procempa

24.12.00000011-1

LICITAÇÃO ELETRÔNICA 032/2024

AQUISIÇÃO DE SERVIDORES PARA IA

ESCLARECIMENTOS

Questionamento 01: 1º ESCLARECIMENTO (PROPOSTA INICIAL) = No que tange à **PROPOSTA DE PREÇO INICIAL**, estamos entendendo que o licitante deverá enviar a mesma mediante, **apenas**, o preenchimento, no sistema eletrônico, dos campos ali existentes, **SEM A NECESSIDADE DO ENVIO DE QUALQUER ANEXO**. Está correto nosso entendimento? Caso contrário favor esclarecer.

Resposta 01: Sim, está correto.

Questionamento 02:PRAZO DE ENVIO DA PROPOSTA
Após a análise do edital em questão, identificamos que o prazo para o envio da proposta reajustada ao lance final não está claramente definido.
Diante dessa situação, entendemos que o prazo será de duas horas, conforme o que é considerado um "costume administrativo". Segundo Matheus Carvalho, "o costume administrativo é caracterizado como uma prática reiteradamente observada pelos agentes administrativos em situações concretas. Essa prática comum na Administração Pública é aceita em casos de lacuna normativa e atua como uma fonte secundária de Direito Administrativo, podendo gerar direitos para os administrados, em virtude dos princípios da lealdade, boa-fé e moralidade administrativa, entre outros." Nosso entendimento está correto? Caso contrário, favor informar o prazo.

Resposta 02: A proposta final adequada ao seu último lance será solicitada ao final da disputa, sendo o tempo administrado pelo Pregoeiro.

Questionamento 03:MANIFESTAÇÃO DO RECURSO
O edital é omisso em informar o prazo para manifestação de recurso após a declaração do vencedor. Dessa forma, entendemos que o prazo para manifestar a intenção de recorrer será de 30 (trinta) minutos, a contar da declaração do vencedor. Nosso entendimento está correto?

Resposta 03: As informações encontram-se no item 5.2 de nosso edital.

Questionamento 04: Em relação aos itens 5.4. do Termo de Referência para o Lote 1 e, 5.3. para o Lote 2, segundo o que o próprio NIST informa em seu website: “Os requisitos FIPS 140-2 e FIPS 140-3 são aplicáveis a todas as agências federais dos EUA. As agências devem usar sistemas de segurança baseados em criptografia para fornecer segurança de informação adequada para todas as operações e ativos, conforme definido em 15 U.S.C. § 278g-3.

A criptografia não validada é vista como não oferecendo nenhuma proteção às informações ou dados — na verdade, os dados seriam considerados texto não criptografado desprotegido. Se a agência especificar que as informações ou dados sejam protegidos criptograficamente, o FIPS 140-2 ou FIPS 140-3 é aplicável. Em essência, se a criptografia for necessária, ela deve ser validada. Caso o módulo criptográfico seja revogado, o uso desse módulo não é mais permitido.”

Nosso entendimento é que a expressão “seguir as especificações do NIST”, não dá garantia ao CONTRATANTE, que a solução ofertada pelo CONTRATADO, apresente as condições de segurança esperadas, tal qual o próprio NIST determina.

Em recente discussão, pelo Serpro, em seu processo de Pregão Eletrônico 90555/2024, vimos o seguinte:

