Segurança da Informação

Profª Rebeca Fiss

Aula 1 – Introdução à Segurança da Informação

O que é Segurança da Informação?

O que é Segurança da Informação?

Para entender o que é segurança da informação preciso saber o que é **Informação**, correto?

- Existência de informação:
  - impressa, escrita em papel, armazenada eletronicamente, transmitida pelo correio, apresentada em filmes, falada em conversas.

O que é Segurança da Informação?

Como proteger diferentes formas de informação?

- Conhecendo o inimigo e se protegendo sob diferentes aspectos, para que se tenha:
  - a continuidade do negócio
  - minimizar o risco ao negócio
  - maximizar o retorno sobre o investimento e as oportunidades de negócio

O que é Segurança da Informação?

Definições

- A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida.

(NBR 17999)

O que é Segurança da Informação?

Importante

- As informações que manipulamos podem existir de diferentes formas...
- Vulnerabilidades e ameaças da mesma forma
- Vamos proteger o que? Como? De quem?

Ciclo de vida da Informação?

Manuseio

- Momento em que a informação é criada e manipulada
    - manusear e catalogar papéis
    - digitar informações em um sistema
    - inserir informações em uma planilha

Ciclo de vida da Informação?

Armazenamento

- Momento em que uma informação é armazenada
  - Banco de Dados
  - Em um papel
  - Impressa
  - CD, DVD, Pen Drive, Nuvem...

Ciclo de vida da Informação?

Transporte

- Momento em que a informação é transportada
    - enviar um e-mail
    - falar por telefone uma informação confidencial
    - postar um arquivo em um FTP

Ciclo de vida da Informação?

Descarte

- Fase em que a informação é descartada
    - Jogar no lixo um material impresso
    - Excluir um arquivo do computador
    - Descartar um CD, DVD

Propriedades da Informação

Confidencialidade

- A informação só pode ser acessada por pessoas que tenham permissão (autorizadas)
    - Informação escrita, falada, armazenada
    - Prover mecanismos para garantir a identificação e autenticação das partes envolvidas

Propriedades da Informação

Disponibilidade

- Estar a informação ou o meio informático (sistema, servidor, etc) disponível 24 x 7 (24 horas por dia, 7 dias por semana)
- Estar disponível no momento em que a mesma for acessada
- Disponibilidade passa pelas estratégias (planos) de contingência

Propriedades da Informação

Integridade

- Informação não foi alterada de forma indevida, não-autorizada ou acidentalmente
- Quebra de integridade
    - Informação é corrompida, roubada, falsificada...

Propriedades da Informação

Outros fatores importantes...

- **Auditoria:** exame de eventos históricos dentro de um computador ou sistema
- **Autenticidade**: a pessoa realmente é quem ela diz ser
- **Legalidade:** legalidade jurídica da informação ou de ativos
- **Não-repúdio**: não é possível dizer que não foi feito (não é pessível negar)
- **Privacidade**: informação privada pode ser lida, alterada, entre outros, somente pelo seu dono

Conceitos

Ativos

- Qualquer elemento que tenha valor para a empresa ou organização (ISO 27.002)
- Ativos fornecem suporte aos processos de negócios, portanto necessitam de segurança
- Neste quesito enquadram-se todos os elementos utilizados para: armazenar, processar, transportar, manusear e descartar a informação

Conceitos

Categorias de Ativos

- Informações
- Hardware
- Software
- Ambiente Físico
- Pessoas
- Aplicações
- Usuários
- Processos

Conceitos

Ameaças

- Conhecido também pelo termo «*threat*»
- Caracterizado como qualquer ação, acontecimento ou entidade que possa agir sobre:
- um ativo, pessoa ou processo
- através de uma vulnerabilidade e consequentemente gerando determinado impacto

Obs.: ameaças só existem se houverem vulnerabilidades

Conceitos

Classificação das Ameaças

- Naturais
    - Decorrentes de fenômenos da natureza
- Involuntárias
    - Inconscientes, causadas pelo desconhecimento
- Voluntárias
    - Propositais, causadas por agentes humanos
        - crackers, invasores, espiões, ladrões, etc...

Conceitos

Outras ameaças aos sistemas de informação

- Falha de software/hardware
- Invasão pelo terminal de acesso
- Roubo de dados e equipamentos
- Incêndio
- Problemas elétricos
- Erros de usuário
- Erros de Programação

