PROCESSO:	065.10933.2024.0004168-84
OBJETO:	<Insira aqui o objeto do processo>
ÓRGÃO INTERESSADO:	<Insira aqui o órgão interessado>

RESPOSTA

Em resposta aos questionamentos da empresa ICTS contidos no documento SEI nº 00099257699, respondemos:

Questionamento 01: "**Em relação ao Processo Administrativo n° 24/049-00, Processo SEI nº 065.10933.2024.0004168-84, que tem por objeto Implantação de sistema de registro de preço para eventual contratação, através de subscrição, de solução automatizada de conscientização em segurança da informação, incluindo testes de phishing e treinamento através de diversos recursos: treinamento baseado em computador (CBT), módulos interativos, vídeos, jogos, cartazes e documentos de segurança da informação, pelo período de 36 (trinta e seis) meses, solicitamos esclarecimento sobre:**
Atestado de capacidade técnica: é obrigatório a apresentação de um atestado que comprove o fornecimento de 30.000 licenças? Um atestado que comprove de forma satisfatória a execução de fornecimento de 1200 licenças poderia ser considerado?".

Resposta:

Para maior clareza, o Termo de Referência foi ajustado com o acréscimo do item 15.4:

15.4 Para que a licitante vencedora comprove sua capacidade operacional em executar o volume de serviço previsto no objeto da contratação, o somatório dos atestados deve corresponder, no mínimo, a 30% do volume previsto no objeto. Esse percentual se justifica para comprovar o desempenho de atividade pertinente e compatível em características e quantidades com o objeto da licitação, mitigando assim os riscos de inexecução do contrato.

Documento assinado eletronicamente por **Walter Trovijo Junior**, **Assessor I**, em 05/11/2024, às 16:12, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00101999963** e o código CRC **714938F9**.

PROCESSO:	065.10933.2024.0004168-84
OBJETO:	<Insira aqui o objeto do processo>
ÓRGÃO INTERESSADO:	<Insira aqui o órgão interessado>

RESPOSTA

Em resposta aos questionamentos da empresa INTEROP contidos no documento SEI nº 00099257795, respondemos:

Questionamento 01:

"5.1.12. O fabricante da solução deverá possuir certificações de segurança ISO 27.001, ISO 27.017, ISO 27.018 e ISO 27.701;"
Que exige que o fabricante da solução possua certificações de segurança ISO 27001, ISO 27017, ISO 27018 e ISO 27701, gostaríamos de solicitar esclarecimentos sobre a justificativa técnica para que tais certificações sejam diretamente vinculadas ao fabricante do produto.
Analisando cada uma das certificações mencionadas, verificamos que elas se referem majoritariamente a práticas relacionadas à gestão de segurança da informação, ao tratamento de dados em nuvem e à proteção de dados pessoais, conforme descrito abaixo:
*** ISO 27001: Define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI), focado em gerenciar a segurança de dados e informações, principalmente em termos de controle de acesso e proteção contra ameaças externas.**
*** ISO 27017: Específica para segurança em serviços de computação em nuvem, define diretrizes para garantir a segurança no provisionamento de serviços em nuvem, ou seja, está relacionada ao ambiente em que os dados são armazenados e processados.**
*** ISO 27018: Trata especificamente da proteção de dados pessoais em serviços de nuvem pública, garantindo que os dados pessoais sejam tratados em conformidade com as legislações de proteção de dados.**
*** ISO 27701: Complementa a ISO 27001 com foco na privacidade e na proteção de dados pessoais, sendo uma extensão voltada à implementação de um Sistema de Gestão de Privacidade da Informação, o que é diretamente aplicável à conformidade com legislações como a LGPD (Lei Geral de Proteção de Dados).**

Observa-se que essas certificações estão mais relacionadas à gestão de serviços, acesso, manipulação e tratamento de dados em ambientes de nuvem e ao cumprimento de normas de privacidade de dados, do que ao desenvolvimento da solução propriamente dita.

Dessa forma, entendemos que, para ampliar a competitividade e garantir uma maior participação de fornecedores, seria permitido que essas certificações sejam atendidas tanto pelo fabricante quanto pelo datacenter utilizado para a hospedagem da solução, desde que este último seja o responsável pela segurança física e lógica do ambiente.