"... relacionada ao item 4, subitem 2.14.1.1.24 do edital. 2.14.1.1.24. A controladora de gerenciamento do servidor deverá permitir operar em modo de segurança criptográfica padrão FIPS 140-2 ou versão superior." A recorrida apresentou uma declaração do fabricante ..... registrando que o controlador de gerenciamento de servidor (.....) é "capaz de executar SSL no modo de segurança criptográfica padrão FIPS 140-2 ou versão superior através da importação de certificação SSL". Realizamos uma análise detalhada da documentação da recorrida e não foi identificado qualquer referência acerca da ativação e desativação do modo de segurança FIPS 140-2 para que a controladora de gerenciamento possa operar segundo o padrão solicitado. Ato contínuo, verificando no site do NIST (National Institute of Standards and Technology), não foram encontradas referências à controladora de gerenciamento do fabricante ..... relacionada à operação no modo de segurança criptográfica FIPS 140-2 ou superior. Considerando que este é um padrão de segurança amplamente utilizado pelo mercado por diversos fabricantes, e que especifica os requisitos de segurança que serão atendidos por um módulo criptográfico, incluindo especificação, portas e interfaces, funções, serviços e autenticação, modelo de estado finito, segurança física, ambiente operacional, gerenciamento de chaves criptográficas, interferência eletromagnética/compatibilidade eletromagnética (EMI/EMC), autotestes, garantia de projeto e mitigação de outros ataques, a utilização deste traz garantias ao Serpro de que a controladora de gerenciamento dos servidores executará e estará em conformidade com os rigorosos padrões de segurança criptográfica internacionais, de forma a resguardar, proteger e afastar riscos aos ambientes de datacenter do Serpro, de seus equipamentos e serviços, sendo este um requisito indispensável à essa administração. A importação de chaves criptográficas ou chaves geradas externamente ao módulo, indicado pelo licitante, não possui garantia mínima de segurança, como podemos verificar em advertências (Key/Entropy Caveats – link Cryptographic Module Validation Program | CSRC (nist.gov)., replicado abaixo. Ou seja, essas advertências destacam a importância de garantir que quaisquer chaves criptográficas carregadas externamente atendam a requisitos de segurança rigorosos para manter a segurança geral do módulo criptográfico. "No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or off SSPs established with externally loaded SSPs The module receives SSPs (e.g., keys or bit strings) from outside of its boundory for use within on approved algorithm (e.g., a key used for AES encryption; or a bit string used for generating the k values of DSA and ECDSA gigGen algarithms). This caveat does not apply to a seed used for an internal DRBG, or a seed in an asymmetric key generation algorithm since that must be obtained from an approved DRBG in compliance with SP 800-133r2".

Adicionalmente, realizamos um questionamento, por e-mail, diretamente ao NIST (National Institute of Standards and Technology), o qual recebemos a seguinte resposta: ENC: Use of FIPS 140-3 or FIPS 140-2 Logo and Phrases Enviado: quarta-feira, 28 de agosto de 2024 15:02 De: cmvp <cmvp@nist.gov> Para: ...@serpro.gov.br>; cmvp <cmvp@nist.gov> Assunto: RE: Use of FIPS 140-3 or FIPS 140-2 Logo and Phrases Hi Please see the our web site, Cryptogrephic Module Validation Program I CSRC (nit.gov). You will be able to find the detail with the links to our FIPS 140-2, FIP 140-3, and CMVP Validation Process on the rigt panel of this page. If the module are not validated by our CMVP, we are not able to provide any comments on rather they do or do not meet the standards. Regards, Janet Jing NIST, Computer Security Division, CMVP From: ...@serpro.gov.br> Sent: Wednesday; August 28, 2024 10:23 AM To: cmvp <cmvp@nist.gov> Subject: Use of FIPS 140-3 or FIPS 140-2 Logo and Phrases Importance: High Hi If a manufacturer claims to meet the FIPS 140-2 standard or higher, but is not on the list of NIST validated modules, com they use the FIPS 140-2 nomenclature or claim to meet it? Thank you very much for your attention. We look forward to your response asap. Best regards.

A recorrida tenta esclarecer que o ..... encontra-se dentro do mesmo padrão FIPS 140-2 ou versão superior, como exige o edital. Entretanto essa alegação não comprova que segue o padrão estipulado para o FIPS 140-2, pois na consulta ao NIST acima, fomos informados que se os módulos não forem validados pelo Cryptographic Module Validation Program (CMVP), não é possível fornecer comentários sobre se eles atendem ou não aos padrões, ou seja, se não está validado e listado no site. Neste sentido, não há garantia necessária de que a controladora ..... possa operar em modo de

segurança criptográfica padrão FIPS 140-2 ou versão superior, pois, alguns dos serviços como SNMP, IMPI, dentre outros existentes na controladora de gerenciamento, que não são compatíveis com o modo de segurança FIPS 140-2, não serão desabilitados na simples importação de um certificado SSL, conforme indicado pela recorrente e ratificado pelo NIST (FIPS 140-2 Non-Proprietary Security Policy), disponível no link: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3122.pdf . Portanto, pelas informações demonstradas acima, concluímos pela aceitação dos recursos apresentados"

