



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

Barueri, 08 de junho de 2026.

Às

Empresas interessadas

Ref.: Esclarecimento nº 003 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.

“Prezados,

Solicitamos esclarecimentos referente ao Edital do Pregão Eletrônico de nº 90006/2026, Uasg:926656, conforme abaixo:

Questionamento 1:

De acordo com o item 4.3.1 do Anexo I (Termo de Referência), temos o seguinte requisito:

“4.3.1. A atividade deve ser provida através de Centro de Operações de Segurança (Security Operations Center - SOC), contemplando, no mínimo, 02 (dois) ambientes próprios da CONTRATADA, estruturados de forma redundante.”

Entendemos que a CONTRATADA poderá utilizar o modelo operacional baseado em infraestrutura cloud, de maneira a garantir a redundância necessária para atendimento aos SLAs exigidos, em substituição à exigência literal de “dois ambientes próprios da CONTRATADA” físicos distintos. Está correto o nosso entendimento?

Questionamento 2:

De acordo com o item 4.3.2 do Anexo I (Termo de Referência), temos o seguinte requisito:

4.3.2. A CONTRATADA deverá possuir, ao menos, as seguintes certificações: ISO 27001, ISO 27701, ISO 37001, ISO 37301 e ISO 20000-1, a fim de garantir que adota padrões internacionais de segurança da informação, privacidade de dados, prevenção à corrupção e conformidade legal e regulatória. Deverá, ainda, apresentar os atestados de certificações válidos, de forma a garantir que seu ambiente e processos seguem os procedimentos e controles estabelecidos nas respectivas ISOs.”

Uma vez que o objeto da licitação foca em serviços de Firewall, SIEM e SOC, entendemos que a posse da ISO 27001 (Gestão de Segurança da Informação), que é o padrão global e mais abrangente para a proteção de dados e ativos, bem como a posse da ISO 20000-1 (Gestão de Serviços de Tecnologia da



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

Informação), seriam consideradas suficientes para garantir que a CONTRATADA adota padrões internacionais de segurança da informação exigidos pela FIEB.

A exigência concomitante de cinco normas ISO distintas (incluindo normas de compliance e anticorrupção como a 37001 e 37301) pode ser interpretada como um requisito excessivamente restritivo, limitando a competitividade do certame e afastando empresas tecnicamente aptas que possuem as certificações core de segurança da informação. Entendemos ainda que tais certificações relativas a compliance e anticorrupção podem ser substituídas por políticas da CONTRATADA a serem apresentadas como alternativa às certificações ISO em questão.

Ressaltamos que a Lei nº 14.133/2021 estabelece que as exigências de habilitação devem ser estritamente necessárias e proporcionais ao objeto da contratação, visando sempre a ampliação da disputa.

Diante do exposto, entendemos que a CONTRATADA deverá possuir, ao menos, duas das seguintes certificações: ISO 27001, ISO 27701, ISO 37001, ISO 37301 e ISO 20000-1, sendo obrigatória a apresentação da certificação ISO 27001 e mais uma. Está correto o nosso entendimento?

RESPOSTA:

- 1) O entendimento apresentado não está correto.

A exigência constante do item 4.3.1 do Termo de Referência estabelece que a prestação dos serviços deverá ocorrer por meio de Centro de Operações de Segurança (SOC) suportado por, no mínimo, 02 (dois) ambientes próprios da CONTRATADA, estruturados de forma redundante, visando assegurar a continuidade operacional dos serviços, a alta disponibilidade da operação e a resiliência da infraestrutura utilizada para monitoramento, correlação, tratamento e resposta a incidentes de segurança.

Para fins de atendimento ao requisito, os ambientes redundantes deverão estar localizados em sites distintos, com separação geográfica adequada, recomendando-se distância mínima de 50 km entre eles, em conformidade com as melhores práticas de continuidade de negócios, recuperação de desastres (Disaster Recovery – DR) e resiliência operacional adotadas pelo mercado. Tal requisito tem como objetivo mitigar riscos decorrentes de indisponibilidades locais, desastres naturais, falhas de infraestrutura, interrupções de energia, problemas de telecomunicações ou quaisquer eventos que possam comprometer simultaneamente ambos os ambientes.

