



Barueri, 08 de junho de 2026.

Às

Empresas interessadas

Ref.: Esclarecimento nº 002 a respeito ao Pregão Eletrônico 90006.2026.

Objeto: Contratação de empresa especializada na prestação de serviços gerenciados de segurança da informação para a infraestrutura de TI da FIEB e suas unidades. O escopo inclui locação de equipamentos, prestação de serviços de instalação, configuração, manutenção ON-SITE, gestão tecnológica e treinamento, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Foi apresentado Pedido de Esclarecimento referente ao PE 90006.2026, de forma tempestiva, conforme prazo estipulado no edital com o objetivo de obter os esclarecimentos necessários para a correta elaboração da proposta.

“Visando a elaboração de uma proposta técnica e comercial fidedigna à realidade do ambiente da FIEB, e em observância ao Princípio do Planejamento (Art. 18 da Lei 14.133/21), solicitamos os seguintes esclarecimentos acerca do Itens Firewall e Gerência centralizada (SGC):

1. Sobre a Interface de Gerenciamento (Item 4.16.2.1.2): O item 4.16.2.1.1 exige uma Solução de Gerência Centralizada (SGC) para a consolidação de todos os ativos. Contudo, o item 4.16.2.1.2 impõe que o gerenciamento suporte interface web no próprio dispositivo. Considerando que soluções de alta performance focadas em segurança *enterprise* priorizam o gerenciamento centralizado e seguro (via console dedicada ou API), eliminando interfaces web locais para reduzir a superfície de ataque e evitar conflitos de configuração, pergunta-se:

- A Administração aceitará soluções cujo gerenciamento seja realizado exclusivamente de forma centralizada pela SGC exigida no item 4.16.2.1, dispensando a necessidade de interface administrativa web residente no hardware do firewall?

2. Sobre os Requisitos de Throughput (Itens 4.16.1.4.3 e 4.16.1.4.4): Observa-se uma inconsistência técnica nos valores de throughput exigidos. O item 4.16.1.4.4 (Threat Protection) exige um desempenho de 25,5 Gbps, valor este superior aos 23 Gbps exigidos no item 4.16.1.4.3 (NGFW). Tecnicamente, a ativação de camadas adicionais de segurança (como Proteção de Malwares) consome mais recursos de processamento, resultando em um throughput inferior ao modo NGFW. Diante disso, pergunta-se:

- Poderia a Administração retificar os valores de throughput, confirmando os patamares corretos para cada nível de inspeção, de modo a permitir o dimensionamento adequado do hardware?”

RESPOSTA:

- 1) Considerando que o Termo de Referência exige a utilização de Solução de Gerência Centralizada (SGC) para administração dos ativos de segurança, bem como interface administrativa baseada em web, questiona-se:



FUNDAÇÃO INSTITUTO DE EDUCAÇÃO DE BARUERI

Avenida Andrômeda, 500 | Alphaville | Barueri - SP | CEP 06473-000
CNPJ 65.700.239/0001-10 | Tel 11 2078-7810

A Administração entende que a solução deverá prover ambos os modelos de gerenciamento, sendo:

- gerenciamento centralizado por meio da SGC, para controle unificado, auditoria e aplicação de políticas globais; e
- gerenciamento local por meio da interface administrativa web residente no próprio equipamento, para atendimento a necessidades específicas de cada site, troubleshooting e intervenções pontuais?

Como referência de mercado, soluções como Fortinet operam nesse modelo híbrido, combinando gerenciamento centralizado (ex: FortiManager) com gerenciamento local por dispositivo (ex: interface web do FortiGate).

- 2) Os requisitos de throughput previstos no edital devem ser interpretados considerando metodologias distintas de benchmark utilizadas pelos fabricantes de soluções NGFW. Os requisitos são independentes e devem ser comprovados individualmente pelo fabricante.

No mercado de segurança corporativa, não existe padronização absoluta entre os critérios utilizados para medição de throughput NGFW, Threat Protection, IPS, TLS Inspection e proteção avançada. Diferentes fabricantes utilizam combinações distintas de assinaturas, tamanhos de pacote, fluxos simultâneos, mecanismos de inspeção e perfis de segurança.

Assim, a diferença entre os valores exigidos para NGFW e Threat Protection não representa necessariamente inconsistência técnica, podendo refletir metodologias distintas de aferição de desempenho entre fabricantes e arquiteturas de processamento específicas.

Adicionalmente, soluções modernas utilizam aceleração por hardware, processamento paralelo, ASICs dedicados e offloading inteligente, permitindo comportamentos distintos conforme o perfil de inspeção ativado.

Portanto, os requisitos definidos no edital permanecem tecnicamente defensáveis e compatíveis com o objetivo da contratação, que é garantir solução de alta capacidade, adequada ao ambiente corporativo da FIEB e preparada para crescimento operacional futuro.

Na certeza de termos prestado o devido esclarecimento, cujo teor deu-se conhecimento aos demais interessados conhecidos, subscrevemo-nos.

Atenciosamente,

Comissão de Licitação

Portaria nº 331/2025