

(CMPSEGS)

# Segurança de Sistemas

Tecnologia em Análise e Desenvolvimento de Sistemas

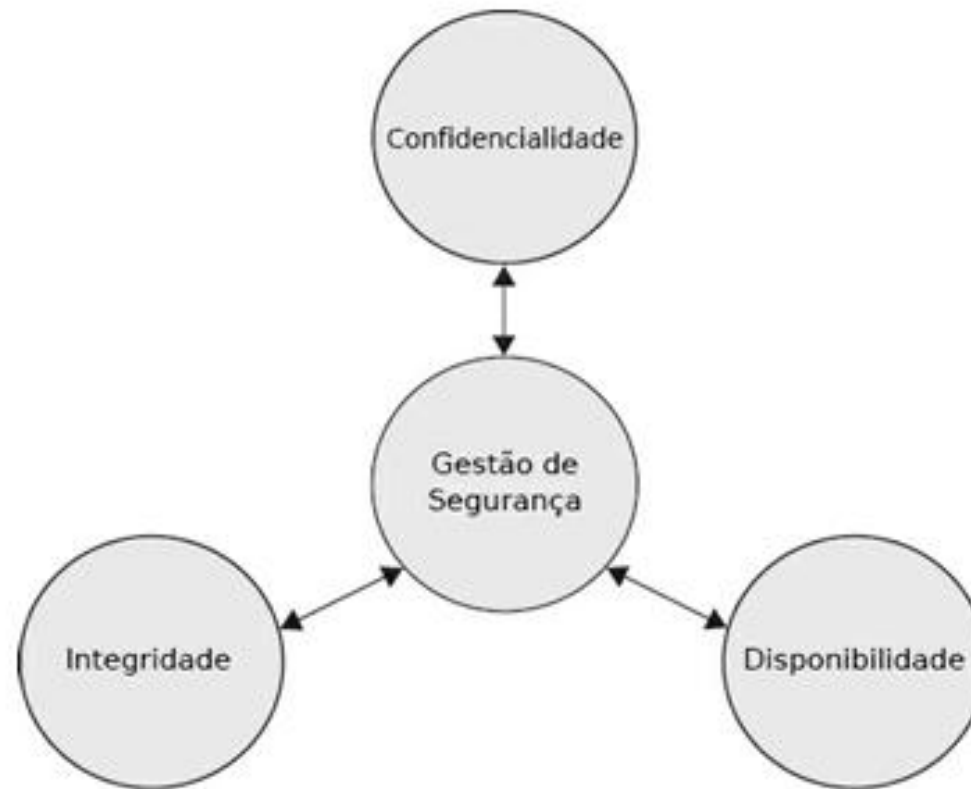
**Autenticação e Autorização**

**Prof. Me. Leonardo Arruda**

[leonardo.arruda@ifsp.edu.br](mailto:leonardo.arruda@ifsp.edu.br)