Ainda que os padrões de segurança mencionados sejam exigidos por órgãos de outros países, entende-se, por melhores práticas de segurança da informação, que na ausência de um padrão nacional que ofereça maior proteção, a adoção de outros, ainda que estrangeiros, é indicada para a proteção dos ambientes de TI. Por este motivo, o CONTRATANTE refere-se ao padrão NIST, buscando dar ao seu ambiente, que possui enorme criticidade para serviços públicos essenciais, a melhor proteção possível.

Sendo assim, nosso entendimento é que quando o CONTRATANTE se refere a "segundo as especificações NIST", está se referindo a que o módulo tenha sido avaliado "e certificado" pelo NIST, com a devida publicação em seu website. Está correto o nosso entendimento?

Resposta 04: O entendimento não está correto, pois segundo informação do próprio NIST, o mesmo não certifica fornecedores, fazendo apenas a avaliação e análise de componentes de software de diversos fornecedores frente as políticas/práticas de segurança da informação. Nos itens 5.4 (lote 1) e 5.3 (lote 2), estamos solicitando que a BIOS/UEFI sigam as normas determinadas pelos padrões citados.

Questionamento 05: Referente aos itens 2.3 do TR "Servidor para IA Tipo A" e item 2.2 do TR "Servidor para IA Tipo B", entendemos que serão aceitos servidores com tecnologias de correção de erros de memórias mais atualizadas, como as tecnologias ADDDC (Adaptive Double DRAM Device Correction) ou Fault Resilient Mode (FRM). Está correto nosso entendimento?

Resposta 05: O entendimento está correto.

Questionamento 06: Referente ao item 7.1.3. de ambos os TRs onde solicita "As fontes devem possuir tensão de entrada de 200VAC a 240VAC a 60Hz", entendemos que também serão aceitos servidores que suportem fontes de tensão de entrada de 100VAC a 240VAC, desde que atendam os demais requisitos das fontes solicitados no item 7.1. Está correto nosso entendimento?

Resposta 06: O entendimento está correto.

Questionamento 07: 1º Em relação ao faturamento, entendemos que, preservado o valor total da licitação, que a licitante vencedora poderá faturar cada item de acordo com a Nota Fiscal prevista pela legislação. Desta maneira, os produtos serão faturados com DANFE (NFe), e os serviços de suporte de hardware, garantia e software serão faturados como serviços (NFS-e), tributadas pelo ISS e de acordo com o código previsto na lista de serviços anexa à Lei Complementar Nº 116, de 31/07/2003. Não havendo restrição alguma da CONTRATANTE, por questões de Dotação Orçamentária e/ou Natureza de Despesa, para o recebimento das respectivas Notas Fiscais de Serviços.

Está correto nosso entendimento?

Importante mencionar, ainda, que em 11/11/2020, no julgamento das ADIs n°s 1945-MT e 5659-SP, o Supremo Tribunal Federal – STF declarou a inconstitucionalidade do ICMS nas operações em questão, decidindo pela incidência do Imposto sobre Serviços - ISS sobre qualquer tipo de operação com software, seja ele padronizado ou não; customizado ou não; desenvolvido sob encomenda ou não; transmitidos via download, por meio de acesso à nuvem ou gravado em suporte informático. Solicitamos confirmar ou esclarecer como poderá ser feito o faturamento.

Aguardamos resposta, para o melhor entendimento da questão acima.

Resposta 07: Após análise do questionamento, manifestamos concordância quanto à forma de emissão de NFs, bem como a ciência da decisão do STF no que tange ao tratamento tributário às operações de software.