Desta forma, nosso entendimento está correto?"

Resposta:

A exigência refere-se ao ambiente de nuvem utilizado para hospedagem da solução. O termo de referência foi ajustado para maior clareza.

Questionamento 02:

“5.1.9. Através da integração com o AD, a solução deve permitir a identificação de dados do gestor do usuário cadastrados no AD, de forma a permitir o envio de alertas para os gestores desses usuários, de acordo com as funcionalidades da plataforma

Que especifica que 'Através da integração com o AD, a solução deve permitir a identificação de dados do gestor do usuário cadastrados no AD', gostaríamos de esclarecer nosso entendimento:

O Microsoft Active Directory (AD) não possui um campo nativo específico para armazenar dados de quem é o gestor de um usuário, desta forma impossibilitando de forma automática a vinculação de um usuário ao seu gestor.

Diante disso, entendemos que essa identificação poderia ser feita de forma manual, após a importação dos dados de usuários, vinculando um usuário do tipo 'gestor' a um grupo de usuários que ele gerencia. Essa operação seria realizada no próprio ambiente da solução ou por meio de uma personalização do AD.

Está correto nosso entendimento de que a vinculação de gestores e usuários pode ser feita de forma manual?

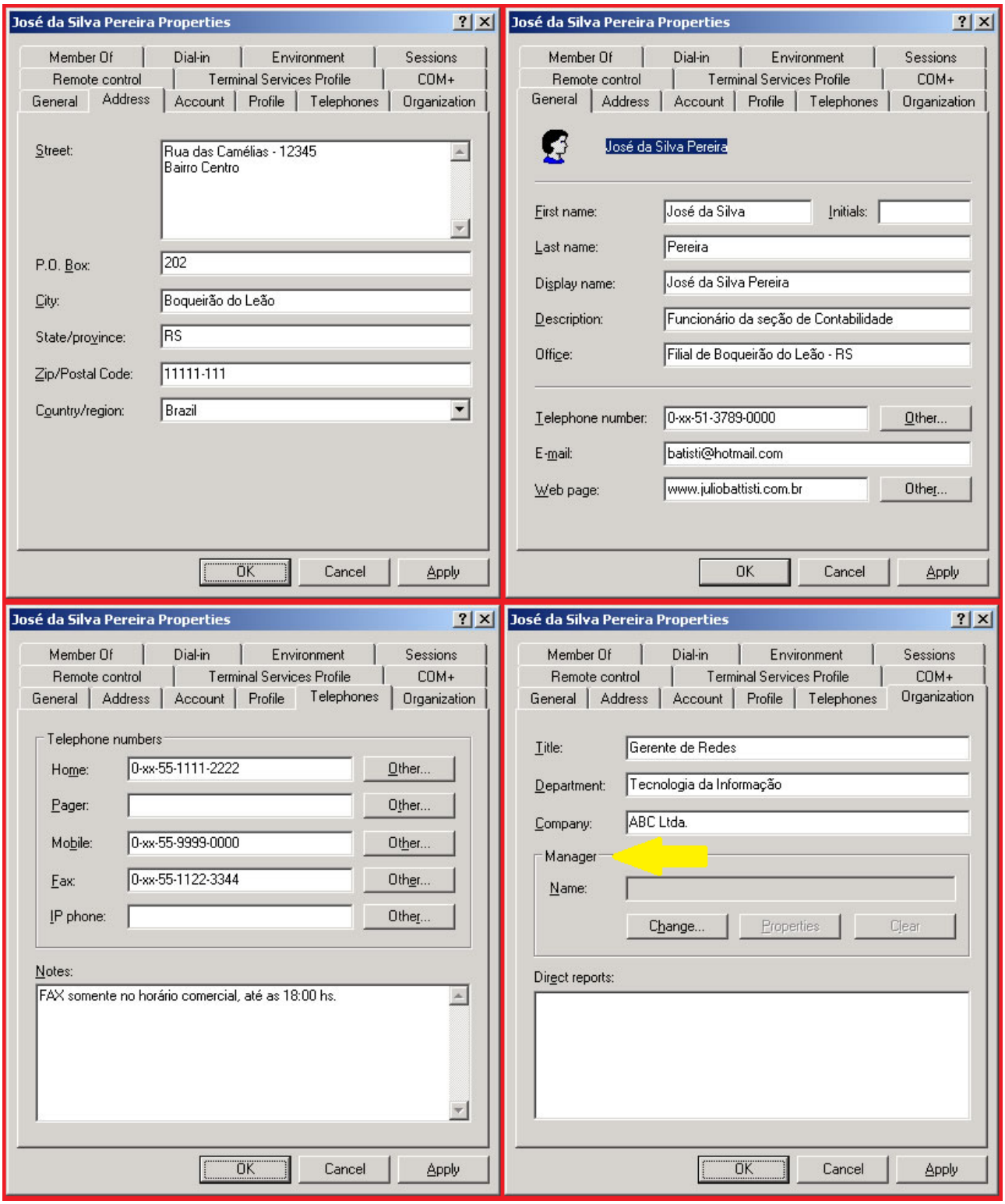
Caso essa vinculação manual não seja permitida, como a solução implementaria essa funcionalidade de forma automática? Poderiam ser fornecidos exemplos práticos de como essa identificação de gestores seria realizada no ambiente de produção, considerando que o AD, por si só, não contém esses dados hierárquicos?

