(CMPSEGS)

Segurança de Sistemas

Tecnologia em Análise e Desenvolvimento de Sistemas

Princípios da segurança de Sistemas de Informação
Ameaças, vulnerabilidades e ataques

Prof. Me. Leonardo Arruda
leonardo.arruda@ifsp.edu.br

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Aula anterior: Segurança física de sistemas

- Definir um local físico adequado para o datacenter;
- Considerações: desastres naturais, falhas de energia e internet.
- Ameaças: incêndios, inundações e acessos não autorizados;

Aula anterior: Segurança física de sistemas

- **Controle de acesso**:
  - Senhas, Smartcards, tokens e biometria (impressão digital, íris, voz, etc.) e CFTV para monitoramento.

- **Políticas de segurança física:**
  - Restrições de acesso, etiquetagem de materiais, controle de temperatura e planos de contingência.

- **Vulnerabilidades:**
  - Falta de controle de acesso, servidores usados como estações de trabalho e ausência de backups adequados;

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança da Informação

Conceitos Fundamentais

Qual a importância da informação?

- A informação abarca diversos atributos no cotidiano do ser humano:
- Exemplos: Adquirimos cidadania, cultura, desenvolvimento profissional, pessoal e social;
- Aprendemos a ser competitivos;
- Sinalização para influência e poder;

Conceitos Fundamentais

A informação no contexto de Sistemas de Informação:

- É um ativo;
- Elemento de valor para um indivíduo ou organização;
- Necessita de proteção adequada;

Conceitos Fundamentais

Proteger a informação é fundamental em várias vertentes:

Organizacional:
Informações comerciais, patentes, direitos, etc.

Legal:
Direito de propriedade, responsabilidade por atos praticados.

Pessoal:
Anonimato e privacidade (LGPD)

Política/Administrativa:
Transparência, informações estratégicas de um país ou empresa.

Conceitos Fundamentais

Proteger a informação é fundamental em várias vertentes:

Organizacional:
Informações comerciais, patentes, direitos, etc.

Legal:
Direito de propriedade, responsabilidade por atos praticados.

Pessoal:
Anonimato e privacidade (LGPD)

Política/Administrativa:
Transparência, informações estratégicas de um país ou empresa.

O responsável pela definição da política de informação de uma organização ou empresa, leva em consideração todos estes aspectos.

Leis e Normas

Lei nº 12.737/2012

- Dispõe sobre a tipificação criminal de delitos informáticos;
- **Art. 154-A**.
  - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança;
  - Obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo;
  - Instalar vulnerabilidades para obter vantagem ilícita:
- **Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.**

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Família ISO/IEC 27000

A **Família ISO/IEC 27000** é um **conjunto de normas internacionais** voltadas para a **gestão da segurança da informação**.

Essas normas fornecem **conceitos**, **requisitos**, **diretrizes** e **boas práticas** para proteger dados contra acessos não autorizados, alterações indevidas e perdas.

Elas são utilizadas por organizações no mundo todo para criar, **implementar**, **monitorar** e **melhorar** continuamente sistemas de gestão de segurança da informação (SGSI)

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Família ISO/IEC 27000

- ISO/IEC 27000:2016 – Apresenta a visão geral da família de normas e define a terminologia utilizada.
- **ISO/IEC 27001:2013 (ABNT NBR)** – Estabelece requisitos para implementar e manter um Sistema de Gestão da Segurança da Informação (SGSI).
- **ISO/IEC 27002:2013 (ABNT NBR)** – Código de prática com controles e medidas de segurança para proteger informações.

INSTITUTO FEDERAL São Paulo Campus Campinas

Família ISO/IEC 27000

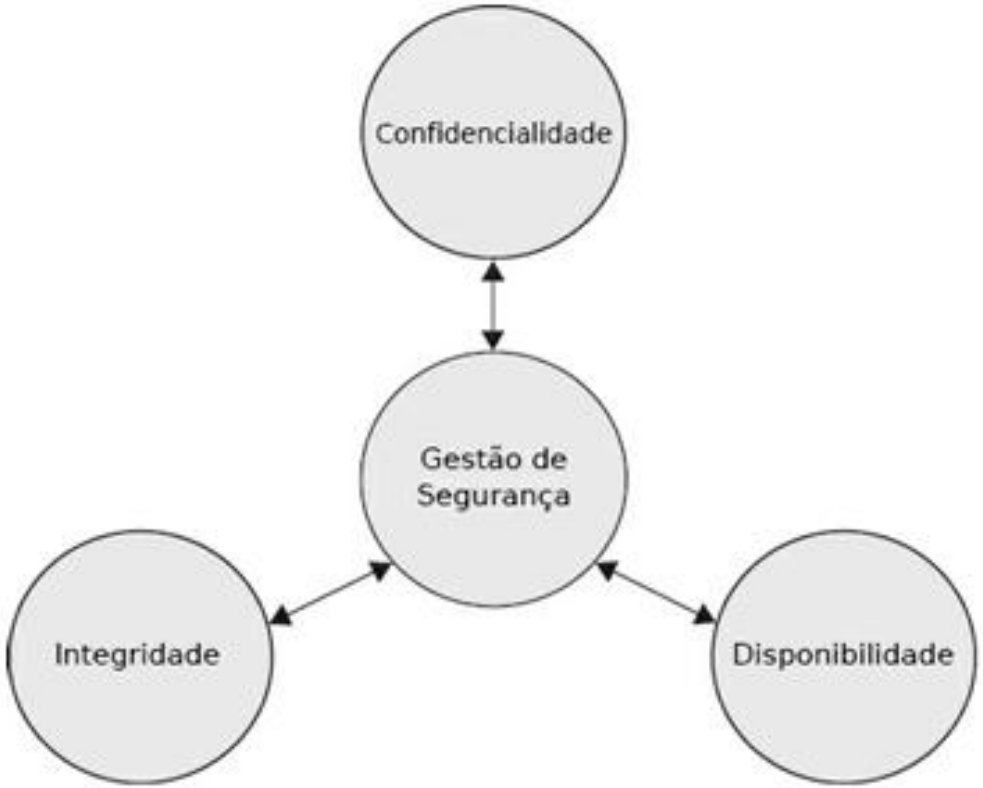
- ISO/IEC 27003:2015 (ABNT NBR) – Diretrizes para implantação de um SGSI, orientando o planejamento e execução.
- ISO/IEC 27005:2011 (ABNT NBR) – Gestão de riscos de segurança da informação, com métodos para identificar, avaliar e tratar riscos.
- ISO/IEC 27007:2012 (ABNT NBR) – Diretrizes para auditoria de sistemas de gestão da segurança da informação.
- ISO/IEC 27014:2013 (ABNT NBR) – Governança da segurança da informação, alinhando práticas de segurança aos objetivos estratégicos da organização.

Princípios da Segurança da Informação

A segurança da informação é a área do conhecimento dedicada à proteção dos ativos de informação contra acessos não autorizados, alterações indevidas ou indisponibilidade. Ela também pode ser entendida como a prática de gestão de riscos que possam comprometer três princípios fundamentais: **confidencialidade**, **integridade** e **disponibilidade** das informações (HINTZBERGEN et. al, 2018).

