

PREGÃO ELETRÔNICO NACIONAL NF 0152-26**PRESTAÇÃO DE SERVIÇOS ESPECIALIZADOS NA ÁREA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECIMENTO DE SOFTWARE, ANÁLISE DE VULNERABILIDADES DO AMBIENTE CORPORATIVO, RESPOSTA A INCIDENTES DE SEGURANÇA E SUPORTE TÉCNICO ESPECIALIZADO****ADITAMENTO 3**

I) Em conformidade com o disposto no subitem 2.6.1 do Caderno de Bases e Condições do Pregão Eletrônico Nacional NF 0152-26, a ITAIPU responde perguntas realizadas por empresas interessadas nesta licitação:

PERGUNTA 1.

“Com relação ao item 1.4.2, alínea “c” do edital, que trata da certificação ISO/IEC 27001:2022, solicitamos o seguinte esclarecimento: Entendemos que, para fins de habilitação, deverá ser apresentada apenas a Declaração de Compromisso assinada pelo representante legal da licitante, e que a certificação ISO/IEC 27001:2022 válida será exigida apenas no momento da execução contratual, caso a empresa seja declarada vencedora. Está correto o nosso entendimento?”

RESPOSTA

Entendimento correto. Vale ressaltar que a CONTRATADA deverá apresentar a certificação ISO/IEC 27001:2022 apenas no momento da execução contratual em um prazo de até 10 (dez) da Ordem de Inícios de Serviços, nos termos da Cláusula 6ª da Minuta de Contrato, Anexo IV do CBC.

PERGUNTA 2.

“Em atenção ao item 1.4.2, alínea “c” do edital, que trata da apresentação de Declaração de Compromisso quanto à certificação ISO/IEC 27001:2022 válida para execução contratual, gostaríamos, respeitosamente, de submeter o seguinte esclarecimento:

Considerando que a finalidade da exigência é garantir que a futura contratada possua capacidade técnica e aderência às melhores práticas de gestão de segurança da informação, entendemos que tal objetivo também pode ser plenamente atendido quando a empresa dispõe, em seu quadro funcional, de profissional com vínculo empregatício formal, devidamente certificado na ISO/IEC 27001.

Nesse sentido, questiona-se se será aceito, para fins de atendimento ao item em referência, a comprovação de que a proponente possui em seu corpo técnico profissional com certificação ISO/IEC 27001 vigente, acompanhada do respectivo vínculo empregatício, em substituição à certificação institucional da empresa.

Tal interpretação encontra respaldo nos princípios que regem as contratações públicas, especialmente os previstos na Lei nº 14.133/2021, como o da competitividade, da razoabilidade e da ampliação da disputa (art. 5º), bem como no entendimento de que as exigências de habilitação devem se limitar ao estritamente necessário para garantir a execução do objeto (art. 67). Ademais, a jurisprudência do Tribunal de Contas da União orienta que requisitos de qualificação técnica não devem restringir indevidamente a participação de licitantes quando existirem meios equivalentes de comprovação da capacidade técnica.

Dessa forma, entendemos que a aceitação da certificação vinculada ao profissional da equipe técnica atende ao interesse público sem comprometer a qualidade e a segurança da execução contratual, ao mesmo tempo em que amplia a competitividade do certame”.

RESPOSTA

Entendimento incorreto. A ITAIPU reitera que a exigência do subitem 1.4.2, alínea “c” refere-se à Certificação ISO/IEC 27001:2022, em nome da pessoa jurídica (Proponente), ainda que apresentada sob a forma de Declaração de Compromisso para obtenção e validade durante a execução contratual. Importante destacar que a ISO/IEC 27001 possui natureza institucional, atestando a existência e a manutenção de um Sistema de Gestão de Segurança da Informação implementado no âmbito da organização, não sendo suprida por certificações individuais de profissionais, ainda que integrantes do corpo técnico da proponente.

PERGUNTA 3.

“As especificações técnicas dispostas no ANEXO I detalham os requisitos a serem atendidos pelas soluções que deverão ser entregues pela CONTRATADA. No entanto, no que se refere ao item 5 - Software de Análise e Gestão de Vulnerabilidades, verificamos que o subitem 5.7 apresenta uma listagem de soluções específicas de um único fabricante, ainda que explicita que tal relação não possui caráter limitativo para o atendimento ao edital.

