

COMPRASNET

Pregão Eletrônico



Esclarecimento 18/11/2020 08:53:50

1 - Considerando que foi editada a Medida Provisória n. 983, de 16 de junho de 2020, a qual dispõe sobre as assinaturas eletrônicas em comunicações com entes públicos, e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos. Assim, com base na validade reconhecida para a assinatura eletrônica em todos os poderes do Estado (inclusive nos processos judiciais eletrônicos, tais como SEI, PJe, Projudi, eProc, etc.), e também nos dispositivos e na expressa previsão de racionalização dos procedimentos administrativos da Lei 13.726/2018. Entendemos que, tendo em vista todo este contexto legal, aliado aos demais normativos que regem a assinatura eletrônica de documentos, esse órgão permitirá, que as proponentes licitantes possam apresentar suas propostas e demais documentos solicitados, exclusivamente por via eletrônica, desde que assinada digitalmente através da estrutura de chaves pública e privada (e-cpf), dispensando a apresentação desses mesmos documentos pelo meio físico (de papel). Está correto o nosso entendimento? Dessa maneira, os documentos de Proposta Comercial, Técnico e Declarações poderão ser enviadas com assinatura Eletrônica. 2 - Decorrendo análise dos termos dispostos no instrumento convocatório n. 20/2020 desse MDR, identificamos junto ao item 9.11, exigência de comprovação de aptidão para prestação de "serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente", entretanto, consta como "características mínimas" o suporte técnico apenas para a produtos "Veritas". Prezando pela ampliação da competitividade e adstrito a busca da proposta mais vantajosa, capaz de trazer maiores benefícios financeiros a esse órgão, é essencial oferecer igual tratamento aos que desejam participar do processo, conforme expresso no art. 3º da Lei n. 8666/93, oferecendo assim, ao nosso ver, a isonomia necessária e a maior amplitude do número de participantes no certame. Considerando a quantidade de fabricantes representadas por diversas revendas junto ao mercado e que são aptas a demonstrar experiência obtida através da comercialização de outros produtos, entendemos que "serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente" podem ser demonstrados através da aptidão adquirida com fornecimento de suporte técnico de licenciamento de produtos de outros fabricantes, desde que comprovada a aptidão com produto VERITAS através de declaração do fornecedor. Está correto o nosso entendimento?

Fechar

COMPRASNET
Pregão Eletrônico



Resposta 18/11/2020 08:53:50

1 - Resposta: Sim. Está correto o entendimento. Citam-se os itens 5.1 e 5.2 do Edital: 5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio desse documento; 5.2 O Envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha. 2 - Resposta: Está correto o entendimento. Visando ampliar a competitividade do certame, serão aceitos atestados de soluções similares em conjunto com declaração de capacidade do fabricantes Veritas.

Fechar



Esclarecimento 24/11/2020 09:08:57

“4.8.32. Deve possuir arquitetura baseada em camadas que permita a proteção contra “ransomware attack”, independente do software de backup, com as seguintes características: a) No caso de equipamentos com multi-camadas de armazenamento, deve possuir pelo menos uma camada isolada do acesso externo, onde os dados retidos ao longo do tempo devem ser armazenados; b) Esta camada deve ser isolada logicamente da demais camadas e o acesso aos dados ali armazenados deve ser através de comunicação exclusiva, interna do equipamento, não podendo ser através de protocolos padrão de mercado, como CIFS, NFS e OST; c) Deve possuir configuração de atraso de deleção, de pelo menos 15 dias, que permita a recuperação de dados mesmo quando o pedido de expiração/deleção seja feito pelo software de backup; d) Os dados armazenados na camada isolada devem ser sempre imutáveis, ou seja, não podem ser alterados, apenas removidos mediante expiração do backup; e) Caso o equipamento ofertado possua outro tipo de arquitetura ou não possua todas as características solicitadas no item anterior e subitens, deve ser entregue com um segundo equipamento (para cada unidade contratada no certame), possuindo as mesmas características do equipamento primário, juntamente com um mecanismo que realize o filtro da replicação de dados entre eles para isolar os dados replicados do repositório primário e impedir a propagação do ataque de ransomware no momento da sincronização entre os sistemas (Air-Gap, Atraso de Sincronismo). Todos os componentes para o funcionamento dessa proteção devem ser fornecidos com a solução.” Visto os últimos ataques de hackers, principalmente em Órgãos da Administração Pública, é totalmente compreensível a solicitação de proteção contra-ataques de Ransomware. Entretanto, as características de proteção requisitadas, por si só não garantem essa proteção, uma vez que os dados podem ser criptografados na camada primária/de entrada (não isolada) antes de serem migradas para a área imutável como descrito no item. A solução a ser ofertada por esta Proponente, é mais segura e superior pois possui funcionalidades que impedem o acesso não autorizado aos volumes de armazenamento dedicado ao backup já na área primária/de entrada através de soluções de segurança independente do software de backup, tais como sistema de detecção de intrusos e sistema de prevenção de intrusos sem qualquer ônus adicional e que foram comprovadas em eventos de segurança (Black Hat) como impenetráveis por 5 anos consecutivos. Entendemos que serão aceitas soluções que oferecem funcionalidades já comprovadas contra ataques de ransomware, em conformidade ao requisito “proteção contra ransomware”. Está correto o nosso entendimento?

