, ou centros de atendimento ao cidadão (CACs). A indisponibilidade da internet nesses locais impede o acesso a sistemas vitais, como prontuários eletrônicos, sistemas de matrícula, ou bases de dados criminais.
- Monitoramento Proativo 24/7: O NOC permite identificar e resolver problemas de rede antes que eles afetem os usuários ou causem uma interrupção significativa nos serviços, garantindo que as unidades estejam sempre operacionais.

- 2) **Otimização e Eficiência Operacional da Municipalidade:**

- Fluxo de Trabalho Contínuo: Servidores públicos dependem da conectividade para acessar sistemas internos, comunicar-se e realizar suas tarefas diárias. Um NOC garante que essa infraestrutura de suporte esteja sempre disponível.
- Gestão de Incidentes Centralizada: Problemas de conectividade em 91 pontos podem ser caóticos sem um NOC. Ele centraliza o monitoramento, diagnóstico e a coordenação de equipes de campo para a resolução de forma eficiente, reduzindo o MTTR (Mean Time To Repair).

PREFEITURA MUNICIPAL DE SÃO JOAQUIM DA BARRA

ESTADO DE SÃO PAULO

Praça Prof. Ivo Vannuchi S/N – Fone PABX (16) 3810-9000 – FAX (16) 3810-2056



Proc. Nº

0554/2025

FOLHA DE RESPOSTA

Fl. Nº 03

Rubrica

- Planejamento de Capacidade para Demanda Pública: Serviços digitais da prefeitura tendem a crescer. O NOC monitora o uso dos links e projeta futuras necessidades de largura de banda, garantindo que a infraestrutura suporte novas demandas e serviços digitais.
- 3) Qualidade do Atendimento ao Cidadão:
 - Redução de Filas e Esperas: Serviços online e sistemas conectados agilizam o atendimento. Interrupções na internet causam filas, frustração e perda de tempo para o cidadão e para o servidor. Um NOC robusto reduz essas ocorrências.
 - Confiabilidade e Transparência: A prefeitura ganha credibilidade ao oferecer serviços digitais que funcionam de forma contínua e eficiente.
- 4) Gerenciamento do Parque de IPs (IPv4 Classe C e IPv6 GUA):
 - Com IPs roteáveis em 91 unidades, o NOC será responsável por uma gestão precisa desses endereços, garantindo que cada unidade tenha a conectividade adequada e que não haja conflitos de IP, algo crucial para a comunicação interna e externa da prefeitura.

- **Justificativa para o SOC (Security Operations Center) em Serviços Públicos**

O SOC é absolutamente mandatário para proteger a infraestrutura digital da municipalidade, os dados dos cidadãos e a integridade dos serviços públicos, contra ameaças cibernéticas que podem ter consequências devastadoras.

- 1) Proteção de Dados Sensíveis dos Cidadãos:
 - Informações Pessoais e Financeiras: Unidades de atendimento público lidam com uma vasta gama de dados sensíveis dos cidadãos (RG, CPF, endereço, informações de saúde, rendas, etc.). O vazamento ou comprometimento desses dados pode gerar processos legais, multas e uma enorme perda de confiança pública.
 - Conformidade com a LGPD (Lei Geral de Proteção de Dados): O SOC é fundamental para demonstrar e garantir a conformidade com a LGPD, protegendo os dados pessoais e respondendo a incidentes de forma adequada.
- 2) Defesa contra Ciberataques à Infraestrutura Pública:
 - Alvo Estratégico: Governos e prefeituras são alvos frequentes de ataques cibernéticos (ransomware, DDoS, espionagem, sabotagem) devido à criticidade dos serviços e à riqueza de dados que detêm.
 - Ransomware: Um ataque de ransomware em sistemas municipais pode paralisar completamente a administração, impedindo o acesso a sistemas críticos e forçando pagamentos de resgate exorbitantes, como já ocorreu em diversas prefeituras. O SOC é a primeira linha de defesa contra isso.
 - Fraudes e Sabotagem: A ausência de um SOC pode abrir portas para fraudes, manipulação de dados ou sabotagem de sistemas, comprometendo a prestação de serviços.
- 3) Manutenção da Credibilidade e Confiança Pública:
 - Crise de Imagem: Um incidente de segurança cibernética grave em uma prefeitura pode gerar uma crise de imagem sem precedentes, abalando a confiança da população na administração e nos serviços digitais.
 - Continuidade de Serviços: A interrupção de serviços públicos por um ataque cibernético não é apenas um transtorno, mas pode ter impactos sociais graves, como a interrupção de pagamentos de benefícios, fechamento de escolas ou impossibilidade de registro de nascimentos/óbitos.
- 4) Gestão de Vulnerabilidades e Inteligência de Ameaças:
 - O SOC não apenas reage, mas atua proativamente. Identifica vulnerabilidades nos sistemas da prefeitura, mantém-se atualizado sobre novas ameaças e fortalece as defesas para prevenir ataques antes que aconteçam.

PREFEITURA MUNICIPAL DE SÃO JOAQUIM DA BARRA

ESTADO DE SÃO PAULO

Praça Prof. Ivo Vannuchi S/N – Fone PABX (16) 3810-9000 – FAX (16) 3810-2056



Proc. Nº

0554/2025

FOLHA DE RESPOSTA

Fl. Nº 04

Rubrica

- A natureza dos IPs roteáveis em cada unidade aumenta a superfície de ataque, tornando a monitorização e a gestão de vulnerabilidades pelo SOC ainda mais cruciais.
- 5) Resposta a Incidentes de Segurança (RIS) Eficaz:
 - Em caso de ataque, o SOC coordena a resposta, contenção, erradicação e recuperação, minimizando o tempo de inatividade e o dano. Para uma municipalidade, uma resposta rápida é vital para restaurar a normalidade dos serviços.

Conclusão: Imprescindibilidade para a Governança Digital

Para uma municipalidade que atende 91 pontos com serviços públicos e utiliza internet com IPs roteáveis, o NOC e o SOC não são apenas um diferencial tecnológico, mas uma infraestrutura fundamental para a governança digital, a segurança jurídica e a responsabilidade social.

- NOC: Garante que a espinha dorsal de comunicação (os 91 links) esteja sempre ativa e com performance, sustentando a operação diária da prefeitura e o atendimento ao cidadão.
- SOC: Protege o ativo mais valioso de uma prefeitura no ambiente digital: os dados dos cidadãos e a integridade dos serviços públicos.

Ignorar a implementação de um NOC e um SOC é expor a municipalidade a riscos inaceitáveis de indisponibilidade de serviços, vazamento de dados, ataques cibernéticos e consequente perda de confiança da população e responsabilização legal. É um investimento estratégico na resiliência e na modernização da gestão pública.

São Joaquim da Barra, 23 de Maio de 2025.

PREFEITURA MUNICIPAL DE SÃO JOAQUIM DA BARRA

ESTADO DE SÃO PAULO

Praça Prof. Ivo Vannuchi S/N – Fone PABX (16) 3810-9000 – FAX (16) 3810-2056