



17000107



08006.000003/2021-38



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

RESPOSTA AO PEDIDO DE ESCLARECIMENTO 7 - CRS

1. Trata-se de resposta ao pedido de esclarecimento nº 07 (16924661) 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 (16833424).

2. No referido pedido de esclarecimento foram feitos 28 (vinte e oito) questionamentos. Abaixo seguem as respostas aos questionamentos.

2.1. **Esclarecimento 1** - No Termo de Referência, pág..26, item 3.4.2.7 - temos a seguinte redação “Idealmente estes times devem ser composto por profissionais de empresas diferentes, para que a equipe que venha a realizar os ataques, não tenha contribuído para a estratégia de defesa atualmente aplicada pela outra equipe, pois isto poderia gerar um conflito de interesses em relação aos testes, a partir da atitude de não querer buscar realmente, ou mesmo expor, as fraquezas disponíveis na infraestrutura da corporação, e que não tenham sido cobertas pelas defesas que ajudaram a implantar. Dificultando até possíveis futuras auditorias. Nesse sentido, a empresa licitante vencedora do grupo 1 está automaticamente impedida de se tornar vencedora do grupo 2 e a vencedora do grupo 2 não poderá ser a vencedora do grupo 1.” Nosso entendimento é que as proponentes licitantes, desde que possuam capacitação técnica para tal, poderão oferecer propostas e participar na fase de lances tanto no grupo 1 quanto no grupo 2. Entretanto, se uma das proponentes licitantes em um dos grupos, seja 1 ou 2, for homologada como vencedora de um dos grupos, 1 ou 2, será, de ofício, declarada como impedida de ser declarada vencedora no outro grupo, tendo sua proposta desclassificada e descartada pelo pregoeiro para fins de julgamento daquele outro grupo para qual está inelegível de participar. Está correto nosso entendimento?

2.2. Resposta: Sim, o entendimento está correto. As proponentes licitantes, desde que possuam capacitação técnica para tal, poderão oferecer propostas e participar nas fase de lance tanto no grupo 1 quanto no grupo 2. Caso a licitante, após a fase de lances, fique classificada em primeiro para os dois grupos, será analisada a documentação referente ao Grupo 1, seguindo a ordem indicada nos itens 3.4.2.7.1 e 3.4.2.7.2. Caso a proposta e habilitação estejam de acordo com o TR, a empresa será aceita para o Grupo 1 e, conseqüentemente, desclassificada para o Grupo 2.

2.3. **Esclarecimento 2** - No Termo de Referência, pág.23, item 3.1.13- temos a seguinte redação “Em contrapartida um Network Operations Center - NOC, Centro de Operações de Rede em tradução direta, é uma estrutura que funciona também de forma ininterrupta como um SOC, porém com foco somente na disponibilidade. Um SOC e um NOC não se confundem em suas atribuições, apesar de algumas vezes terem que operar em paralelo.”. Nosso entendimento é que será útil aos proponentes licitantes conhecerem se há um contrato de prestação de serviços de NOC em curso, qual a duração do mesmo, a data de encerramento do mesmo e o nome/razão social da empresa prestadora dos serviços de NOC ao MJSP. Está correto nosso entendimento (obs: caso positivo, explicitar a duração do mesmo, a data de encerramento do mesmo e o nome/razão social da empresa prestadora dos serviços de NOC ao MJSP)?

2.4. Resposta: A CONTRATANTE possui contrato de NOC, conforme o Segundo Termo Aditivo ao Contrato 40/2019. Entretanto, entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

