16996536 08006.000003/2021-38

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

RESPOSTA AO PEDIDO DE ESCLARECIMENTO 6 - CRS

1. Trata-se de resposta ao DESPACHO Nº 7/2022/DILIC/COPLI/CGL/SAA/SE (16915681), por meio do qual o Pregoeiro versa sobre o pedido de esclarecimento nº 06 (16915542 e 16915567) 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 36 (trinta e seis) questionamentos, todos de ordem técnica. Seguem as respostas aos questionamentos.

3. Nas tabelas abaixo seguem os esclarecimentos encaminhados via planilha em excel (16915567).

| Esclarecimento | Item | Questionamentos Cipher / Grupo 1 item 1 |
|---|---|---|
| 1 | 3.1.16 Tabela 3 | Poderia nos fornecer maiores detalhes sobre a técnologias/ativos utilizados pelo Ministério da Justiça e Segurança Pública (Quantidade, tipo de ativos, marca, modelo, fabricante) ? |
| 2 | 3.1.16 Tabela 3 | Dos 728 equipamentos e tecnologias do MJSP citados, quantos estão integrados e enviando logs para o Sentinel? Poderiam compartilhar maiores informações das integrações ativas? |
| 3 | 2.2.2 | No corpo deste TR diz que o dimensionamento da equipe para os serviços objeto deste edital é responsabilidade da contratada, entendemos que tal equipe pode pertencer ao pool de analistas do SOC da contratada, sendo assim não é requirido ser uma equipe dedicada ao Ministerio da Justiça. A exigencia é atrelada ao atendimento do escopo e não uma equipe exclusiva. Está correto o entendimento? |
| 4 | 4.1.14.1.5 | Entendemos que o time técnico da contratada não possui as capacidades necessárias para substituir a atuação dos times de gestão de infra e/ou apps da contratante ou de terceiros, sendo portanto imprescindível a atuação conjunta destes em situações de crise, ainda que afetados por indisponibilidade do ambiente, sem prejuíso ao escopo claro e definido de atuação de todas as partes envolvidas. Tal entendimento está correto? |
| 5 | 4.1.14.1.12 | Neste item entendemos que a contratante se obriga e se compromete a manter licenciamento, hardware, software e o respectivo suporte dos fabricantes adequadamente dimensionados para o seu parque de assets durante todo o tempo de vigência do contrato objeto deste edital. Tal entendimento está correto? |
| 6 | 4.1.14.2.15 | Por gentileza, qual é o volume histórico de melhorias solicitadas pela contratante mensalmente? Entendemos que melhorias complexas darão origem à um projeto fora do escopo de prestação de serviços especificados neste edital, correto? |
| 7 | 4.1.14.2.18 | É solicitado que seja mantido atualizado o CMDB da contratante, qual é a ferramenta atual utlizada? A contratante permitirá a integração automatizada de seu CMDB com a plataforma de gestão da contratada? |
| 8 | 4.1.14.2.25 | Por "instalar e customizar" entendemos que os termos mais adequados seriam "operar e configurar" os softwares listados como objeto deste edital, correto? Uma vez que já se encontram instalados, e customização de software envolveria edição de código fonte. |
| 9 | 4.1.14.2.45 | Entendemos que a única solução que será adminstrada pela contratada é o sentinel SIEM/SOAR/NTA/UEBA/CTI. Está correto nosso entendimento? Todas os tipos das soluções são da marca Microsoft Sentinal. Está correto entendimento. |
| 10 | 4.1.14.2.36 | Entendemos que a participação da contratante em projetos se limita ao escopo de suporte dos ambientes listados neste edital (sentinel SIEM/SOAR/NTA/UEBA/CTI), e desde que não causem prejuíso ou sobrecarga ao atendimento/suporte operacional, correto? |
| 11 | 4.1.14.2.44 | No item é solicitado a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Entedemos que este item está limitado a planforma SIEM/SOAR/NTA/UEBA/CTI do Ministério e não aos ativos que enviam logs ao SOC, está correto nosso entendimento? |
| 12 | 4.1.14.2.39. | Entendemos que a participação da contratante em projetos se limita ao escopo de suporte dos ambientes listados neste edital (* listar ferramentas *), e desde que não causem prejuíso ou sobrecarga ao atendimento/suporte operacional, correto? |
| 13 | 4.1.14.2.43 | A contratante possui mapeamento de processos? Se sim, o mesmo pode ser compartilhado? |
| 14 | 4.1.14.2.43 | A contratante já tem uma visão clara do escopo para o GCN? Será o mesmo escopo contemplado no trabalho anterior com inclusão dos processos que sofreram alterações e novos processos? |
| 15 | 4.1.14.2.43 | A contratante possui organograma atualizado das áreas de negócios e tecnológicas? Se sim, podem compartilhar? |
| 16 | 4.1.14.2.43 | Quantas unidades de negócios (físicas – prédios) serão contempladas neste projeto? |
| 17 | 4.1.14.2.43 | Existem unidades de Data Center nesses prédios? Eles serão escopo do projeto? Se sim, quantos DC´s? |