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p

Princípios da Segurança da Informação



Tríade CID

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p

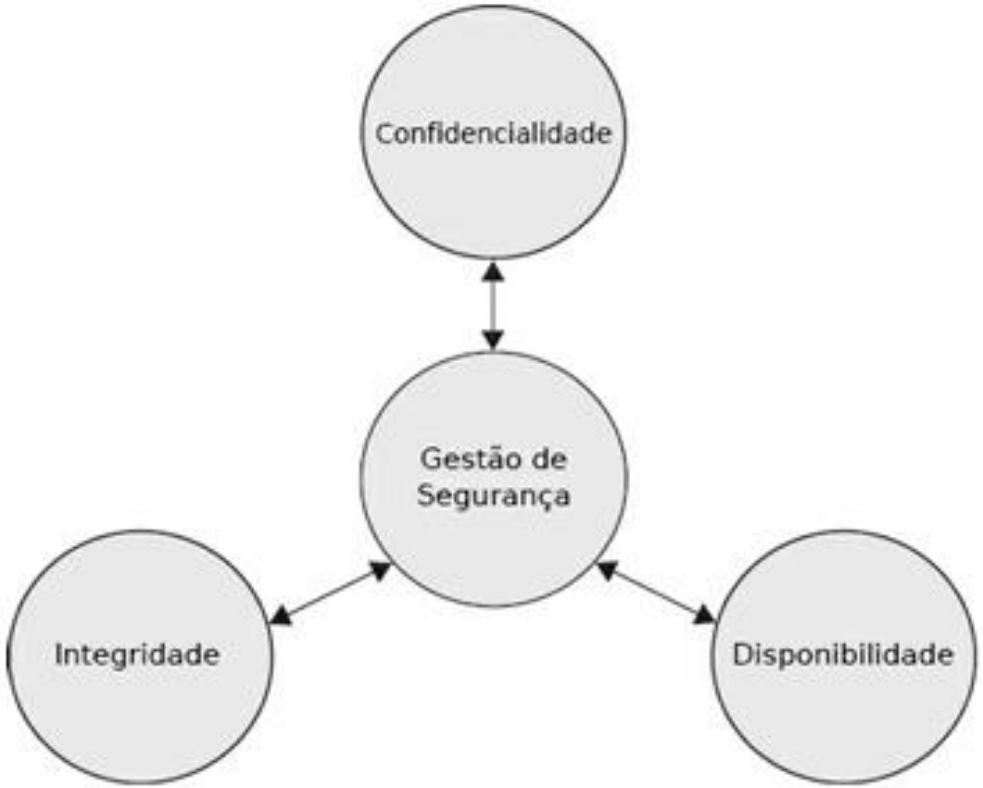
Aspectos da Segurança da Informação

No ambiente corporativo, a segurança da informação se amplia para alinhar-se aos desafios do negócio, incorporando dois conceitos-chave:

- **Autenticidade**, que garante a veracidade das informações e a legitimidade das partes envolvidas, e
- **Conformidade**, que assegura o cumprimento de leis, regulamentos e compromissos dentro do modelo GRC (Gestão de Governança, Risco e Conformidade).

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 2. ed. Rio de Janeiro: Elsevier, 2014.

Princípios da Segurança da Informação



Tríade CID

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p

Princípios da Segurança da Informação

Confidencialidade:

- Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas a quem é destinada.
  - **Exemplo corporativo**: Executivos protegem planos estratégicos contra concorrentes.
  - **Exemplo pessoal**: Pessoas protegem seus registros financeiros de acesso não autorizado.

- Mantida em todos os momentos: armazenamento, transmissão ou utilização;

Princípios da Segurança da Informação

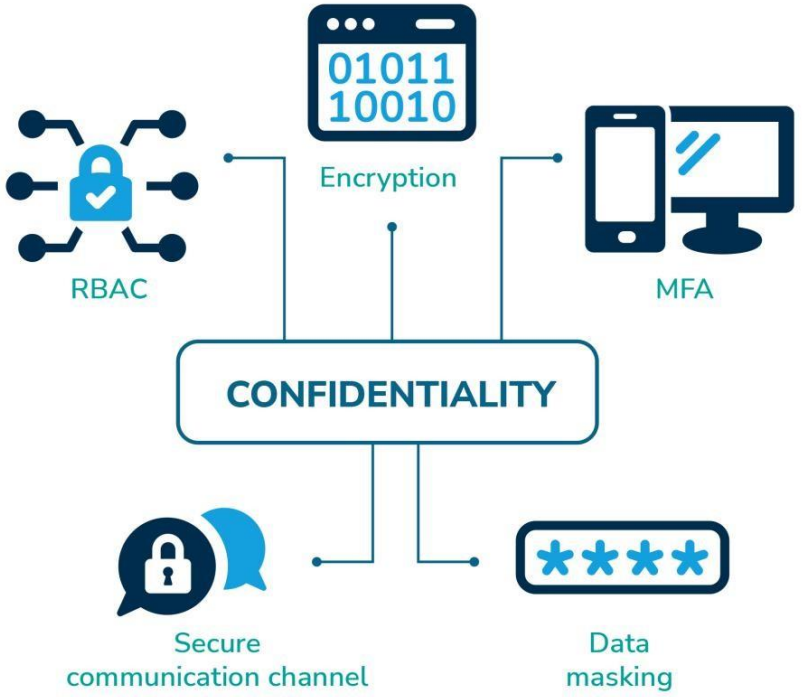
Como é aplicada a confidencialidade:

- **Criptografia**: Protege dados em trânsito e em repouso, garantindo que apenas usuários autorizados consigam ler a informação.
- **Controle de acesso**: Permite que apenas quem precisa conhecer determinada informação tenha acesso a ela (“necessidade de conhecer”).
- **Políticas físicas e de comportamento**: Não deixar documentos confidenciais sobre a mesa; Separação de funções, como desenvolvimento e processamento de sistemas, para evitar conflito de interesses.
- **Autenticação de usuários**: Combinação de login, senha e, às vezes, tokens ou senhas temporárias (one-time password).
- **Preenchimento de tráfego (traffic padding):** Técnica que envia dados aleatórios junto com os dados reais, dificultando que um atacante descubra padrões de tráfego e volume de dados.

Princípios da Segurança da Informação

Confidencialidade:

- Confidencialidade é **manter a informação secreta e protegida**, usando métodos técnicos (criptografia, autenticação), administrativos (regras, políticas, separação de funções) e físicos (controle de acesso a documentos e ambientes).
- O objetivo é que somente pessoas ou sistemas autorizados possam acessar dados, evitando vazamentos e uso indevido.



Princípios da Segurança da Informação

Integridade:

- Garante que a informação seja correta, completa e consistente com o estado ou valor desejado. Qualquer modificação não autorizada, deliberada ou acidental, é uma violação da integridade.
  - **Exemplos:**
    - Dados armazenados em discos devem permanecer estáveis;
    - Programas devem gravar informações corretamente sem introduzir valores errados;
    - Um usuário não deve, por engano, apagar arquivos essenciais ou inserir valores incorretos em sistemas.

Princípios da Segurança da Informação

Como a integridade pode ser comprometida:

- **Ataques maliciosos:** Vírus, hackers que alteram preços em um e-commerce, modificam registros bancários ou inserem dados falsos em sistemas corporativos.
- **Erros de usuários:** Apagar arquivos por engano, inserir valores incorretos ou modificar registros incorretamente.

Princípios da Segurança da Informação

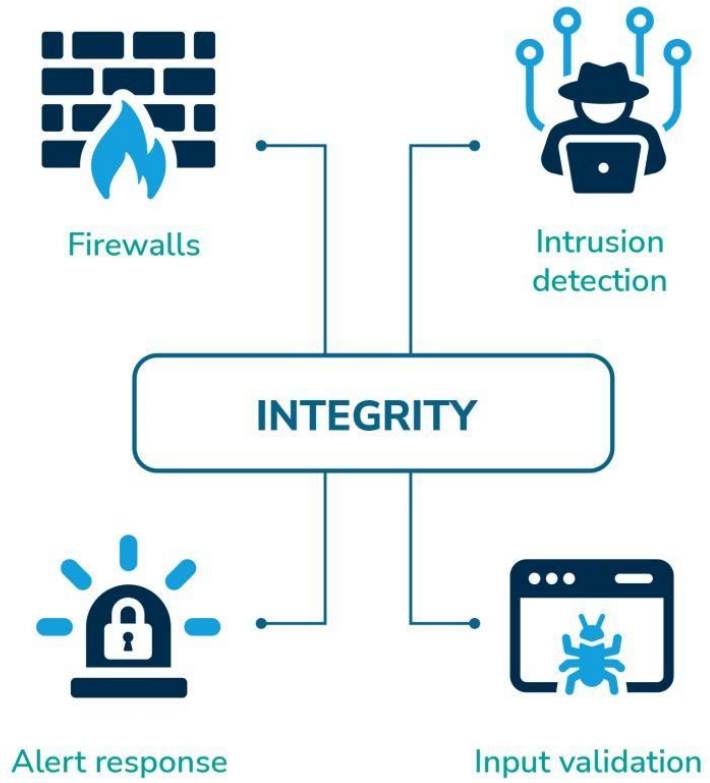
Medidas para garantir integridade:

- **Autorização de alterações:** Apenas pessoas autorizadas podem modificar sistemas e dados.
- **Padronização de termos e dados**: Evitar inconsistências, como usar “cliente” sempre e não “freguês”.
- **Registro de ações (logging):** Rastrear quem modificou a informação.
- **Segregação de funções:** Ações críticas exigem a participação de mais de uma pessoa.
- **Criptografia:** Protege dados de alterações ou acessos não autorizados.