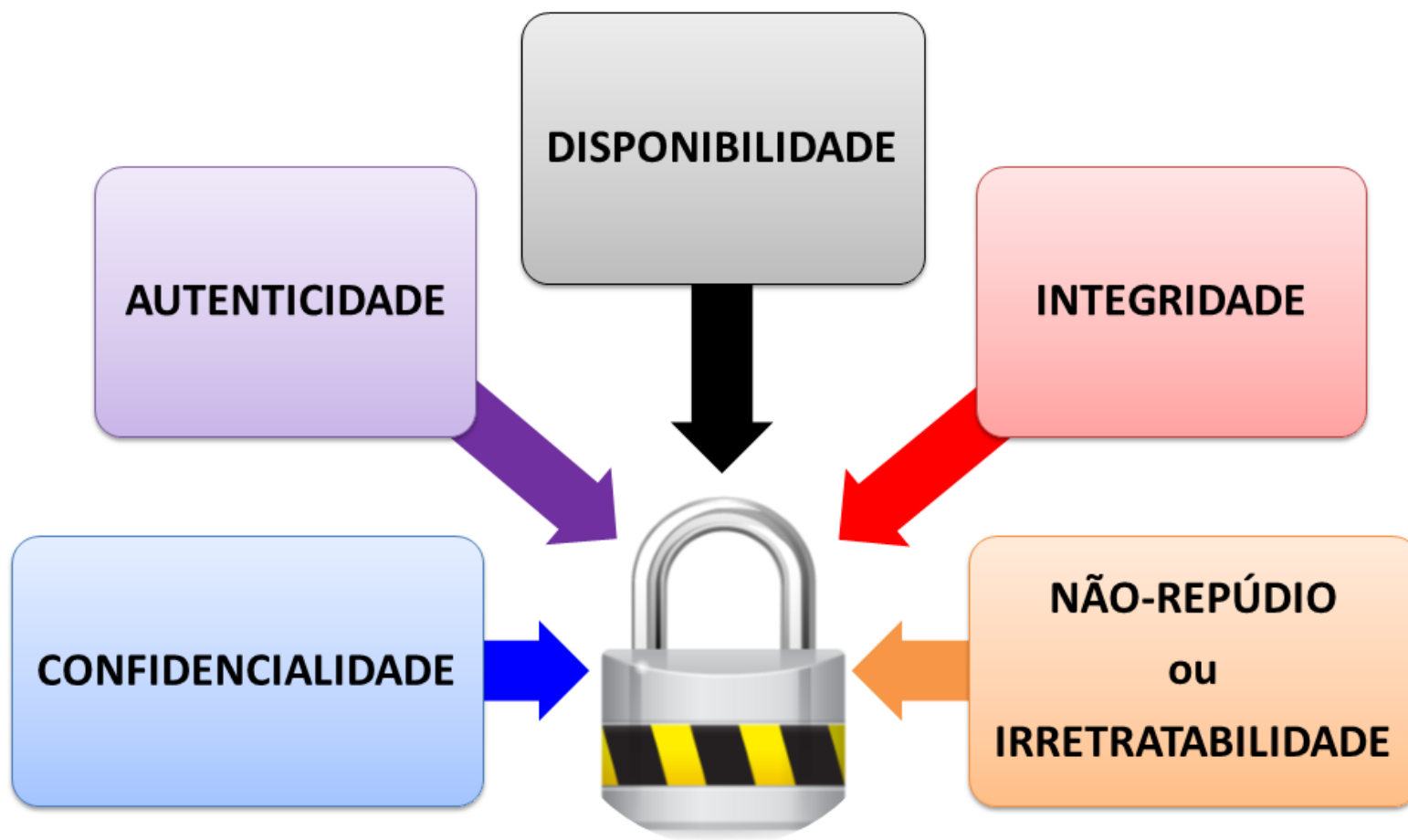


# Aula anterior: princípios da segurança de informação



Tríade CID

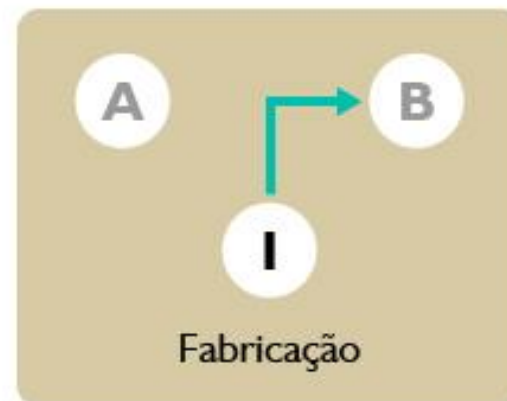
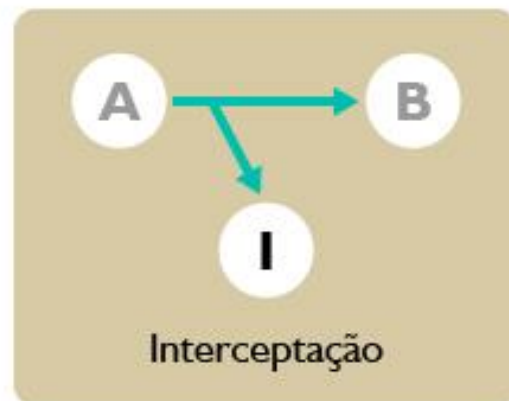
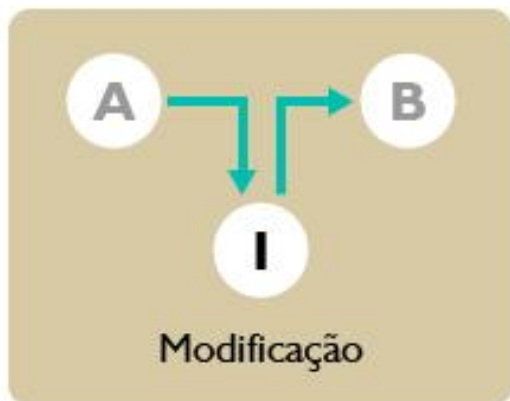
# Aula anterior: princípios da segurança de informação



# Aula anterior: princípios da segurança de informação

- **Confidencialidade:** dados acessíveis apenas a autorizados.
- **Integridade:** dados corretos, completos e confiáveis.
- **Disponibilidade:** dados e sistemas sempre acessíveis.
- **Autenticidade:** garante origem e veracidade da informação.
- **Irretratabilidade:** impede negação de envio ou recebimento de dados.

# Aula anterior: princípios da segurança de informação



# Autenticação

# Introdução

**A autenticação prova a identidade de diversas entidades do sistema computacional.**

Objetivos:

- Identificar usuários para o sistema;
- Identificar sistema para os usuários;
- Identificar sistemas para outros sistemas (módulo de pagamento);
- Garantir a origem de uma aplicação etc.

