Segurança da informação

Introdução

FURB
UNIVERSIDADE DE BLUMENAU

Importância da Segurança da Informação

Prosegur fecha site no Brasil por 24 horas após ransomware

A **Prosegur** (...) foi atingida pelo malware **RYUK**, que trancou todos os seus arquivos no mundo.

A empresa fechou por um dia, mandando todos os seus 170 mil funcionários para casa. A estratégia para controlar os danos incluiu derrubar os sites da Prosegur ao redor do mundo, incluindo no Brasil.

Fonte: https://epocanegocios.globo.com/Tecnologia/noticia/2019/12/os-maiores-casos-de-violacao-de-dados-de-2019.html

O que é segurança da informação?

- Problemas de segurança podem pode trazer muitos prejuízos à empresa:
  - Parada de processos (prejuízo operacional)
  - Retrabalho (por perder informações)
  - Processos judiciais
  - Danos à 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

Os pilares da segurança da informação representam capacidades que um sistema deve possuir para ser considerado seguro.

Confidencialidade

Proteger os dados contra acesso não autorizado.

Integridade

Princípio que garante que a informação não seja alterada indevidamente

Disponibilidade

Garante que as informações e os sistemas estejam acessíveis sempre que necessário, para usuários autorizados.

Tríade da segurança

Outros princípios da segurança da informação

Alguns autores também consideram os seguintes princípios:

- **Autenticidade**: princípio que garante que a informação (ou o remetente) é genuína. 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.

Exemplo – Sistema de Saúde

Permitir que somente o paciente e médico consulte exames realizados

Confidencialidade

Garantir que os dados não sejam alterados indevidamente

Integridade

Estar disponível 24/7 para médicos e hospitais

Disponibilidade

Identificar corretamente o profissional que acessa o sistema

Autenticidade

Registrar ações para que ninguém negue depois o que fez

Não repúdio

Problemas de segurança

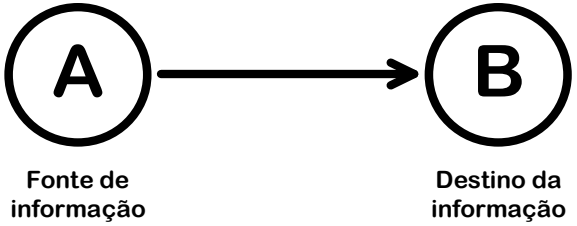
- Um **problema de segurança** é a perda de qualquer princípio de segurança que seja importante para o sistema.

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

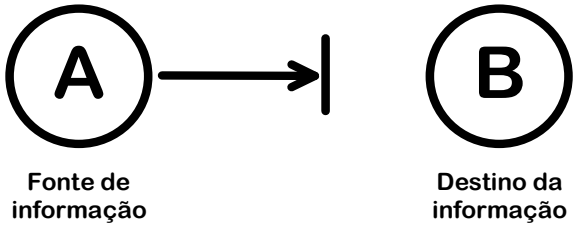
Ataques de sistema

- Um ataque ao sistema é uma ação intencional com objetivo de comprometer algum pilar da segurança da informação
- Ataques de sistema são compostos por três elementos:
  - **Agente** – Quem realiza o ataque (hacker, invasor, atacante, malfeitor, cibercriminoso, fraudador, golpista).
  - **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 princípios da segurança que são impactados



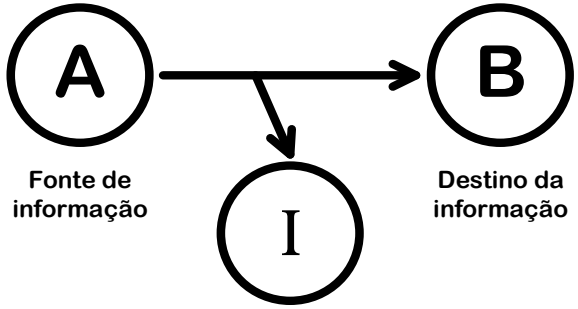
Fluxo normal



Interrupção

⇩

Disponibilidade

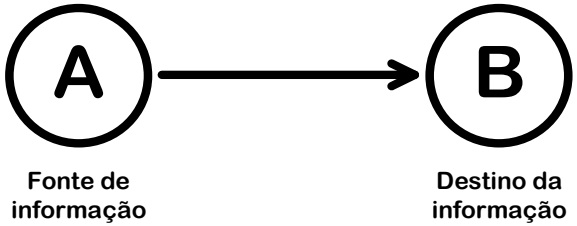


Intercepção

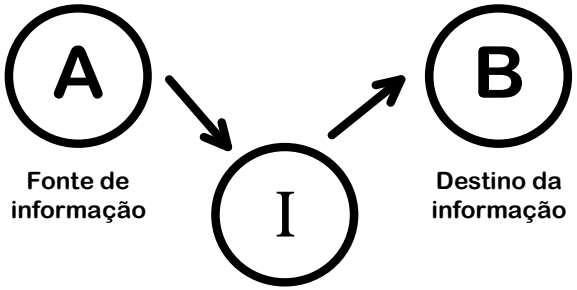
⇩

Confidencialidade

Tipos de ataques



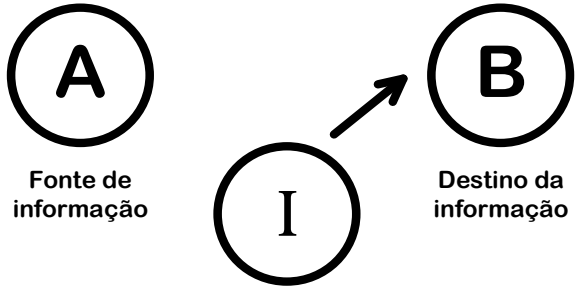
Fluxo normal



Modificação

⇩

Integridade



Fabricação

⇩

Autenticidade

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.

