



17433488



08006.000003/2021-38



Ministério da Justiça e Segurança Pública  
Secretaria-Executiva  
Coordenação de Riscos e Segurança de TIC

## RESPOSTA AO PEDIDO DE ESCLARECIMENTO 16 - CRS

1. Trata-se de resposta ao pedido de esclarecimento nº 16 (17430614) ao edital do Pregão Eletrônico nº 21/2021, cujo objeto é a contratação de empresa especializada, para o fornecimento de Serviço de Centro de Operações de Segurança (Security Operations Center - SOC) com funcionamento e suporte 24h por dia e 7 dias por semana, Serviço de tratamento e resposta aos incidentes cibernéticos - CSIRT - Blue Team e Serviço de teste de invasão - Red Team, pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses, para o atendimento das necessidades da Diretoria de Tecnologia da Informação e Comunicação - DTIC do Ministério da Justiça e Segurança Pública - MJSP, conforme informações constantes do Edital.

2. No referido pedido de esclarecimento foram feitos 2 (dois) questionamentos de ordem técnica. Abaixo seguem as respostas aos questionamentos.

2.1. Esclarecimento 1) Indo ao encontro do esclarecimento 8 "Esclarecimento 08 - Referente os itens 3.4.3.2 e Tabela 10 "Teste de Invasão - Red Team : Sistemas Web" "3.4.3.2. A Tabela 10, do Estudo Técnico Preliminar, Anexo I-N, demonstra que um alvo é um ativo, o qual pode ser um sistema, appliance de segurança, ativo de rede, dentre outros. Nesse contexto, considera-se que um sistema possui em média dez ativos. Dessa forma, nota-se similaridade e complementariedade entre os itens 3 e 4 do grupo 2, uma vez que, para efeitos desta contratação, ambos são considerados alvos. Sendo que o item 4 (Serviço de Teste de Invasão - Red Team: Infraestrutura) constitui um serviço a ser realizado em um único alvo, enquanto que o item 3 (Serviço de Teste de Invasão - Red Team: Sistemas Web) constitui um serviço que pode contemplar múltiplos alvos" Tabela 10 - Considerando que um sistema possui em média 10 ativos (Gateway de Rede, Firewall, DNS, Balanceador de Carga, Firewall de APP, 2x Servidores de App, 2x Servidores de Transação, Servidor de Banco de Dados - Clusterizado dentre outros ativos) Entendemos, que se o sistema possui em média 10 ativos, o correto seria considerar a quantidade de alvos presente nesta licitação multiplicada por 10 (dez), totalizando 2.170 (alvos), para serem contabilizados na proposta de preços",

2.2. No que concerne ao teste de Invasão de Sistemas Web, para o correto dimensionamento dos custos, entendemos ser imprescindível que o CONTRATANTE informe a quantidade exata e/ou aproximada de URLs/Endpoints, visto que a respectiva quantidade reflete diretamente na composição das propostas.

2.3. Mister ressaltar, que em se tratando de Sistemas Web o total de URLs / Endpoints para cada aplicação pode variar, ou seja, uma aplicação pode ter 10 URLs ou possuir 100 URLs, aumentando, portanto, o esforço e, por consequência, os custos.

2.4. Assim, solicitamos que seja informada de forma clara e inequívoca, a quantidade de URLs/Endpoints para cada aplicação web (para que todos os licitantes estejam na mesma página), de modo a zelar pelos princípios basilares de toda e quaisquer contratações públicas, quais sejam: legalidade, isonomia, ampla concorrência etc.

2.5. Resposta: Não, o entendimento está incorreto. Informa-se que o Estudo Técnico Preliminar - ETP - é um documento orientador para justificar ou não uma aquisição pela Administração Pública Federal, a forma da aquisição; entre outros fatores. A estimativa de ativos que compõe um sistema foi utilizada de modo exemplificativo no Estudo Técnico Preliminar para estimar a complexidade e o universo associado a um teste de invasão que envolve análise de software (aplicações web) e hardware (servidores, equipamentos, máquinas de usuário, etc). No Termo de Referência, considerando os estudos realizados no ETP, foi possível diferenciar os testes de invasão em dois itens, sistemas WEB e infraestrutura, de tal modo que seja possível emitir uma Ordem de Serviço de teste de invasão apenas para hardwares, apenas para Sistema WEB ou mista envolvendo ambos os ativos. Dessa forma, é na Ordem de Serviço que constará o escopo, prazos e profundidade do teste. Assim, Na ordem de serviço constará se o teste deverá atingir apenas a aplicação como escopo, a aplicação com servidor que a hospeda, a aplicação com o servidor que a hospeda e mais movimentações laterais. Além disso, o Termo de Referência e o Edital são os documentos que irão reger o contrato, sendo assim, o licitante deverá se ater a quantidade máxima especificada. Portanto, a informação da quantidade de URLs é irrelevante frente ao limite que será imposto pela Ordem de Serviço, pois considera-se um sistema web como um alvo com todos os seus links internos, ou seja, os links internos da hierarquia da aplicação. Cada teste de invasão terá objetivo e escopo restritos aos definidos nas Ordens de Serviços emitidas. Assim, um teste de invasão em um equipamento como um firewall, por exemplo, será diferente de um teste de invasão em um sistema que tenha servidor de aplicações, de banco de dados, entre outros. Entende-se, dessa forma, que os dados contidos no Termo de Referência são suficientes para formação de preços.

2.6. Esclarecimento 2) Ainda sobre o teste de invasão de sistemas web, caso não seja informada a quantidade de URLs/Endpoints, correta/aproximada, de cada aplicação, entende-se que o ente publico poderá estar exposto a uma contratação que o onerará pois, ou será uma proposta deficitária com escopo subdimensionado ou acarretará em uma contratação sujeita a rescisão visto a possibilidade de desequilíbrio contratual ensejando a onerosidade excessiva.

2.7. Resposta: Entende-se que a resposta fornecida ao esclarecimento nº 08, SEI nº 16913155, é suficiente para dirimir quaisquer dúvidas acerca dos itens relacionados aos testes de invasão. O especificado no Termo de Referência atual foi dimensionado para as necessidades do Ministério. Ratifica-se que cada teste de invasão terá objetivo e escopo restritos aos definidos nas Ordens de Serviços emitidas.

Restitua-se o presente processo para continuidade do certame.

Atenciosamente,



Documento assinado eletronicamente por **Cintia Mye Yonekawa Yamaguti, Integrante Técnico(a)**, em 11/03/2022, às 12:28, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.



A autenticidade do documento pode ser conferida no site <http://sei.autentica.mj.gov.br> informando o código verificador **17433488** e o código CRC **4C427A4E**. O trâmite deste documento pode ser acompanhado pelo site <http://www.justica.gov.br/aceso-a-sistemas/protocolo> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.