2.5. **Esclarecimento 3** - No termo de Referência, pág.26-27, item 3.4.3.4 - temos a seguinte redação no trecho final do item. “...com consequente aumento dos valores contratados em comparação à compra agrupada dos itens, considerando que o item 4 por ser um serviço de baixa complexidade tende a ter um valor menor para sua execução.”. De igual forma, na pág.43 do termo de Referência, itens 4.12.13.4.1. e 4.12.13.4.2 temos todo um rol de certificações e experiência que serão exigidas dos profissionais responsáveis pela execução dos serviços de Testes de Invasão - Red Team (itens 3 e 4 do Grupo 2). Também na pág.28 do termo de Referência, item 4.1.8.3, temos que os serviços de Red Team devem seguir padrões e frameworks internacionais como OSSTMM 3, ISSAF/PTF, NIST SP 800- 115 e 800-42 e OWASP TB 4.1. Nosso entendimento é que; apesar da correta observação quanto ao item 4(Grupo 2) ser um item de serviço de baixa complexidade tendendo a ter um valor menor para sua execução; a cotação de preço e nível de serviço esperado para este item não devem ser considerados pelas proponentes licitantes como item de execução de baixo custo e baixa complexidade de execução funcional, sendo vedada a prestação destes serviços por meio de ferramentas automatizadas e genéricas de pentest, com geração de relatórios superficiais quanto ao teste de intrusão realizado, com análise gerais e diagnósticos imprecisos descritos em idioma que não seja o português; devendo os proponentes licitantes entregar nível serviço de excelência à altura das especificações do termo de referência e executados por profissionais com os requisitos descritos nos itens 4.12.13.4.1. e 4.12.13.4.2.. Está correto nosso entendimento?

2.6. Resposta: Sim, o entendimento está correto.

2.7. **Esclarecimento 4** - Na pág.29, o item 4.1.9.5.8 - temos a seguinte redação “A Ordem de Serviço estabelecerá o prazo para execução por ativo de serviços de teste de invasão - Red Team: infraestrutura, o qual não será inferior a 1 dia nem ultrapassará 1 semana.”. Nosso entendimento é que haverá prejuízo da segurança da informação desejada caso sejam realizados testes isolados por ativo de infraestrutura; entendimento fundamentado, inclusive, nos frameworks indicados na pág.28 - OSSTMM, por exemplo, busca obter uma métrica para a superfície de ataque. Nosso entendimento é que não há no edital cláusula impeditiva quanto a realização de testes concomitantes em múltiplos ativos. Adicionalmente, considerando as melhores práticas descritas nos

frameworks de referência, nosso entendimento é que haverá agrupamento e concomitância de testes nos ativos de infraestrutura, de acordo com a topologia de rede dos ativos da CONTRATANTE, visando a melhor e mais completa execução dos testes de invasão. Está correto nosso entendimento?

2.8. Resposta: Não, o entendimento está incorreto. A critério da contratante poderá ser realizado o serviço de teste de invasão em um ou mais ativos conforme especificado na Ordem de Serviço. Não há no edital cláusula impeditiva quanto a realização de testes concomitantes em múltiplos ativos.

2.9. **Esclarecimento 5** - No termo de Referência, pág.29, item 4.1.9.6 - temos a seguinte redação “ A(s) CONTRATADA(s) deverá(ão) disponibilizar ferramenta de ITSM (Information Technology Service Management) para registro, acompanhamento e controle dos Incidentes e Requisições de Segurança e gerir todo o ciclo de vida dos chamados de SOC e BLUE TEAM, como também para os chamados de RED TEAM. Ao final do contrato, as bases de dados das ferramentas utilizadas, com todos os dados, inclusive históricos das demandas, solicitações, atendimentos e demais informações relativas à prestação de serviços deverão ser entregues e permanecerão sob a custódia exclusiva do Ministério.”. Nosso entendimento é que será útil aos proponentes licitantes conhecerem se o MJSP/DTIC/CRS já faz uso de alguma ferramenta de ITSM em outros serviços (exemplo: utilizada no NOC ou Service Desk). Está correto nosso entendimento? (obs: caso positivo, explicitar o nome, versão, fabricante, tipo de licenciamento, quantidade de licenças em uso atualmente)

2.10. Resposta: Não, o entendimento está incorreto. Conforme o item citado "A(s) CONTRATADA(s) deverá(ão) disponibilizar ferramenta de ITSM (Information Technology Service Management)". A empresa de NOC possui ITSM próprio que não deverá ser utilizado pelo SOC. O item 4.1.9.6 foi alterado conforme Termo de Referência atualizado.