| | | |
|---|---|---|
| 18 | 4.1.14.2.43 | Existe alguma estratégia de GCN já definida? Se sim, quais? |
| 19 | 4.1.14.2.43 | A contratante possui Política de Continuidade de Negócios estabelecida? |
| 20 | 4.1.14.2.43 | A contratante possui metodologia de GCN estabelecida? Se não, gostariam da elaboração dela neste projeto? |
| 21 | 4.1.15.15 e 4.1.15.16 | Para Itens 4.1.15.15 e 4.1.15.16 = scans de vulnerabilidade + relatorios<br><br>Será permitida a instalação de sensores na rede do cliente para efetuarmos os scans de vulnerabilidades ? |
| 22 | 3.4.2.7 | Mediante item 3.4.2.7 (pg. 26) do Termo de Referência, entendemos que a proponente não poderá ser habilitada nos dois grupos. Está correto o entendimento? |
| 23 | | Sobre a prestação dos serviços, entendemos que a equipe ficará nas instalações da proponente. Está correto o entendimento? |
| 24 | 8 (pg.56) | Sobre o orçamento disponivel para a contratação, entendemos que os valores máximos são os listados na tabela pg. 56. Está correto o entendimento? |

| Esclarecimento | Item | Questionamentos Cipher / Grupo 1 item 2 |
|---|---|---|
| 25 | 4.1.15.2.1 | Além de utilizarmos como base para análise do Framework NIST, podemos utilizar também o padrão base do CIS 8? |
| 26 | 4.1.15.2 | Entendemos que a execução da atividade de Assessment de Maturidade (Gap Analysys) pode ser realizada de forma remota, com reuniões no Teams ou outras plataformas de comunicação. Nosso entendimento e |
| 27 | 4.1.15.2 | Quais e quantas são as áreas do MJSP? Citar qualquer área que possa ter (mesmo que ainda não sabido) acesso a qualquer informação da empresa, mesmo que só usuário no domínio. |
| 28 | 4.1.15.2 | Há terceiros que acessam o ambiente computacional ou ambientes críticos do MJSP? Informar quantidades e em quais situações.<br>O MJSP tem uma equipe capaz de implementar e manter um SGSI de acordo com os requisitos da ISO 27001? |
| 29 | 4.1.15.2 | Há um time interno dedicado à Segurança da Informação? |
| 30 | 4.1.15.2 | Um Assessment de Maturidade já foi efetuado anteriormente? Quando foi?Há outros processos de conformidade de Segurança da Informação em curso? Se sim citar quais. |
| 31 | 4.1.15.2 | O MJSP é aderente a alguma norma ou certificação de segurança? Como ISO 27001, PCI DSS, outras? Se sim citar quais e ano da última certificação. O MJSP é cobrado de atender alguma regulamentação, como<br>Se sim citar quais |
| 32 | 4.1.15.2 | Empresa possui todas as políticas e padrões do SGSI, como políticas de segurança da informação, classificação das informações, gerenciamento de acesso, resposta a incidentes, etc.? |
| 33 | 4.1.15.2 | A empresa tem controle sobre a existência, utilização e criação de credenciais privilegiadas? Leia-se por credenciais privilegiadas aquelas que permitem acessos a sistemas críticos para o negócio do MJSP, bem c<br>do ambiente de TI. |
| 34 | 4.1.15.15 | Neste item é solicitado a realização e apresentação de relatório de testes de vulnerabilidades de todo o ambiente tecnológico, conforme as práticas de Segurança da informação. A contratante possui ferramenta par<br>de vulnerabilidades? Qual a periodicidade para a relização destes testes de vulnerabilidades? Qual a quantidade de Assests a serem scaneados ou que fazem parte do escopo do serviço de gestão de vulnerabilidade |
| 35 | 4.1.15.21 | Neste item é solicitado que a CONTRATADA que realize os testes em todos os sistemas ou ativos informados neste Termo de Referência. Poderiam detalhar melhor quais testes serão realizados? |
| 36 | 4.1.15.19 | Entendemos que a contratada não será pensalizada no caso de falhas que não tenham sido devidamente tratadas por outros fornecedores da contratante. Neste caso a atuação da contratada se dará envidando os me<br>Nosso entendimento está correto? |