Princípios da Segurança da Informação

Integridade:

- A integridade garante que a informação seja **precisa, completa e confiável**, prevenindo alterações acidentais ou maliciosas, e assegurando que os dados permaneçam consistentes e corretos ao longo do tempo.



Princípios da Segurança da Informação

Disponibilidade:

- Garante que a informação e os sistemas estejam **acessíveis** e **utilizáveis quando necessário**. Ou seja, os dados devem estar sempre à disposição de quem precisa deles, mesmo diante de falhas, ataques ou problemas técnicos.

Principais características da disponibilidade:

- **Oportunidade**: Informação acessível no momento em que é necessária;
- **Continuidade:** Equipe consegue trabalhar mesmo diante de falhas ou interrupções;
- **Robustez:** Capacidade do sistema de suportar toda a equipe trabalhando simultaneamente

Princípios da Segurança da Informação

Como a disponibilidade pode ser comprometida:

- **Falhas técnicas**: Problemas em discos, servidores, softwares ou equipamentos.
- **Questões ambientais**: Calor, frio, umidade, eletricidade estática ou contaminantes.
- **Ataques de hackers:** Denial-of-Service (DoS) que impedem o acesso a sistemas ou informações.
- **Atrasos:** Qualquer atraso acima do nível de serviço esperado pode ser considerado violação da disponibilidade

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Princípios da Segurança da Informação

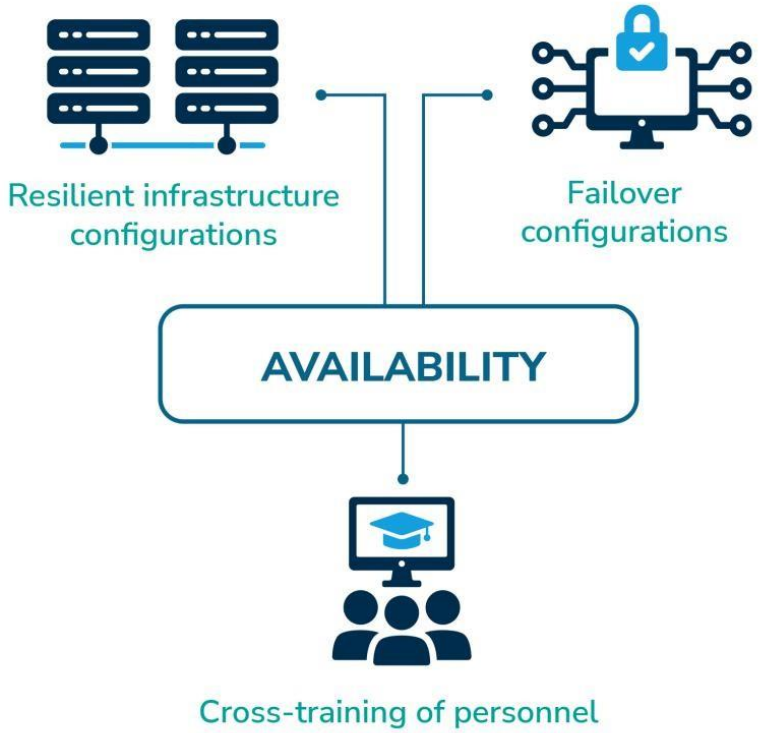
Como garantir a disponibilidade:

- **Backup e redundância:** Dados armazenados em discos de rede, cópias físicas separadas do negócio, procedimentos de backup definidos.
- **Treinamento e equipe qualificada**: Pessoas preparadas para restaurar sistemas rapidamente.
- **Proteção ambiental**: Sistemas devidamente aterrados, monitorados e protegidos contra fatores externos.
- **Segurança de rede**: Configuração adequada de roteadores, firewalls e monitoramento de tráfego por IDS.
- **Planos de emergência**: Procedimentos para recuperação rápida das atividades após interrupções.
- **Conformidade legal**: Armazenamento de dados conforme exigências regulatórias locais.

Princípios da Segurança da Informação

Disponibilidade:

- Disponibilidade é **garantir que os dados e sistemas estejam sempre acessíveis**, mesmo diante de falhas técnicas, ambientais ou ataques, mantendo a continuidade das operações e minimizando perdas de informação.



HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p

Princípios da Segurança da Informação

Autenticidade:

- Garante que as entidades envolvidas em uma comunicação — **informações**, **máquinas** ou **usuários** — sejam exatamente quem dizem ser e que a mensagem ou informação **não foi alterada** após seu envio ou **validação**.

Princípios da Segurança da Informação

Principais pontos da autenticidade:

1. **Origem correta**: O remetente de uma mensagem é **corretamente identificado** pelo destinatário.
2. **Certificação Digital**: aplica **criptografia e hash**, especialmente em infraestruturas de chave pública (PKI), para garantir: Irretratabilidade, Identidade, Autenticidade, Autoria, Originalidade, Integridade e Confidencialidade;
3. **Verificação contínua:** A autenticidade deve ser **checada durante toda a comunicação**, para garantir que o usuário ou sistema que iniciou a troca de informações continue sendo o mesmo.

Sistema bancário online: a autenticidade garante que todas as transações realizadas sejam realmente iniciadas pelo usuário autorizado, prevenindo fraudes ou transações falsas.

Princípios da Segurança da Informação

Irretratabilidade:

- Garante que o emissor e o destinatário de uma informação não possam negar que a informação foi enviada, recebida ou que estiveram em posse dela (não repúdio).

- Irretratabilidade é a garantia de que **nenhuma das partes envolvidas em uma comunicação possa negar sua participação**, sendo uma ferramenta importante em transações eletrônicas e contratos digitais.

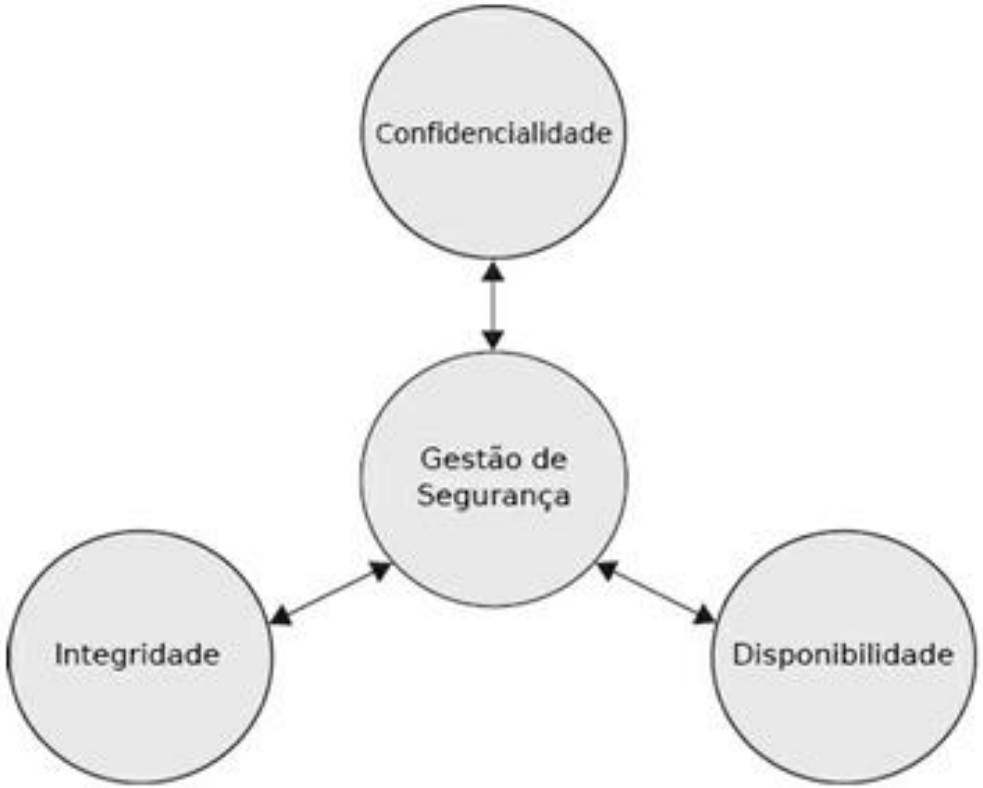
Princípios da Segurança da Informação

Principais pontos:

1. **Garantia adicional à autenticidade**: Além de confirmar a identidade do remetente e receptor, permite provar a origem e a transmissão dos dados, inclusive perante terceiros.
2. **Relacionamento com assinaturas digitais:** Funciona de forma similar a uma assinatura manual, mas com garantias matemáticas que comprovam a autoria e a integridade da informação.