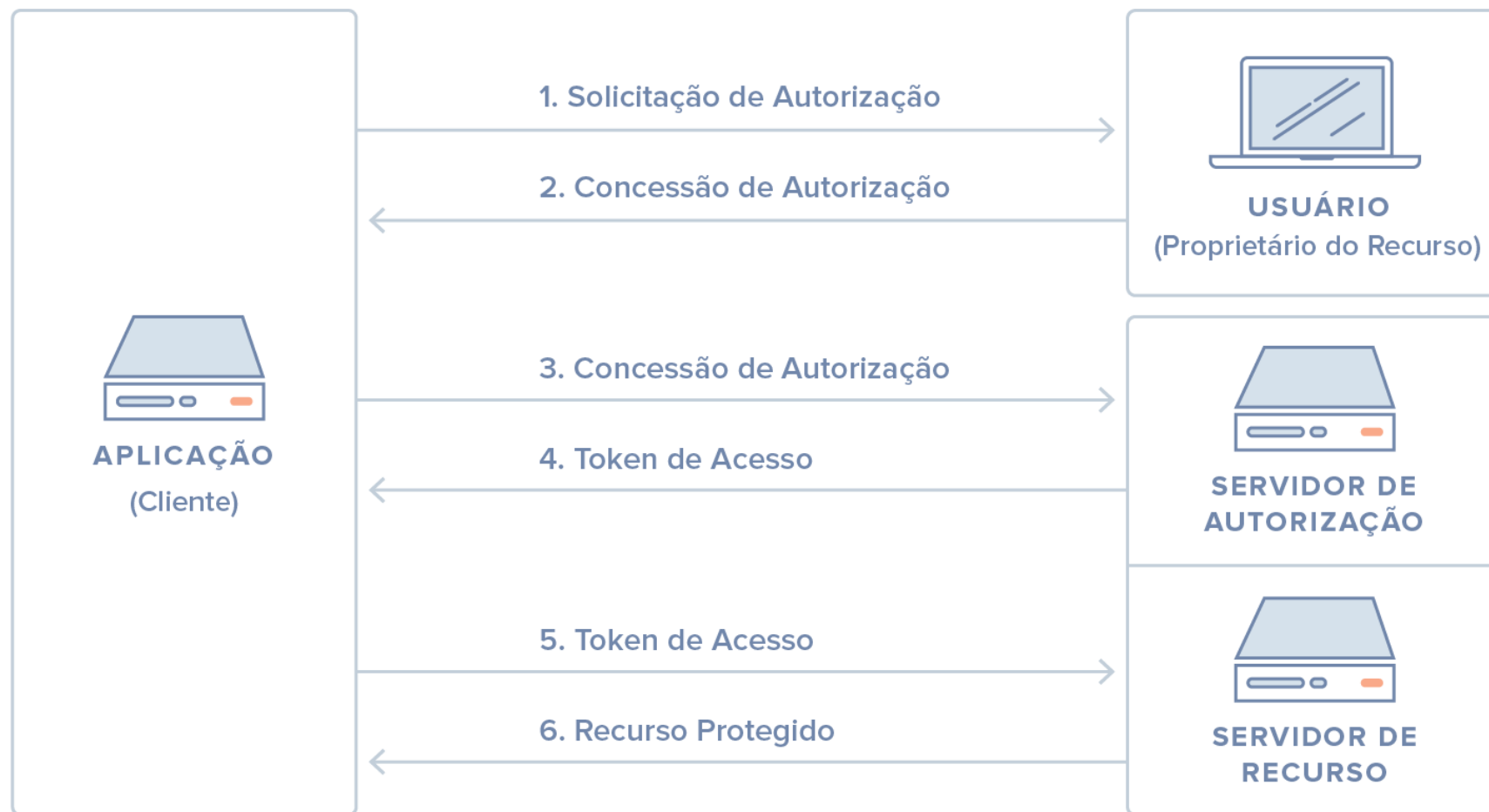
# Introdução

Etapas de autenticação em um servidor:

1. Login (inicia a sessão do usuário);
2. Autenticação do cliente;
3. Criação de processos;
4. Utilizar os sistemas criados pelos processos;
5. Finalizar a sessão do usuário (logout);



# Fluxo Geral



# Fluxo Geral

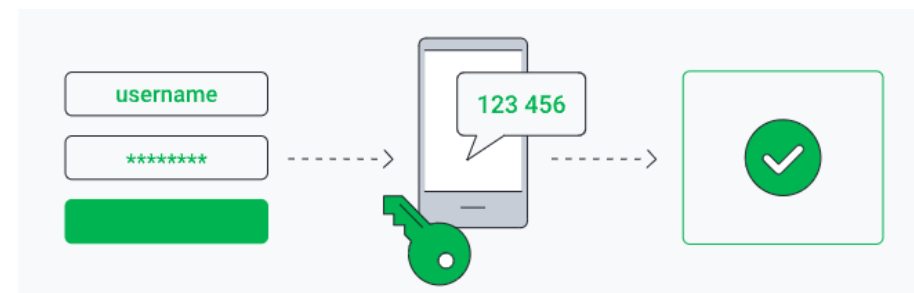
1. Cliente solicita autorização ao usuário.
2. Se autorizado, o cliente recebe uma concessão.
3. Cliente solicita token de acesso ao Servidor de Autorização.
4. Servidor valida concessão e emite token de acesso.
5. Cliente solicita recurso protegido usando token.
6. Servidor valida token e entrega o recurso.

