
OFÍCIO N. 236/2024

ASSUNTO: Pedido de esclarecimentos ao Edital do PE nº 028/2024.

PROCESSO N. 8510187-89.2024.8.06.0000

Fortaleza, 23 de agosto de 2024.

Prezado(s) Senhor(es),

Em resposta ao questionamento enviado ao endereço eletrônico da Comissão Permanente de Contratação do TJCE, em 20/08/2024, às 16:19, por empresa interessada em participar da Pregão Eletrônico n. 028/2024, informo os esclarecimentos, que seguem:

Pergunta 01:

Em relação ao ofício nº 179/2024, assunto: Pedido de esclarecimentos ao Pregão Eletrônico nº 028/2024 (...). Pergunta 06: DO DIRECIONAMENTO DA SOLUÇÃO.

(...)

“De acordo com a resposta fornecida, a funcionalidade solicitada visa automatizar tarefas com base em critérios definidos, demonstrando que a realocação de ativos pode aprimorar significativamente a segurança e a eficiência na gestão desses ativos.

Reconhecemos que essa funcionalidade é de extrema importância para o TJCE. A automatização das tarefas, ao permitir a importação da estrutura do Active Directory, facilita a movimentação de novos ativos para Unidades Organizacionais específicas, possibilitando a instalação automatizada da solução. Além disso, a movimentação de ativos infectados para OUs específicas, com a ativação de GPOs de proteção e bloqueio, é crucial para garantir a segurança do sistema. No entanto, notamos que esse requisito essencial de acordo com o adendo publicado será excluído do edital e não mais considerado, o que contraria a resposta fornecida anteriormente.

Dada a importância crítica dessa funcionalidade para a segurança e eficiência operacionais, entendemos que o conjunto de requisitos técnicos mencionado no questionamento acima e confirmado pela resposta deste órgão, deve ser incluído na solução ofertada e continuará a ser exigido neste edital.

Nosso entendimento está correto?”

Resposta 01:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Pergunta 02:

Em relação ao ofício nº 179/2024, assunto: Pedido de esclarecimentos ao Pregão Eletrônico nº 028/2024 (...). Pergunta 08: DA FUNCIONALIDADE DE GERAR IMAGENS DE SISTEMAS OPERACIONAIS.

(...)

“De acordo com a resposta fornecida, a funcionalidade solicitada visa garantir a integridade e a segurança dos sistemas operacionais utilizados, permitindo a restauração rápida e eficiente de um estado limpo e seguro em caso de contaminação por malware ou outras ameaças.

Reconhecemos que a funcionalidade solicitada visa, portanto, garantir que as máquinas possam ser rapidamente restabelecidas a partir de imagens seguras, minimizando o impacto de eventuais infecções por software mal-intencionado e assegurando a integridade dos dados e a continuidade das operações no TJCE, reduzindo a necessidade de intervenção manual e aumentando a resiliência contra ameaças cibernéticas. No entanto, observamos que esse requisito essencial de acordo com o adendo publicado será excluído do edital e não mais considerado, o que contraria a resposta fornecida anteriormente?

Dada a importância crítica dessa funcionalidade para a segurança e eficiência operacionais, entendemos que este requisito, assim como o conjunto de requisitos técnicos mencionado no questionamento acima e confirmado pela resposta deste órgão, deve ser incluído na solução ofertada e continuará a ser exigido neste edital.

Nosso entendimento está correto?”

Resposta 02:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Pergunta 03:

Em relação ao ofício nº 179/2024, assunto: Pedido de esclarecimentos ao Pregão Eletrônico nº 028/2024 (...). Pergunta 09: DA FUNCIONALIDADE DE GERENCIAMENTO DE PATCHES.

(...)

“De acordo com a resposta fornecida, a funcionalidade solicitada visa garantir que todos os sistemas e aplicações estejam atualizados com as últimas correções de segurança, reduzindo o risco de exploração de vulnerabilidades conhecidas.

Reconhecemos que ao assegurar que os patches sejam aplicados de maneira consistente e oportuna, a solução promove uma proteção robusta contra ameaças cibernéticas, previne possíveis brechas de segurança e mantém a integridade dos dados e a operabilidade dos sistemas do TJCE. Esse processo também facilita a conformidade com normas de segurança e regulamentações aplicáveis, fortalecendo a postura geral de segurança da do Órgão. No entanto, observamos que o requisito essencial de acordo com o adendo publicado será excluído do edital e não mais considerado, o que contraria a resposta fornecida anteriormente.

