Resposta Nº 3 as solicitações de esclarecimento para o edital 0004/2021 do CRM-MG:

Item 2 da tabela:

Que tipo de inventário o cliente está esperando? Atendemos caso seja um inventário de dados. Podemos receber o cadastro dos assets como parte do inventário de ambientes tecnológicos.

**Resposta**:

Esperamos receber todo o data mapping do ambiente considerando todas as etapas, desde de motivação da coleta, consentimento, processamento\tratamento (compartilhamento interno\externo), backup até o descarte.

Item 3 da tabela:

O Pentest será executado em modo Black Box ou Gray Box?

**Resposta:**

Entendemos que o modelo Gray Box como mais interessante neste momento pelo fato de o time ter conhecimento parcial de algumas aplicações, hoje mantidas pelo Conselho federal de Medicina.

O escopo compreende apenas teste externo ou também teste na rede interna?

**Resposta:**

Rede interna e externa.

Qual a estimativa de quantidade de ativos a serem testados?

**Resposta:**

Temos aproximadamente 25 servidores com sistemas operacionais (Linux e Windows), aproximadamente 150 microcomputadores (laptops e desktops), 48 impressoras e 30 ativos de rede.

Sobre o item 3.3.4.9.8 “Quem acessa e quem deu acesso e por qual finalidade”, entendemos que a solução que forneça maneiras gráficas de como o dado entra, é armazenado e processado dentro da empresa atenda ao item.

Está correto nosso entendimento?

**Resposta:**

Correto

Sobre o item 3.3.4.9.9 "Quais são os direitos atendidos dos proprietários dos dados pessoais e por qual instrumento tecnológico e legal o direito está sendo atendido;" gostaríamos de esclarecimentos adicional.

**Resposta:**

Esta relacionado ao direito dos titulares de dados sobre : confirmação e acesso a dados , correção, anonimização, portabilidade, cancelamento e etc, onde devemos ter todo os registros de solicitações com os respectivos carimbos de data\hora e responsável.

Sobre o item 3.3.4.26 “A solução deve ter barramento de Integração – ESB/SOA para integrar com os sistemas  internos do Conselho, inclusive notificações e eventos automatizados”, entendemos que a solução que seja cloud e de maneira distribuída garantindo as melhores práticas para sustentação atenda ao item. Está correto nosso entendimento?

**Resposta:**

Este ponto refere-se a possíveis necessidades de integrações com aplicações e painéis que podem ser feitas através do uso de API´s para compartilhamento.

Sobre o item 3.3.4.27 "A solução deve arquitetura web em 3 camadas com persistência de dados em banco de dados relacional, servidor de middleware para hospedar a aplicação e camada de visão em HTML 5 responsivo.", entedemos que a solução que consiga prover através de Cloud, a abstração sobre qual será a arquitetura, garantindo a segregação do dado do cliente atende ao item. Está correto nosso entendimento?

Resposta:

Correto. Considerando cenário SaaS

O item 3.3.4.29 "Deve suportar os principais bancos de dados utilizados pelo Conselho, a saber: Oracle, SQL Server, PostgreSQL, MySQL." cita somente as bases de dados estruturados, porém o item 2.1.3 cita a plataforma do Gsuite, precisamos entender a volumetria esperada para o Guite e se o servidor de arquivos da companhia também será parte deste certame?

**Resposta:**

O servidor de arquivo(file server) também esta considerado no escopo da proposta, já sobre o Gsuite a ideia é que seja validada questões de vulnerabilidades referentes a logs de acesso, anti-spam e outras oportunidades de incremento do nível de segurança associado ao pacote google contratado atualmente.

Belo Horizonte, 06/04/2021

Mário Augusto V. Teixeira

Pregoeiro