JUNHO 2025 | EDIÇÃO NO. 2

INSTRUÇÃO PARA O TRABALHO

Vazamento de dados pessoais

Vazamento de Dados Pessoais

O que é um incidente com vazamento de dados?

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma lei brasileira que estabelece regras sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade das pessoas. Em seu art. 46, determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Um incidente de segurança com vazamento de dados pessoais acontece quando informações confidenciais, como dados pessoais, informações financeiras ou dados de uma instituição, são expostas indevidamente, seja por meio de acesso não autorizado ou divulgação sem permissão. Isso pode ocorrer devido a falhas de segurança em sistemas, ataques cibernéticos, falha humana ou até mesmo devido à divulgação não intencional de informações.

Na Universidade Federal do Rio de Janeiro (UFRJ), há uma cartilha sobre a LGPD. Para saber mais, acesse aqui!

Exemplos de incidente de segurança relacionados a vazamento de dados pessoais

Uso Impróprio de Recursos: compreende o uso indevido de ferramentas e equipamentos corporativos, tais como:

- Utilização do e-mail corporativo para envio de spam ou promoção de negócios pessoais;
- Instalação de softwares não autorizados;
- Uso de pendrives de forma não autorizada;
- Impressão de documentos sem permissão.

Ameaças Digitais Diversas: incluem ações maliciosas que comprometem a integridade ou a disponibilidade de sistemas e dados, como:

- Infecção por vírus ou outros códigos maliciosos;
- Sequestro de dados (ransomware);
- Desfiguração de sites (defacement);
- Modificação de sistemas sem o conhecimento, autorização ou instrução do proprietário.

Violações de Políticas: refere-se ao descumprimento das normas internas de segurança da informação, incluindo:

- Quebra da Política de Segurança da Informação;
- Desrespeito à política de uso aceitável da instituição ou do provedor de acesso.

Ataques de Negação de Serviço (DoS): consistem em ações que visam interromper ou degradar a disponibilidade de serviços. São exemplos:

- Forçar o reinício de sistemas ou o consumo excessivo de recursos (como memória ou processamento), comprometendo a prestação de serviços;
- Bloqueio de canais de comunicação, impedindo que os usuários se comuniquem adequadamente.

Vazamento e Acesso Não Autorizado a Dados: envolve o acesso, exposição ou uso indevido de informações pessoais, confidenciais ou sensíveis. Alguns exemplos são:

- Exposição não autorizada de dados pessoais e informações privadas;
- Roubo ou comprometimento de credenciais de acesso;
- Tentativas de acessar sistemas ou dados utilizando credenciais de terceiros;
- Uso inadequado ou indevido de sistemas;
- Provocação de falhas que impeçam acessos legítimos e autorizados.

Como agir em caso de suspeita de vazamento de dados pessoais na UFRJ?

*. A DIVSEG, confirmando o incidente como um vazamento de dados, comunica a Encarregada de Dados para que sejam adotados os trâmites legais cabíveis.