A utilização de infraestrutura em nuvem (cloud) poderá ser empregada como componente da solução tecnológica da CONTRATADA, desde que não descaracterize o atendimento ao requisito de existência dos dois ambientes redundantes e independentes, sendo necessária a comprovação de que a arquitetura implementada garante segregação física e lógica adequada, operação contínua, mecanismos de contingência, recuperação de desastres e manutenção dos níveis de serviço exigidos pela contratação.



Dessa forma, a simples utilização de uma infraestrutura cloud, sem a demonstração de ambientes redundantes e independentes que atendam aos objetivos de continuidade operacional e resiliência previstos no Termo de Referência, não será considerada suficiente para o atendimento do requisito estabelecido no item 4.3.1.

2) O entendimento apresentado não está correto.

A exigência constante do item 4.3.2 do Termo de Referência foi estabelecida com fundamento na necessidade de garantir que a futura contratada possua um sistema de gestão corporativa maduro, abrangente e auditado por organismo independente, compatível com a criticidade dos serviços objeto da contratação, que envolvem monitoramento contínuo de segurança, tratamento de eventos e incidentes cibernéticos, gestão de ativos de informação, proteção de dados pessoais e operação de serviços essenciais de tecnologia.

As certificações requeridas não possuem caráter redundante ou sobreposto, mas sim complementar, contemplando diferentes dimensões de governança, segurança, conformidade e qualidade operacional, conforme descrito a seguir:

- ISO 27001 – estabelece os requisitos para implementação e manutenção de um Sistema de Gestão de Segurança da Informação (SGSI), assegurando a proteção da confidencialidade, integridade e disponibilidade das informações;
- ISO 27701 – complementa a ISO 27001 ao estabelecer controles específicos voltados à gestão da privacidade e proteção de dados pessoais, alinhando processos às melhores práticas internacionais de privacidade e aos princípios previstos na legislação de proteção de dados;
- ISO 20000-1 – estabelece requisitos para gestão e entrega de serviços de tecnologia da informação, assegurando qualidade, controle operacional, gerenciamento de incidentes, mudanças, disponibilidade e melhoria contínua dos serviços prestados;
- SO 37001 – estabelece mecanismos de prevenção, detecção e tratamento de atos de suborno e corrupção, fortalecendo a integridade corporativa e a transparência na execução contratual;
- ISO 37301 – estabelece requisitos para sistemas de gestão de compliance, assegurando aderência a requisitos legais, regulatórios, normativos e contratuais, especialmente relevantes em contratos firmados com a Administração Pública.

A Administração entende que a contratação de serviços de SOC, SIEM, Firewall Gerenciado e demais atividades correlatas não se limita à mera operação tecnológica de ferramentas. Trata-se de uma contratação que envolve acesso a informações sensíveis, tratamento de eventos de segurança, gestão de registros, interação com ambientes críticos da instituição, cumprimento de requisitos regulatórios e observância permanente de controles de governança, integridade, privacidade e conformidade.

Nesse contexto, a exigência conjunta das certificações busca assegurar que a contratada adote um conjunto integrado de boas práticas internacionalmente reconhecidas, abrangendo não apenas segurança da informação, mas também privacidade, gestão de serviços, integridade corporativa e compliance organizacional.



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

Adicionalmente, políticas internas, códigos de ética, programas de integridade ou procedimentos corporativos, embora relevantes, não constituem equivalentes às certificações requeridas, uma vez que não são submetidos ao mesmo processo formal de auditoria independente, validação periódica e certificação por organismo acreditado, características essenciais das normas ISO exigidas.

Por fim, a Administração entende que os requisitos estabelecidos guardam pertinência e proporcionalidade com a natureza, criticidade e responsabilidade inerentes ao objeto da contratação, tendo sido definidos com o objetivo de mitigar riscos operacionais, regulatórios, de privacidade, de integridade e de continuidade dos serviços.

Dessa forma, permanece inalterada a exigência prevista no item 4.3.2 do Termo de Referência, sendo necessária a comprovação de todas as certificações expressamente requeridas, não sendo admitida sua substituição por políticas internas ou pela apresentação parcial das certificações listadas.

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