**Esclarecimentos relativos ao grupo 1**

3.1. **Esclarecimento** 1 - item 3.1.16 Tabela 3 - Poderia nos fornecer maiores detalhes sobre a tecnologias/ativos utilizados pelo Ministério da Justiça e Segurança Pública (Quantidade, tipo de ativos, marca, modelo, fabricante) ?

3.2. Resposta: 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.

3.3. **Esclarecimento** 2 - 3.1.16 Tabela 3 - Dos 728 equipamentos e tecnologias do MJSP citados, quantos estão integrados e enviando logs para o Sentinel? Poderiam compartilhar maiores informações das integrações ativas?

3.4. Resposta: 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.

3.5. **Esclarecimento** 3 - item 2.2.2 - No corpo deste TR diz que o dimensionamento da equipe para os serviços objeto deste edital é responsabilidade da contratada, entendemos que tal equipe pode pertencer ao pool de analistas do SOC da contratada, sendo assim não é requirido ser uma equipe dedicada ao Ministério da Justiça. A exigência é atrelada ao atendimento do escopo e não uma equipe exclusiva. Está correto o entendimento?

3.6. Resposta: Sim, o entendimento está correto. Conforme item "6.1.4.12 A contratação dos itens mencionados não exige mão de obra com dedicação exclusiva, mas a prestação do serviço dentro dos níveis mínimos de serviços exigidos e com o sigilo adequado, conforme termos e documentações previamente assinadas." no Termo de Referência atualizado.

3.7. **Esclarecimento** 4 - item 4.1.14.1.5 - Entendemos que o time técnico da contratada não possui as capacidades necessárias para substituir a atuação dos times de gestão de infra e/ou apps da contratante ou de terceiros, sendo portanto imprescindível a atuação conjunta destes em situações de crise, ainda que afetados por indisponibilidade do ambiente, sem prejuízo ao escopo claro e definido de atuação de todas as partes envolvidas. Tal entendimento está correto?

3.8. Resposta: Não, o entendimento está incorreto. Conforme item "4.1.14.1.5 - 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.", do Termo de Referência atualizado, o SOC atuará em casos excepcionais durante incidentes, quando definidos os protocolos de atuação pela Contratante. Dessa forma, estando impedido de atuação conjunta no exato momento.

3.9. **Esclarecimento** 5 - item 4.1.14.1.12 - Neste item entendemos que a contratante se obriga e se compromete a manter licenciamento, hardware, software e o respectivo suporte dos fabricantes adequadamente dimensionados para o seu parque de assets durante todo o tempo de vigência do contrato objeto deste edital. Tal entendimento está correto?

3.10. Resposta: Não, o entendimento está incorreto. O referido item "4.1.14.1.12 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." não cita a obrigatoriedade e comprometimento da CONTRATANTE em relação aos licenciamentos, hardware, software e o respectivo suporte dos fabricantes. O item trata somente do possível complemento à solução do Grupo 1 - SOC e Blue Team em relação a hardware e software, conforme Termo de Referência atualizado.

3.11. **Esclarecimento** 6 - item 4.1.14.2.15 - Por gentileza, qual é o volume histórico de melhorias solicitadas pela contratante mensalmente? Entendemos que melhorias complexas darão origem à um projeto fora do escopo de prestação de serviços especificados neste edital, correto?

3.12. Resposta: Não, o entendimento está incorreto. O atual certame trata da contratação de serviços que atualmente não existem no Ministério. Dessa forma, não é possível fornecer histórico de melhorias referente a aberturas de chamados para tal serviço. Independente da complexidade das melhorias solicitadas, essas melhorias não estarão fora do escopo de atividades estabelecidas no Termo de Referência. Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.13. **Esclarecimento** 7 - item 4.1.14.2.18 - É solicitado que seja mantido atualizado o CMDB da contratante, qual é a ferramenta atual utilizada? A contratante permitirá a integração automatizada de seu CMDB com a plataforma de gestão da contratada?