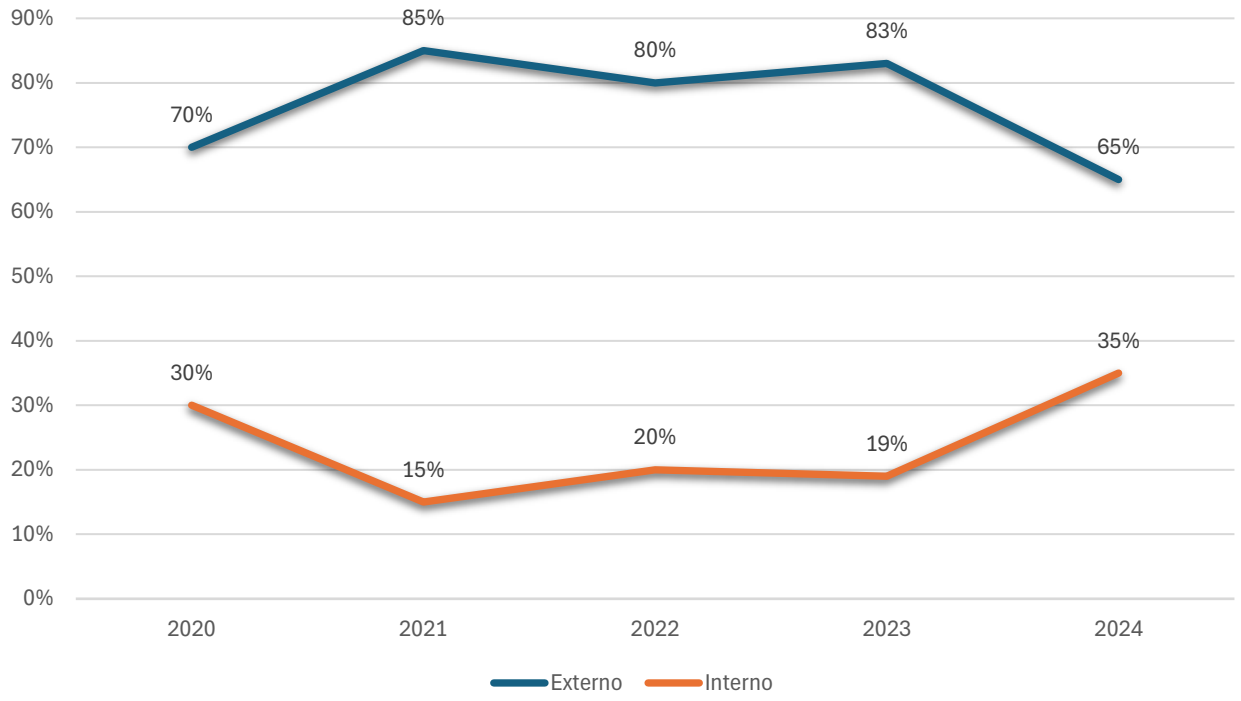
- Estas definições são do ISO/IEC 15.408.

  - 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 é alguém que vai ganhar algo com a eventual exploração da vulnerabilidade.
- 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



Fonte: Verizon DBIR

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.

Security by design

- Consiste em envolver segurança da informação desde as fases iniciais de concepção do software e não como uma etapa posterior ou corretiva.

- Busca evitar retrabalho e falhas em produção
  - Reduz custos
  - Maior resiliência
  - Conformidade legal
  - Aumento de confiança

Princípio do Security by design

- **Menor privilégio**: O usuário ou a aplicação deve ter apenas os privilégios necessários para realizar sua função
- **Fail-Safe Defaults**: A configuração padrão deve ser a mais segura possível. Negar acesso por padrão
- **Defesa em profundidade**: Aplicar controles em várias camadas. Se uma falhar, não compromete todo o sistema
- **Segurança como padrão**: A segurança é inegociável, mesmo que comprometa a usabilidade
- **Auditabilidade**: O sistema deve manter uma trilha de auditoria para detectar suspeitas ou violação

Exemplo – Trilha de auditoria

Data	Hora	Login	Ação
18/07/2025	10:32	user01	Login realizado com sucesso
18/07/2025	10:34	user01	Inclusão do produto código 123: "Teclado Gamer", preço R$ 80,00
18/07/2025	10:45	user01	Alteração do preço do produto código 123 para R$ 100,00
18/07/2025	10:59	user02	Login realizado com sucesso
18/07/2025	11:00	user02	Consulta de dados do produto código 123
18/07/2025	11:15	user01	Alteração do nome do produto código 123 para "Teclado Gamer RGB"
18/07/2025	11:20	user02	Inclusão do produto código 456: "Mouse Óptico", preço R$ 45,00