Considerando a ausência de justificativa para a indicação explícita de modelo e fabricante da solução a ser fornecida, entendemos que as ferramentas elencadas no item 5.7 possuem caráter meramente exemplificativo. Dessa forma, compreendemos que a entrega de solução equivalente, de outro fabricante amplamente reconhecido no mercado, desde que atenda integralmente às especificações técnicas estabelecidas, será considerada aderente às exigências do edital”. Nosso entendimento está correto?”

RESPOSTA

Entendimento incorreto. A indicação do software constante no subitem 5.7 das Especificações Técnicas decorre de padronização tecnológica da ITAIPU, que já possui investimentos realizados em capacitação, integrações, configurações e processos operacionais vinculados à solução especificada. Além disso, o processo de gestão de vulnerabilidades e incidentes encontra-se integralmente estruturado com base nesse software, de modo que a adoção de solução diversa, ainda que equivalente, não atenderia às necessidades técnicas e operacionais atualmente estabelecidas. Favor remeter ao Item II deste Aditamento.

PERGUNTA 4.

“Referente ao item 9.4.1, a CONTRATANTE estabelece que os técnicos alocados no item 3 (Blue Team) devem possuir duas ou mais das seguintes certificações:

- I. GIAC Certified Intrusion Analyst (GCIA)
- II. GIAC Certified Incident Handler (GCIH)
- III. GIAC Cyber Incident Leader (GCIL)

Entendemos que certificações com escopo técnico equivalente podem ser aceitas para fins de atendimento ao requisito, considerando a abrangência e reconhecimento no cenário de segurança da informação. Dessa forma, entendemos que a certificação, CompTIA Cybersecurity Analyst (CySA+) atendem como equivalente a certificação GIAC Certified Intrusion Analyst (GCIA). Nosso entendimento está correto quanto às certificações equivalentes, comprovando assim a aderência técnica às competências exigidas?”

RESPOSTA

Entendimento correto. A CompTIA Cybersecurity Analyst (CySA+) será aceita como equivalente à certificação GIAC Certified Intrusion Analyst (GCIA) indicada no subitem 9.4.1 inciso I, das Especificações Técnicas, Anexo I.

PERGUNTA 5.

“Considerando que o item 5 do quadro orçamentário apresenta a contratação de “*Software de Análise Contínua de Vulnerabilidades*” de forma genérica, com quantitativo de 6.000 unidades, e que o item 5.7 do Termo de Referência detalha o licenciamento mínimo contemplando:

- 5.7.1 TruRisk Eliminate - 6.000 ativos;
- 5.7.2 VMDR - 6.000 ativos;
- 5.7.3 Qualys TotalAppSec - 400 APIs;

Solicitamos esclarecer: O quantitativo de 6.000 unidades previsto no item 5 do orçamento refere-se exclusivamente ao licenciamento de ativos para as soluções *TruRisk Eliminate* e *VMDR*, conforme itens 5.7.1 e 5.7.2 do TR?”

RESPOSTA

Não. A Solução ofertada deve suportar a quantidade de 6.000 ativos e ser licenciada para todas as funcionalidades que envolvem a gestão contínua de vulnerabilidades e funções complementares para atingir a maior segurança no funcionamento da solução, nos termos dos subitens 5.1, 5.2 e 5.7 das Especificações Técnicas. Dessa forma, todos os custos de licenciamento e das funcionalidades necessárias à solução deverão ser consolidados em um único item orçamentário, conforme previsto no Item 5 do Orçamento Estimado, Anexo II do CBC.

PERGUNTA 6.

“Considerando que o item 5 do quadro orçamentário apresenta a contratação de “*Software de Análise Contínua de Vulnerabilidades*” de forma genérica, com quantitativo de 6.000 unidades, e que o item 5.7 do Termo de Referência detalha o licenciamento mínimo contemplando:

- 5.7.1 TruRisk Eliminate - 6.000 ativos;
- 5.7.2 VMDR - 6.000 ativos;
- 5.7.3 Qualys TotalAppSec - 400 APIs;

Solicitamos esclarecer: O licenciamento da solução *Qualys TotalAppSec (400 APIs)*, conforme item 5.7.3, está contemplado dentro deste mesmo item orçamentário ou deverá ser considerado separadamente na composição de preços?”

RESPOSTA

Favor reportar-se à resposta da pergunta anterior.

PERGUNTA 7.

