

INTRODUÇÃO

à segurança da informação

Vamos compreender os principais conceitos de segurança da informação.

PRINCIPAIS CONCEITOS

A segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.

É preciso garantir os princípios da segurança da informação: confidencialidade, integridade, disponibilidade.

É preciso trabalhar com os elementos do risco: ativos, vulnerabilidades, agentes de ameaça, ameaças, vulnerabilidades, probabilidade, impacto.

A aplicação de mecanismos de defesa, controles de segurança e técnicas de segurança de redes é definida a partir de uma visão de riscos.

Segurança da informação é identificar, proteger, detectar, responder e recuperar.



Fonte: elaborada pelo autor.

Em segurança da informação, proteger significa implementar controles de segurança a partir da identificação e da avaliação dos riscos. Essa é a prevenção, e uma vez feita, um ataque em andamento é identificado, uma resposta, então, é dada e a recuperação do ambiente original é realizada.



Fonte: elaborada pelo autor.

Princípios da segurança da informação CID



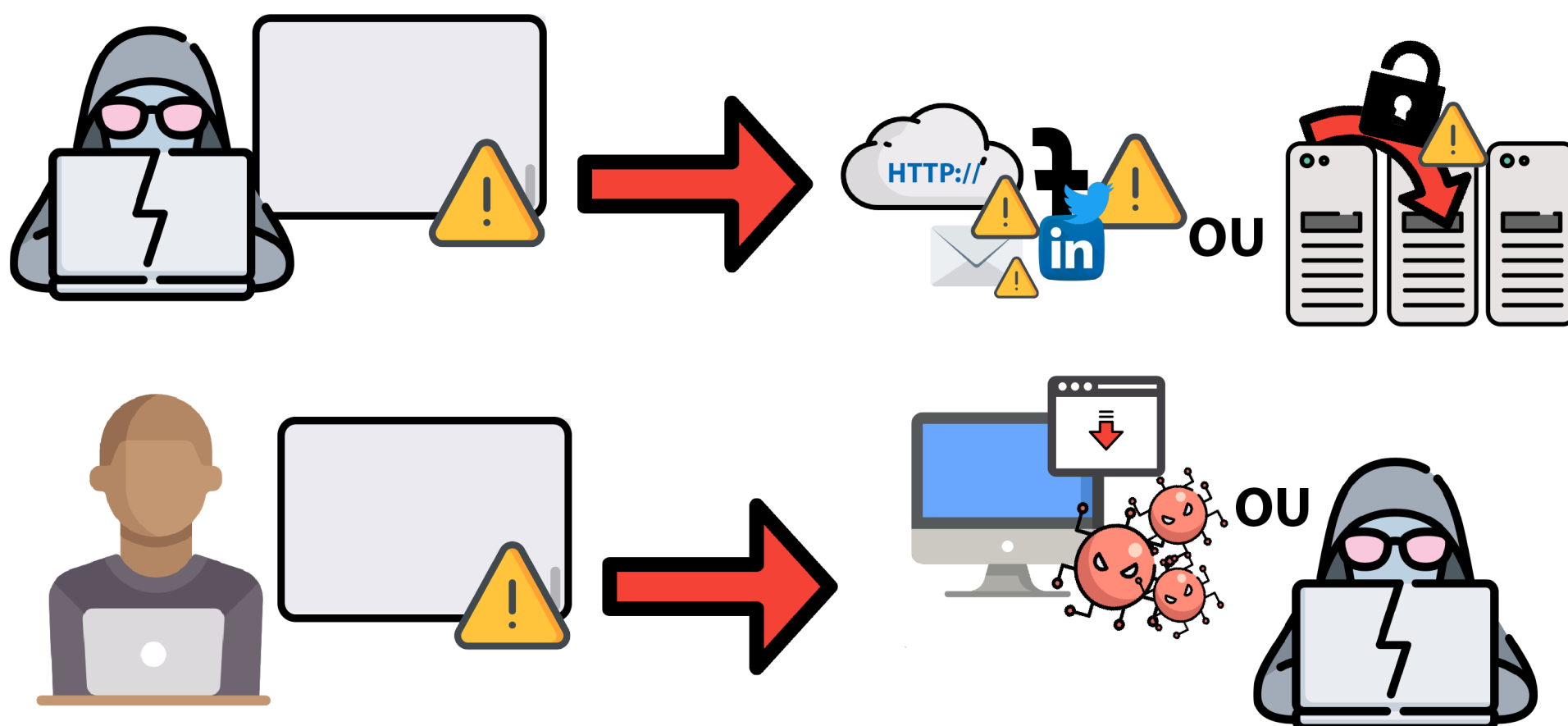
RISCOS DE SEGURANÇA

Riscos de segurança podem virar incidentes de segurança quando um agente de ameaça explora vulnerabilidades de um ativo. Quando isso ocorre, uma ameaça se torna um incidente de segurança e o nível de risco é calculado pela probabilidade e pelo impacto existente.

Risco (R) é o produto da Probabilidade (P) com o Impacto (I).

$$R = P * I$$

Exemplo: um *cracker* (agente de ameaça) utiliza um *exploit* para fazer um ataque, ou seja, para explorar uma vulnerabilidade de um ativo, um ativo pode ser a informação, as pessoas, os sistemas, os banco de dados e os dispositivos físicos, como um notebook.



Fonte: elaborada pelo autor.

SAIBA MAIS

Diferentes tipos de riscos existem e devem ser considerados. Danos à reputação ou à marca, crime cibernético, risco político e terrorismo são alguns dos riscos que as organizações privadas e públicas de todos os tipos e tamanhos do mundo devem enfrentar cada vez mais. Há uma norma de gestão de riscos, a ABNT NBR ISO 31000:2018, que abrange riscos de forma mais ampla, e, em segurança da informação, há uma norma específica, a ABNT NBR ISO/IEC 27005:2019. Isso reforça a importância da visão de riscos para que possamos trabalhar com segurança da informação, pois é a partir da identificação dos riscos que a proteção pode ser realizada.

CONTROLES DE SEGURANÇA

Controles de segurança devem ser aplicados nos ativos, para eliminarem vulnerabilidades. Os controles podem ser:

FÍSICOS

Exemplo:
Controle de acesso

TECNOLÓGICOS

Exemplo:
Gerenciamento de contas e senhas

PROCESSOS

Exemplo:
Norma de atualização de senhas

Foram apresentados os principais conceitos que o acompanharão durante toda sua jornada em segurança da informação. Lembre-se sempre de que a segurança da informação envolve identificação, proteção, detecção, resposta e recuperação.

[Pesquise mais](#)