Fechar

COMPRASNET
Pregão Eletrônico



Resposta 24/11/2020 09:08:57

O entendimento está parcialmente correto. As funcionalidades contra ataques de ransomware que não se enquadram nos subitens "a", "b", "c" e "d" do item 4.8.32 podem ser ofertadas desde que acompanhem um segundo equipamento (para cada unidade contratada no certame), possuindo as mesmas características do equipamento primário, conforme especificado no subitem "e".

Fechar

COMPRASNET
Pregão Eletrônico



Esclarecimento 24/11/2020 09:09:14

Entendemos que o item 4.8.32 "e" deve ser atendido caso a solução não atenda os itens 4.8.32 "a", "b", "c" e "d", está correto nosso entendimento?

Fechar

COMPRASNET Pregão Eletrônico



Resposta 24/11/2020 09:09:14

Resposta: Sim, está correto o entendimento.

Fechar

**Esclarecimento** 24/11/2020 09:09:37

Com relação ao item: 4.8.12. Todos os valores de capacidade de armazenamento deste documento devem ser calculados considerando o sistema de cálculo BASE 2, ou seja, 1 Terabyte (TB) é igual a 1024 Gigabytes (GB)", gostaríamos de esclarecimento sobre qual metodologia de cálculo deve ser considerada. TB em BASE 2 é, de acordo com a literatura de tecnologia da informação, relativo a TiB, onde cada TB corresponde a 0,909495 TiB. Dessa forma, se considerarmos que o pedido é por 200TiBs (Tebibytes, base 2) corresponderiam a 219TB (Terabytes, Base 10). Se considerarmos a conversão informada, onde cada TB corresponde a 1024GB, teremos 204,8TB como resultado. Sendo fato que TB Base 2 não corresponde a 1024GB (e sim a 10244 bytes) e que a conversão correta de TB (Terabyte) para GB (Gigabyte) é por 1000 e não por 1024, gostaríamos de esclarecer qual base de cálculo deve ser utilizada, já que as referências do requisito estão confusas.