2.11. **Esclarecimento 6** - No item 4.1.14.1 - temos a seguinte redação "... o SOC funcionará 24 horas por dia e 7 dias por semana, tendo por objetivo sustentar e operar a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério da Justiça e Segurança pública, bem como...". Entendemos que a Plataforma de SIEM/SOAR/NTA/UEBA/CT já existe como contratada no MJSP, incluindo as licenças necessárias, já instaladas e inicialmente configuradas no ambiente tecnológico do MJSP. Adicionalmente, nosso entendimento é que esta plataforma de SIEM/SOAR/NTA/UEBA/CT é, atualmente, gerenciada em sua sustentação e funcionamento pelo time do NOC /infraestrutura. Concluído, nosso entendimento é que nos primeiros 60(sessenta) dias do novo contrato resultante deste certame, a proponente licitante vencedora do Grupo 1 (Blue Team - SOC + CSIRT) terá a oportunidade de fazer um acompanhamento de transferência (handover) da operação atual para a nova operação. Está correto nosso entendimento?

2.12. Resposta: Não, o entendimento está incorreto. A Plataforma de SIEM/SOAR/NTA/UEBA/CT já existe como contratada no MJSP, já se encontra instalada e em funcionamento. Entretanto, caberá à CONTRATADA realizar, durante a vigência contratual do presente objeto, as parametrizações, customizações e manutenções da plataforma para fornecer todos os serviços relacionados à supracitada Plataforma objeto da presente contratação.

2.13. **Esclarecimento 7** - No item 1.1 - objeto deste certame, temos a seguinte redação “serviços de tecnologia da informação e comunicação, através da seleção 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 e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses “. Nosso entendimento é que o presente edital tem o objetivo de contratar serviços especializados para tal objeto, divididos em duas especializações distintas (Grupo 1 Blue Team/CSIRT & Grupo 2 Red Team), com operação via profissionais especializados na forma remota (SOC da Contratada) ou presencial (instalações do MJSP, em Brasília), sem a necessidade de exclusividade ou dedicação exclusividade de tais profissionais. Assim, nosso entendimento é que os profissionais

especializados da contratada alocados para o projeto com o MJSP poderão ser também alocados em outras demandas já existentes na contratada. Está correto nosso entendimento?

2.14. Resposta: Sim, o entendimento está correto. Não será exigido mão de obra com dedicação exclusiva, mas a prestação dentro dos níveis mínimos de serviços exigidos. Dessa forma, caberá a contratada avaliar se para cumprir os níveis mínimos de serviço será necessário a prestação de serviço de forma remota, presencial ou mista e as circunstâncias necessárias para o envio de recurso especializado para prestar serviços presencialmente. Conforme Tabela 8 do Termo de Referência.

2.15. **Esclarecimento 8** - No item 1.1 - objeto deste certame, temos a seguinte redação “serviços de tecnologia da informação e comunicação, através da seleção 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 e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses “. Nosso entendimento é que o presente edital tem o objetivo de contratar serviços especializados, com atuação majoritariamente remota (sempre que possível) e, em casos pontuais nos quais não houver a possibilidade de execução remota, será requerida uma atuação presencial nas instalações do MJSP/DTIC/CRS (Esplanada dos Ministérios, Palácio da Justiça, Bloco T, Edifício sede – CEP: 70064900). Está correto nosso entendimento?

2.16. Resposta: Não será exigido mão de obra com dedicação exclusiva, mas a prestação dentro dos níveis mínimos de serviços exigidos. Dessa forma, caberá a CONTRATADA avaliar se para cumprir os níveis mínimos de serviço será necessário a prestação de serviço de forma remota, presencial ou mista e as circunstâncias necessárias para o envio de recurso especializado para prestar serviços presencialmente. Conforme Tabela 8 do Termo de Referência.