Uma empresa envia um contrato assinado digitalmente; a assinatura garante que o remetente **não possa negar o envio**, e o destinatário **não possa negar o recebimento**

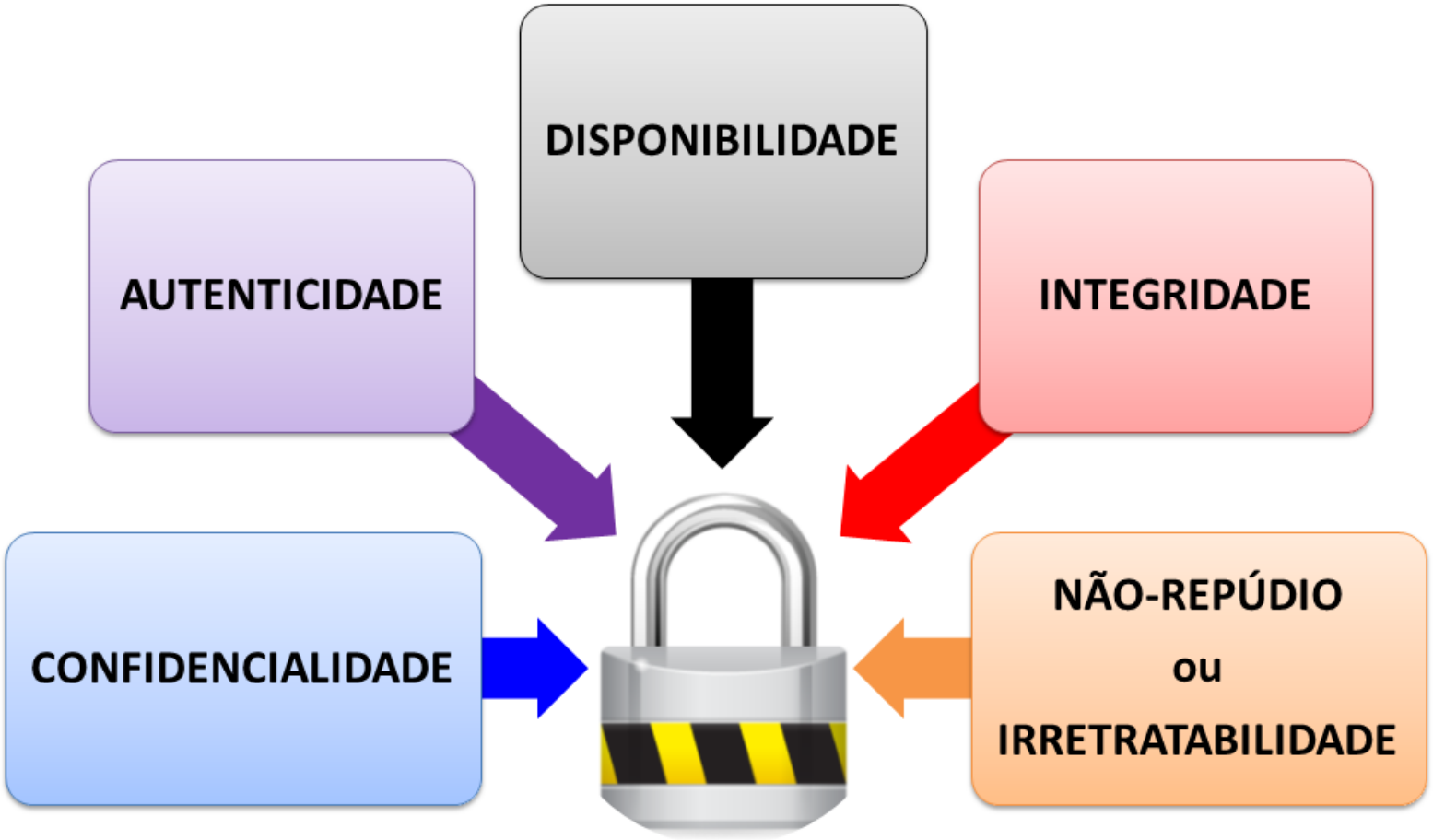
Princípios da Segurança da Informação



Tríade CID

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***. 1. ed. Rio de Janeiro: Brasport, 2018. 256 p

Princípios da Segurança da Informação



SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 2. ed. Rio de Janeiro: Elsevier, 2014.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Vulnerabilidade

Uma vulnerabilidade é uma fraqueza em um ativo ou grupo de ativos que pode ser explorada por ameaças, permitindo a ocorrência de **incidentes de segurança** que afetam **confidencialidade**, **integridade** ou **disponibilidade**.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Vulnerabilidade

Tipos de vulnerabilidades:

- **Físicas**: instalações inadequadas, controle de acesso fraco, falta de extintores;
- **Naturais**: riscos de desastres naturais ou condições ambientais.
- **Hardware**: falhas em computadores, servidores ou componentes mal configurados.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Vulnerabilidade

Tipos de vulnerabilidades:

- **Software**: erros de codificação, instalação ou configuração.
- **Mídias**: problemas em discos, fitas, relatórios ou impressos.
- **Comunicação**: vulnerabilidades em sistemas de comunicação.
- **Humanas**: falta de treinamento, conscientização ou verificação de antecedentes.

Ameaças

Uma **ameaça** é qualquer agente ou condição que possa explorar vulnerabilidades em ativos de informação, causando **incidentes de segurança** que afetam **confidencialidade, integridade e disponibilidade** e gerando impactos nos negócios da organização.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