Dada a importância crítica dessa funcionalidade para a segurança e eficiência operacionais, entendemos que a solução ofertada deverá ter a capacidade de não somente reconhecer, mas também, realizar a aplicação de patches para corrigir as vulnerabilidades detectadas nos endpoints. Este requisito, assim como o conjunto de requisitos técnicos mencionado no questionamento acima e confirmado pela resposta deste órgão, deve ser incluído na solução ofertada e continuará a ser exigido neste edital.

Nosso entendimento está correto?”

Resposta 03:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Pergunta 04:

“Em relação à alteração do item 3.4.1.1.8, onde anteriormente estava estipulado:

‘3.4.1.1.8. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;’ e que agora lê-se: ‘3.4.1.1.8. As licenças e proteção devem estar disponíveis durante toda a vigência do suporte e garantia;’ (...)

Sob a redação original, a condição de licenças perpétuas garantia que, mesmo após a expiração da licença, o produto continuaria a funcionar para a proteção contra ameaças, com base nas definições em vigor até o momento da expiração. Isso é fundamental para assegurar que, em caso de problemas na renovação da licença ou suporte, o órgão ainda teria proteção contra ameaças cibernéticas com as definições previamente adquiridas.

A nova redação, que condiciona a proteção à vigência do suporte e garantia, pode levar à interrupção da proteção contra códigos maliciosos caso o suporte e a garantia expirem, o que coloca em risco a segurança dos dados e sistemas do órgão. Sem uma proteção contínua garantida, o órgão pode enfrentar vulnerabilidades graves que podem ser exploradas por agentes maliciosos.

Além dos problemas de segurança, há uma preocupação adicional: a nova redação pode resultar na interrupção do acesso ao produto caso as licenças expirem. Isso não só compromete a continuidade da proteção, mas também coloca o órgão em uma posição de refém em relação ao fornecedor que vencer a licitação. Se o suporte e a garantia não forem renovados, o órgão pode enfrentar dificuldades para manter o acesso ao produto, forçando-o a negociar sob pressão e potencialmente enfrentar custos e condições desfavoráveis para a renovação ou substituição da solução.

Portanto, dada a importância crítica dessas alterações, entendemos que a solução ofertada deverá ser entregue com licenças perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer acessível e funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença.

Nosso entendimento está correto?”

Resposta 04:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Pergunta 05:

“Em relação à remoção dos itens 3.4.2.4.9, 3.4.2.4.10, 3.4.2.4.11 3.4.2.4.34, onde anteriormente estava estipulado:

‘3.4.2.4.9. Controle de acesso a sites por horário;’

‘3.4.2.4.10. Controle de acesso a sites por usuários;’

‘3.4.2.4.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;’

‘3.4.2.4.34. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;’

A filtragem de conteúdo de URL avançada, que inclui a classificação de sites em categorias, é uma funcionalidade crucial para garantir um nível adequado de proteção e controle sobre o acesso à internet. Esta capacidade permite a identificação e a restrição de sites potencialmente prejudiciais ou inapropriados, além de possibilitar a aplicação de políticas de segurança baseadas em categorias específicas de conteúdo. Sem essa funcionalidade, o órgão ficaria vulnerável a diversos riscos.

Primeiramente, em termos de segurança cibernética, a ausência de filtragem avançada pode permitir o acesso a sites maliciosos, comprometendo a integridade e a segurança dos sistemas do órgão. A classificação de sites é essencial para bloquear conteúdo nocivo e prevenir ataques cibernéticos.

Além disso, a conformidade e proteção de dados são comprometidas sem esse recurso. Muitos órgãos devem seguir regulamentos e políticas que exigem o bloqueio de certos tipos de conteúdo. A remoção desse requisito pode resultar em violações de conformidade e possíveis penalidades legais.

A produtividade e a proteção de recursos também são impactadas. A filtragem avançada contribui para a eficiência ao restringir o acesso a sites não relacionados ao trabalho. Sem essa funcionalidade, pode haver um aumento no tempo gasto em atividades não produtivas e no consumo desnecessário de largura de banda.