# Autenticação

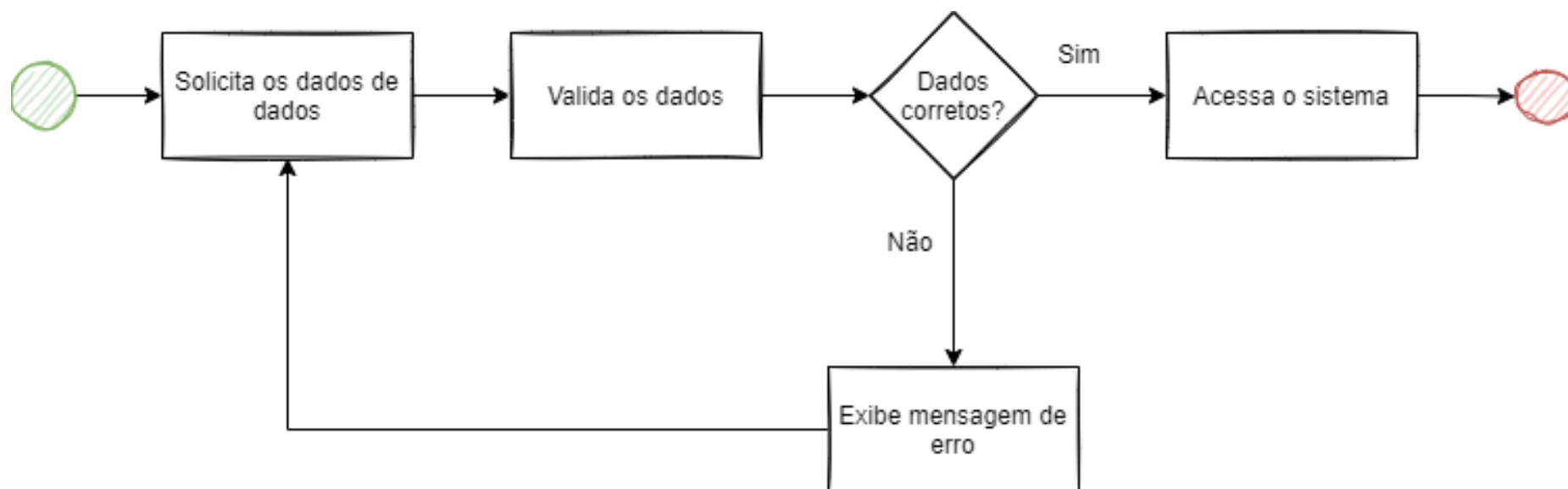
Consistem em dois passos:

- **Identificação:** fornecer **identidade** (nome de usuário, cartão magnético, cartão de proximidade etc.);
- **Verificação:** apresentar ou gerar informações de autenticação para **provar identidade** (senha alfanumérica, senha numérica (PIN), digitais etc.)

A autenticação de usuários é a base para grande parte dos tipos de **controle de acesso** e para a **responsabilização do usuário**.



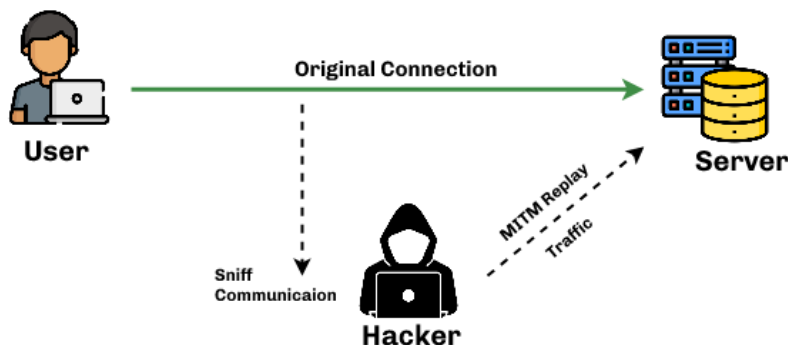
# Autenticação e Autorização



# Autenticidade vs. Autenticação

## Autenticidade:

- Garantia de que a informação, mensagem ou transação é verdadeira e confiável;
- Dado não foi falsificado e que realmente veio de quem afirma ter enviado;
- Uma mensagem autêntica não garante, por si só, que o usuário seja autêntico.



## Autenticação:

- Processo de verificar a identidade de um usuário, sistema ou entidades antes de conceder acesso a recursos;
- Identificação e verificação;
- Ex.: Usuário e senha (validação);