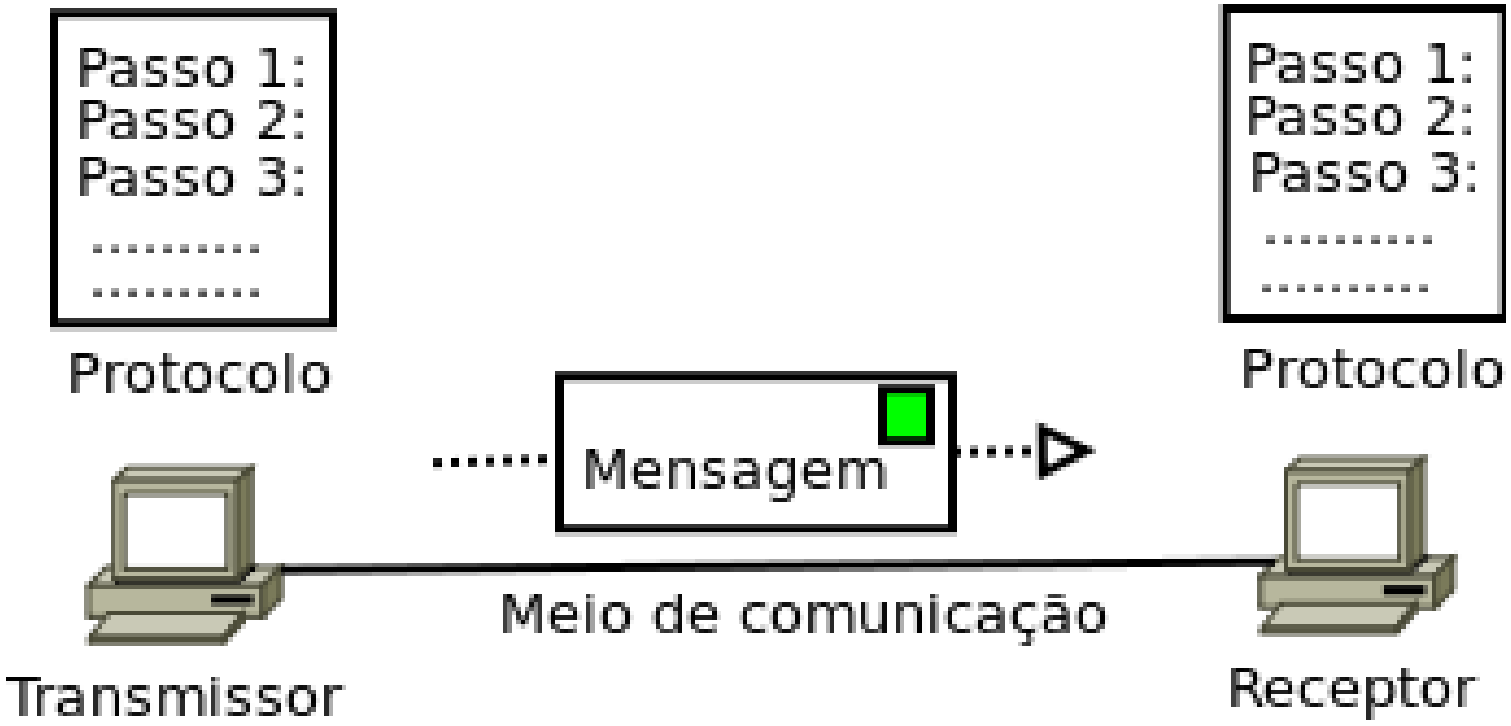
Ameaças

Tipos de ameaças:

- **Naturais**: Decorrentes de fenômenos da natureza.
- **Involuntárias**: Decorrentes de ações humanas inconscientes ou desconhecimento (acidentes, erros de operação, falhas de energia etc.).
- **Voluntárias**: intencionalmente por agentes humanos maliciosos (hackers, espiões corporativos, ladrões etc.).

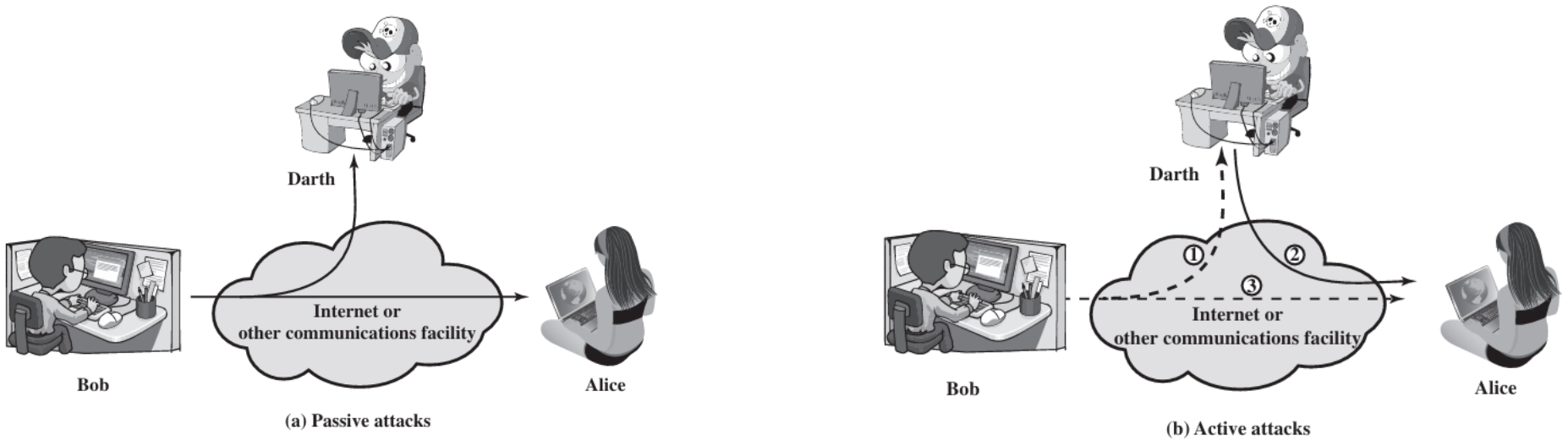
INSTITUTO FEDERAL
São Paulo
Campus Campinas

Fluxo de Comunicação



Ataques

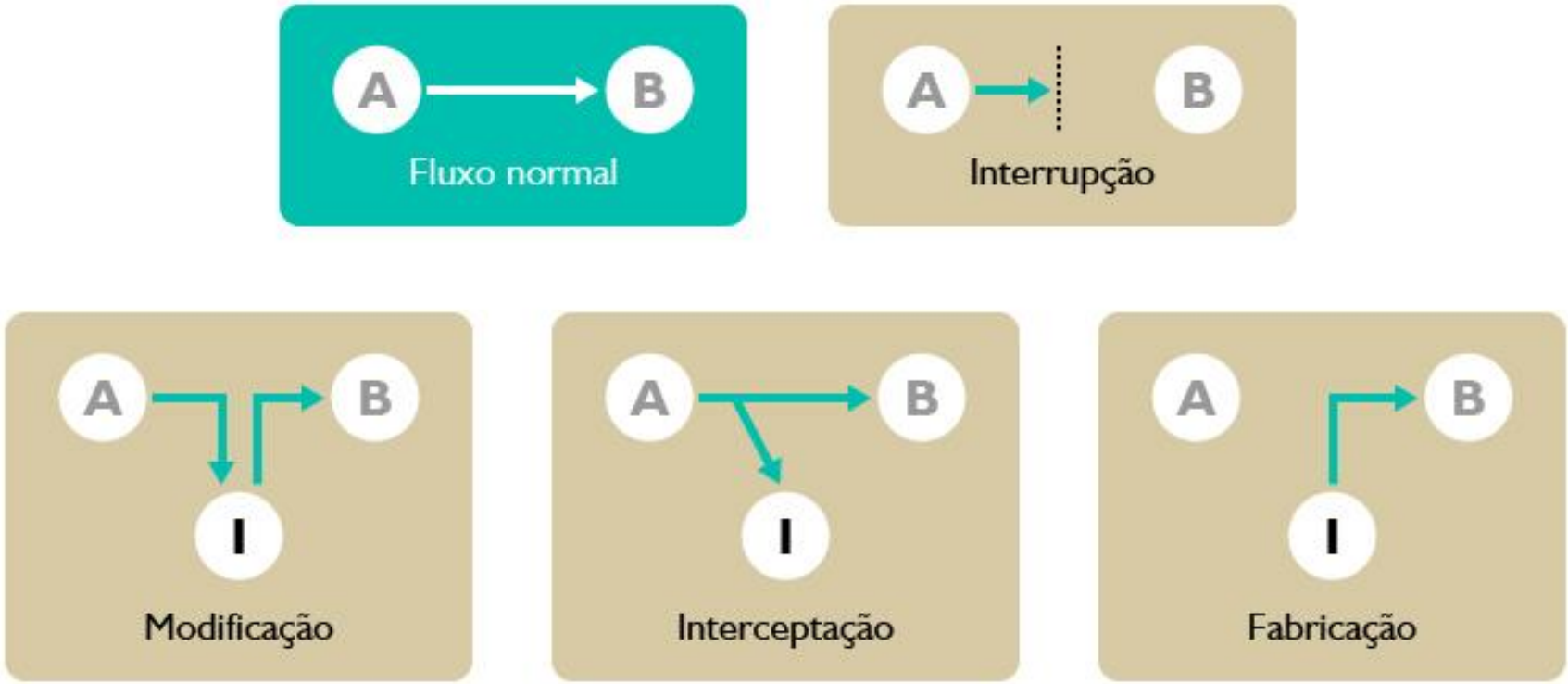
Um **ataque** é definido como uma técnica utilizada por um agente malicioso para explorar uma vulnerabilidade em um sistema de informação, com o objetivo de comprometer a segurança, afetando a confidencialidade, integridade ou disponibilidade dos dados ou serviços (STALLINGS, 1999).



