PREGÃO ELETRÔNICO - PE.PPSA.010/2024

TESTES DE PENETRAÇÃO E VULNERABILIDADE PARA A PPSA

(Atualizado em: 02/09/2024 – Esclarecimento nº 02, Perguntas e Respostas de 01 até 14)

ESCLARECIMENTO Nº 02

Pergunta nº 01: A utilização de acessos remotos ao ambiente da CONTRATANTE, permitem a execução de testes de forma remota sem prejuízo aos resultados. É correto o entendimento de que os testes de intrusão e testes de vulnerabilidades podem ser executados de forma remota?

Resposta nº 01: Sim, o entendimento está correto.

Pergunta nº 02: Para os testes em formato remoto, é correto o entendimento que a responsabilidades pelos acessos, quando necessário serão da CONTRATANTE?

Resposta nº 02: Sim, o entendimento está correto. A PPSA irá fornecer acesso remoto a CONTRATADA quando necessário.

Pergunta nº 03: Dentro dos volumes informados no item 17, qual expectativa de targets/alvos devem ser considerados para cada lote de teste de intrusão? Para dimensionamento da equipe de ethical hackers, é fundamental a informação de quantitativos em FQDNs, quantidade de endereços IP/URLs ou dispositivos de infraestrutura. Também é solicitada a quantidade de APIs de Integração, caso houver.

Resposta nº 03: A PPSA esclarece que a estratégia que definirá o dimensionamento do teste será de inteira responsabilidade da licitante, cabe salientar que a estratégia deverá respeitar o disposto no item 3 e no item 4.1 do Termo de Referência do Edital.

Pergunta nº 04: Dentro dos volumes informados no item 17, qual expectativa de targets/alvos devem ser considerados para cada lote de teste de vulnerabilidade? Para dimensionamento da equipe é fundamental a quantificação do ambiente onde a varredura será executada.

Resposta nº 04: A PPSA esclarece que a estratégia que definirá o dimensionamento do teste será de inteira responsabilidade da licitante, cabe salientar que a estratégia deverá respeitar o disposto no item 3 e no item 4.1 do Termo de Referência.

Pergunta nº 05: Para as dúvidas anteriores, é importante declarar quais alvos serão objeto do teste de intrusão e quais alvos serão objeto do teste de vulnerabilidades.

Resposta nº 05: A PPSA esclarece que a estratégia que definirá o dimensionamento do teste será de inteira responsabilidade da licitante, cabe salientar que a estratégia deverá respeitar o disposto no item 3 e no item 4.1 do Termo de Referência.

Pergunta nº 06: Em relação ao item 13.3.2.b do edital, que trata das certificações dos profissionais, gostaríamos de solicitar um esclarecimento. No caso de a empresa não possuir no momento da habilitação as certificações requeridas, seria permitido apresentar, em substituição, uma declaração de compromisso de contratação futura de profissionais que possuam as certificações exigidas, dentro do prazo estipulado para a execução do contrato?

Resposta nº 06: De acordo com a publicação do TCU - Licitações e Contratos 5ª. Edição, 2024, página 579 - in verbis:, "os critérios de habilitação técnica, previstos no art. 67 da Lei 14.133/2021, prestam-se a comprovar que o licitante possui a qualificação técnica necessária para bem executar o objeto da contratação. Referem-se, portanto, a características inerentes ao licitante, não se confundindo com os critérios técnicos de aceitabilidade da sua proposta, relacionados ao objeto da contratação. A documentação para habilitação técnica deve comprovar, a depender do tipo de objeto a ser contratado, a qualificação técnico-profissional e a técnico-operacional cumulativamente. A qualificação técnico-profissional trata da vinculação ao licitante de profissionais com conhecimento técnico e experiência necessários à execução do objeto do certame. O licitante deve indicar profissional (registrado no conselho profissional competente, quando for o caso) detentor de atestado de responsabilidade técnica por execução de obra ou serviço de características semelhantes, que será o responsável técnico caso o licitante seja contratado. É importante mencionar que, sob a égide da Lei 8.666/1999, o TCU se posicionou no sentido de que não é necessário o vínculo empregatício entre o profissional indicado e o licitante. A disponibilidade do profissional pode ser demonstrada por meio de outros documentos, como contrato de prestação de serviços, vínculo societário entre a empresa e o profissional especializado, ou mesmo declaração de contratação futura do profissional detentor do atestado apresentado. Essa declaração deve ser acompanhada de declaração de anuência do profissional. O profissional indicado pelo licitante deve participar da execução do contrato, sendo admitida a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pela Administração. A exigência constante do item 13.3.2.b refere-se à qualificação técnico-profissional, portanto não há nenhum impedimento para sua exigência. Todavia, em linha com o entendimento do TCU a referida comprovação poderá ser realizada por meio de declaração de contratação futura do profissional, desde que a referida contratação ocorra até 10 dias após a assinatura do contrato (data de realização da reunião inicial prevista na letra B do cronograma do item 5.1 do termo de Referência). Essa declaração deve ser acompanhada de declaração de anuência do profissional.

