

Pergunta 01 - Ao analisar minuciosamente o Edital, especialmente o item 5.18 e ss, verificamos que são concedidos às micro e pequenas empresas os benefícios dispostos nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015. Contudo, o art. 4º, §1º, inciso I, estabelece que, no caso de licitação para aquisição de bens ou contratação de serviços em geral, se o valor estimado do item for superior à receita bruta máxima permitida para enquadramento como empresa de pequeno porte – atualmente, R\$ 4,8 milhões –, não se aplicam as disposições da referida Lei Complementar que beneficiam as micro e pequenas empresas. Diante disso, entendemos que não serão concedidos direitos às micro e pequenas empresas, pois tal concessão violaria o disposto no art. 4º, §1º, inciso I, da Nova Lei de Licitações, o que torna o presente processo passível de anulação.

Resposta 01 - O item “5.18” e seguintes faz parte da abertura da sessão, classificação das propostas e formulação de lances, cláusulas padronizadas nos editais do CREA-SP, independente do objeto. Quanto aos aspectos dos direitos previstos no art. 4º da Nova Lei de Licitações, independentemente do citado no Edital, o sistema Comprasnet do Governo Federal quando cadastra uma licitação o mesmo registra se o Pregão terá ou não o Benefício para ME/EPP. No Edital mencionado, ou seja, nº 90009/2024, constou no sistema a seguinte informação “Sem benefícios ME/EPP”, sendo liberada a consulta no sistema a qualquer interessado.

Pergunta 02 - Referente ao item 4.24.1 - ANEXO A - Caderno Técnico, entendemos que o item referido resulta em um total de 12 execuções de pentest ao longo da vigência contratual, está correto esse entendimento?

Resposta 02 - Sim, seu entendimento está correto.

Pergunta 03 - Ainda sobre o item 4.24.1- ANEXO A - Caderno Técnico, dada a prática de pentest e retest, onde as vulnerabilidades encontradas durante um pentest são colocadas a prova de modo que seja constatado quais foram realmente corrigidas e isso através de um retest, considerando a periodicidade de 03 meses, essa execução seria unicamente de pentest ou pode ser considerado um retest como sendo uma execução para, por exemplo, 06 meses adiante do teste executado?

Resposta 03 - As informações técnicas necessárias estão devidamente descritas no caderno técnico. A prática de retest envolve a validação das correções das vulnerabilidades encontradas durante os pentests anteriores. Considerando a periodicidade de 03 meses para os pentest, é importante esclarecer que cada execução de um novo pentest, deve incluir retests dos pentests anteriores.

Pergunta 04 - A contratação de Pentest deve, obrigatoriamente, ter um escopo definido de modo que seja dimensionado corretamente, neste sentido, faz-se necessário especificar o tipo de caixa ((black, gray ou white box), tipo de ativo (aplicação web, aplicação mobile iOS ou android, servidor e seu tipo de atividade, infra interna ou externa, infra física etc.) e se há necessidade de reteste. O CREA pode, por gentileza, disponibilizar essas informações, sem as quais fica impreciso o dimensionamento?

Pergunta 05 - Sobre o item 4.2.4.2 do anexo A – Caderno Técnico, visto que cada tipo de ativo mencionado como exemplo demanda um dimensionamento de esforço diferente por parte da equipe técnica, o que impacta diretamente na composição dos custos, faz necessário saber: qual o descritivo quantitativo e qualitativo dos elementos considerados alvo do pentest?

Resposta 04 e 05 - O modelo de pentest será aquele onde as informações de escopo e ambientes estão sendo fornecidas, assim como usuários e VPN para a realização dos testes internos, quando e se necessário.

No que tange à equipe técnica e os quantitativos de ativos, as informações necessárias para dimensionamento estão descritas no Caderno Técnico, que são os números de servidores, até 300, e quanto ao qualitativo, são Aplicações Web, APIs, Front-end e backend, servidores web, servidores de banco de dados, servidores de arquivos, servidores de autenticação.