2.17. **Esclarecimento 9** - No item 1.1 - objeto deste certame, temos a seguinte redação “serviços de tecnologia da informação e comunicação, através da seleção 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 e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses “. Nosso entendimento é que o presente edital tem o objetivo de contratar serviços especializados; logo, não considera a obrigatoriedade de precificação e transferência de propriedade de qualquer tipo de software ou hardware licenciado por parte da contratada, uma vez que serão utilizadas as ferramentas, softwares e hardwares já existentes na infraestrutura tecnológica do MSJP/DTIC/CRS. Está correto nosso entendimento?

2.18. Resposta: O edital do pregão eletrônico nº 21/2021 e anexos tem por objetivo a contratação de serviços de segurança da informação, mas também prevê no item 4.1.14.1.12, que caso as ferramentas de propriedade do Ministério não atendam a completa execução dos serviços objeto da presente contratação a contratada poderá adotar solução tecnológica complementar em termos de hardware e software. No entanto, no referido edital e anexos não considera a obrigatoriedade de precificação e transferência de propriedade de qualquer tipo de software ou hardware licenciado por parte da contratada.

2.19. **Esclarecimento 10** - No termo de Referência, item 4.1.14.1.5 - temos a seguinte redação "Atuar no sentido de interromper um incidente quando da inoperância do NOC ou suporte N1, N2 e N3. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC não esteja disponível ou não possa atuar, serão definidos protocolos para atuação da equipe de SOC e Blue Team." Nosso entendimento é que já existe previsão no contrato atual com a prestadora de serviço do NOC / infraestrutura de níveis de serviço SLAs na operação. Entendemos também que o objetivo do item supracitado é provocar redundância no processo e aumentar a sua resiliência. Entretanto, nosso entendimento é que as atuações da prestadora de serviços de SOC-Blue Team/CSIRT (Grupo 1) e a operadora de serviços de NOC tendem a gerar área de sobreposição de atuação; podendo incorrer em aplicações de penalidades (glosas / multas) que são diretamente relacionados a esse "backup de operação" pretendido pelo item supracitado. Está correto nosso entendimento? (obs: caso positivo, esclarecer como pode ser evitada tal sobreposição de responsabilidades antevistas com a aplicação do item supracitado.)

2.20. Resposta: Não, o entendimento está incorreto. Não haverá sobreposição de responsabilidades entre CONTRATADAS. Conforme Termo de Referência atualizado em que consta no item "4.1.14.5 Atuar no sentido de interromper um incidente quando a equipe do NOC ou suporte N1, N2 e N3 estiver limitada contratualmente ou em sua capacidade operacional. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC não esteja disponível ou não possa atuar, serão definidos protocolos para atuação da equipe de SOC e Blue Team.", o SOC atuará nessas circunstâncias em casos excepcionais durante incidentes, quando definidos os protocolos de atuação pela Contratante.

2.21. **Esclarecimento 11** - No termo de Referência, item 4.1.14.1.5 - temos a seguinte redação "Atuar no sentido de interromper um incidente quando da inoperância do NOC ou suporte N1, N2 e N3. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC não esteja disponível ou não possa atuar, serão definidos protocolos para atuação da equipe de SOC e Blue Team.". Nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem o índice/métrica em ocorrências de indisponibilidade do time NOC ou suporte N1, N2, N3 (contrato atual) ocorrido nos últimos 12 meses. Está correto nosso entendimento? (obs: caso positivo, solicita-se informar o índice/métrica em ocorrências de indisponibilidade do time NOC ou suporte N1, N2, N3 do contrato atual de serviços NOC ocorrido nos últimos 12 meses.)

2.22. Resposta: Não, o entendimento está incorreto. Conforme Termo de Referência atualizado em que consta no item "4.1.14.5 Atuar no sentido de interromper um incidente quando a equipe do NOC ou suporte N1, N2 e N3 estiver limitada contratualmente ou em sua capacidade operacional. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC não esteja disponível ou não possa atuar, serão definidos protocolos para atuação da equipe de SOC e Blue Team.", o SOC atuará nessas circunstâncias em casos de excepcionais durante incidentes, quando definidos os protocolos de atuação pela Contratante.