Solicitamos esses esclarecimentos para entender como a funcionalidade deve ser implementada de forma eficaz, considerando as limitações do AD e os requisitos do edital.”

Resposta:

A solução deverá importar os dados especificados pela CONTRATANTE a partir da Profile do Usuário do AD (Ver imagem anexa como exemplo). O cadastro das informações do gestor do usuário no AD será realizado pela equipe da CONTRATANTE. O termo de referência foi ajustado para maior clareza.

Destacado com uma seta amarela o campo correspondente ao Gestor do usuário.



Questionamento 03:

“5.1.10. A solução deve passar por avaliações periódicas de segurança, tais como testes de intrusão (pentest) e gestão de vulnerabilidades de segurança;

Do edital, que estabelece que 'A solução deve passar por avaliações periódicas de segurança, tais como testes de intrusão (pentest) e gestão de vulnerabilidades de segurança', gostaríamos de solicitar mais detalhes sobre os seguintes pontos:

1. Existe um modelo pré-definido de relatório para essas avaliações?

Haverá um formato padronizado a ser seguido para a entrega dos relatórios de testes de intrusão e

gestão de vulnerabilidades?
Caso exista um modelo, pedimos que seja disponibilizado ou que sejam informados os critérios que deverão constar no relatório (ex.: escopo, metodologias, vulnerabilidades encontradas e mitigadas, etc.).

2. Esses testes serão realizados no ambiente de produção?

Se os testes de segurança forem executados diretamente no ambiente de produção, como será garantida a continuidade da operação da solução durante essas avaliações?
Os testes de intrusão em produção serão previamente agendados para evitar interrupções nas atividades dos usuários?

3. Agendamento e frequência das avaliações:

Qual será a frequência dessas avaliações? Há um cronograma definido ou elas serão realizadas sob demanda?
Quem será responsável por definir e coordenar esses agendamentos? Será o contratante, o fornecedor ou uma empresa terceira especializada?

4. Responsabilidade pela execução dos testes:

Quem será responsável pela execução dos testes de intrusão e gestão de vulnerabilidades? Será a empresa fornecedora da solução, uma empresa terceira contratada pelo fornecedor ou o próprio contratante?
Em caso de contratação de uma empresa terceira, como será garantida a imparcialidade e a qualidade da avaliação de segurança?
Em caso de contratação de uma empresa terceirizada, de quem será o custo? Caso seja da CONTRATADA, este valor deverá estar no custo do valor ofertado? Se sim, de quanto em quanto tempo o relatório deve ser apresentado?

5. Relevância deste item para a compra de uma solução de conscientização em cibersegurança:

Considerando que o objeto do edital é uma solução de conscientização em cibersegurança, questionamos a importância e relevância de avaliações de segurança, como testes de intrusão e gestão de vulnerabilidades, para a aquisição de uma plataforma voltada para a educação e conscientização de usuários."