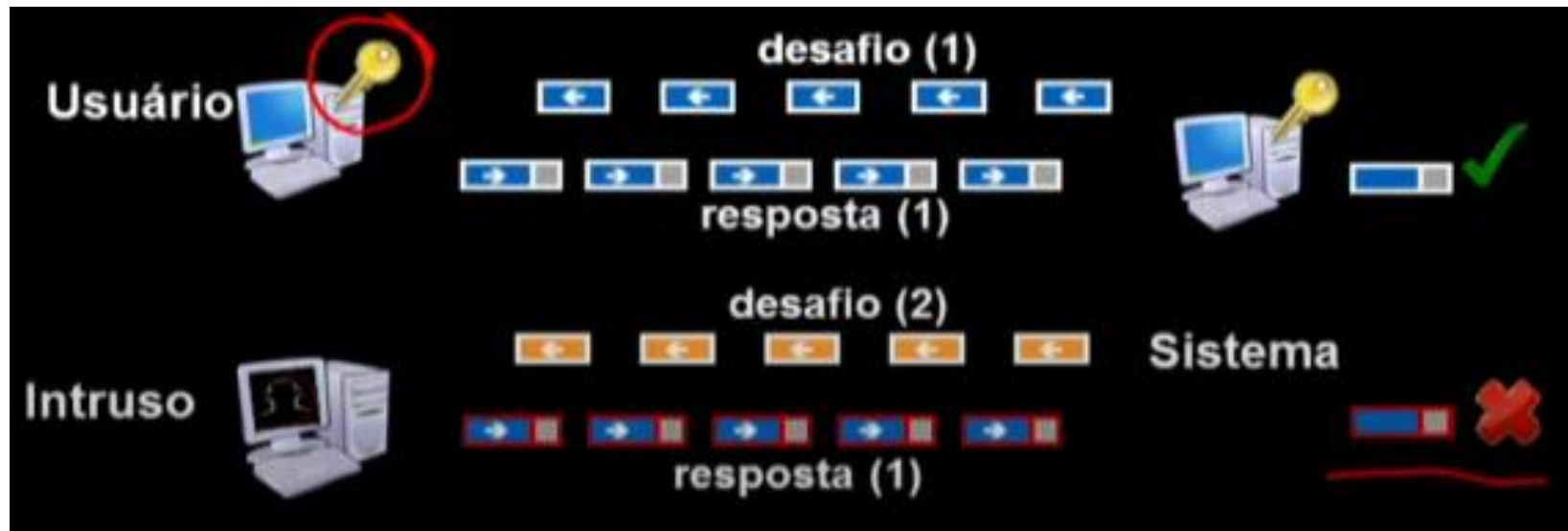


# Como evitar o ataque de repetição?

Autenticação de mensagens resistente a ataques de repetição

- **Túnel seguro:** impede captura de mensagens por atacante (HTTPS);
- **Desafio-resposta:**
  - MACs calculados sobre **nonces** (token criptográfico) ou **carimbos de tempo**;
  - Sistema envia um código e o usuário deve responder rapidamente;
  - Intruso que tenta repetir a mensagem envia tag incorreta
  - Ex.: Token de banco ou serviços de autenticação (Google Authenticator)

# Como evitar o ataque de repetição?



# Estratégias de autenticação

- **Algo que o indivíduo conhece ou sabe:**
  - Senhas, número de identificação pessoal (PIN) e respostas a perguntas de segurança;
- **Algo que o indivíduo possui:**
  - Cartões eletrônicos com senhas, smart cards e chaves físicas (token);
- **Algo que o indivíduo é (biometria estática):**
  - Impressão digital, retina e face;
- **Algo que o indivíduo faz (biometria dinâmica):**
  - Reconhecimento de voz, características de escrita e andar.



# Estratégias de autenticação

Usadas **individualmente** ou de **forma combinada** (“autenticação multifator”):

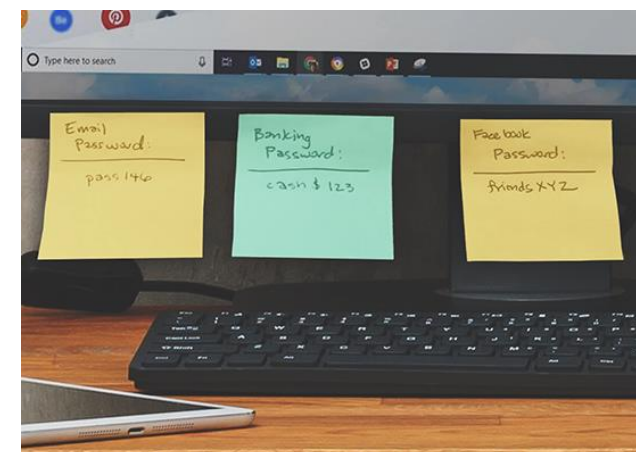
- Todas podem prover autenticação;
- Todas apresentam vantagens e desvantagens;



# Senhas: Vulnerabilidades (1)

## Captura de Senhas:

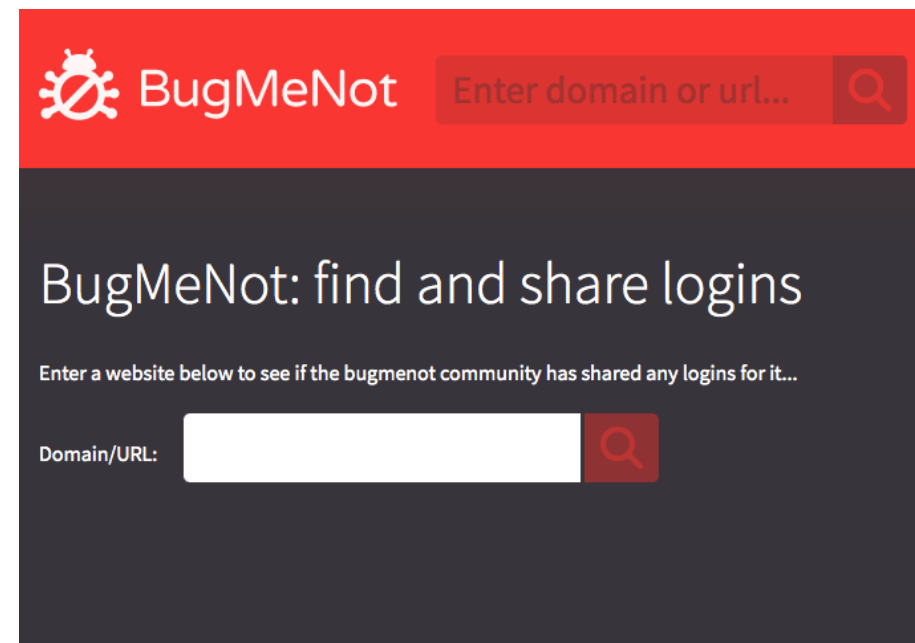
- Na **rede**, se enviada às claras (Ex.: HTTP, telnet)
  - Solução: usar túnel seguro (HTTPS, SSH);
- **Durante a digitação (“keyloggers”)**
  - Solução: antimalware
- **Explorando mau uso:** senha escrita em arquivo ou anotada em papel; engenharia social.
  - Solução: educação de usuários



# Senhas: Vulnerabilidades (2)

## Reuso de senhas por usuários

- **Problema:** a mesma senha em múltiplos sistemas aumenta o risco caso seja capturada;
- **Soluções:**
  - **Gerenciador de senhas:** armazenam senhas de forma cifrada, protegidas por uma senha mestre (Browser);
  - **Single Sign-On (SSO):** login único via provedores confiáveis (Google, Facebook, etc), que verificam a identidade do usuário.
  - **Educação de usuários:** não reutilizar senhas em serviços críticos; usar e-mails descartáveis ou ferramentas como “**BugMeNot**” para serviços irrelevantes (logins compartilháveis).