2.23. **Esclarecimento 12** - No termo de Referência, item 4.1.14.1.6 - temos a seguinte redação "Outros serviços os quais o SOC atuará em substituição ao NOC, poderão ser definidos durante a vigência do contrato, por meio de reuniões entre a CONTRATANTE e a CONTRATADA". Nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem as obrigatoriedades contratuais atualmente existentes com o prestador de serviço atual, incluindo SLAs que PODEM ser transferidos para contrato Grupo 1 (SOC + CSIRT). Está correto nosso entendimento? (obs: caso positivo, para correta dimensão e precificação das proponentes licitantes em suas propostas para o Grupo 1, solicita-se informar em quais o SOC atuará em substituição ao NOC.)

2.24. Resposta: Não, o entendimento está incorreto. Não haverá transferência de SLAs do contrato do NOC para o contrato do SOC, Grupo 1, devendo a CONTRATADA observar os Níveis de Serviço que constam no Termo de Referência do presente certame. Conforme Termo de Referência atualizado em que consta no item "4.1.14.6 Outros serviços os quais o SOC atuará em substituição ao NOC, não definidos inicialmente nos protocolos do item anterior, poderão ser definidos durante a vigência do contrato, por meio de reuniões entre a CONTRATANTE e a CONTRATADA.", o SOC atuará nessas circunstâncias em casos excepcionais durante incidentes, quando definidos os protocolos de atuação pela Contratante.

2.25. **Esclarecimento 13** - No termo de Referência, item 10.1.1 - temos a seguinte redação "ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal." Nosso entendimento é que a assinatura e as rubricas físicas sobre papel podem ser substituídas por uma assinatura digital ICP-Brasil, nos termos da LEI Nº 14.063, DE 23 DE SETEMBRO DE 2020. Está correto nosso entendimento?

2.26. Resposta: Sim, o entendimento está correto. Pode ser aceita assinatura digital.

2.27. **Esclarecimento 14** - Em referência ao item 4.3.2.3 do Termo de Referência - em face das exigências do DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012, bem como da IN GSI/PR NO 2, DE 5 DE FEVEREIRO DE 2013, nosso entendimento é que, em relação à tempestividade, o "Termo de Compromisso" constante no Anexo I-F deverá ser assinado no momento da contratação, pela contratada. Está correto nosso entendimento?

2.28. Resposta: Não, o entendimento está incorreto. Conforme Termo de Referência, o Termo de Compromisso será entregue na Reunião Inicial, conforme item 6.1.1.6.3.

2.29. **Esclarecimento 15** - Em referência ao item 4.3.2.3 do Termo de Referência - em face das exigências do DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012, bem como da IN GSI/PR NO 2, DE 5 DE FEVEREIRO DE 2013, nosso entendimento é que, em relação à tempestividade, o "TCMS" do Anexo I do DECRETO Nº 7.845 deve ser assinado pelos prestadores de serviços da contratada, antes do engajamento dos referidos colaboradores nas atividades contratuais. Está correto nosso entendimento?

2.30. Resposta: Não, o entendimento está incorreto. Ver esclarecimento 14.

2.31. **Esclarecimento 16** - No item 3.1.16 do Termo de Referência - são apresentados alguns quantitativos na "Tabela 3". Nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem quais os tipos de "Sistemas" quanto à tecnologia e origem (prateleira vs proprietários do MJSP, web vs aplicações tradicionais, etc). Está correto nosso entendimento? (obs: caso positivo, explicitar as características de tecnologia e origem de tais componentes de sistemas.)

2.32. Resposta: Não, o entendimento está incorreto. Entende-se que os dados contidos no termo de referência são suficientes para formação de preço. Demais esclarecimentos poderão ser obtidos na vistoria, conforme item 4.16.1. Requisitos de Vistoria do Termo de Referência.

2.33. **Esclarecimento 17** - No item 3.1.16 do Termo de Referência - são apresentados alguns quantitativos na "Tabela 3". Nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem quais as tecnologias de nuvem, qual o número de servidores/serviços instanciados em cada provedor. Está correto nosso entendimento? (obs: caso positivo, explicitar as tecnologias de nuvem, qual o número de servidores/serviços instanciados em cada provedor.)