3.14. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços. Esse ponto deverá ser alinhado em momento posterior à contratação.

3.15. **Esclarecimento** 8 - item 4.1.14.2.25 - Por "instalar e customizar" entendemos que os termos mais adequados seriam "operar e configurar" os softwares listados como objeto deste edital, correto? Uma vez que já se encontram instalados, e customização de software envolveria edição de código fonte.

3.16. Resposta: Não, o entendimento está incorreto. Em relação ao termo "customizar" entende-se que refere-se a configuração, criação de regras, scripts ou outros para atender as necessidades do CONTRATANTE em relação a utilização das ferramentas existentes. Embora as ferramentas citadas no Termo de Referência já estejam instaladas, o Ministério poderá, a qualquer momento, adquirir outras ferramentas relacionadas à Segurança da Informação.

3.17. **Esclarecimento** 9 - item 4.1.14.2.45 - Entendemos que a única solução que será administrada pela contratada é o Sentinel SIEM/SOAR/NTA/UEBA/CTI. Está correto nosso entendimento? Todas os tipos das soluções são da marca Microsoft Sentinel. Está correto entendimento.

3.18. Resposta: Não, o entendimento está incorreto. A CONTRATADA deverá administrar todas as ferramentas relacionadas à Segurança da Informação instaladas ou que venham a ser adquiridas pelo Ministério e que façam parte das atribuições do SOC e Blue Team.

3.19. **Esclarecimento** 10 - item 4.1.14.2.36 - Entendemos que a participação da contratante em projetos se limita ao escopo de suporte dos ambientes listados neste edital (sentinel SIEM/SOAR/NTA/UEBA/CTI), e desde que não causem prejuízo ou sobrecarga ao atendimento/suporte operacional, correto?

3.20. Resposta: Não, o entendimento está incorreto, o item é claro e objetivo. "4.1.14.2.36 Participar da implantação de projetos/soluções, substituição e atualização de **soluções destinadas à Segurança da Infraestrutura de rede**;"

3.21. **Esclarecimento** 11 - item 4.1.14.2.44 - No item é solicitado a atualização de versão de todos os softwares e hardwares do parque tecnológico que sustenta a Plataforma de SIEM/SOAR/NTA/UEBA/CTI do Ministério. Entendemos que este item está limitado a plataforma SIEM/SOAR/NTA/UEBA/CTI do Ministério e não aos ativos que enviam logs ao SOC, está correto nosso entendimento?

3.22. Resposta: Não, o entendimento está incorreto. O item 4.1.14.2.44 trata de **sugestão** de atualização de versão dos hardwares e software que sustenta a plataforma mencionada. O item não solicita a atualização de versão desses ativos.

3.23. **Esclarecimento** 12 - item 4.1.14.2.39 - Entendemos que a participação da contratante em projetos se limita ao escopo de suporte dos ambientes listados neste edital (* listar ferramentas *), e desde que não causem prejuízo ou sobrecarga ao atendimento/suporte operacional, correto?

3.24. Resposta: Não, o entendimento está incorreto. A CONTRATADA deverá administrar todas as ferramentas relacionadas à Segurança da Informação instaladas ou que venham a ser adquiridas pelo Ministério e que façam parte das atribuições do SOC e Blue Team.

3.25. **Esclarecimento** 13 - item 4.1.14.2.43 - A contratante possui mapeamento de processos? Se sim, o mesmo pode ser compartilhado?

3.26. Resposta: Entendemos que os dados contidos no termo de referência são suficientes para formação de preço e demais esclarecimento deverá ser obtida na vistoria, conforme item 4.16.1.

3.27. Resposta: Atualmente nem todos os processos do Ministério estão mapeados. Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.28. **Esclarecimento** 14 - item 4.1.14.2.43 - A contratante já tem uma visão clara do escopo para o GCN? Será o mesmo escopo contemplado no trabalho anterior com inclusão dos processos que sofreram alterações e novos processos?

3.29. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços. O serviço de GCN não faz parte do escopo da presente contratação.

3.30. **Esclarecimento** 15 - item 4.1.14.2.43 - A contratante possui organograma atualizado das áreas de negócios e tecnológicas? Se sim, podem - compartilhar?