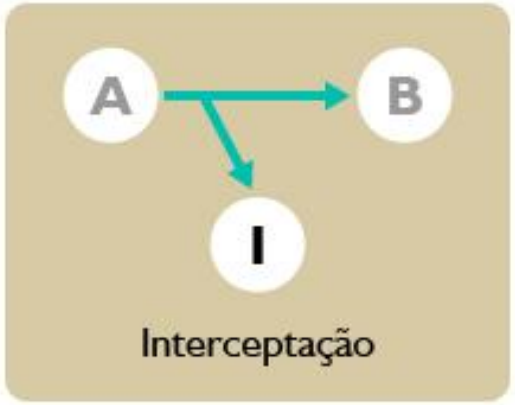
STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. 2. ed. Upper Saddle River: Prentice Hall, 1999.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Ataques vs. Serviços



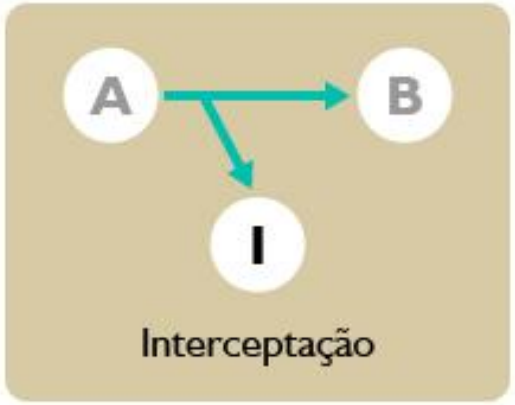
Ataques vs. Serviços



Interceptação

- Vazamento de informações (ex.: senhas);

Ataques vs. Serviços



Interceptação

- Vazamento de informações (ex.: senhas);
- Para evitar que o intruso entenda o conteúdo das mensagens é necessário cifrar os dados (**confidencialidade**);

Ataques vs. Serviços

Interrupção

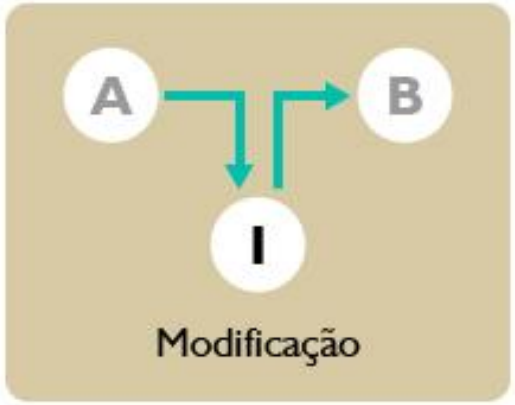
- Dados (requisição ou resposta) nunca chegam ao destino. Ex.: “derrubar um site”.

Ataques vs. Serviços

Interrupção

- Dados (requisição ou resposta) nunca chegam ao destino. Ex.: “derrubar um site”.
- É necessário a segurança física dos recursos de processamento e de comunicação de dados (**disponibilidade**);

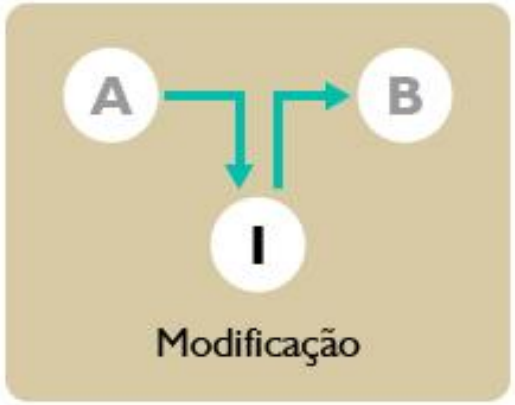
Ataques vs. Serviços



Modificação

- Informações corrompidas/falsas. Ex.: “alterar o destino de um pagamento bancário”.

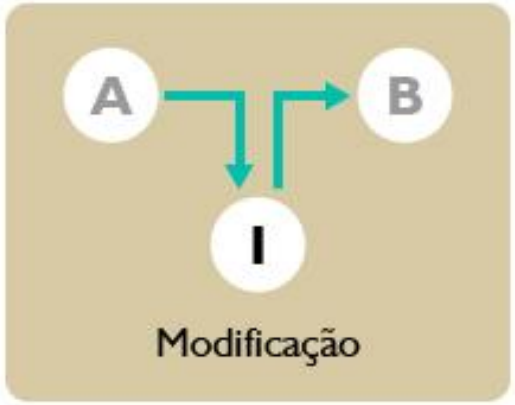
Ataques vs. Serviços



Modificação

- Informações corrompidas/falsas. Ex.: “alterar o destino de um pagamento bancário”.
- Para evitar este ataque é preciso garantir a **integridade** e **autenticidade** dos dados.

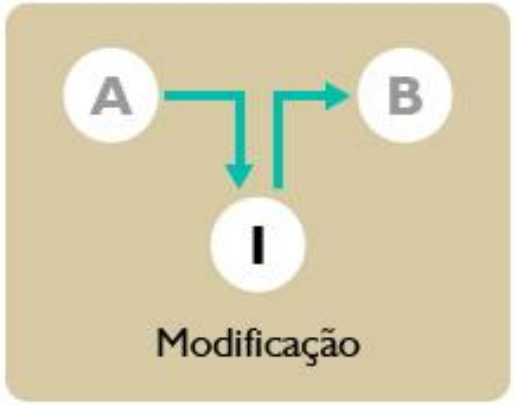
Ataques vs. Serviços



Modificação

- Informações corrompidas/falsas. Ex.: “alterar o destino de um pagamento bancário”.
- Para evitar este ataque é preciso garantir a **integridade** e **autenticidade** dos dados.
- **Confidencialidade?**

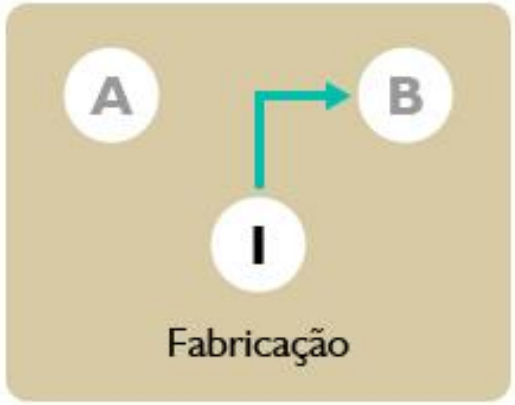
Ataques vs. Serviços



Modificação

- Informações corrompidas/falsas. Ex.: “alterar o destino de um pagamento bancário”.
- Para evitar este ataque é preciso garantir a **integridade** e **autenticidade** dos dados.
- Confidencialidade: Não resolveria pois o intruso pode não conseguir alterar do jeito que gostaria a mensagem.

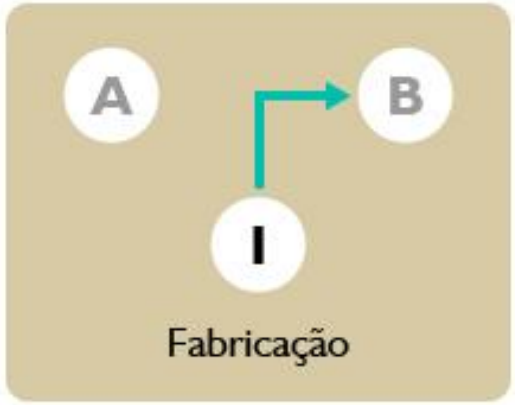
Ataques vs. Serviços



Fabricação

- Mensagens criadas por atacante. Ex.: gerar uma ordem de pagamento falsa.