2.34. Resposta: Não, o entendimento está incorreto. Entende-se que os dados contidos no termo de referência são suficientes para formação de preço. Demais esclarecimentos poderão ser obtidos na vistoria, conforme item 4.16.1. Requisitos de Vistoria do Termo de Referência.

2.35. **Esclarecimento 18** - No termo de referência, considerado o diagrama da figura do item 4.1.7 - aliada à justificativa exposta no item 3.4.2.7, nosso entendimento é que a atual contratada do MJSP que opera, nos termos da "Figura 4"/TR, as funções de "Suporte N1, N2 e N3" e "NOC" está impedida de participar como proponente licitante do certame; já que atua como responsável pela infraestrutura e coleta de chamados; em posição de conflito de interesses funcional frente às atividades que serão demandas a contratada, seja para oferecer proposta para o Grupo 1 (SOC Blue Team/CSIRT) e também para o Grupo 2 (Red Team – Testes de Invasão). Está correto nosso entendimento? (obs: Na hipótese do entendimento não estar correto, consignamos desde já solicitação para que o item 3.4.2.7 do Termo de Referência seja derogado; em observância ao princípio da isonomia entre proponentes licitantes, bem como do princípio do venire contra factum proprium, que veda o comportamento contraditório da Administração Pública.)

Resposta: Não, o entendimento está incorreto. No Termo de Referência atualizado não há restrição quanto a participação da empresa responsável pela infraestrutura no certame em questão para o grupo 1. Com relação ao grupo 2 verificou-se que há conflito de interesses, por isso, foi inserido o item "3.4.5 Justificativa para impedimento da empresa responsável pelo serviço de *service desk* e sustentação de infraestrutura de TI".

2.36. **Esclarecimento 19** - No termo de referência, item 4.1.9.13 - temos a seguinte redação "A CONTRATADA ficará, durante a vigência contratual do presente objeto, incumbida de realizar parametrizações, customizações e manutenções na Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Atualmente, a ferramenta implantada e em utilização, é a Azure Sentinel da fabricante Microsoft. Caso o Ministério opte por outra solução a mesma deverá ser absorvida pela CONTRATADA sem ônus para a CONTRATANTE.". Nosso entendimento é que, em caso em que a proponente licitante resolva utilizar "outra solução" que não a plataforma Azure Sentinel atualmente contratada pelo MJSP, entendemos que a licitante deverá mandatoriamente detalhar a plataforma alternativa (de SIEM/SOAR/NTA/ UEBA/CTI, com modelo de licenciamento, se a instalação é do tipo em nuvem ou on-premise) a ser utilizada no momento da apresentação da proposta ajustada (item 7.28.4) para fins de avaliação da aceitabilidade da proposta vencedora, nos termos do item 8.2.1 (previsão do item 9.1 do Anexo VII-A da In SEGES/MP n. 5/2017). Está correto nosso entendimento?

2.37. Resposta: Não, o entendimento está incorreto. O item 7.28.4 e o item 8.2.1 do Edital referem-se ao valor da proposta relativa ao pregão.

2.38. **Esclarecimento 20** - No termo de referência, item 4.1.14.10.1.11 - temos a seguinte redação "Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.". Nosso entendimento é que a proponente licitante deverá comprovar conformidade com a norma no momento da contratação. Está correto nosso entendimento? (obs: caso negativo, explicitar em qual momento deverá a proponente licitante demonstrar a conformidade com a Norma.)