3.31. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços. A informação solicitada pode ser obtida no sítio eletrônico do Ministério https://www.gov.br/mj/pt-br/acesso-a-informacao/institucional/organogramas.

3.32. **Esclarecimento** 16 - item 4.1.14.2.43 - Quantas unidades de negócios (físicas – prédios) serão contempladas neste projeto?

3.33. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.34. **Esclarecimento** 17- item 4.1.14.2.43 - Existem unidades de Data Center nesses prédios? Eles serão escopo do projeto? Se sim, quantos DC´s?

3.35. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.36. **Esclarecimento** 18 - item 4.1.14.2.43 - Existe alguma estratégia de GCN já definida? Se sim, quais?

3.37. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.38. **Esclarecimento** 19 - item 4.1.14.2.43 - A contratante possui Política de Continuidade de Negócios estabelecida?

3.39. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.40. **Esclarecimento** 20 - item 4.1.14.2.43 - A contratante possui metodologia de GCN estabelecida? Se não, gostariam da elaboração dela neste projeto?

3.41. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.42. **Esclarecimento** 21 - item 4.1.15.15 e 4.1.15.16 - Para Itens 4.1.15.15 e 4.1.15.16 = scans de vulnerabilidade + relatorios /Será permitida a instalação de sensores na rede do cliente para efetuarmos os scans de vulnerabilidades ?

3.43. Resposta: No que se refere às ferramentas de vulnerabilidades, o Ministério da Justiça e Segurança Pública por meio do Termo de Contrato Nº 69/2021, realizou a contratação de empresa especializada, mediante Sistema de Registro de Preços, para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado(Tenable.sc). E, por meio do Termo de Contrato Nº 63/2021, realizou a contratação de empresa especializada para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado(Qualys Web Application Scanning - WAS). Conforme o item "4.1.9.4.20 A CONTRATADA poderá utilizar as ferramentas de Vulnerabilidades em ativos de rede e aplicações Web disponíveis no Ministério. A CONTRATADA também poderá utilizar outras ferramentas de Vulnerabilidades, se julgar necessário, ou para complementar as ferramentas disponíveis, desde que não tenha custos para a CONTRATANTE." (Termo de Referência atualizado).

3.44. **Esclarecimento** 22 - item 3.4.2.7 - Mediante item 3.4.2.7 (pg. 26) do Termo de Referência, entendemos que a proponente não poderá ser habilitada nos dois grupos. Está correto o entendimento?

3.45. Resposta: Não, o entendimento está incorreto. 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, consequentemente, desclassificada para o Grupo 2.

3.46. **Esclarecimento** 23 - Sobre a prestação dos serviços, entendemos que a equipe ficará nas instalações da proponente. Está correto o entendimento?

3.47. Resposta: Não, o entendimento está incorreto. 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.

3.48. **Esclarecimento** 24 - item 8 (pg.56) - Sobre o orçamento disponível para a contratação, entendemos que os valores máximos são os listados na tabela pg. 56. Está correto o entendimento?

3.49. Resposta: Sim, o entendimento está correto. Conforme Termo de Referência atualizado.

3.50. **Esclarecimento** 25 - *Item 4.1.15.2.1 Além de utilizarmos como base para análise do Framework NIST, podemos utilizar também o padrão base do CIS 8?*

3.51. Resposta: Sim.

3.52. **Esclarecimento** 26 - *Item 4.1.15.2 Entendemos que a execução da atividade de Assessment de Maturidade (Gap Analysys) pode ser realizada de forma remota, com reuniões no Teams ou outras plataformas de comunicação. Nosso entendimento está correto?*

3.53. Resposta: Sim, o entendimento está correto. As reuniões ocorrerão de forma alinhada com a equipe de fiscalização do contrato.