Ataques vs. Serviços



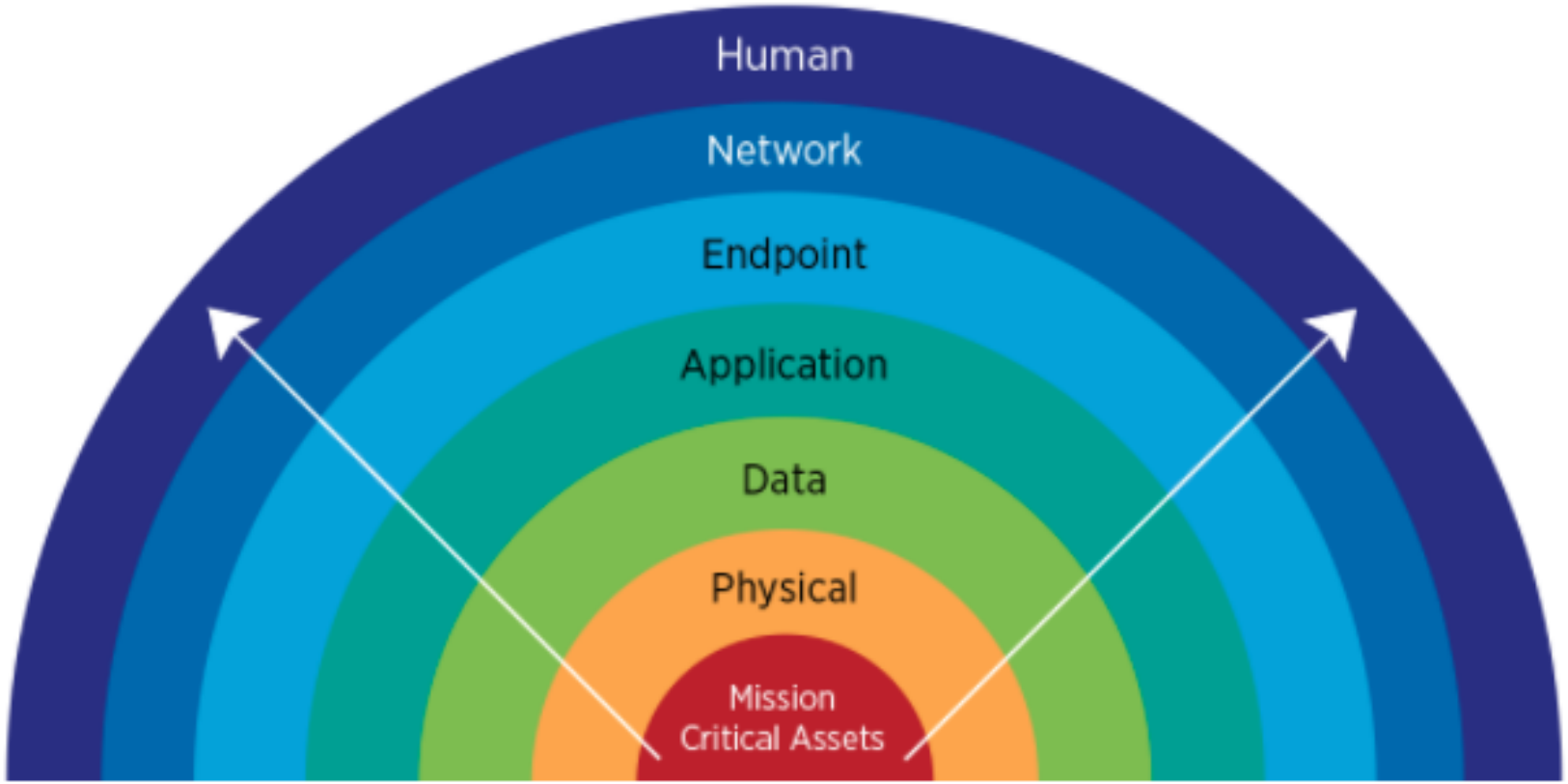
Fabricação

- Mensagens criadas por atacante. Ex.: gerar uma ordem de pagamento falsa.
- Para evitar este ataque é preciso garantir a **autenticidade**.

Estatísticas do CERT.br

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança em camadas



INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança em camadas

Combinação de múltiplos controles de segurança para proteger sistemas em várias camadas, dificultando ataques.

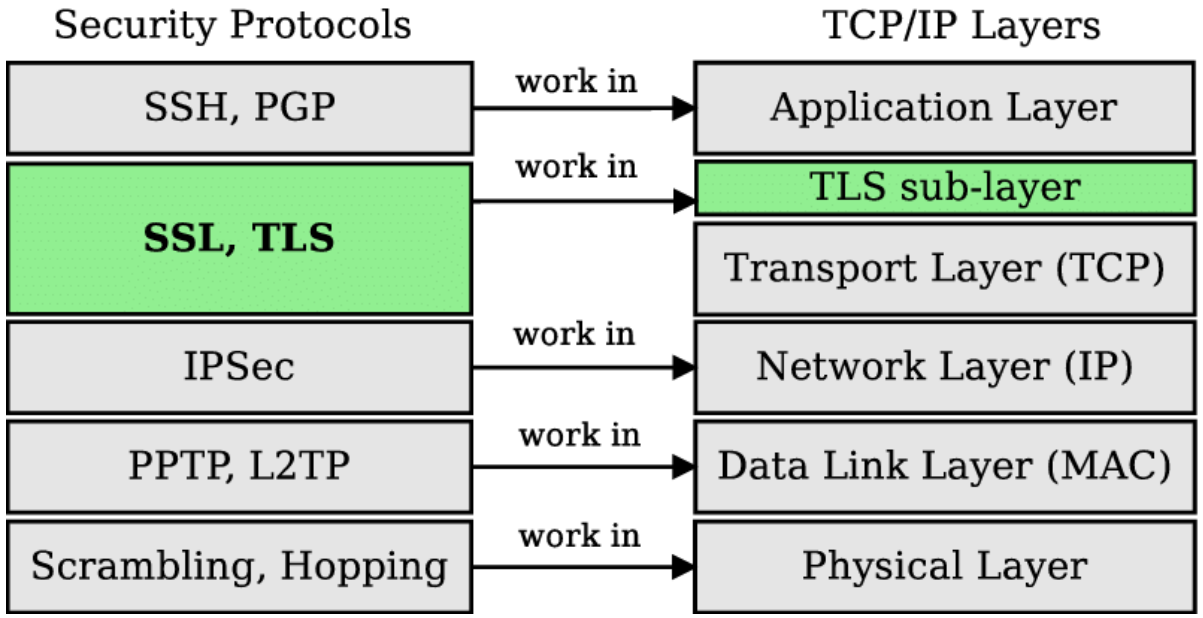
Objetivos: equilibrar segurança e desempenho — muita segurança pode prejudicar o desempenho, e muito desempenho pode comprometer a segurança

Inspiração: Utiliza conceitos comuns em computação e comunicação, como o Modelo OSI, onde cada camada possui mecanismos próprios de segurança

Segurança em camadas

Protocolos da camada de aplicação:

- **SSH (Secure Shell):** protege sessões remotas e gerencia conexões TCP de forma segura.
- **PGP (Pretty Good Privacy):** protege emails e arquivos de aplicações específicas.

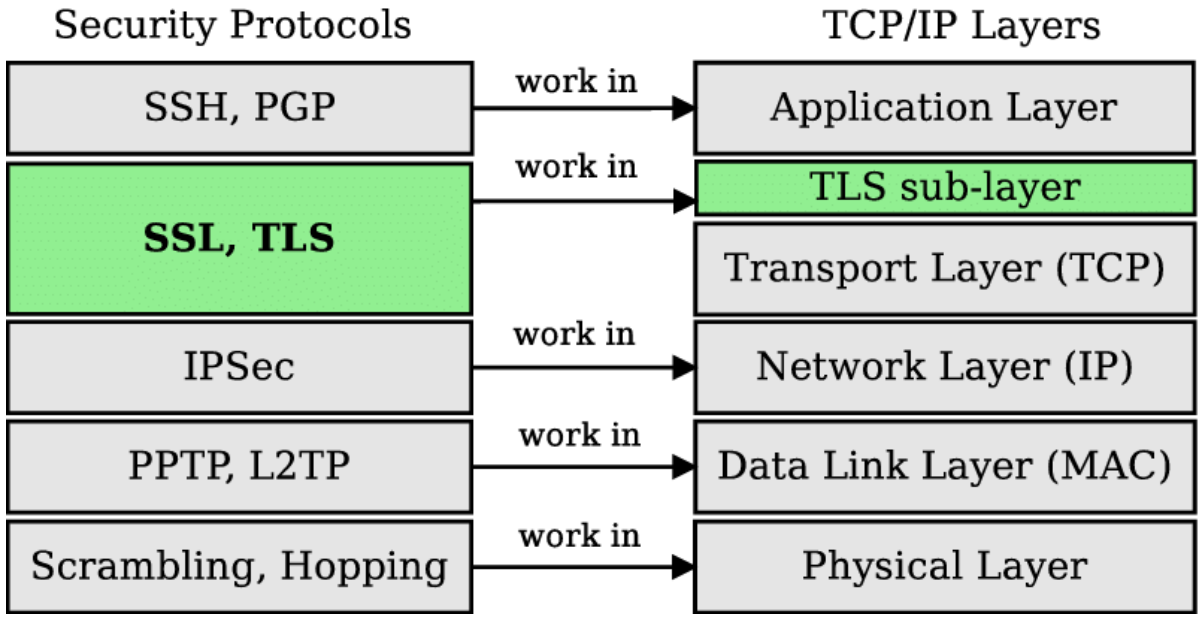


Segurança em camadas

SSL (Secure Sockets Layer) e TLS (Transport Layer Security):

- Camada de aplicação e a camada de transporte.

