PREGÃO ELETRÔNICO 03/2020

Objeto (resumido): Aquisição de solução para gestão de acessos privilegiados (Privileged Access Manager - PAM)

Pedido de Esclarecimentos nº 05

Às 16:59h do dia 17 de novembro de 2020, foi recebido pedido de esclarecimento no endereço eletrônico licitacoes@agerio.com.br, conforme descrito a seguir:

"(...) solicita esclarecimentos acerca do PE 03/2020 cujo objeto é Aquisição de solução para gestão de acessos privilegiados (Privileged Access Manager - PAM).

Questionamento 01:

No item

2.2.1.2.26 A solução deve ser rotineiramente testada quanto a vulnerabilidades, tendo testes de penetração executados por uma organização terceira. Este teste deve ser comprovado através de um documento oficial da empresa, se possível público na página Web da companhia ou da companhia terceira que executou o teste.

Dúvida: A comprovação dos testes de penetração/vulnerabilidades é necessária para todos os componentes da solução ofertada, inclusive para o componente "2.2.1.13 PORTAL DE ACESSO REMOTO SEGURO". Está correto o nosso entendimento?

Questionamento 02:

Nos itens

2.2.1.12.2.3 A solução deve continuar funcionando localmente mesmo com a falha de um dos nós, em uma das 02 (duas) localidades, TODOS os elementos que compõem a solução, devem ser instalados em regime de alta disponibilidade:

2.2.1.12.2.3.1 A solução deve replicar as configurações nas 02 (duas) localidades, de modo que, no evento de falha total de seus elementos instalados em uma localidade, a solução continue disponível via uso dos elementos da outra localidade;

2.2.1.12.3 O modelo mínimo de funcionamento e tolerância a falhas a ser implantado é:

2.2.1.12.3.1 Site principal: Ativo;
2.2.1.12.3.2 Site secundário: Ativo;

2.2.1.12.4 O acesso primário (em situação normal) dos usuários à solução deve ser sempre via os elementos instalados em sua rede local.

Dúvida 1: O modelo de tolerância a falhas que deve ser apresentado é Ativo/Ativo, onde ambos os componentes da solução estarão funcionais, por completo, nos dois datacenters, está correto nosso entendimento?

Dúvida 2: É correto afirmar que o ambiente deve ter dois nós ativos em dois datacenters, ambos completamente funcionais e sem dependências um do outro. No caso de queda em um dos lados, nenhuma ação é necessária para habilitar o outro lado, ou torná-lo um nó

funcional. Logo não haveria um nó primário, uma vez que ambos devem estar ativos e com possibilidade de ações/mudanças em ambos os datacenters. Está correto o nosso entendimento?

Questionamento 03:

Nos itens:

2.2.1.13 PORTAL DE ACESSO REMOTO SEGURO
2.2.1.13.1 Integrado à solução ou através de módulo adicional, desde que do fabricante, deverá ser fornecido portal de acessos seguros totalmente integrado ao cofre de senhas;

Dúvida 1: Entendemos que o item se refere a solução de acesso remoto, totalmente integrada à solução de cofre de senhas. O módulo adicional de acesso remoto deverá ser atendido por um gateway de acesso independente ao gateway do módulo do cofre de senhas. Uma vez que, por questões de segurança e acessos advindos da internet, o acesso remoto não poderia acessar o gateway de acesso interno (e protegido) do cofre de senhas. Está correto o nosso entendimento?

Dúvida 2: Entendemos ainda que o módulo adicional da solução de acesso remoto, por questões de segurança, não poderá se utilizar de serviços de VPN (Virtual Private Network), nem protocolos como RDP de fora para dentro da rede (apenas por jumpservers internos), para entregar tal funcionalidade. Está correto o nosso entendimento?

Questionamento 04:

No item

2.2.1.13.5 A solução, ou módulo adicional, deve evitar o uso de protocolos de comunicação legados necessários para acesso, dando preferência a um protocolo totalmente criptografado, como por exemplo TLS 1.2;

Dúvida1: Os protocolos de comunicação legados citados aqui, incluem RDP e SSH?

Dúvida2: O item 2.2.1.13.5 visa que a solução de acesso remoto não trafegue de fora para dentro usando protocolos legados, sendo preferível a criptografia de fim a fim. Ou seja, o usuário externo deve ser criptografado até o dispositivo a ser acessado, através de TLS ou outra forma de criptografia. Está correto o nosso entendimento?

Questionamento 05:

No item

2.2.1.13.7 Solução, ou módulo adicional, deve suportar a injeção automática de credenciais, permitindo que os usuários autentiquem ou elevem privilégios para sistemas remotos, sem revelar credenciais e senhas de texto simples. Permitindo que os usuários selecionem a credencial a ser utilizada a partir de lista de credenciais que têm privilégios nos sistemas aprovados para acesso;

Dúvida: Uma vez que seria inseguro uma "perna" do cofre de senhas para o acesso externo, acreditamos que a única forma de oferecer a funcionalidade de acesso remoto, sem adicionar riscos a rede, é ter uma solução específica para o acesso. Sem ter uma interface

de acesso externa ligada diretamente ao cofre, ou trafegando protocolos inseguros para acessos externos da internet (ex. RDP e SSH) para dentro da rede de forma direta. Sendo necessário um jump server local para assegurar acessos seguros de RDP e SSH. Está correto afirmar que a solução ou módulo adicional de acesso remoto, deve permitir a integração ao cofre de senhas, e não uma parte do cofre de senhas em si para esta função. Está correto o nosso entendimento?

