Disciplina: Segurança e Auditoria de Sistemas

Prof. Carlos Barreto Ribas
ribas@pucminas.br

Unidade 1- Gestão da Segurança da Informação

Segurança da Informação

Motivação para se praticar a Gestão da Segurança da Informação

***Dados** e **informações** podem ser:*

- perdidos; - roubados; - adulterados;

- processados errados; - acessados indevidamente;

Segurança da Informação

Podendo causar sérios impactos sobre:

- a continuidade dos processos;

- a imagem das pessoas / organizações;

- credibilidade; - competitividade;

- finanças; - etc.

Segurança da Informação

Foco dos modelos de segurança, inclusive os aplicados à Segurança da Informação:

- todo e qualquer modelo de segurança possui como objetivo central a palavra

"Continuidade".

Segurança da Informação

- Segurança da informação é a proteção da informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizando os riscos, maximizando o retorno sobre os investimentos e oportunidades para as organizações.

Segurança da Informação

De acordo com a Norma ISO-17799, que hoje tem o número de ISO-27002,

Segurança da Informação é a preservação da confidencialidade, integridade e disponibilidade da informação.

Segurança da Informação

Confidencialidade

- Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

Segurança da Informação

Integridade

- Salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

Segurança da Informação

Disponibilidade

- Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessários.

Segurança da Informação

- A segurança da informação é obtida a partir da implementação de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Segurança da Informação

Fontes de requisitos de

Segurança da Informação:

-Análise / Avaliação de Riscos;

-Legislação e normas vigentes;

-Princípios e objetivos de negócio.

Segurança da Informação

Grandes classes de problemas:

- sinistros; - fraudes e sabotagens;

- erros operacionais; - falhas de hardware;

- falhas em comunicações;

- erros em entrada de dados;

Segurança da Informação

Sinistros

- enchentes; - explosões; - desabamentos;

- curtos-circuitos; - descargas atmosféricas;

- furacões; - terremotos; - incêndios;

- atentados terroristas;

- quedas e picos de energia;

Segurança da Informação

Fraudes e Sabotagens

- cópias não autorizadas de projetos, processos, sistemas, programas e dados;

- roubo de informações; - adulteração de dados;

- espionagem industrial/comercial; - etc;

Segurança da Informação

Erros Operacionais

- perda de dados históricos; - apagar arquivos indevidos; - uso equivocado de versões de sistemas, programas e dados;

- não realização de rotina de backup;

- outros;

Segurança da Informação

Falhas de Hardware

- falhas em conexões físicas; - problemas em componentes; - problemas em mídias móveis como HD externo, pen drive, cd, fita;

- falhas intermitentes em equipamentos;

- etc;

Segurança da Informação

Falhas em Comunicações

- problemas em provedores de acesso;

- problemas em equipamentos (roteadores, switch, modem, ..) e em componentes de rede; - falhas nos meios de transmissões de dados (antenas, satélite, cabos, fibras, etc);

Segurança da Informação

Erros em Entrada de Dados

- todo e qualquer processo que pode levar a uma falta de consistência na entrada de um dado.

Segurança da Informação

Conceitos básicos para se pensar segurança na prática

Proprietário da Informação

Pessoa que tem o poder e a responsabilidade total sobre um conjunto de dados e sistemas a ele vinculado.

Segurança da Informação

Usuário da Informação

Pessoa autorizada pelo proprietário a acessar e utilizar dados e sistemas para a realização do seu trabalho.