Questionamento 08: Referente ao item "8.1.7. Deverá possuir subscrição do software NVIDIA AI Enterprise por GPU para 60 meses" do TR Servidor para IA Tipo A e do item "8.1.8. Deverá possuir subscrição do software NVIDIA AI Enterprise por GPU por 60 meses" do TR Servidor para IA Tipo B, entendemos que deverão estar inclusos juntamente com a licenças de subscrições do software NVIDIA AI Enterprise o suporte 24x7 do fabricante NVIDIA para 60 meses. Está correto nosso entendimento?

Resposta 08: O entendimento está correto, pois entendemos que a subscrição do mencionado software também deverá fornecer o suporte pelo mesmo período da subscrição adquirida.

Questionamento 09: 1) O licitante vencedor poderá **OPTAR** por faturar parte dos equipamentos que são objeto deste Pregão por um dos estabelecimentos (MATRIZ ou FILIAL) e a outra parte dos equipamentos por outro dos seus estabelecimentos (MATRIZ e FILIAL), à sua livre escolha, e será considerado como participante do Pregão unicamente a PESSOA JURÍDICA da licitante (independente do número – ou prefixo - do CNPJ)?

2) Caso o entendimento em relação à questão 1) anterior não esteja correto, quais são; no entender de V.Sas. e para fins de participação neste Pregão, os requisitos que permitirão ao licitante vencedor faturar por seus diferentes estabelecimentos (MATRIZ e/ou FILIAIS)?

3) No caso de serem indicados os requisitos mencionados no item 2) anterior, os mesmos requisitos deverão ser cumpridos pelos licitantes no momento da entrega da proposta escrita ou apenas na ocasião do efetivo faturamento dos equipamentos, quando for o caso?

4) Considerando que o edital de licitação em questão engloba o fornecimento de equipamentos eletrônicos (hardwares) e seus inerentes e intrínsecos serviços de instalação e garantia, indagamos:
Em estrita observância à legislação vigente, denota-se que a tributação incidente nos equipamentos (hardware), qual seja ICMS, é diferente da aplicada nos serviços (garantia e softwares), ISS. À vista disso, entendemos que ambos não devem constar na mesma nota fiscal e que podemos emitir uma nota fiscal para os equipamentos (hardware) e outra para os serviços. Está correto nosso entendimento?

Respostas 09: 1) O entendimento da Divisão de Contabilidade segue a premissa inicial dos contratos administrativos, que possuem natureza personalíssima (*intuitu personae*). Ou seja, a entidade que é responsável pela assinatura do contrato deve ser a mesma entidade a emitir as NFs, enviar certidões negativas, informações fiscais, dados bancários, e demais obrigações contratuais. Procedimento diferente resultaria em oneroso procedimento auxiliar administrativo de controle por parte da Procempa, pois a título de exemplo, os cadastros bancários estão

vinculados a determinado CNPJ. Como explicar ao Tribunal de Contas, Controladoria Geral do Município, Ministério Público, ou demais instâncias de controle e fiscalização, que os contratos foram assinados com uma empresa Matriz, a certidões estão enviadas por outra Filial, e a conta bancária pertencente a outro CNPJ.

Desta forma, toda documentação decorrente da obrigação conratual deve pertencer à entidade responsável pelo contrato.

2) Conforme resposta ao Item 1, este procedimento não é permitido. O contrato e as obrigações deverão ser cumpridos e atendidos pela empresa responsável pela licitação.

3) Conforme resposta ao Item 1, este procedimento não é permitido. O contrato e as obrigações deverão ser cumpridos e atendidos pela empresa responsável pela licitação.

4) Sim, o entendimento está correto.

Questionamento 10: Devido à natureza de tributação distinta sobre mercadorias e serviços, entendemos que será aceito o faturamento separado dos produtos e serviços, sendo uma NF emitida para as mercadorias e outra distinta para os serviços de extensão de garantia exigidos, desde que a soma do valor de ambas as NF's confiram com o valor total do pedido. Está correto nosso entendimento?

Resposta 10: Sim, o entendimento está correto.