Questionamento 06:

No item

10.1.1.1 Na primeira parcela serão faturados: as licenças da solução; os serviços de instalação, configuração e passagem de conhecimento; e os primeiros 12 (doze) meses do serviço de suporte e subscrição da solução;

Dúvida: No item acima, podemos ver referenciadas as licenças da solução. Por este motivo, entendemos que toda a oferta da solução, incluindo o módulo "2.2.1.13 Portal De Acesso Remoto Seguro", deve ser baseada em implementação ON-PREMISSE e licenças perpétuas. Como também que após o tempo de garantia e suporte do contrato, as licenças continuaram em funcionamento, apenas sem direito a atualização de versão. Está correto nosso entendimento?

Questionamento 07:

Nos itens

2.2.1.2 ESPECIFICAÇÃO TÉCNICA;

ANEXO II - FORMULÁRIO DE PROPOSTA DE PREÇOS

Dúvida: No item "2.2.1.2 ESPECIFICAÇÃO TÉCNICA" estão descritas todas as características técnicas obrigatórias da solução ora adquirida. Como também, no item "ANEXO II - FORMULÁRIO DE PROPOSTA DE PREÇOS" orienta que a proposta deverá conter o detalhamento de custos de cada item sob pena de inabilitação no certame.

A fim de permitir que o AGE-RJ consiga identificar o atendimento técnico de cada item na proposta comercial, entendemos que a proposta vencedora deverá ser entregue com a comprovação de atendimento técnico do tipo ponto-a-ponto aonde deverão ser apontadas na documentação do fabricante o atendimento aos requisitos técnicos do edital. Está correto o nosso entendimento?

(...)"

A Agência de Fomento do Estado do Rio de Janeiro S.A. – AgeRio, instituição financeira de fomento fiscalizada pelo Banco Central do Brasil – BACEN, sociedade de economia mista cuja personalidade jurídica é de direito privado, dotada de orçamento empresarial próprio e autonomia administrativa e financeira, por intermédio de seu pregoeiro titular, apresenta a resposta aos esclarecimentos formulados pelo interessado:

RESPOSTAS AO QUESTIONAMENTO nº 1:

a) Tendo em vista a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, entendemos que todos os servidores que compõem a solução de PAM deverão ser testados quanto a vulnerabilidades, sejam eles físicos ou virtuais, na tentativa de explorar (teste de penetração) qualquer tipo de vulnerabilidade encontrada nos mesmos, sejam elas no SO (sistema operacional) ou quaisquer módulos componentes da solução de PAM.

RESPOSTAS AO QUESTIONAMENTO nº 2:

a) Segundo a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, informa-se que com relação a Dúvida nº 1, sim, está correto o vosso entendimento. Relativamente a Dúvida nº 2, informa-se que é necessário que os mesmos sincronizem todas as configurações e/ou dados (logs de acesso e etc.) entre eles. De fato não há um nó primário, mas, conforme o item "2.2.1.12.4" do edital citado anteriormente, existe um nó preferencial para acesso e o outro, apesar de "ATIVO", ficará como contingência.

RESPOSTAS AO QUESTIONAMENTO nº 3:

a) Considerando a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, informa-se que com relação a Dúvida nº 1, não é vedado o fornecimento do módulo adicional de acesso remoto utilizando um gateway independente. A liberação de acessos quando advindos da internet, será avaliada pela equipe técnica da AgeRio quando da execução do projeto. Relativamente a Dúvida nº 2, nos cabe informar que a utilização, ou não, de VPN ou protocolos como RDP, será avaliada pela equipe técnica da AgeRio quando da execução do projeto.

RESPOSTAS AO QUESTIONAMENTO nº 4:

a) Tendo em vista a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, informa-se, com relação a Dúvida nº 1, que sim, desde que estes estejam utilizando protocolos de criptografia obsoletos. Relativamente a Dúvida nº 2, informa-se que o entendimento está correto, desde que também considere os usuários internos.

RESPOSTAS AO QUESTIONAMENTO nº 5:

a) Segundo a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, conforme informado anteriormente, não é vedado o fornecimento do módulo adicional de acesso remoto utilizando um gateway independente (jump server local). A liberação de acessos quando advindos da internet, será avaliada pela equipe técnica da Agerio quando da execução do projeto.

RESPOSTAS AO QUESTIONAMENTO nº 6:

a) Considerando a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, comunica-se que está correto o vosso entendimento.

RESPOSTAS AO QUESTIONAMENTO nº 7:

a) Tendo em vista a manifestação técnica formal da área de Tecnologia da Informação da AgeRio, exarada na data de hoje (19/11/2020) e constante dos autos do processo administrativo, informa-se que a empresa arrematante poderá apresentar documento técnico (posterior ao pregão) do tipo ponto-a-ponto, a fim de agilizar as atividades da equipe técnica da AgeRio.