Por fim, a falta de capacidade para classificar e filtrar sites pode expor os usuários a conteúdos impróprios ou não autorizados, afetando a reputação da organização e criando riscos adicionais.

Diante desses pontos, a remoção dos itens acima citados representa um sério risco para a segurança e a eficácia das operações do órgão. Portanto, entendemos que este conjunto de requisitos técnicos devem ser incluídos na solução ofertada e continuará a ser exigido neste edital.

Nosso entendimento está correto?”

Resposta 05:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Pergunta 06:

“Em relação à remoção do item 3.4.2.4.26, onde anteriormente estava estipulado: ‘3.4.2.4.26. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.’

A detecção de ameaças na BIOS ROM é uma funcionalidade crítica para garantir a segurança completa dos endpoints. A BIOS ROM, sendo um componente essencial que carrega o sistema operacional e controla o hardware, pode ser alvo de ataques sofisticados que visam comprometer a integridade do sistema desde seu início.

A ausência dessa capacidade pode representar um sério risco de segurança. Sem a detecção de ameaças na BIOS, o TJCE pode ficar vulnerável a ataques que podem não ser identificados por soluções de segurança tradicionais. Esses ataques podem resultar em comprometimento total dos endpoints, além de permitir que atacantes mantenham controle persistente e não detectado sobre os sistemas.

Além dos riscos de segurança, a remoção desse requisito pode afetar a conformidade com políticas de segurança e regulamentações que exigem proteção abrangente contra

todas as formas de ameaça, incluindo aquelas que se instalam na BIOS. Ignorar essa proteção pode levar a violações de conformidade e possíveis repercussões legais.

Garantir a segurança completa dos endpoints, desde o nível da BIOS, é fundamental para proteger a integridade e a segurança dos sistemas do TJCE.

Portanto, entendemos que o requisito técnico citado acima deve ser incluído na solução ofertada e continuará a ser exigido neste edital.

Nosso entendimento está correto?"

Resposta 06:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Pergunta 07:

"Em relação à remoção dos itens 3.4.1.1.34, 3.4.1.1.35, 3.4.1.1.36, 3.4.1.1.37, 3.4.1.1.38, 3.4.1.1.39, 3.4.1.1.40, 3.4.1.1.41 e 3.4.1.1.42 (...)

A capacidade de importar a estrutura do Active Directory e usar diversas técnicas de descoberta de dispositivos é crucial para garantir uma visibilidade completa e uma gestão eficaz da proteção de endpoints. Essas funcionalidades permitem a detecção de novos dispositivos e a integração contínua de máquinas à proteção, o que é essencial para manter a segurança da rede e a conformidade com políticas de segurança.

Sem a capacidade de descobrir novos dispositivos e monitorar subnets e grupos de trabalho, o TJCE corre o risco de deixar dispositivos novos ou não autorizados fora do escopo de proteção. Isso pode resultar em lacunas significativas na segurança, permitindo que dispositivos vulneráveis permaneçam não monitorados e expostos a possíveis ameaças. Além disso, a falta dessas capacidades pode dificultar a administração eficiente da solução e a resposta rápida a novos dispositivos que necessitam de proteção.

Garantir uma detecção abrangente e a proteção de todos os dispositivos é essencial para manter a integridade e a segurança do ambiente de TI.

Diante desses pontos, a remoção dos itens acima citados representa um sério risco para a segurança e a eficácia das operações do órgão. Portanto, entendemos que este conjunto de requisitos técnicos devem ser mantidos na solução ofertada e continuará a ser exigido neste edital.

Nosso entendimento está correto?"

Resposta 07:

O entendimento não está correto. Os questionamentos e impugnações apresentadas destacam a necessidade de ajustes para um ambiente mais justo e competitivo, sem nenhuma deficiência e/ou comprometimento de funcionalidade da solução para o TJCE, uma vez que essa atividade poderá ser realizada de várias formas distintas.

Atenciosamente,

PREGOEIRO DA COMISSÃO PERMANENTE DE CONTRATAÇÃO DO TJCE

Às empresas interessadas em participar do Pregão Eletrônico nº 028/2024.