procempa

23.12.000001330-3

# LICITAÇÃO ELETRÔNICA 06/2025

**Contratação de solução de segurança de E-mail (Secure E-mail Gateway – inbound e outbound)**

## ESCLARECIMENTOS

**Questionamento 01:** No item 4.10 A solução, com necessidade de assegurar alta disponibilidade, deve ser apresentada na forma de Appliance Virtual (conjunto de máquina virtual, sistema operacional e aplicação) compatível com a plataforma Vmware, devendo suportar plataforma de virtualização VMware Vsphere versão 7 ou superior.

Entende-se que devem ser fornecidas 2 VMs licenciadas para garantir a alta disponibilidade solicitada?

No item 3.2. Os fornecedores da solução devem apresentar documentos de atestados de capacidade técnica- operacional, com comprovação de fornecimento e de prestação de serviços semelhantes em outras empresas, que atestem que instalaram, configuraram e sustentaram soluções de segurança com esse objeto, em outros clientes, públicos e/ou privados

Entende-se como semelhante a implantação de uma solução de segurança de e-mail, não necessariamente da mesma marca ou modelo ofertada?

**Resposta 01**: Está correto o entendimento nos itens 4.10 e 3.2.

**Questionamento 02:**No item 4.14. do Anexo I está descrito - "A solução entregue deverá suportar a expansão de funcionalidades tais como: Data Loss Prevention (DLP), compliance e criptografia por meio de aquisição e ativação de licenças, sem a necessidade de aquisição de novos equipamentos de hardware e software de terceiros". Assim sendo, entendemos que essas funcionalidades deverão ser contempladas pela solução, porém, não serão contratadas nesse momento e não deverão ser ofertadas, permitindo a aquisição e implementação destes módulos em futura expansão/upgrade, sem modificação na arquitetura da solução. Está correto nosso entendimento?

**Resposta 02**: O entendimento está parcialmente correto. As funcionalidades podem ser ofertadas sim, mas se não forem ofertadas, o que não é exigido nesse processo, quando, e, se forem inseridas e/ou licenciadas, em momento posterior, devem ser aderentes à solução, sem necessidade adquirir novos equipamentos de hardware e software de terceiros para seu funcionamento.

**Questionamento 3:**Nos itens 4.129. – 4.137 do Anexo I encontram-se diversas referências ao termo ”CRIPTOGRAFIA”. Considerando que o item 4.14. do referido Anexo descreve que o módulo de criptografia deverá ser suportado em futura expansão, mas não contratado nesse momento, entendemos que esses Itens apenas referenciam o que deverá ser contemplado pelo módulo de Criptografia, se e quando ele for contratado. Deste modo, entendemos que esses itens são meramente informativos e suas funcionalidades não serão exigidas nesse momento. Está correto nosso entendimento?

**Resposta 03:** Caso o módulo de criptografia seja disponibilizado na solução ofertada, os itens 4.129, 4.130, 4.131, 4.132, 4.133, 4.134, 4.135, 4.136, 4.137, devem ser atendidos imediatamente. Caso não seja disponibilizado e esse módulo venha a ser inserido em momento posterior, a solução deve estar apta a atender esses itens descritos, imediatamente, no momento em que forem incorporados à solução.

**Questionamento 04:** No Item 4.120. do Anexo I encontra-se a seguinte descrição - "A proteção URL deverá acompanhar o destinatário na URL reescrita. Quando uma mensagem for dirigida a vários destinatários, o envelope será dividido de modo que existam apenas um receptor associado com uma URL reescrita para permitir que administradores possam controlar quais usuários clicaram na URL reescrita". No nosso entendimento, não está claro o requisito do item e solicitamos mais informações sobre o mesmo, no sentido de compreender a ação esperada.

**Resposta 04:** Se ficaram claros os itens 4.115, 4.116, 4.117, 4.118 e 4.119, a única novidade no item 4.120 é que ele requer que também estejam contempladas, nos eventos de interceptação e análise, para reescrita das URLs potencialmente maliciosas, também os endereço de e-mail que identificam grupos de usuários de e-mail, tipicamente, endereços SMTP de listas de distribuição. O objetivo é garantir que cada usuário tenha uma URL de reescrita única para permitir rastreamento de quem clicou nessa URL. Quando um e-mail é enviado para um grupo de pessoas (lista de distribuição), deve-se criar URLs individuais para cada usuário, dividindo o envelope do e-mail, que foi enviado para o endereço do grupo, para endereços dos usuários do grupo.

**Questionamento 05:** No Item 4.138. do Anexo I encontra-se a seguinte descrição - "Deve suportar o algoritmo de criptografia AES192 bits". Considerando o Gartner Magic Quadrant for E-mail Security Platforms 2024, com a lista dos principais fornecedores de soluções de e-mail gateway, todos oferecem módulos de criptografia AES256, sabidamente uma proteção mais robusta e mais resistente a ataques de força bruta. Nesse sentido, entendemos que seria adequado a solicitação mínima de criptografia AES256 objetivando um melhor nível de proteção para o ambiente de correio eletrônico. Está correto nosso entendimento?