# Senhas: Vulnerabilidades (3)

## Ataques de força bruta

- **Baixa entropia de senhas**
  - Média de 40 bits; piora com políticas inadequadas (proibir caracteres especiais, limitar tamanho, manter senhas padrão);
- **Ataques Online:**
  - Tentativas repetidas diretamente no sistema (Ex.: login de bancos, e-mails etc.);
  - Solução: bloqueio temporário de usuários após várias tentativas falhas.

# Senhas: Vulnerabilidades (3)

- **Ataques offline:**
  - Roubo de base de dados ou dispositivo (Ex.: Yahoo, Dropbox);
  - Senhas armazenadas em texto claro podem ser reutilizadas em outros sistemas;
  - Ferramentas automatizadas: password crackers automatizados (Ex.: [Cain](#), [John the Ripper](#));
  - **Solução:** uso de **password hashing** para proteger senhas.

# Senhas: Vulnerabilidades (3)

ECONOMIA

## Ataque ao Dropbox expõe senhas de 68 milhões de usuários

Dados foram roubados em 2012, mas hackers só divulgaram agora

O Globo

31/08/2016 - 09:41 / Atualizado em 31/08/2016 - 11:05

<https://oglobo.globo.com/economia/ataque-ao-dropbox-expoe-senhas-de-68-milhoes-de-usuarios-20023920>

## Hack Brief: 4-Year-Old Dropbox Hack Exposed 68 Million People's Data

Dropbox had a security "incident" in 2012, but the true scale and severity of that hack is only now coming to light.



GETTY IMAGES

<https://www.wired.com/2016/08/hack-brief-four-year-old-dropbox-hack-exposed-68-million-peoples-data/>

# Senhas: Vulnerabilidades (3)

## HACKING

### Yahoo corrige informação e diz que vazamento de dados afetou ao menos 500 milhões de usuários

Por Redação - 23 de setembro de 2016

Like 0



<https://tiinside.com.br/23/09/2016/yahoo-corrige-informacao-e-diz-que-vazamento-de-dados-afetou-ao-menos-500-milhoes-de-usuarios/>

## Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts

Ten months ago, Yahoo disclosed the biggest breach in history. As it turns out, the company severely underestimated the impact. Think a billion users is bad? Try three billion.



WIRED

<https://www.wired.com/story/yahoo-breach-three-billion-accounts/>

# Senhas: Vulnerabilidades (3)

**Ataques de força bruta** se base/dispositivo armazena:

- **Senhas armazenadas às claras (texto simples):**
  - O atacante que obtém o banco de dados tem custo praticamente zero para descobrir a senha, porque já está disponível.
  - **Consequência:** se o usuário reutiliza a mesma senha em outros sistemas, todos eles ficam vulneráveis.

Usuário	Senha (Texto Claro)
alice	senha123
bob	qwerty!
carol	123456
david	minhaSenha2025



# Senhas: Vulnerabilidades (3)

## Senhas armazenadas como hash:



- O hash é uma **função criptográfica unidirecional** que transforma a senha em uma sequência fixa de caracteres.
- **Ataque possível:** o atacante usa **tabelas pré-computadas** (como *rainbow tables*) ou serviços online gratuitos que associam hashes comuns a senhas conhecidas.
- **Exemplo:** hashes de senhas de 16 caracteres ou menos podem ser rapidamente resolvidos usando essas tabelas ou serviços online.
- **Custo do ataque:** mais alto que senhas em texto claro, mas ainda possível para senhas fracas ou populares.

Usuário	Senha (Texto Claro)	Hash (SHA-256 simplificado)
alice	senha123	ef92b778bafe771e89245b89ecbc0b8c
bob	qwerty!	d8578edf8458ce06fbc5bb76a58c5ca4
carol	123456	8d969eef6ecad3c29a3a629280e686cf
david	minhaSenha2025	3c8b2f1c9d2e6b4f7a2c9f1d5e0a6b7c

# Senhas: Vulnerabilidades (3)

## Hash + Salt

- **Conceito:** Cada senha é combinada com um **salt** (valor aleatório, ex.:128 bits) antes gerar hash.
- **Objetivo:** impedir ataques baseados em tabelas pré-calculadas (*Rainbow tables*). Para cada salt, seria necessário gerar uma tabela nova, o que exige um armazenamento imenso ( $\sim 2^{128}$  bits)



		
Password	p4s5w3rdz	p4s5w3rdz
Salt	et52ed	ye5sf8
Hash	1vn49sa	z32i6t0

# Senhas: Vulnerabilidades (3)

## Hash + Salt

- **Conceito:** Cada senha é combinada com um **salt** (valor aleatório, ex.:128 bits) antes gerar hash.
- **Objetivo:** impedir ataques baseados em tabelas pré-calculadas (*Rainbow tables*). Para cada salt, seria necessário gerar uma tabela nova, o que exige um espaço imenso ( $\sim 2^{128}$  bits)
- **Desempenho / Ataque:**
  - Pouco prático em computadores comuns, mas ataques podem ser feitos **em paralelo**.
  - Ex.: Cluster de GPUs ( $>10^{12}$  hashes/s) consegue quebrar uma **senha alfanumérica de 8 caracteres em ~5,5 horas** (2012).

