# Segurança da informação

## Introdução

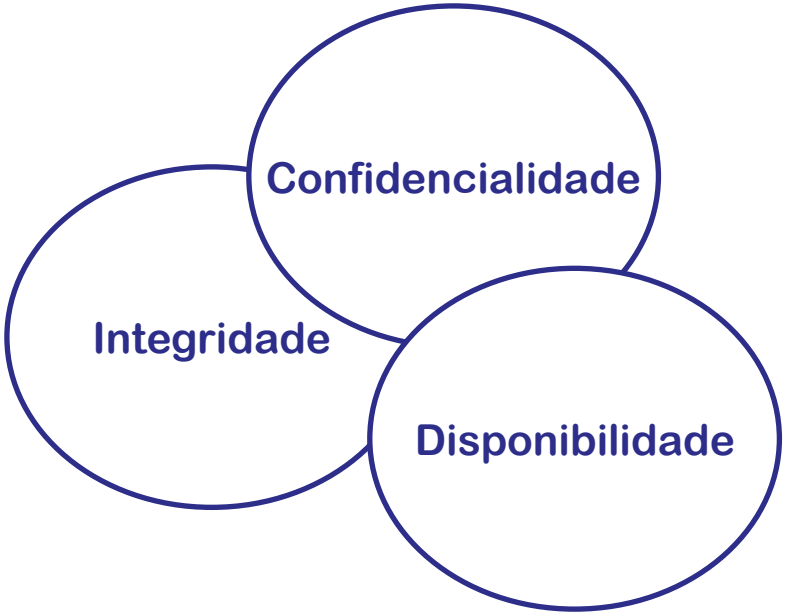
FURB
UNIVERSIDADE DE BLUMENAU

# O que é segurança da informação?

- Toda empresa lida diariamente com informações, várias delas confidenciais. Normalmente estas informações são vitais para o bom funcionamento dos processos.
- Riscos que a empresa está sujeita:
  - Adulteração ou fraude nas informações
  - Roubo ou vazamento de informações
- Comprometer as informações vitais pode trazer muitos prejuízos à empresa:
  - Parada de processos (prejuízo operacional)
  - Retrabalho (por perder informações)
  - Processos judiciais
  - Prejuízos para a imagem da empresa
- A segurança da informação refere-se à proteção de informações sensíveis, confidenciais ou importantes para uma organização.

# Pilares da segurança da informação

Existem alguns aspectos da segurança da informação que são considerados centrais ou principais, por isso são considerados como sendo pilares da segurança da informação




**Tríade da segurança**

Alguns autores chamam estes aspectos de:

- Princípios da segurança da informação
- Objetivos da segurança da informação
- Atributos da segurança da informação
- Dimensões da segurança da informação

# Pilares da segurança da informação

- **Confidencialidade** - capacidade do sistema de impedir que usuários não-autorizados tenham acesso à determinada informação, ao mesmo tempo em que usuários autorizados podem acessar a informação.

- **Integridade:** atributo de uma informação que indica que esta não foi alterada, ou se foi, o foi de forma autorizada; capacidade de um sistema de impedir que uma informação seja alterada sem autorização.

- **Disponibilidade:** indica a quantidade de vezes que o sistema cumpriu uma tarefa solicitada sem falhas em relação ao número de vezes em que foi solicitado a fazer uma tarefa.

# Outros princípios da segurança da informação

Alguns autores também consideram os seguintes princípios:

- **Autenticidade**: capacidade de garantir que um usuário, sistema ou informação é mesmo quem alega ser.

- **Não repúdio**: capacidade do sistema de provar que um usuário executou determinada ação no sistema. Também conhecido como irrefutabilidade.

# Problemas de segurança

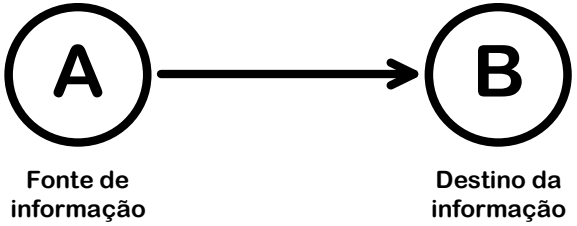
- Um problema de segurança é a perda de qualquer princípio de segurança que seja importante para o sistema.

- Os problemas de segurança podem ser causados por:
  - Desastre naturais
  - Operação incorreta por usuário
  - Ataque de sistema

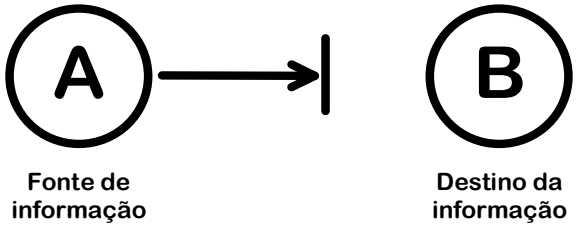
# Ataques de sistema

- Um ataque ao sistema é um problema de segurança em que um indivíduo busca obter algum retorno e com isso, provocar prejuízo para a empresa.
- Ataques de sistema são compostos por três elementos:
  - **Agente** – Quem realiza o ataque (invasor, atacante).
  - **Ativo** – algo de valor que é resguardado pelo sistema. O ativo incorpora algum atributo de segurança, como confidencialidade, por exemplo.
  - **Vulnerabilidade** – É uma fraqueza do sistema. Pode ser por um erro no código ou uma falha na especificação de segurança
- Denominamos de **ameaça** um ataque em potencial, isto é, um conjunto destes três elementos que permitem um ataque, causando a quebra de segurança