Podemos informar as qualificações atuais, mas que poderão variar durante a vigência do contrato, e não devem ser utilizadas como limitador. Portanto a contratada deverá estar preparada para qualquer formato de qualitativo de aplicações que possam ser instaladas no número máximo de 300 servidores objetos desta contratação durante toda a vigência contratual.

Servidores: até 300 - Tecnologias: CentOS 6; CentOS 7; CentOS 8; Ubuntu 12; Ubuntu 20; Ubuntu 22; Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2022; Banco de dados atuais: MySQL, PostgreSQL, MongoDB, DB2

Pergunta 06 - Sobre o item 4.25.1.3 do Anexo A – Caderno técnico, qual ou quais os sistemas que compõem a arquitetura de login da intranet do CREA-SP? O respectivo questionamento faz-se necessário tendo em

vista que, impacta diretamente no dimensionamento do recurso de programação para a elaboração desse tipo de personalização de acordo com a solução utilizada.

Resposta 06 - Todos os sistemas de intranet, necessariamente são acessados através de autenticação via SSO, com base centralizada. Ademais todas as publicações serão realizadas pela área de comunicação do CREA-SP.

Pergunta 07 - Sobre o item 4.25.2 do Anexo A – Caderno técnico, O “programa” mencionado, refere-se ao treinamento e o conteúdo das palestras ou ao conteúdo administrado aos colaboradores como conscientização contínua?

Resposta 07 - A menção ao "programa", refere-se ao "conteúdo programático" contido no item 4.25.4 do Anexo A – Caderno técnico.

Pergunta 08 - No item 4.25.4 do Anexo A – Caderno técnico, qual a solução de domínio e caixa de e-mail utilizada pelo CREA-SP?

Resposta 08 - Exchange online / Office 365

Pergunta 09 - No anexo do Edital_Serviços_de_Monitoramento_NO - anexo III, item 9.1.20 a) é informado que as licenças de EDR são para aproximadamente 200 servidores, já no anexo A - Caderno Técnico NOC SOC no item 4.22.1 é informado que o EDR deverá ser fornecido para até 300 servidores. Entendemos que a CONTRATADA deverá considerar licenciamento suficiente para os 300 servidores. Está correto o nosso entendimento?

Resposta 09 - Sim, seu entendimento está correto. A contratada deverá atender o especificado no Caderno Técnico, item 4.22.1.

Pergunta 10 - Existe contrato semelhante vigente ou recém encerrado? Se sim, qual o número do contrato? Se sim, com qual empresa? Se sim, qual o valor atual do contrato?

Resposta 10 - Todas as informações referentes à contratos do CREA devem ser encontradas no portal de transparência.

Pergunta 11 - Referente ao Item 4.24.2 do caderno técnico, tendo em vista que o alvo dos testes de invasão é o ambiente de tecnologia da informação da contratante, entendemos que as atividades de pentest poderão ser efetuadas remotamente com as devidas tecnologias e acessos concedidos de acordo com cada escopo definido, está correto esse entendimento?

Resposta 11 - Todos os testes deverão ser executados pelos profissionais alocados da contratada nas dependências do CREA-SP, nos endereços indicados neste edital, acompanhados dos gestores do contrato.

Pergunta 12 - Item 4.25.1.1 do Caderno técnico, requer duas palestras, sendo uma para todo o público-alvo aqui descrito e a outra para o Público Estratégico, neste sentido entendemos que as palestras citadas seriam ministradas remotamente, está correto o nosso entendimento?

Resposta 12 - Sim, está correto o entendimento

Pergunta 13 - Item 4.25.4. Serviços de Campanha de Conscientização de Segurança e Prevenção de Phishing, qual o número total de endereços de e-mail que serão considerados alvo da atividade de simulação de phishing e qual o número de campanhas estimadas durante a execução do contrato?

Resposta 13 - A campanha deverá ser executada no domínio do CREA-SP alcançando todos os colaboradores, claramente descrita no edital, número este, não menor que 5.500. O número de campanhas não deverá ser menor que 06 (seis), com o cuidado de ser executada de forma efetiva em cada um dos semestres, conforme definido claramente nos itens do edital 4.25.1 a 4.25.4.7.