**Resposta 05:** O entendimento está parcialmente correto. A especificação requer que o tamanho da chave seja de 192 bits, o que não impede que seja de 256 bits. Portanto, deve, no mínimo, suportar algoritmo de criptografia com chave de 192 bits e a solução pode entregar algoritmo de criptografia AES-256.

Questionamento 06: No Item 4.139 do Anexo I encontra-se a seguinte descrição - "A solução deve possuir console única de gerenciamento para interface de criptografia, compliance, antispam e antivírus, ou seja, para todos os módulos exigidos e suportáveis da solução". Considerando que se trata de módulos distintos, muitas vezes ocorre que determinadas funcionalidades operam melhor com uma console específica ao invés de uma console única e genérica e que essa não consiga cobrir em detalhes todas as funcionalidades. Por outro lado, considerando que as consoles são interligadas (do mesmo fabricante) e que de uma console é possível navegar-se para outra console, sem um novo acesso ou abertura de outra interface, entendemos que dessa forma a solução estaria contemplando o requisito do item. Está correto nosso entendimento?

**Resposta 06:** Está correto o entendimento.

**Questionamento 07:** No item 8 do Anexo I - Termo de Referência estão descritos requisitos de treinamentos da solução ofertada, na modalidade hands-on, abrangendo aspectos para administração e gerenciamento da solução e ministrado por profissionais com certificações do fabricante. No item 9.7 do mesmo anexo, sobre Prazos e Condições, abordando o treinamento, é referenciado treinamento oficial do fabricante. Apresentadas essas observações, entendemos que o treinamento na modalidade hands-on pode ser ministrado por profissionais certificados da empresa contratada (parceiro do fabricante) e

não obrigatoriamente ser ministrado por profissionais do próprio fabricante. Está correto nosso entendimento?

**Resposta 07:** Está correto o entendimento.

**Questionamento 08:** No item 8.1.5 do Anexo I estão descritas exigências para o ambiente do treinamento hands-on, no formato EAD. Considerando o volume mínimo de horas de treinamento e o requisito máximo de 4horas/dia, e ainda os custos adicionais para configuração e manutenção da infraestrutura necessária, perguntamos: seria possibilitado o uso de recursos da Procempa para a infraestrutura do treinamento, levando-se em conta a realização em um cenário mais próximo possível do ambiente de operação da Procempa?

**Resposta 08:** Nesse item 8.1.5 é esperado que o fornecedor da solução possua plataformas virtuais de ambientes de treinamento, assim como, geralmente possui, ambientes para demonstração de degustação de seus produtos e navegação por suas funcionalidades e utilização. É nesse cenário que foi imaginado o treinamento no modelo hands-on, a ser ministrado no decorrer da implantação. Não está garantido o provisionamento de ambiente virtualizado para esse tipo de treinamento na infraestrutura da Procempa e, não estando garantido, ele precisa ser disponibilizado para cumprir essa etapa de treinamento.

**Questionamento 09:** Considerando a amplitude do ambiente de correio eletrônico e a complexidade para gerenciar um alto volume de mensagens de diferentes orgãos e entidades do município, sob a responsabilidade tecnológica da Procempa, entendemos como essencial a adoção de uma solução de secure e-mail gateway desenvolvida e mantida integralmente por um mesmo fabricante. Essa abordagem assegura a funcionalidade completa do sistema, além de garantir desenvolvimento, atualizações e suporte contínuo. Fatores como suporte 24x7, SLAs de atendimento, atualizações constantes, correção de vulnerabilidades, segurança avançada e inteligência de ameaças - incluindo análise comportamental, machine learning, equipes especializadas em pesquisa e bases próprias de ameaças - são necessários. Além disso, conformidades e certificações como LGPD, ISO 27001, SOC 2/3 também devem ser considerados. Com base nesses critérios, entendemos que soluções construídas pela integração de módulos escritos como código aberto (open source) por diferentes desenvolvedores não serão aceitas nas propostas para esse certame. Está correto nosso entendimento?

**Resposta 09:** No item de Habilitação técnica, é requerido que os fornecedores enviem e façam conhecer os datasheets de sua solução, possibilitando a comprovação do atendimento da especificação técnica da solução completa. Somente nesse momento, da Habilitação Técnica, serão avaliados todos os itens e se os mesmos tem adesão aos requisitos técnicos solicitados. A priori, não se pode antecipar nada sobre qualquer tipo de integração, sem conhecermos a integralidade, conjunto e/ou partes do que será ofertado como solução de Secure E-Mail Gateway. Portanto, como o pedido de esclarecimento não se refere a nenhum item específico da especificação técnica, se configura uma hipótese, que pode nem se tornar realidade, não tendo esclarecimentos de entendimento a manifestar no momento presente.