# Tipos de ataques e os aspectos da segurança que são impactados



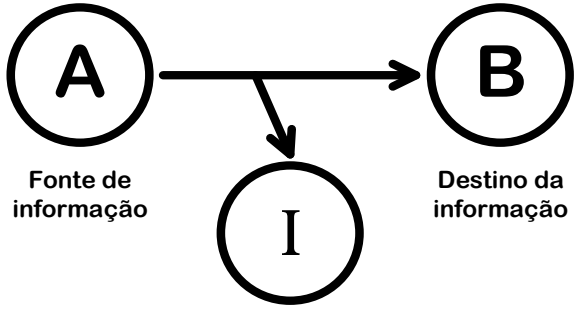

Fluxo normal




Interrupção

⇩

Disponibilidade

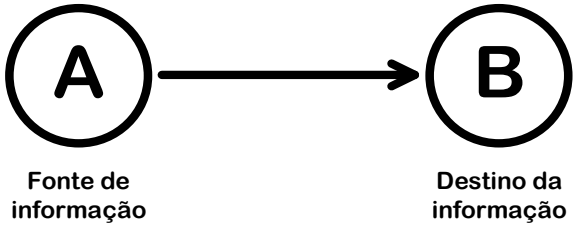



Intercepção

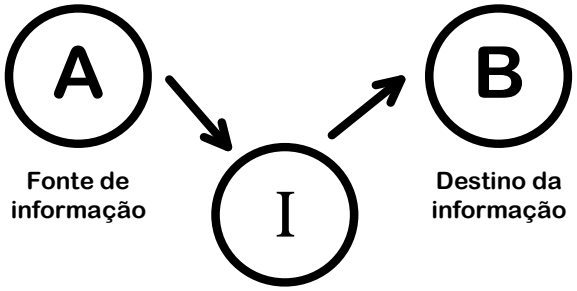
⇩

Confidencialidade

# Tipos de ataques



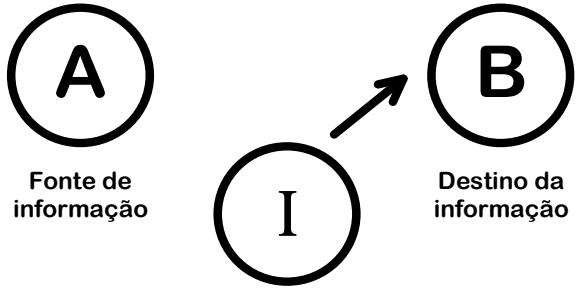

Fluxo normal




Modificação

⇩

Integridade




Fabricação

⇩

Autenticação

# Segurança da informação

- A área de segurança da informação é recente, por isso diversos autores utilizam os termos ameaça, ativo, vulnerabilidade e ataque com conotações diferentes.
- Estas definições são do ISO/IEC 15.408.
    - ISO/IEC 15.408 é um padrão internacional para segurança de computadores, voltado para a segurança lógica das aplicações e para o desenvolvimento de software seguro.

# Agentes de ataques

- O agente de uma ameaça é alguém que vai ganhar algo com sua eventual exploração.
- O objetivo do agente pode ser:
  - Financeiro – Interesse em obter retorno financeiro
  - Dano – Interesse em prejudicar uma empresa
  - Imagem – interesse em destacar suas habilidades
  - Aprendizado – interesse em estudar ferramentas
- Para o sucesso de um ataque, o autor precisa ter conhecimento do funcionamento do sistema.
- Usuários comuns podem ser perigosos se tiverem amplo acesso e conhecimento do sistema.

# Agentes de ataques

- Os agentes, não estão apenas na Internet. É comum que os agentes estejam dentro da própria empresa.

- Exemplos de agentes:
  - Estudantes
  - Estagiários ou ex-estagiários
  - Funcionários ou ex-funcionários
  - Prestadores de serviço
  - Polícia
  - Agência de inteligência

# Segurança em desenvolvimento de software

- Existem duas preocupações básicas quando se fala em segurança em desenvolvimento de software:
  - **Segurança do ambiente de desenvolvimento** – refere-se à preocupação em evitar que haja o roubo de código fonte ou sua indisponibilidade da equipe de desenvolvimento.
  - **Segurança da aplicação desenvolvida –** refere-se à uma aplicação que foi construída segundo uma especificação de segurança e não contenha acessos ocultos (*backdoors*), código malicioso ou falhas que comprometam a segurança.

# Vulnerabilidades e seus mecanismos

FURB
UNIVERSIDADE DE BLUMENAU

# Mecanismos

- Os mecanismos são formas de explorar as vulnerabilidades de um sistema.

- Para a concretização de uma ameaça, pode ser necessário mais de um mecanismo de ataque a ser usado de forma complementar.

- A redução dos erros nos sistemas de informação significa a redução de riscos e de vulnerabilidades. Portanto reduz as chances da ameaça de concretizar.