Quadro informativo

Pregão Eletrônico N° 90017/2024 (SRP) (Lei 14.133/2021)

UASG 90059 - TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO/MG

Critério julgamento: **Menor Preço / Maior Desconto** Modo disputa: **Aberto/Fechado**

Contratação em período de cadastramento de proposta

Avisos (0) Impugnações (0) Esclarecimentos (7)

06/02/2025 15:43

Referente ao questionamento apresentado cujo o trecho é o seguinte: "Entendemos relativo aos controles de

A solução deverá suportar políticas de proteção de DNS granulares contendo metadados como IDP,

06/02/2025 13:42

I - Da tempestividade do presente pedido de esclarecimentos: Em consonância com o item 13.1 do edital, os pedidos de esclarecimento devem ser enviados em "até 3 (três) dias úteis antes da data da abertura do certame". Como esta solicitação de esclarecimentos está sendo protocolizada em 04/02/2025 e a abertura prevista para 10/02/2025, resta indubitavelmente tempestivo a Solicitação de Esclarecimentos ora apresentado, em razão de atender o lapso temporal devidamente normatizado. II – Do pedido de esclarecimentos propriamente dito:

Esclarecimento 01: Observa-se que Matriz e filial nada mais são do que estabelecimentos de uma mesma pessoa jurídica. Isto posto, entendemos que, caso a licitante ofereça proposta por meio de sua matriz, e desejar faturar e executar os serviços por meio de uma de suas filiais, deverá indicar em sua proposta comercial o CNPJ que será utilizado para faturamento, ou seja, a licitante poderá celebrar o contrato com o CNPJ da matriz e faturar com o CNPJ da filial. Está correto o nosso entendimento?

Esclarecimento 02: O item 3.1.11, que estabelece que "o fabricante deve possuir infraestrutura em território brasileiro, não sendo aceitas soluções como...", e seus subitens 3.1.11.1 e 3.1.11.2, estão restringindo indevidamente a competitividade, contrariando os princípios de ampla concorrência e isonomia previstos na Lei de Licitações. Soluções de Secure Service Edge (SSE) baseadas em nuvens públicas de terceiros, como AWS, Azure ou Google Cloud Platform (GCP), com pontos de presença (PoPs) localizados no Brasil, atendem plenamente aos requisitos de infraestrutura nacional e apresentam vantagens técnicas significativas, tais como: Escalabilidade e alta disponibilidade: Infraestruturas em nuvem pública são projetadas para operar em grande escala, garantindo capacidade de expansão dinâmica e resiliência mesmo em situações de alta demanda; Segurança robusta: Nuvens públicas como AWS, Azure e GCP oferecem controles de segurança avançados, certificações internacionais e compliance com regulamentações locais, garantindo a proteção dos dados processados. Dessa forma, entendemos que a permissão expressa para utilização de PoPs em nuvens de terceiros localizados no Brasil ampliará a competitividade do certame. Solicitamos a revisão dos itens citados para garantir maior isonomia e competitividade, permitindo à Administração Pública usufruir dos benefícios técnicos e econômicos associados a soluções de SSE hospedadas em nuvens públicas no território nacional.
Esclarecimento 03: Referente aos itens 3.8.12., 3.8.12.2. e 3.8.12.3., que solicitam a funcionalidade de DLP em repouso para as aplicações Microsoft Teams e Google Meet, é importante ressaltar que essas plataformas são predominantemente utilizadas para comunicação e colaboração em tempo real, não para armazenamento ou transferência de arquivos através de repositórios virtuais. O foco do DLP (Data Loss Prevention) em repouso é proteger dados armazenados em locais onde são mais vulneráveis a acessos não autorizados ou compartilhamentos inadequados. Como Microsoft Teams e Google Meet são usados principalmente para videoconferências e chats, onde a troca de arquivos é mínima e geralmente se dá em um contexto de confiança entre usuários corporativos, a aplicação de DLP nessas plataformas pode ser considerada redundante. Além disso, os próprios controles de segurança integrados nessas ferramentas já oferecem medidas adequadas para garantir a integridade e a segurança das informações compartilhadas durante as sessões. Entendemos que a solução deve permitir a varredura das aplicações Microsoft 365 OneDrive, Sharepoint e Google Drive uma vez que estes possuem justificativa técnica para tal varredura.