- Infraestrutura de Chave Pública (PKI) para:
  - Autenticação (verificar identidade de servidores e clientes);
  - Criptografia simétrica para manter a confidencialidade dos dados;



Segurança em camadas

HUMANA

Refere-se aos usuários e colaboradores da organização.

Objetivo: ensinar boas práticas de segurança, como reconhecer fraudes e proteger informações sensíveis.

Ameaças mais comuns: engenharia social, que induz o funcionário a realizar ações que comprometem a segurança

Segurança em camadas

FÍSICA

Abrange infraestrutura física e equipamentos (CPD, servidores, hardware crítico).

Objetivo: impedir acesso não autorizado e proteger equipamentos, mantendo-os operacionais 24h.

Exemplos de proteção: câmeras, alarmes, travas, guardas e senhas físicas

Segurança em camadas

ENDPOINT

Foca nos dispositivos de acesso à rede, como computadores, notebooks e dispositivos móveis.

Objetivo: proteger contra programas maliciosos e garantir a comunicação segura entre aplicações.

Exemplo de ação: uso de APIs seguras, antivírus e gerenciamento de patches

Segurança em camadas

REDES

Protege a comunicação entre dispositivos, servidores e datacenters.

Objetivo: garantir integridade, confidencialidade e disponibilidade dos dados em trânsito.

Medidas típicas: criptografia de tráfego, monitoramento de rede, firewalls e sistemas de detecção de intrusos.

Segurança em camadas

APLICAÇÃO

Refere-se à segurança dos softwares e serviços usados pelos usuários.

Objetivo: evitar que vulnerabilidades das aplicações sejam exploradas.

Ações recomendadas: Programação segura e teste de aplicações; Correção de vulnerabilidades após alertas de segurança; Uso de softwares de terceiros confiáveis para comunicação segura entre sistemas.

Segurança em camadas

DADOS

Abrange o armazenamento e proteção das informações.

Objetivo: garantir que apenas pessoas autorizadas tenham acesso e que todos os acessos sejam monitorados.

Práticas importantes: criptografia de dados, controle de acesso e auditoria de incidentes.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança em camadas

A estratégia de segurança em camadas demonstra que a proteção de sistemas não depende de uma única medida, mas da combinação de diversas barreiras que tornam os ataques mais complexos e demorados.

Cada camada adiciona obstáculos que desestimulam a ação de invasores, interceptadores ou agentes maliciosos, dificultando o acesso indevido a informações e sistemas críticos

INSTITUTO FEDERAL
São Paulo
Campus Campinas

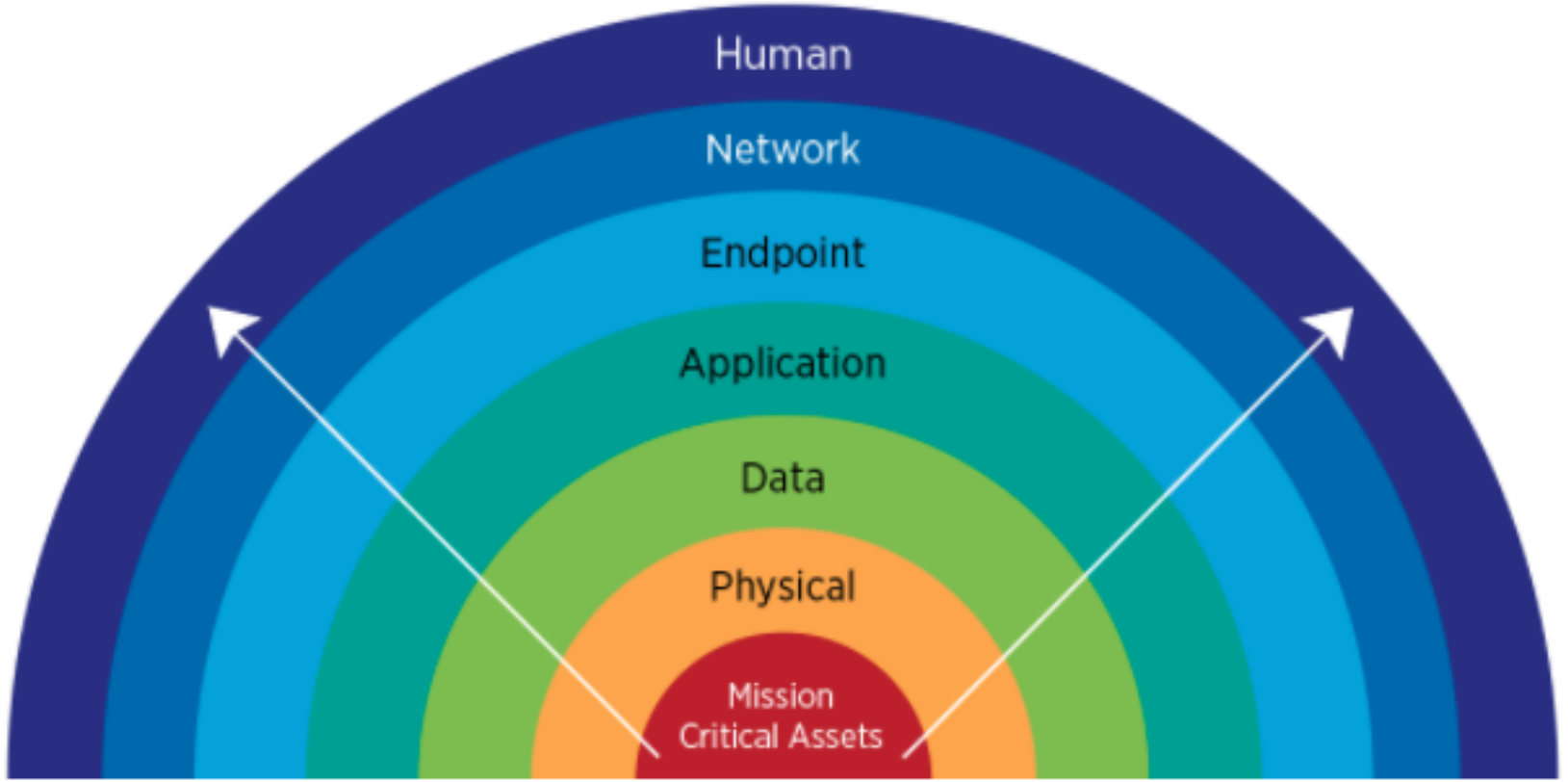
Segurança em camadas

Mesmo que um atacante consiga superar a primeira barreira, ele ainda precisa enfrentar as demais, aumentando o esforço e a probabilidade de detecção.

Essa abordagem reduz riscos como perda de dados, exposição de informações sensíveis e prejuízos financeiros, reforçando que a segurança eficaz depende da integração e do equilíbrio entre medidas humanas, físicas, de rede, de endpoints, de aplicações e de dados.

INSTITUTO FEDERAL
São Paulo
Campus Campinas

Segurança em camadas



INSTITUTO FEDERAL
São Paulo
Campus Campinas

Dúvidas?