Proteja-se!

Secretaria de Tecnologia da Informação e Comunicação – **SETIN**
Coordenadoria de Apoio à Governança e Gestão de TIC – **CGOV**
Seção de Gestão da Segurança da Informação – **SGSI**

Incidentes de Segurança da Informação

Nº 24, junho de 2019

Um **incidente de segurança da informação** é constituído por um único evento adverso ou um conjunto destes, que tenha capacidade de afetar a segurança da informação, causando prejuízo a quaisquer dos seus princípios básicos: confidencialidade, integridade e disponibilidade*.

Outra definição possível, ainda que mais simples, pode ser descrita de modo que um incidente de segurança da informação seja a ocorrência de algum evento indesejado ou inesperado, trazendo ameaça à segurança da informação e que tenha grande probabilidade de comprometer as operações do negócio.

A **gestão de incidentes** é obrigatória em todas as organizações que se preocupam com a segurança de suas informações. Trata-se de um processo que tem como objetivo recuperar a normalidade de um serviço danificado por violações de segurança o mais rápido possível. A gestão de incidentes também deve tentar minimizar qualquer prejuízo, garantindo a qualidade dos serviços e informações.

Exemplos de incidentes de segurança da informação

Em 2013, um grupo de cibercriminosos comprometeu informações pessoais – incluindo senhas – de 3 bilhões de usuários do Yahoo!, à época, o serviço dominante na categoria portal de internet.

No ano de 2016, o serviço de transporte urbano Uber sofreu um ataque que comprometeu informações pessoais de 57 milhões de usuários e de 600.000 motoristas da plataforma.

Em março de 2019, o grupo Toyota/Lexus sofreu ataques que culminaram no vazamento de dados de mais de 3 milhões de clientes.

Importante!

* Os três princípios da Segurança da Informação:

Confidencialidade: a informação tem o acesso limitado tão somente aos usuários autorizados;

Integridade: a informação mantém todas as características originais, desde sua criação;

Disponibilidade: a informação permanece disponível para o uso legítimo pelos usuários autorizados.

Dicas para evitar danos causados por incidentes de segurança da informação:

- Tenha sempre um antivírus atualizado e ativo;
- Controle os acessos ao seu computador utilizando um *firewall*;
- Mantenha sempre o sistema operacional atualizado;
- Atualize o seu navegador e todas as extensões instaladas;
- Não execute programas recebidos em anexos de e-mails;
- Não preencha formulários recebidos por e-mail solicitando informações pessoais ou senhas;
- Evite acessar sites nos quais tenha cadastro a partir de estações públicas ou compartilhadas, como cybercafés e *lan houses*. É possível que o antivírus não esteja atualizado ou que exista algum programa de captura de informações sendo executado.