Resposta:

*Numeração alterada para **5.1.11.** O ambiente que hospeda a solução bem como a aplicação devem passar por avaliações periódicas de segurança, tais como testes de intrusão (pentest) e gestão de vulnerabilidades de segurança, visando preservar a confidencialidade e integridade das informações da CONTRATANTE armazenadas no ambiente da solução. O termo de referência foi ajustado para maior clareza.*

Questionamento 04:

"5.1.44. A solução deve possuir dashboards que permitam visualizar em tempo real o desempenho dos usuários, permitindo a realização de benchmarks com outros usuários do mesmo segmento de negócio;

do edital, que exige que 'A solução deve possuir dashboards que permitam visualizar em tempo real o desempenho dos usuários, permitindo a realização de benchmarks com outros usuários do mesmo segmento de negócio', gostaríamos de obter mais esclarecimentos sobre a relevância e a implementação dessa funcionalidade:

1. Definição de 'segmentos de negócio':

O termo 'segmentos de negócio' refere-se a grupos internos da ferramenta, definidos pela própria plataforma, ou ele se refere a uma categorização externa baseada no setor de atuação das empresas (ex.: indústrias, serviços, comércio, etc.)?
Caso seja uma categorização externa, como a solução determinará esses segmentos de negócio? Será baseada em informações inseridas manualmente pelos administradores ou a ferramenta será capaz de identificar automaticamente o setor de atuação dos usuários?

2. Relevância de benchmarks por 'segmento de negócio':

Qual é a justificativa técnica para a realização de benchmarks entre usuários de diferentes empresas ou organizações do mesmo segmento de negócio, no contexto de uma solução de conscientização em cibersegurança?
Como esses benchmarks auxiliam na melhoria do desempenho individual dos usuários e na eficácia da solução, considerando que as necessidades e realidades de segurança podem variar significativamente entre empresas, mesmo dentro de um mesmo segmento de negócio?

3. Base para comparação:

Com base em quais critérios será definida a categorização de 'segmento de negócio' para a realização desses benchmarks? Haverá uma padronização de parâmetros, como o porte da empresa, setor de atuação ou outros fatores?
Como será feita a coleta e o tratamento desses dados para garantir a precisão e a equidade nas comparações entre os usuários? Haverá integração com sistemas externos ou bases de dados setoriais para definir esses benchmarks?

4. Confidencialidade e segurança:

Dado que os benchmarks envolvem comparações com outras empresas do mesmo segmento, como será garantida a segurança e a confidencialidade dos dados dos usuários ao realizar essas comparações?
A solução oferecerá algum tipo de anonimização ou criptografia para evitar o compartilhamento indevido de informações sensíveis entre diferentes organizações?

Por fim, considerando a irrelevância de correlacionar dados de usuários com outros segmentos de negócios em uma solução de conscientização de cibersegurança, entendemos que uma solução que possua apenas dashboards que permitam visualizar em tempo real o desempenho dos usuários já seria suficiente para atender as demandas, sem a necessidade de benchmarks externos. Acreditamos que isso poderia ampliar a concorrência e permitir a participação de mais fornecedores, mantendo a qualidade e a funcionalidade desejada.

Está correto nosso entendimento?"

Resposta:

A solução deve possuir dashboards que permitam visualizar o desempenho da organização, permitindo a realização de benchmarks com outras organizações do mesmo segmento de negócio. O termo de referência foi ajustado para maior clareza.

Questionamento 05:

"5.1.45 do edital, que exige que 'A solução deve permitir a exibição de campanhas por destinatário,

campanha entregue, aberta, clicada ou rejeitada', solicitamos esclarecimentos sobre como será realizado o controle de e-mails rejeitados, considerando que:

1. E-mails retidos por camadas de antispam:

Como a solução lidará com e-mails que podem ser retidos por camadas de antispam em servidores externos, uma vez que esses bloqueios podem não ser identificados ou não gerarem respostas claras (como bounces)?
Quais métodos a solução utilizará para identificar esses e-mails, visto que as regras de antispam variam amplamente entre diferentes provedores e servidores de e-mail, e em muitos casos, o bloqueio ocorre sem retorno de notificação?"