<https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/>

		
Password	p4s5w3rdz	p4s5w3rdz
Salt	et52ed	ye5sf8
Hash	1vn49sa	z32i6t0

# Senhas: Vulnerabilidades (3)

## *Password hashing (com salt)*

- **Custo configurável:** define  $t$  (tempo de processamento) segundos e  $m$  MB de RAM para gerar o hash.
  - Quanto menor a memória ( $m$ ), maior o custo para o atacante (cresce exponencialmente)
- **Objetivo:** tornar o custo **imperceptível para usuários legítimos**, mas **significativo para atacantes**.
- **Exemplos de configuração (força do cadeado):**
  - $t = 1s$ ,  $m = 1GB \rightarrow$  usuário espera 1s ao logar e atacante precisa de milhões de GB de RAM.
  - $t = 100\text{ ms}$ ,  $m = 20MB \rightarrow$  login rápido e mesmo com GPU, o consumo de memória por tentativa limita os ataques em massa.

*Configurável				
Algoritmo	1 núcleo de processamento		1000 núcleos de processamento	
	testes/s	uso de memória	testes/s	uso de memória
1 hash	> 10000	< 1 KiB	> 10.000.000	alguns KiB
PBKDF/bcrypt	1	< 1 KiB	1000 (todos)	alguns KiB
Lyra2/Argon2	1	1 GiB	8 (992 parados)	8 GiB

Limita paralelismo (e.g.: clusters de GPUs) 

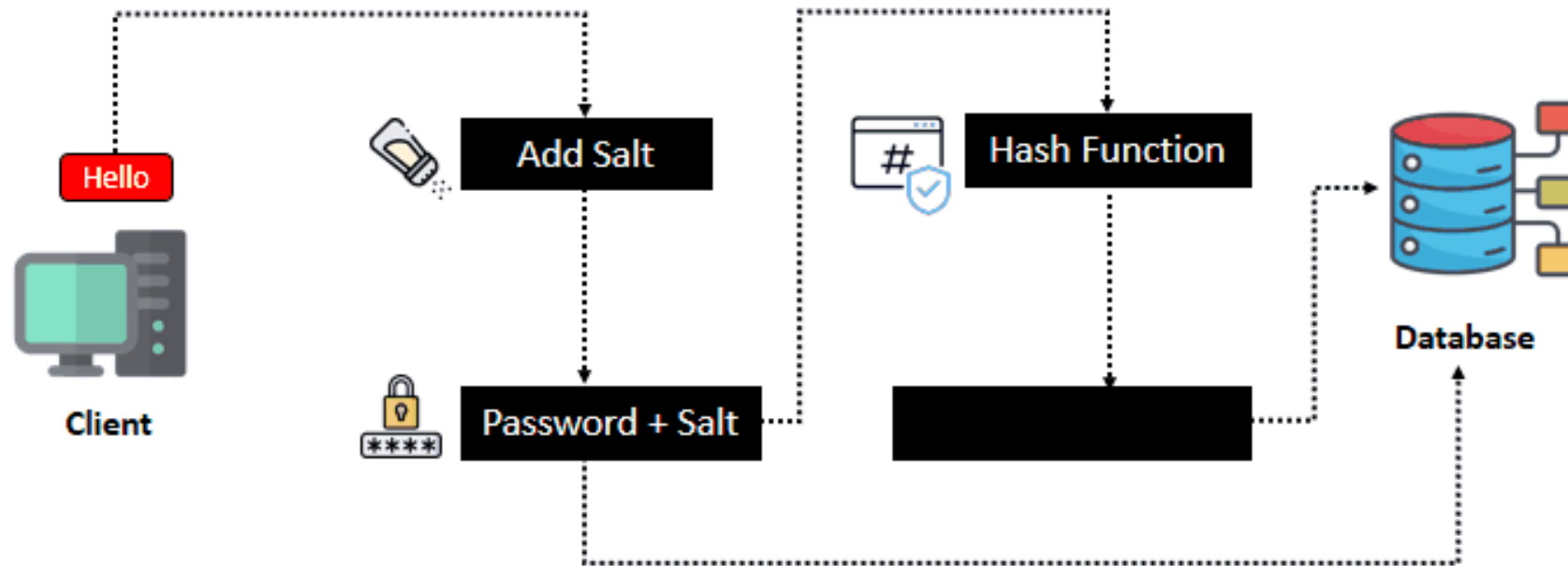
O usuário ajusta para que não atrapalhe quem tem a chave (usuário), mas dificulta ao máximo o atacante.

<https://stytych.com/blog/what-is-password-hashing/>

# Password Hashing com Salt

## Salted Password & Hashing

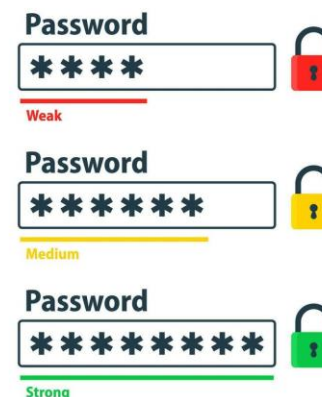
Mohamed Rimsan



<https://www.geeksforgeeks.org/python/how-to-hash-passwords-in-python/>

# Criando boas senhas

- **Use variedade:** inclua letras maiúsculas, minúsculas, números e símbolos (até espaços podem ser usados);
- **Evite fragilidades:** não use palavras de dicionário, nomes pessoais ou dados óbvios.
  - Se usar palavras, combine várias (*passphrase*) ou aplique erros propositais de ortografia.