- 2.39. Resposta: Não, o entendimento está incorreto. A comprovação deverá atender aos prazos definidos no item 7.3.2 e subitens do termo de referência ou a qualquer momento por solicitação da equipe de fiscalização, após a contratação.
- 2.40. **Esclarecimento 21** - No termo de referência, item 4.1.14.10.1.11 - temos a seguinte redação “Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.”. Nosso entendimento é que não será aceita comprovação de conformidade sem a apresentação de certificado válido dentro do ano da contratação; devendo a contratada manter tal certificado válido durante todo o período de vigência do contrato. Está correto nosso entendimento?
- 2.41. Resposta: Não, o entendimento está incorreto. O presente item não exige certificação e sim a comprovação de processos implementados que garantam a segurança das informações do CONTRATANTE para os controles aplicáveis da norma ABNT NBR ISO/IEC 27001.
- 2.42. **Esclarecimento 22** - No termo de referência, item 4.1.14.10.1.11 - temos a seguinte redação “Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.”. Nosso entendimento é que os processos, documentações, artefatos exigidos pela referida norma devem estar 100% implantados e 100% em utilização pela proponente licitante e serem comprovados durante a fase de contratação do certame. Está correto nosso entendimento?
- 2.43. Resposta: Não, o entendimento está incorreto. Tal requisito será avaliado somente após a contratação da licitante vencedora.
- 2.44. **Esclarecimento 23** - No termo de referência, item 4.1.14.10.1.11 - temos a seguinte redação “Deverá possuir processos implementados que garantam a segurança das informações do CONTRATANTE, em conformidade com a norma ABNT NBR ISO/IEC 27001.”. Nosso entendimento é que a proponente licitante deverá comprovar conformidade com a norma no momento da contratação. Caso não o faça nesta fase, não atendendo ao item referido do edital, nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem qual será o método de verificação utilizado pelo MJSP caso a vencedora não possua a certificação válida. Está correto nosso entendimento?
- 2.45. Resposta: Não, o entendimento está incorreto. A comprovação de conformidade com a norma será realizada de acordo com os prazos fixados no item 7.3.2 e subitens, após a assinatura do contrato. Cabe a contratada a comprovação de que seus processos estão em conformidade com a norma ABNT NBR ISO/IEC 27001. A certificação ISO 27001, por exemplo, pode ser um modo de comprovação.
- 2.46. **Esclarecimento 24** - No termo de referência, item 4.4.1 - temos a seguinte redação “Caso seja necessário substituir licenças equivalentes durante a vigência do Contrato, isso deverá ocorrer sem qualquer ônus para o Ministério da Justiça e Segurança Pública.”. Nosso entendimento é que a responsabilidade pelas renovações(upgrades) de licenças atualmente usadas pelo MJSP permanece sendo do próprio Ministério e que à contratada cabe os ônus aplicados somente às eventuais licenças adicionais necessárias para fins de atendimento de escopo dos serviços prestados durante a vigência do contrato. Está correto nosso entendimento? (obs: em caso negativo, seria relevante para as proponentes licitantes do certame conhecerem o nome, tipo, fabricante, versão das licenças atualmente usadas pelo Ministério, incluindo informações de volumetria e datas de expiração das mesmas.)