Pergunta nº 07: Para a realização dos testes de vulnerabilidades, é correto o entendimento de que a CONTRATANTE disponibilizará hardware para instalação de scanner de vulnerabilidade dentro do seu ambiente?

Resposta nº 07: Caso seja necessário a PPSA poderá fornecer hardware para instalação de ferramenta.

Pergunta nº 08: Todos os requisitos de qualificação técnica devem ser cumpridos no momento da habilitação para garantir a capacidade técnica do proponente. Entretanto, a nova Lei de Licitações e Contratos (Lei nº 14.133/2021), no artigo 67, inciso I, removeu a regra prevista na legislação anterior que exigia que o profissional já fizesse parte do quadro permanente da empresa durante a fase de habilitação. Portanto, a apresentação da certificação requerida deve ser realizada até a assinatura do contrato, não sendo possível adiar para um momento posterior.

Resposta nº 08: Ver resposta ao questionamento 06, acima.

Pergunta nº 09: No Edital na página 11, item 13.3.2. na alínea b) solicita que o proponente tenha pelo menos 1 funcionário certificado em uma das certificações listadas. Entendemos a importância destas certificações para o processo, contudo gostaríamos de um entendimento sobre o momento da entrega da certificação, visto que em nosso entendimento a certificação poderá ser entregue no decorrer do contrato visto que tal exigência poderá gerar custo a proponente no período anterior a assinatura do contrato, tema este vedado pela lei de licitação. Está correto nosso entendimento de ser permitido a entrega da certificação nos primeiro 90 dias após a assinatura do contrato?

Resposta nº 09: Ver resposta ao questionamento 06, acima.

Pergunta nº 10: 3.2- TESTE DE PENETRAÇÃO (INTRUSÃO) 3.2.17 - Para os testes de DoS e DDOS a PPSA irá definir quais os horários poderão ser utilizados para a execução deles; Questionamento: 1) Qual a expectativa da contratante em relação a execução e resultados dos ataques de DDoS? Solicitamos esclarecer este item

Resposta nº 10: O objetivo dos testes de DoS e DDoS é avaliar a eficácia e a resiliência dos serviços de proteção atualmente em vigor na PPSA em relação a esses tipos de ataques. A expectativa é que os testes permitam identificar possíveis vulnerabilidades na infraestrutura tecnológica da CONTRATANTE, além de medir a capacidade dos sistemas de manter a estabilidade e a disponibilidade dos serviços sob condições de ataque.

Pergunta nº 11: 3.2- TESTE DE PENETRAÇÃO (INTRUSÃO) 3.2.8- Os testes não poderão comprometer a continuidade dos serviços em questão, qualquer atividade que seja interrompida sem autorização da PPSA será de responsabilidade da CONTRATADA, que deverá restabelecer o serviço imediatamente; Questionamento: 1) Dado a natureza invasiva do serviço solicitado, sempre existe um risco mínimo de indisponibilidade do alvo dos testes. A licitante entende que para os ativos alvo dos testes de intrusão que forem alinhados com a contratante, o item em questão não se aplica, ou seja, a contratada não será responsável por restabelecer o ativo e serviços. O entendimento está correto?

Resposta nº 11: Qualquer interrupção dos serviços da PPSA SEM autorização, deverá ser restabelecido. Devido à natureza dos serviços, a PPSA entende que poderão ocorrer interrupções, desde que sejam previamente acordas e aprovadas pela PPSA durante a execução do contrato.

Pergunta nº 12: 3.3- TESTE DE VULNERABILIDADE: 3.3.4- A equipe técnica da GTI (Gerência de Tecnologia da Informação) da PPSA realizará o acompanhamento dos testes de vulnerabilidades que deverão ser realizados no escritório da PPSA; Questionamento: 1) A contratada entende que os testes de vulnerabilidades poderão ser realizados remotamente, seguindo a mesma lógica do teste de intrusão grey box. O entendimento está correto?

Resposta nº 12: Sim, o entendimento está correto.

Pergunta nº 13: 3.3- TESTE DE VULNERABILIDADE: 3.3.4- A equipe técnica da GTI (Gerência de Tecnologia da Informação) da PPSA realizará o acompanhamento dos testes de vulnerabilidades que deverão ser realizados no escritório da PPSA; Questionamento: 1) A contratada entende que assim como os testes greybox, o item também poderá ser realizado de forma remota. O entendimento está correto?

Resposta nº 13: Sim, o entendimento está correto.

Pergunta nº 14: De acordo com o item 13.2 do Termo de Referência, temos as exigências de habilitação técnica do licitante. Diante disto, entendemos que as certificações Claroty CyberSecurity Analyst (CCA 601) e Claroty Support Engineer (CSE 501), bem como os treinamentos ministrados pela U.S. Department of Homeland Security - Cybersecurity ans Infrastructure Security Angency (CISA) são suficientes para comprovar a capacitação do profissional. Está correto o entendimento?

Resposta nº 14: O entendimento não está correto. De acordo com o item 13.2 do Termo de Referência, as certificações exigidas são especificamente selecionadas para garantir que os profissionais possuam habilidades comprovadas em testes de penetração e segurança ofensiva, cobrindo uma gama de técnicas necessárias para a execução do serviço contratado.