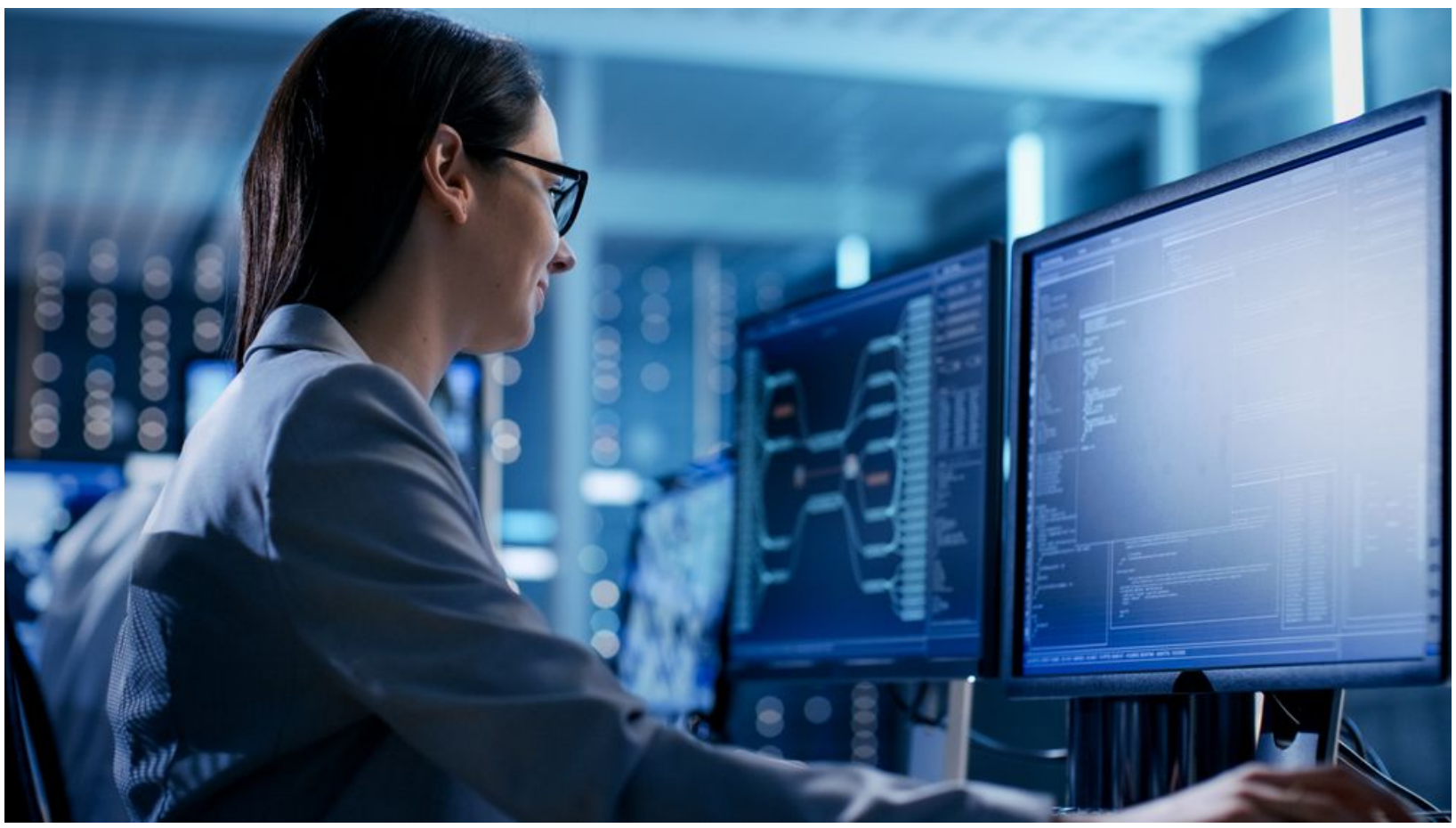
FOCO NO MERCADO DE TRABALHO

ARMAZENAMENTO DE DADOS

Emilio Tissato Nakamura

MECANISMOS PARA PROTEÇÃO DOS DADOS

Além da criptografia, há mecanismos como a anonimização, pseudonimização e mascaramento de dados.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você, como gerente de processos de segurança, deve alinhar as informações e as ações com os gerentes de tecnologias de segurança e a de governança de segurança.

Estruture a sua apresentação com um contexto sobre a empresa, que é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. O desenvolvimento de novas tecnologias é feito por uma equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

Um ponto importante para ser colocado na apresentação é que a empresa trata de diversos dados e informações confidenciais e sigilosos, e este não é o foco desta apresentação, que foca nos dados pessoais. Reforce que LGPD trata de proteção de dados pessoais, mas dados confidenciais e sigilosos são tratados em um outro contexto, de uma forma integrada e sinérgica.

