Alexandra Lacerda Ferreira Rios

De:	Sigmar Frota <sigmar.frota@kryptus.com>
Enviado em:	terça-feira, 8 de março de 2022 23:17
Para:	MJ-Licitação; Coordenação de Riscos de Segurança de TIC; Cintia Mye Yonekawa Yamaguti; Ivanildo de Oliveira da Silva JR
Cc:	Rafael Cividanes; Ana Flavia Goncalves
Assunto:	MJSP - Edital PE 021/2021 - Solicitação de Esclarecimentos ao edital - em 08/03/2022
Anexos:	Questionamentos ao edital MJSP 02102021 - em 08 03 2022 - vrs 2.pdf

Questionamentos ao edital MJSP

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
EDITAL DE LICITAÇÃO PREGÃO ELETRÔNICO Nº 21/2021
(08006.000003/2021-38)

Prezados integrantes da Coordenação de Procedimentos Licitatórios/COPLI – MJSP e equipe técnica DTIC/CRS-MJSP,

A empresa **Kryptus Segurança da Informação S.A**, CNPJ n° 05.761.098/0001-13, tendo examinado os termos e anexos do EDITAL DO PREGÃO ELETRÔNICO MJSP nº 21/2021, vem, respeitosamente, solicitar **ESCLARECIMENTOS** referentes ao edital em referência, conforme abaixo:

---

1. No nos termos do edital, pág.3, itens 4.5 e 4.5.1. , temos a seguinte redação "*Conforme item 3.4.2.7.1 do Termo de Referência, é vedada a contratação de uma mesma empresa para dois ou mais serviços licitados, quando, por sua natureza, esses serviços exigirem a segregação de funções, tais como serviços de execução e de avaliação, mensuração ou apoio à fiscalização, assegurando a possibilidade de participação de todos licitantes em ambos os itens seguindo-se a ordem de adjudicação entre eles (ou lotes/grupos) indicada no subitem seguinte. Será adjudicado primeiro o grupo 1 e posteriormente o grupo 2.*". É conhecido pelos proponentes licitantes que, após a publicação do edital, seguem-se as fases de apresentação das propostas, classificação das propostas, disputa de lances, classificação das propostas após a fase de lances, negociação, análise de documentação e a declaração da licitante provisoriamente vencedora, seguindo-se a fase recursal, o julgamento dos recursos e contrarrecursos, e, por fim, a homologação e a adjudicação da vencedora de um certame. Nosso entendimento é que será útil aos proponentes licitantes conhecerem como a área administrativa (pregoeiro) do certame irá efetuar tal julgamento até a adjudicação do grupo 1; para só então – depois de todas as fases acima - efetuar o julgamento do grupo 2 conforme o comando do item 4.5.1. Solicitamos esclarecimentos.

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*)?

3. No termo de Referência, pág.29, 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.46 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.31 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?

4. No termo de Referência, pág.33, o ítem 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 ativos de infraestrutura; entendimento fundamentado, inclusive, nos *frameworks* indicados na pág.31 - 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?

5. No termo de Referência, pág.33, item 4.1.9.6. , temos a seguinte redação "*...a CONTRATADA deverá 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...*". 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*)

6. No termo de Referência, pág.34, 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/CTI 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. Concluindo, 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?

7. No termo de Referência, pág.1, 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 execução dos serviços pelo uso de profissionais especializados, de forma remota, sem a necessidade de pessoalidade de tal prestação ou dedicação exclusiva 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, desde que sejam entregues os níveis de serviços definidos no edital e seus anexos. Está correto nosso entendimento?

8. No termo de Referência, pág.1, 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 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?

9. No termo de Referência, pág.1, 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?

10.No termo de Referência, pág.34, 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.*)

11.No termo de Referência, pág.34, 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.*)

12.No termo de Referência, pág.34, 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.)*

13.No termo de Referência, pág.15, 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?

14.No termo de Referência, pág.44, item 4.3.2.3, em relação ao acesso de informações. Em face das exigências vigentes 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 - em relação à tempestividade aplicada ao "Termo de Compromisso" constante no Anexo I – F e o comando do item 4.15.4. – é que o mesmo deverá ser assinado apenas na fase de contratação pela licitante vencedora. Está correto nosso entendimento?

15.No termo de Referência, pág.44, item 4.3.2.3, em relação ao acesso de informações. Em face das exigências vigentes 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 - em relação à tempestividade aplicada ao "Termo de Compromisso" constante no Anexo I – F e o comando do item 4.15.4. – é que o mesmo deve ser assinado pelos prestadores de serviços da licitante vencedora, antes do engajamento dos referidos colaboradores nas atividades contratuais. Está correto nosso entendimento?

16.No termo de Referência, pág.25, item 3.1.16, são apresentados alguns quantitativos de tecnologias na "Tabela 3". Nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem quais os tipos de "Sistemas" (Tabela 3 – Item 4) 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.)*

17.No termo de Referência, pág.25, item 3.1.16, são apresentados alguns quantitativos de tecnologias na "Tabela 3". Nosso entendimento é que seria relevante para as proponentes licitantes do certame conhecerem quais as tecnologias de nuvem (Tabela 3 – Item 6), qual o número de servidores/serviços instanciados em cada provedor (Oracle e Microsoft) de nuvem contratados pelo MJSP. Está correto nosso entendimento? (*obs: caso positivo, explicitar as tecnologias de nuvem, qual o número de servidores/serviços instanciados em cada provedor.)*

18. No termo de Referência, pág.37, 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 referida na fase de contratação. Está correto nosso entendimento? (*obs: caso negativo, explicitar em qual momento deverá a proponente licitante demonstrar a conformidade com a Norma.)*

19. No termo de Referência, pág.37, 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 a este item 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 (24 meses). Está correto nosso entendimento?

20.No termo de Referência, pág.37, 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 vencedora; devendo ser integralmente comprovados durante a fase de contratação do certame. Está correto nosso entendimento?

21.No termo de Referência, pág.37, 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 de conformidade utilizado pelo MJSP caso a vencedora não possua a certificação válida; uma vez que o resultado já estará homologado e adjudicado à licitante vencedora. Está correto nosso entendimento?

22.No termo de Referência, pág.34, 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?

Por fim reiteramos nosso apreço às equipes COPLI – MJSP e DTIC/CRS-MJSP.

Atenciosamente,

--

Sigmar Frota

Public Sector - Brazil

sigmar.frota@kryptus.com

www.kryptus.com