Fechar

COMPRASNET Pregão Eletrônico



Resposta 24/11/2020 09:09:37

Resposta: Favor considerar 1TB = 1000GB

Fechar

**Esclarecimento 25/11/2020 10:37:48**

Com o objetivo de entender adequadamente a funcionalidade solicitada de proteção contra ataques cibernéticos do tipo Ransomware Attack, solicitamos os seguintes esclarecimentos: "4.8.32. Deve possuir arquitetura baseada em camadas que permita a proteção contra "ransomware attack", independente do software de backup, com as seguintes características: a) No caso de equipamentos com multi-camadas de armazenamento, deve possuir pelo menos uma camada isolada do acesso externo, onde os dados retidos ao longo do tempo devem ser armazenados; b) Esta camada deve ser isolada logicamente da demais camadas e o acesso aos dados ali armazenados deve ser através de comunicação exclusiva, interna do equipamento, não podendo ser através de protocolos padrão de mercado, como CIFS, NFS e OST; c) Deve possuir configuração de atraso de deleção, de pelo menos 15 dias, que permita a recuperação de dados mesmo quando o pedido de expiração/deleção seja feito pelo software de backup; d) Os dados armazenados na camada isolada devem ser sempre imutáveis, ou seja, não podem ser alterados, apenas removidos mediante expiração do backup; e) Caso o equipamento ofertado possua outro tipo de arquitetura ou não possua todas as características solicitadas no item anterior e subitens, deve ser entregue com um segundo equipamento (para cada unidade contratada no certame), possuindo as mesmas características do equipamento primário, juntamente com um mecanismo que realize o filtro da replicação de dados entre eles para isolar os dados replicados do repositório primário e impedir a propagação do ataque de ransomware no momento da sincronização entre os sistemas (Air-Gap, Atraso de Sincronismo). Todos os componentes para o funcionamento dessa proteção devem ser fornecidos com a solução." QUESTIONAMENTO 1: 1- Entendemos que a arquitetura em camadas descrita no item 4.8.32 refere-se à possibilidade de segmentar o armazenamento em diferentes volumes, cada um com características únicas de armazenamento como, por exemplo, um volume com retenção baseada em tecnologia WORM (Write Once Read Many) e outro volume sem essa característica. Está correto o nosso entendimento? QUESTIONAMENTO 2: 2- Entendemos que se considera uma camada isolada do acesso externo para armazenamento de dados ao longo do tempo, uma determinada camada configurada no Appliance de Backup Enterprise protegida por mecanismos de segurança. Está correto o nosso entendimento? QUESTIONAMENTO 3: 3- Entendemos que o atraso de deleção pode ser configurado por funcionalidade WORM (Write Once Read Many), onde cada imagem de backup receberá um parâmetro de retenção de acordo com as políticas de retenção definidas pelo software de backup. Está correto nosso entendimento? QUESTIONAMENTO 4: 4- Entendemos que, ao prover uma solução que garanta o isolamento e a imutabilidade através de bloqueio de retenção baseado em padrão NAS-WORM, estaremos atendendo ao requerimento. Está correto nosso entendimento? QUESTIONAMENTO 5: 5- Entendemos que a solução que possibilita um administrador do equipamento reverter o estado de bloqueio de retenção do(s) arquivo(s) através das interfaces de administração atende o requerimento de atraso de deleção solicitado no item 4.8.32 subitem "c", ao possibilitar criar um processo ou scripts de automação para essa tarefa. Está correto nosso entendimento?

**Resposta 25/11/2020 10:37:48**

RESPOSTA 1: Não está correto o entendimento. Os dados devem ser armazenados pelo software de backup exclusivamente na camada exposta (camada de recepção de dados) e copiados/movidos para camada que seja de acesso exclusivamente interno no Appliance de Backup (camada de retenção de dados). Essa última não pode estar exposta à rede LAN/SAN), criando uma espécie de Air-Gap entre as camadas. Os dados armazenados na camada de retenção devem ser protegidos contra deleção imediata através de um atraso, conforme subitem 'c', sem que seja imposto o prazo total original de retenção (como a tecnologia WORM pressupõe). Caso a solução ofertada não funcione assim, ela deve ser fornecida de acordo com o descrito no subitem "e". RESPOSTA 2: Não está correto o seu entendimento. A camada isolada deve ser nativa da solução ofertada e somente acessível por intermédio do seu software interno, sem que seja necessário configurar esse isolamento ou instalar qualquer software ou programa adicional no equipamento ou no ambiente. RESPOSTA 3: Não está correto o seu entendimento. O atraso de deleção deve ser independente da política de retenção estabelecida pelo software de backup e nativa do equipamento de armazenamento. RESPOSTA 4: O entendimento não está correto. Deve existir a capacidade de atrasar a deleção dos dados expirados por um determinado número de dias, desde que os dados armazenados não possam ser alterados e estejam em uma camada que não seja exposta a nenhuma rede (LAN, WAN, SAN). Alternativamente será aceita solução que proporcione cópia adicional atrasada (réplica), onde expirações de dados no repositório de retenção primário não afetem de imediato a réplica, que deve ser isolada. Em qualquer das situações todos os componentes de Hardware e Software necessários devem ser fornecidos, licenciados e implementados. RESPOSTA 5: O entendimento não está correto. A funcionalidade de atraso de deleção deve ser nativa do equipamento, atender os requerimentos mínimos do item 4.8.32 e subitens, não sendo aceitas composições, processos ou scripts para o fornecimento de tal funcionalidade.