Introdução

PROPRIEDADES DA SEGURANÇA DA INFORMAÇÃO

* **CONFIDENCIALIDADE**: informação deve ser revelado somente aos usuários autorizados.
* **INTEGRIDADE**: informação não deve ser manipulado acidentalmente ou de maneira não autorizada.
* **DISPONIBILIDADE**: informação deve estar disponível quando necessário.

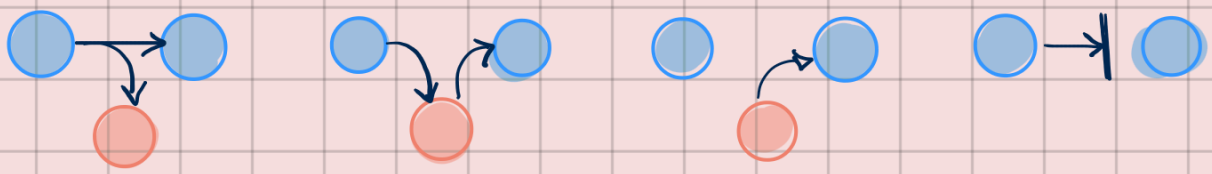
+ 2 PROPRIEDADES

* **AUTENTICIDADE**: garante que a informação é de quem diz ser.
* **RESPONSABILIDADE**: capacidade de rastrear as informações até o indivíduo / processo.

CONFIDENCIALIDADE x PRIVACIDADE

- CONFIDENCIALIDADE → informação de forma geral
- PRIVACIDADE → informação sobre si mesmo

CLASSIFICAÇÃO DE ATAQUES



interceptação | modificação | personificação | interrupção

VULNERABILIDADE, AMEAÇA e ATAQUE

- **VULNERABILIDADE**: fraqueza do sistema que pode ser explorado por um atacante
- **AMEAÇA**: qualquer ação ou entidade que tem potencial de causar danos no sistema.
- **ATAQUE**: concretização do ameaça, quando a vulnerabilidade é explorada.

VULNERABILIDADE DE DIA ZERO:

não é conhecido ainda pelo desenvolvedor, portanto não tem uma correção disponível.

Incidentes de segurança

* **VAZAMENTO de dados**: Compromete confidencialidade.
* **PERDA de dados**: Compromete integridade.
* **indisponibilidade**: Compromete disponibilidade.

SEGURANÇA DA INFORMAÇÃO

* Consiste em proteger sistemas computacionais contra ataques, danos ou acessos não autorizados para garantir a confidencialidade, integridade e disponibilidade.

IOT x SEGURANÇA

* Questão levantada: dispositivos IOT precisam frequentemente de atualizações para se proteger de novas ameaças. Como entregar essa solução para, por exemplo, uma geladeira inteligente já instalada?

"SEGURANÇA É SEMPRE UMA TROCA"

* segurança Vs funcionalidades.
* segurança Vs usabilidade.
* segurança Vs desempenho.
* segurança Vs custo.

CVE e CWE

CWE → FRAQUEZAS

CVE → VULNERABILIDADES

* Catálogos de vulnerabilidades e fraquezas

podem vir a se tornarem vulnerabilidades