“Considerando que o item 5 do quadro orçamentário apresenta a contratação de “*Software de Análise Contínua de Vulnerabilidades*” de forma genérica, com quantitativo de 6.000 unidades, e que o item 5.7 do Termo de Referência detalha o licenciamento mínimo contemplando:

- 5.7.1 TruRisk Eliminate - 6.000 ativos;
- 5.7.2 VMDR - 6.000 ativos;
- 5.7.3 Qualys TotalAppSec - 400 APIs;

Solicitamos esclarecer: Caso estejam consolidadas todas as licenças mencionadas acima, qual o critério esperado para composição do licenciamento (unificação em uma única métrica ou detalhamento por tipo de solução)?”

RESPOSTA

O critério esperado para a composição do licenciamento é a unificação em uma única métrica, com a consolidação das licenças e funcionalidades aplicáveis em um único item, conforme o Item 5 do Orçamento Estimado (Anexo II do CBC).

PERGUNTA 8.

“Considerando que o item 5 do quadro orçamentário apresenta a contratação de “*Software de Análise Contínua de Vulnerabilidades*” de forma genérica, com quantitativo de 6.000 unidades, e que o item 5.7 do Termo de Referência detalha o licenciamento mínimo contemplando:

- 5.7.1 TruRisk Eliminate - 6.000 ativos;
- 5.7.2 VMDR - 6.000 ativos;
- 5.7.3 Qualys TotalAppSec - 400 APIs;

Solicitamos esclarecer: Caso estejam consolidadas todas as licenças mencionadas acima, entendemos que será solicitado o quantitativo total das licenças no primeiro pedido (*Software de Análise Contínua de Vulnerabilidades*, 6.000 unidades), está correto nosso entendimento?”

RESPOSTA

Entendimento incorreto. O quantitativo total das licenças solicitadas será sob demanda da ITAIPU, conforme item 10 das Especificações Técnicas, Anexo I do CBC.

PERGUNTA 9.

“O item “5.7” do Anexo I define que o licenciamento mínimo da solução ofertada deve ser do fabricante Qualys. Visando o favorecimento da competitividade do certame, entendemos que serão aceitas soluções de outros fabricantes desde que todos os requisitos técnicos especificados no item “5. SOFTWARE DE ANÁLISE E GESTÃO DE VULNERABILIDADES” sejam atendidos integralmente. Está correto nosso entendimento?”

RESPOSTA

Entendimento incorreto. Favor remeter-se à resposta do Pergunta 3, bem como Item II deste Aditamento.

II) Em conformidade com o disposto no subitem 2.6.2 do Caderno de Bases e Condições (CBC) do Pregão Eletrônico Nacional NF 0152-26, a ITAIPU:

- A) inclui o subitem 1.2.1 no CBC, contendo a Justificativa de Marca do Fabricante *Qualys* para o Software de Análise de Contínua de Vulnerabilidades, Item 5 das Especificações Técnicas, Anexo I do CBC;
- B) altera o Calendário de Eventos desta licitação, prorrogando a data da Sessão Pública e demais prazos, conforme segue:

(...)

1.3.2 Formalização de consultas:

Até [14/04/2026](#)

1.3.3 Respostas:

Até [16/04/2026](#)

1.3.4 Recepção das propostas:

Até às 9h de [23/04/2026](#)

1.3.5 Início da Sessão Pública com a divulgação das propostas:

Em [23/04/2026](#), a partir das 9h

1.3.6 Início da etapa de disputa de lances:

Em 23/04/2026, a partir das 9h30min

(...)

- C) ajusta as numerações do Subitem 1.2 das Especificações Técnicas, bem como, exclui o subitem 5.1.9 por estar em duplicidade com o subitem 5.1.3, conforme segue:

(...)

~~5.1.9 O Fabricante da solução deve possuir equipe de pesquisa de vulnerabilidades;~~

- D) disponibiliza em anexo a este Aditamento nova versão do CBC e Anexo I, Especificações Técnicas com ajustes efetuados na cor azul.

- E) em face das alterações havidas, as propostas eventualmente já registradas no Portal de Compras sejam canceladas, caso pertinente, e, novamente registradas, observando as alterações promovidas por este Aditamento.

III) Permanecem inalteradas as demais condições contidas no CBC do Pregão Eletrônico Nacional NF 0152-26.

Emitido por: Divisão de Suporte Técnico	Data de emissão: 10 de abril de 2026
---	--------------------------------------