Resposta:

A solução deve permitir a exibição de campanhas de phishing por destinatário, com detalhamento de campanhas entregues, abertas, clicadas, com dados digitados, anexos abertos, phishing reportado pelo usuário ou com falhas na entrega. O termo de referência foi ajustado para maior clareza.

Questionamento 06:

"5.1.8 do edital, que exige que 'Através da integração com o AD, a solução deve permitir a inclusão automática dos usuários na plataforma, a partir de grupo ou grupos de usuários definidos no AD e identificados automaticamente pela plataforma', gostaríamos de obter mais esclarecimentos sobre a automação dos grupos de usuários:

1. **Automatização dos grupos de usuários:**
   - **Como será realizada a identificação automática dos grupos de usuários no Active Directory? A solução importará todos os usuários e grupos do AD ou será possível especificar quais grupos serão sincronizados com a plataforma?**
   - **Caso seja possível especificar os grupos de usuários, como isso deve ser configurado? A plataforma permitirá a seleção manual de grupos diretamente no AD, ou será necessário definir essa especificação dentro da própria plataforma?**
2. **Especificação dos grupos a serem sincronizados:**
   - **Como será feito o controle para garantir que apenas os grupos desejados sejam integrados à solução? Existe alguma interface de gestão onde o administrador poderá definir quais grupos serão automaticamente sincronizados?**
   - **Se a organização tiver muitos grupos de usuários no AD, a plataforma oferecerá uma forma de filtragem ou segmentação para facilitar a inclusão apenas dos grupos relevantes?**
3. **Gerenciamento de alterações nos grupos:**
   - **Caso novos grupos sejam criados ou os usuários sejam movidos entre grupos no AD, a solução detectará essas mudanças automaticamente e refletirá isso na plataforma? Quais serão as opções de controle e ajustes para essas modificações?"**

Resposta:

O termo de referência foi ajustado para maior clareza, conforme itens abaixo.

5.1.8. Através da integração com o AD, a solução deve permitir a inclusão automática dos usuários na plataforma a partir de um grupo ou grupos.
5.1.8.1. A definição do grupo de usuários a serem criados na plataforma será estabelecida entre a CONTRATANTE e a CONTRATADA durante a etapa de implantação.
5.1.8.2. A solução deverá possuir recurso de sincronização periódica com o AD, de forma a identificar a movimentação de usuários no grupo ou grupos AD configurados na plataforma. O termo de referência foi ajustado para maior clareza.

A integração com o AD poderá ser realizada através do protocolo Kerberos, padrão do AD, ou alternativamente através de LDAP seguro.

Questionamento 07:

“5.1.8 do edital, que exige que 'Através da integração com o AD, a solução deve permitir a inclusão automática dos usuários na plataforma, a partir de grupo ou grupos de usuários definidos no AD e identificados automaticamente pela plataforma', gostaríamos de obter mais esclarecimentos sobre a automação dos grupos de usuários:

1. Automatização dos grupos de usuários:

Como será realizada a identificação automática dos grupos de usuários no Active Directory? A solução importará todos os usuários e grupos do AD ou será possível especificar quais grupos serão sincronizados com a plataforma?
Caso seja possível especificar os grupos de usuários, como isso deve ser configurado? A plataforma permitirá a seleção manual de grupos diretamente no AD, ou será necessário definir essa especificação dentro da própria plataforma?

2. Especificação dos grupos a serem sincronizados:

Como será feito o controle para garantir que apenas os grupos desejados sejam integrados à solução? Existe alguma interface de gestão onde o administrador poderá definir quais grupos serão automaticamente sincronizados?
Se a organização tiver muitos grupos de usuários no AD, a plataforma oferecerá uma forma de filtragem ou segmentação para facilitar a inclusão apenas dos grupos relevantes?