Esclarecimento 04: Em relação aos itens 3.1.19. e 3.1.19.4., que solicitam o uso do protocolo VNC e das aplicações TeamViewer e AnyDesk, é crucial destacar que essas ferramentas foram originalmente desenvolvidas para operar com a instalação de software no computador do usuário, pois dependem de

AnyDesk utilizam aplicações cliente e servidor para criar túneis de comunicação seguros e criptografados, garantindo a integridade e confidencialidade dos dados transmitidos. A solicitação para que esses protocolos e aplicações sejam compatíveis com o modelo de acesso ZTNA clientless, que visa permitir o acesso sem software instalado no dispositivo do usuário, não se alinha com a proposta inicial da arquitetura ZTNA clientless. Por fim entendemos que a solução não deve depender de cliente instalado na máquina do usuário para os seguintes tipos de aplicação, como: WEB, RDP e SSH.

Esclarecimento 05: Para o atendimento do item 3.1.29, referente à validação de postura para acesso agentless, entendemos que essa funcionalidade é essencial em pelo menos duas das quatro validações listadas nos subitens do edital. Como o acesso ocorre via browser e os dispositivos podem utilizar diferentes softwares de segurança, pode haver limitações na transmissão de todas as informações necessárias para que a solução de SSE avalie corretamente a conformidade do dispositivo antes de permitir ou negar o acesso com base nas políticas estabelecidas. Realizar a validação diretamente pelo browser é o método mais amplamente utilizado.

Esclarecimento 06: Em relação aos itens 3.5.10. e 3.5.10.2., que recomendam o uso do protocolo IPsec para o encaminhamento do tráfego ao Secure Web Gateway (SWG), é importante considerar a remoção do GRE da especificação. Embora o GRE seja útil para encapsulamento, ele não oferece criptografia nativa, o que pode não ser ideal para todas as necessidades de segurança. IPsec, por outro lado, oferece uma camada robusta de proteção, assegurando que a comunicação seja criptografada e que a integridade e a confidencialidade dos dados sejam mantidas. Para maximizar a segurança e a privacidade dos dados trafegados na solução de Segurança de Serviço de Borda (SSE), recomendamos o uso exclusivo do IPsec. Esta abordagem ajudará a proteger informações sensíveis durante a transmissão, alinhando-se com as práticas recomendadas em segurança cibernética.

1. Questionamento de natureza financeira, razão pela qual deve ser encaminhado à SUCEF para o esclarecimento;
2. O item 3.1.11 deve ser alterado para o texto abaixo:
3.1.11. O fabricante deve possuir infraestrutura em território brasileiro.
3.1.11.1. Admite-se a hospedagem em datacenter de nuvem pública estabelecida no Brasil;
3.1.11.2. REVOGADO
3. A solução deve permitir a varredura nos chats conforme licenciamento do TRF6 junto às nuvens, além de permitir a varredura das aplicações Microsoft 365 OneDrive, Sharepoint e Google Drive, conforme item 3.8.12 e subitens.
4. O item 3.1.19.4 detalha alguns sistemas de acessos a desktops remotos, como bem apontado pela expressão "entre outros". Considerando que os acessos diferem daqueles arrolados nos itens 3.1.19.1 a 3.1.19.3, o item 3.1.19.4 representa uma forma de acesso a ser abarcada pelos acessos agentless.
5. O item 3.1.29 e respectivos subitens contempla o mínimo para uma validação de postura e a solução deve contemplar todas as validações.
6. O item 3.5.10 detalha os mínimos métodos de envio de tráfego Secure Web Gateway (SWG), razão pela qual devem estar incluídos na solução de SSE, sem prejuízo de inclusão de outras vias.

06/02/2025 13:40

1. Referente ao item 3.1.8, entendemos que o provimento de endereços IP's deverão ser xos e dedicados para

1. O item 3.1.11 deve ser alterado para o texto abaixo:

06/02/2025 13:33

1 - Referente aos itens 3.1.4, o qual faz menção a "O serviço deve possuir infraestrutura de filtragem web

1. O item 3.1.11 deve ser alterado para o texto abaixo:

04/02/2025 17:27

"4.2.1.2. A licitante deverá apresentar uma carta ocial do Fabricante, para cada grupo de itens descritos,

Informo que o item 4.2.1.2 deve ser alterado para o texto abaixo:

04/02/2025 17:24

"Entendemos que deverá ser possível oferecer os serviços de SSE mesmo para equipamentos que não

04/02/2025 17:14

- Sobre o pagamento quesonamos: será pago à vista integralmente ou parcelado? caso seja parcelado qual

Informo que os itens 1.2 e 5.1 do Termo de Referência 1051286 detalham as unidades referenciais do objeto e

Incluir esclarecimento