- 2.47. Resposta: Sim, o entendimento está correto. Porém, como o item 4.4.1 estava gerando dúvidas e foi removido do Termo de Referência atualizado, no entanto, o entendimento permanece correto.
- 2.48. **Esclarecimento 25** - No termo de referência, item 4.9.1 - temos a seguinte redação "A CONTRATADA deverá disponibilizar ao Ministério da Justiça e Segurança Pública documentação onde constem as especificações técnicas detalhadas dos produtos ofertados.". No item 1.1, objeto deste certame, temos a seguinte redação "...serviços de tecnologia da informação e comunicação, através da seleção 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 e garantia dos serviços pelo período de 24(vinte e quatro) meses, renováveis até o limite de 60 (sessenta) meses. ". Nosso entendimento é que o objeto da contratação deste certame deixa claro que o que se pretende é estritamente a contratação serviços especializados de cibersegurança (serviços, puramente), para ambos os grupos (1 e 2). Nosso entendimento é que seria relevante para as proponentes licitantes do certame explicitar e esclarecer do que se trata o requerimento de disponibilização de "documentação onde constem as especificações técnicas detalhadas dos produtos ofertados." a que se refere o item 4.9.1 do edital. Está correto nosso entendimento?
- 2.49. Resposta: Sim, o entendimento está correto. A contratação é para o fornecimento de serviços de segurança da informação. O item 4.9.1 foi alterado conforme Termo de Referência atualizado.
- 2.50. **Esclarecimento 26** - No termo de referência, item 4.9.1 - temos a seguinte redação "A CONTRATADA deverá disponibilizar ao Ministério da Justiça e Segurança Pública documentação onde constem as especificações técnicas detalhadas dos produtos ofertados.". Uma vez que seja esclarecido o entendimento anterior (26), nosso entendimento é que a documentação onde constam as especificações técnicas requeridas no item 4.9.1 deverão ser fornecidas pela proponente licitante provisoriamente vencedora(arrematante) no momento de apresentação da proposta ajustada para fins de avaliação da aceitabilidade da proposta (item 8.2.1). Está correto nosso entendimento? (obs: caso seja negativo este entendimento, seria relevante para as proponentes licitantes do certame conhecerem em que fase do certame tal documentação onde constem as especificações técnicas detalhadas dos produtos ofertados deve ser apresentada.)
- 2.51. Resposta: Não, o entendimento está incorreto. O item 4.9.1 foi alterado conforme Termo de Referência atualizado. Em relação ao prazo para entrega dos documentos Plano de Implantação dos Serviços e Cronograma Detalhado, verificar o item na seção Deveres e Responsabilidades da Contratada.
- 2.52. **Esclarecimento 27** - No termo de referência, item 4.1.9.13 -temos a seguinte redação "A CONTRATADA ficará, durante a vigência contratual do presente objeto, incumbida de realizar parametrizações, customizações e manutenções na Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Atualmente, a ferramenta implantada e em utilização, é a Azure Sentinel da fabricante Microsoft. Caso o Ministério opte por outra solução a mesma deverá ser absorvida pela CONTRATADA sem ônus para a CONTRATANTE. ". Nosso entendimento é que se trata apenas de instalar e passar a operar a plataforma e não de ser a responsável pelo licenciamento e renovação/atualizações da referida. Nosso entendimento é que seria relevante para as proponentes licitantes do certame explicitar o que o MJSP define por "absorver" a nova plataforma escolhida pelo Ministério. Está correto nosso entendimento?

2.53. Resposta: Sim, o entendimento está correto. Caso a CONTRATANTE, na vigência do contrato, implante outra plataforma de SIEM/SOAR/NTA/UEBA/CTI, a CONTRATADA deverá realizar as parametrizações, customizações e manutenções necessárias para a consecução dos serviços, objeto da presente contratação.

2.54. **Esclarecimento 28** - No termo de referência, item 4.1.14.1.9 - temos a seguinte redação “Configuração, manutenção, monitoramento e operação da Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério.”. Nosso entendimento é que seria relevante para as proponentes licitantes do certame explicitar se a referida plataforma e todos os seus componentes (SIEM/SOAR/NTA/UEBA/CTI) já encontram em plena operação, 100% instalada e 100% configurada no ambiente do MJSP; ou se a mesma ainda não se encontra em operação, de modo que as funções de “Configuração, manutenção, monitoramento e operação da Plataforma” deverão ser executadas “a partir do zero” como parte integrante dos serviços demandados à contratada durante a vigência do contrato. Está correto nosso entendimento?

2.55. Resposta: A solução se encontra instalada e em operação. Entretanto, entende-se que os dados contidos no termo de referência são suficientes para formação de preços e maiores informações poderão ser fornecidas na vistoria, conforme seção Requisitos de Vistoria.

3. Restitua-se o presente processo para continuidade do certame.

Atenciosamente,



Documento assinado eletronicamente por **IVANILDO DE OLIVEIRA DA SILVA JUNIOR, Integrante Requisitante**, em 10/02/2022, às 20:05, 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 **17000107** e o código CRC **08FCD781**. O trâmite deste documento pode ser acompanhado pelo site <http://www.justica.gov.br/acesso-a-sistemas/protocolo> e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.