3. Protocolo de integração:

Qual será o protocolo utilizado para realizar a integração com o Active Directory (AD)? A integração ocorrerá via LDAP, SCIM ou outro protocolo padrão de gerenciamento de identidade?
Há algum requisito específico para garantir a segurança dessa comunicação entre a plataforma e o AD, como o uso de LDAPS (LDAP sobre SSL) ou SAML para autenticação segura?

4. Componentes instalados no AD:

A solução permitirá ou exigirá a instalação de componentes adicionais no ambiente do AD para realizar essa integração? Caso afirmativo, qual será o impacto desses componentes na infraestrutura de TI e como será garantida a segurança e compatibilidade com as políticas de segurança do AD da organização?
Em caso de uso de agents ou outro tipo de software para integrar o AD à plataforma, como será feita a manutenção e a atualização desses componentes? Quais são os requisitos de compatibilidade com diferentes versões do AD?

4. Gerenciamento de alterações nos grupos:

Caso novos grupos sejam criados ou os usuários sejam movidos entre grupos no AD, a solução detectará essas mudanças automaticamente e refletirá isso na plataforma? Quais serão as opções de controle e ajustes para essas modificações?"

Resposta:

Considerando que algumas questões foram repetidas pela INTEROP, repetimos também as respostas nesse bloco.

O termo de referência foi ajustado para maior clareza, conforme itens abaixo.

5.1.8. Através da integração com o AD, a solução deve permitir a inclusão automática dos usuários na plataforma a partir de um grupo ou grupos.

5.1.8.1. A definição do grupo de usuários a serem criados na plataforma será estabelecida entre a CONTRATANTE e a CONTRATADA durante a etapa de implantação.

5.1.8.2. A solução deverá possuir recurso de sincronização periódica com o AD, de forma a identificar a movimentação de usuários no grupo ou grupos AD configurados na plataforma. O termo de referência foi ajustado para maior clareza.

A integração com o AD poderá ser realizada através do protocolo Kerberos, padrão do AD, ou alternativamente através de LDAP seguro.

Será permitido a instalação de componentes adicionais em servidor virtual dedicado à essa finalidade no ambiente da CONTRATANTE para sincronizações com o AD, desde que garantida a segurança na comunicação com o AD e com o ambiente de nuvem da CONTRATADA.

A CONTRATADA será a responsável por fornecer todas as atualizações e patches relativos à solução provida para instalação on premises e a equipe da CONTRATANTE fica responsável pela aplicação das atualizações e configurações recomendadas, seguindo as orientações técnicas da CONTRATADA.

Com relação ao gerenciamento de alterações nos grupos entendemos que essa questão é esclarecida através da primeira parte dessa resposta, bem como pelas retificações realizadas no termo de referência, também já esclarecidas no bloco anterior de perguntas, pois as mesmas estão duplicadas.

Questionamento 08:

“5.1.21 do edital, que estabelece que 'A solução deve prover a funcionalidade de teste USB drop ou Candy drop: quando o usuário encontra um pendrive perdido em algum local da empresa e tenta verificar seu conteúdo', gostaríamos de solicitar mais informações sobre a implementação dessa funcionalidade:

1. Simulação de USB drop ou Candy drop:

Como será feita a implementação do teste de USB drop ou Candy drop? A solução fornecerá pendrives físicos para a simulação, ou será apenas um teste virtual, no qual os usuários interagem com arquivos simulados?

Se for necessário o uso de pendrives físicos, quem será o responsável pela distribuição e coleta desses dispositivos dentro da empresa?

Nosso objetivo ao levantar esses pontos é garantir que a solução atenda plenamente aos requisitos estipulados no edital, além de ampliar a concorrência, aumentar a competitividade e diminuir os valores envolvidos.

Agradecemos antecipadamente pelos esclarecimentos que poderão fornecer sobre esses pontos.”

Resposta:

O fornecimento dos pendrives para uso nos testes será de responsabilidade da CONTRATANTE. O termo de referência foi ajustado para maior clareza.

Documento assinado eletronicamente por **Walter Trovijo Junior**, **Assessor I**, em 08/11/2024, às 15:54, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00102323049** e o código CRC **90083246**.

Referência: Processo nº 065.10933.2024.0004168-84 SEI nº 00102323049