Mostre na apresentação que você conduziu a criação do mapeamento de dados pessoais, com todo o fluxo nos sistemas da empresa. Um dos dados pessoais identificados na empresa são os de colaboradores, incluindo funcionários diretos, terceiros e prestadores de serviços. Estes dados pessoais são utilizados para os processos internos da empresa, principalmente os relacionados a recursos humanos e financeiro. Como há uma interação grande entre os diferentes locais da empresa (Natal, Belo Horizonte e Santiago), os dados pessoais também são muito utilizados em viagens, que envolve o envio destes dados para agências de turismo e companhias aéreas. Outro dado pessoal identificado foi de clientes, incluindo os militares argentinos. Neste caso, como a empresa realiza negócios B2B, e não B2C, os dados pessoais são mais corporativos, mas há dados pessoais de contatos dos clientes. Você pode continuar citando dados pessoais da empresa, e uma boa forma

de identificar estes dados é analisando os processos da empresa, que indicará a finalidade e quais dados pessoais são necessários para cada atividade.

Mostre para o diretor de segurança da informação da empresa que toda a parte jurídica está equacionada, com os ajustes de termos de ciência, termos de responsabilidade, termos de uso e contratos com fornecedores e prestadores de serviços contendo cláusulas relacionados à privacidade e proteção de dados pessoais.

Para a proteção destes dados pessoais, mostre que a empresa está utilizando a pseudonimização para limitar os riscos em caso de vazamento. Mostre também que a anonimização está sendo utilizada para a criação de indicadores corporativos. Reforce que todas as bases com a pseudonimização e a anonimização estão segmentadas e utilizam controles de segurança que envolvem a gestão de identidades e de acesso. Além disso, relembre que os controles de segurança utilizados para proteger as informações, principalmente as confidenciais e secretas, fazem parte da proteção dos dados pessoais também.

Sobre a criptografia, mostre que ela está sendo utilizada no nível de aplicação, com uso de HSM. Mostre os benefícios do uso do HSM, partindo dos riscos envolvidos com o uso de chaves criptográficas por aplicações.

Para finalizar, mostre que a empresa está adotando práticas de segurança de acordo com as responsabilidades compartilhadas com os provedores de nuvem. A empresa está utilizando dois provedores de nuvem, na modalidade de plataforma como serviço (PaaS). Reforce que, neste modelo, a empresa é responsável pela segurança dos dados e das aplicações.

AVANÇANDO NA PRÁTICA

DEFININDO A ESTRATÉGIA DE ARMAZENAMENTO DE DADOS PESSOAIS DA EMPRESA

Com a necessidade de conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), você deve definir uma estratégia de proteção de dados pessoais da sua própria empresa, que está sendo constituída. A sua empresa é uma loja virtual que precisa coletar os seguintes dados: nome completo, CPF, endereço e referência comercial. Defina sua estratégia de proteção de dados pessoais, considerando o seu armazenamento e o uso de um provedor de nuvem.

RESOLUÇÃO

Sua empresa deverá coletar dados pessoais, incluindo o nome completo, CPF, endereço e referência comercial. O termo de privacidade deve citar quais são os dados que estão sendo coletados, descrevendo claramente a finalidade, e como eles estarão protegidos, citando ainda os provedores de serviços, se estiverem sendo utilizados. Você deve definir também se estes dados serão compartilhados com algum terceiro e, em caso afirmativo, deve obter um consentimento de cada usuário.

Para o armazenamento dos dados coletados, você deve pensar nos mecanismos de proteção. Além dos controles de segurança para proteger os ativos físicos e lógicos, os dados podem ser pseudonimizados. Assim, você pode utilizar um código como “Cliente0001” para o João, “Cliente0002” para Maria, e assim por diante. No banco de dados, você pode armazenar este código do cliente como identificador, juntamente com os dados de CPF, endereço e referência comercial. Este relacionamento entre o código do cliente e o nome real também deve ser armazenado, de uma forma segura e em local distinto da base de dados dos clientes. Para aumentar a segurança, você pode dividir ainda mais o banco de dados, com o CPF em um, e o endereço e referência comercial em outro, usando o código do cliente como identificador.

A anonimização não pode ser aplicada no seu caso, pois você precisa identificar o cliente. Ela pode, no entanto, ser utilizada para criar uma base distinta para inteligência de negócios, por exemplo.

Outro ponto que você deve definir é como a criptografia irá funcionar, se na aplicação ou no banco de dados.

Além disso, devem ser consideradas as responsabilidades de segurança, de acordo com o tipo de serviço contratado do provedor de nuvem. Há as modalidades de contratação de infraestrutura, plataforma ou o serviço.