- podem originar-se de fatores técnicos, organizacionais e ambientais

Conceitos

Vulnerabilidade

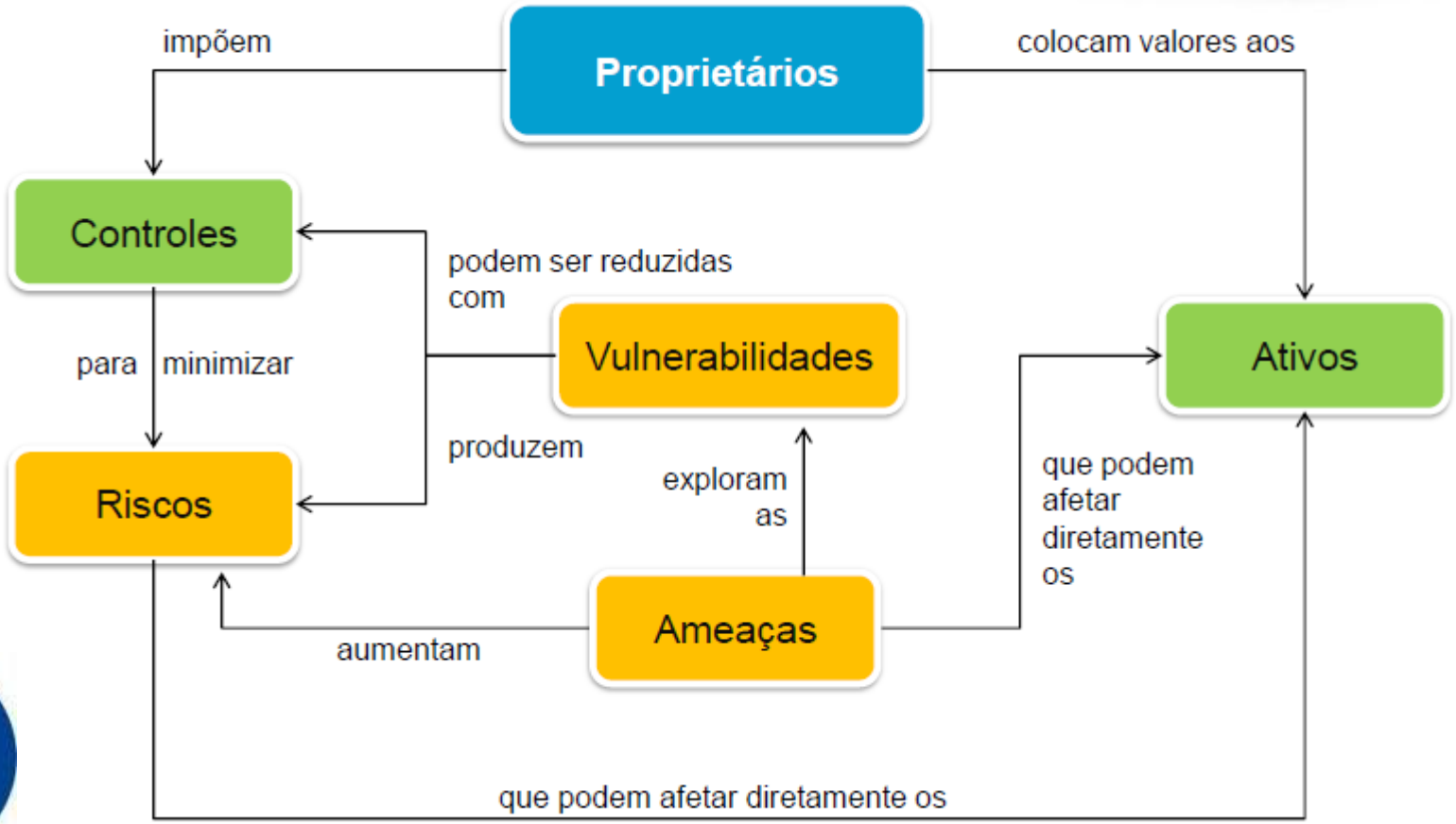
- Fragilidade de um ou mais ativos, que pode ser explorada por uma ou mais ameaças (ISO 27.002)
    - As vulnerabilidades devem ser gerenciadas, ou seja, identificadas e corrigidas

Conceitos

Controles (técnicos, administrativos e de gestão)

- Referem-se as medidas de segurança:
    - práticas, procedimentos e mecanismos utilizados para a proteção de ativos
    - os controles permitem:
        - impedir que as ameaças explorem as vulnerabilidades
        - reduzir o surgimento de vulnerabilidades
        - minimizar o impacto dos incidentes de segurança da informação

Conceitos


impõem
Proprietários
colocam valores aos
Controles
podem ser reduzidas com
Vulnerabilidades
Ativos
para
minimizar
produzem
exploram as
que podem afetar diretamente os
Riscos
Ameaças
aumentam
que podem afetar diretamente os

Conceitos

Entender o Negócio

- Ao iniciar um projeto de segurança, preciso conhecer o ambiente da organização (pessoas, processos, práticas)
- Geralmente a situação é a seguinte:
    - Desconhecimento dos processos (ambiente)
    - Nenhum tipo de controle implementado
    - Elevado índice de riscos
    - Falta de uma cultura de segurança
    - Resistência (interna e externa)
    - Visão limitada da importância/ganho/perda