3.54. **Esclarecimento** 27 - *Item 4.1.15.2 Quais e quantas são as áreas do MJSP? Citar qualquer área que possa ter (mesmo que ainda não sabido) acesso a qualquer informação da empresa, mesmo que só usuário no domínio.*

3.55. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.56. **Esclarecimento** 28 - *Item 4.1.15.2 Há terceiros que acessam o ambiente computacional ou ambientes críticos do MJSP? Informar quantidades e em quais situações. O MJSP tem uma equipe capaz de implementar e manter um SGSI de acordo com os requisitos da ISO 27001?*

3.57. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.58. **Esclarecimento** 29 - *item 4.1.15.2 Há um time interno dedicado à Segurança da Informação?*

3.59. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.60. **Esclarecimento** 30 - *Item 4.1.15.2 Um Assessment de Maturidade já foi efetuado anteriormente? Quando foi?Há outros processos de conformidade de Segurança da Informação em curso? Se sim citar quais.*

3.61. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.62. **Esclarecimento** 31 - *Item 4.1.15.2 MJSP é aderente a alguma norma ou certificação de segurança? Como ISO 27001, PCI DSS, outras? Se sim citar quais e ano da última certificação. O MJSP é cobrado de atender alguma regulamentação, como BACEN, SOX, etc? Se sim citar quais*

3.63. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.64. **Esclarecimento** 32 - *Item 4.1.15.2 Empresa possui todas as políticas e padrões do SGSI, como políticas de segurança da informação, classificação das informações, gerenciamento de acesso, resposta a incidentes, etc.?*

3.65. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.66. **Esclarecimento** 33 - *Item 4.1.15.2 A empresa tem controle sobre a existência, utilização e criação de credenciais privilegiadas? Leia-se por credenciais privilegiadas aquelas que permitem acessos a sistemas críticos para o negócio do MJSP, bem como sistemas críticos do ambiente de TI.*

3.67. Resposta: Entende-se que os dados contidos no termo de referência são suficientes para formação de preços.

3.68. **Esclarecimento** 34 - *Item 4.1.15.15 Neste item é solicitado a realização e apresentação de relatório de testes de vulnerabilidades de todo o ambiente tecnológico, conforme as práticas de Segurança da informação. A contratante possui ferramenta para execução dos testes de vulnerabilidades? Qual a periodicidade para a realização destes testes de vulnerabilidades? Qual a quantidade de Assests a serem scaneados ou que fazem parte do escopo do serviço de gestão de vulnerabilidades?*

3.69. Resposta: No que se refere às ferramentas de vulnerabilidades, o Ministério da Justiça e Segurança Pública por meio do Termo de Contrato Nº 69/2021, realizou a contratação de empresa especializada, mediante Sistema de Registro de Preços, para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação e aplicações web ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado(Tenable.sc). E, por meio do Termo de Contrato Nº 63/2021, realizou a contratação de empresa especializada para prestação de serviços de implementação de solução para avaliação de vulnerabilidades em ativos de tecnologia da informação ao Ministério da Justiça e Segura Pública, compreendendo: a subscrição de licenças de software, abarcando a atualização, o treinamento e o suporte técnico (24x7); e o serviço técnico especializado(Qualys Web Application Scanning - WAS). Conforme o item "4.1.9.4.20 A CONTRATADA poderá utilizar as ferramentas de Vulnerabilidades em ativos de rede e aplicações Web disponíveis no Ministério. A CONTRATADA também poderá utilizar outras ferramentas de Vulnerabilidades, se julgar necessário, ou para complementar as ferramentas disponíveis, desde que não tenha custos para a CONTRATANTE." (Termo de Referência atualizado).

3.70. **Esclarecimento** 35 - *Item 4.1.15.21 Neste item é solicitado que a CONTRATADA que realize os testes em todos os sistemas ou ativos informados neste Termo de Referência. Poderiam detalhar melhor quais testes serão realizados?*

3.71. Resposta - Deverão ser realizados testes de vulnerabilidades, bem como testes relativos à segurança da informação, excetuados aqueles previstos no Grupo 2 Serviço de teste de Invasão - Red Team.

3.72. **Esclarecimento** 36 - *Item 4.1.15.19 Entendemos que a contratada não será pensalizada no caso de falhas que não tenham sido devidamente tratadas por outros fornecedores da contratante. Neste caso a atuação da contratada se dará envidando os melhores esforços. Nosso entendimento está correto?*

3.73. Resposta: Sim, o entendimento está correto. No entanto, será analisado caso a caso, conforme o item "7.3.3.12.7.5 Incidentes comprovadamente ocorridos por fatores alheiros à atuação da contratada não serão computados para fins de aplicação de glosas e penalidades." (Termo de Referência atualizado). Em todo o caso, a CONTRATADA sempre deverá observar os Níveis de Serviços estabelecidos conforme Tabela 11.

4. 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 **16996536** e o código CRC **5563AD4C**
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.

**Referência:** Processo nº 08006.000003/2021-38 SEI nº 16996536