# Criando boas senhas

- **Construa a partir de frases:** fáceis de lembrar, mas difíceis de adivinhar.
  - Ex.: “Esta era uma boa senha.. Até que mostrei ela para vocês da aula!” → **Eeubs...Aqmepvda!**
  - Ex.: “Quem ri por último é porque não entendeu a piada” → **Qrp’u, ‘epneap.**
- **Dica extra:** combine duas ou mais frases para aumentar o comprimento da senha e reforçar a segurança.

# O que o usuário tem: Tokens, Cartões, Smartcard

## Cartões

- **Tipos:** magnéticos, sem contato (NFC), entre outros;
- **Uso:** armazenam apenas um código de segurança fixo.
- **Vulnerabilidades:**
  - Clonagem;
  - Roubo;
  - Compartilhamento indevido.





# O que o usuário tem: Tokens, Cartões, Smartcard

## Tokens

- **Tipos:** papel ou eletrônicos;
- **Uso:** geram senhas temporárias (OTP).
  - Ex.: TOPT é baseado no relógio interno + chave secreta (HMAC).
  - Mesmo código é gerado pelo token e pelo servidor, desde que estejam sincronizados.
  - Funciona bem contra ataques de repetição.
- **Vulnerabilidades:**
  - Papel: fácil de copiar ou clonar;
  - Eletrônico:
    - Recomenda-se usode senha/PIN;
    - Clonagem é rara (OTP não revela a chave secreta);

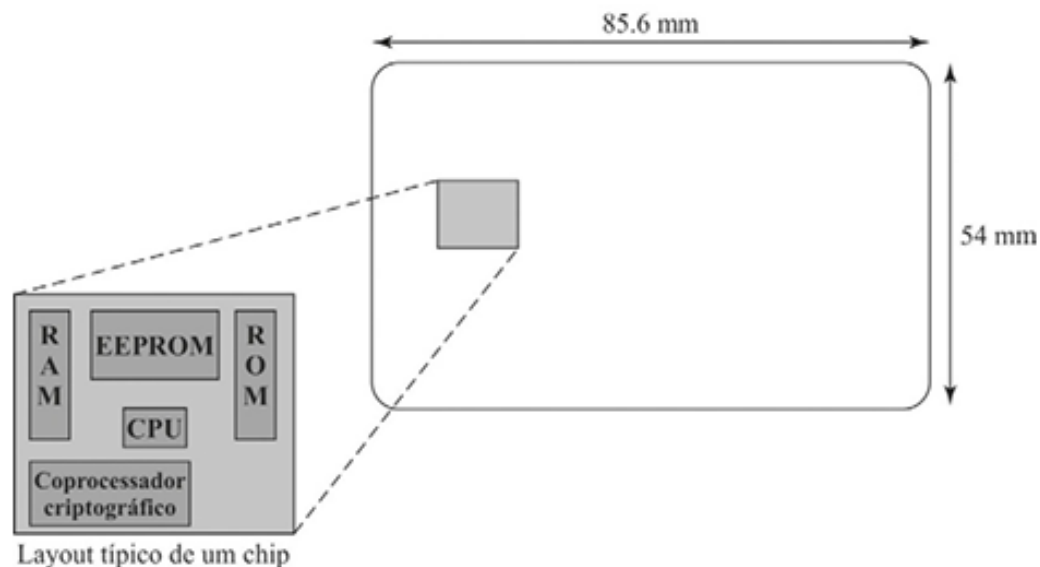


# O que o usuário tem: Tokens, Cartões, Smartcard

## Cartões Inteligentes (Smart Cards)

- **Exemplos:** cartões de crédito, SIM Card, bilhetes eletrônicos
- **Uso:** processamento seguro de código de autenticação.
  - Comunicação via **criptografia** com chaves protegidas;
    - **Fisicamente:** não podem ser extraídas (hardware projeto para isso);
    - **Logicamente:** podem ser apagadas após tentativas incorretas (PIN incorreto);
- **Vulnerabilidades:**
  - Fraude no leitor: o que é mostrado pode não ser o que o cartão realmente envia.
  - **Falhas em algoritmos/protocolos:** Mifare Classic (Bilhete Único) e Cartões de crédito sem contato (NFC). <https://www.usenix.org/system/files/conference/woot13/woot13-roland.pdf>

# O que o usuário tem: Tokens, Cartões, Smartcard



**FIGURA 3.3** Dimensões do smart card O chip do smart card está embutido no cartão plástico e não fica visível. As dimensões seguem o padrão ISO 7816-2.

# O que o usuário tem: Tokens, Cartões, Smartcard

## Após falha técnica, 40 mil Bilhetes Únicos são bloqueados, diz SPTrans

Empresa informa que vai substituir bilhetes que apresentarem falhas

Agência Estado, São Paulo

02/07/23 às 16:54 | Atualizado 03/07/23 às 08:14



Greve começou nesta quinta-feira (23) • Werther Santana/Estadão Conteúdo

<https://www.cnnbrasil.com.br/nacional/apos-falha-tecnica-40-mil-bilhetes-unicos-sao-bloqueados-diz-sptrans/>

# O que o usuário é/faz: biometria

## Biometria

- Método de autenticação que identifica o usuário com base em **características físicas** (como digitais, íris ou face) ou **comportamentais** (como assinatura, digitação ou padrões de voz).
- Permite uma validação **única e individual**, aumentando a segurança em comparação com senhas ou cartões.



# O que o usuário é/faz: biometria

## Impressão Digital

- Leitura de minúcias: coleção de pontos identificáveis em uma impressão digital (terminação e bifurcação são mais utilizadas).





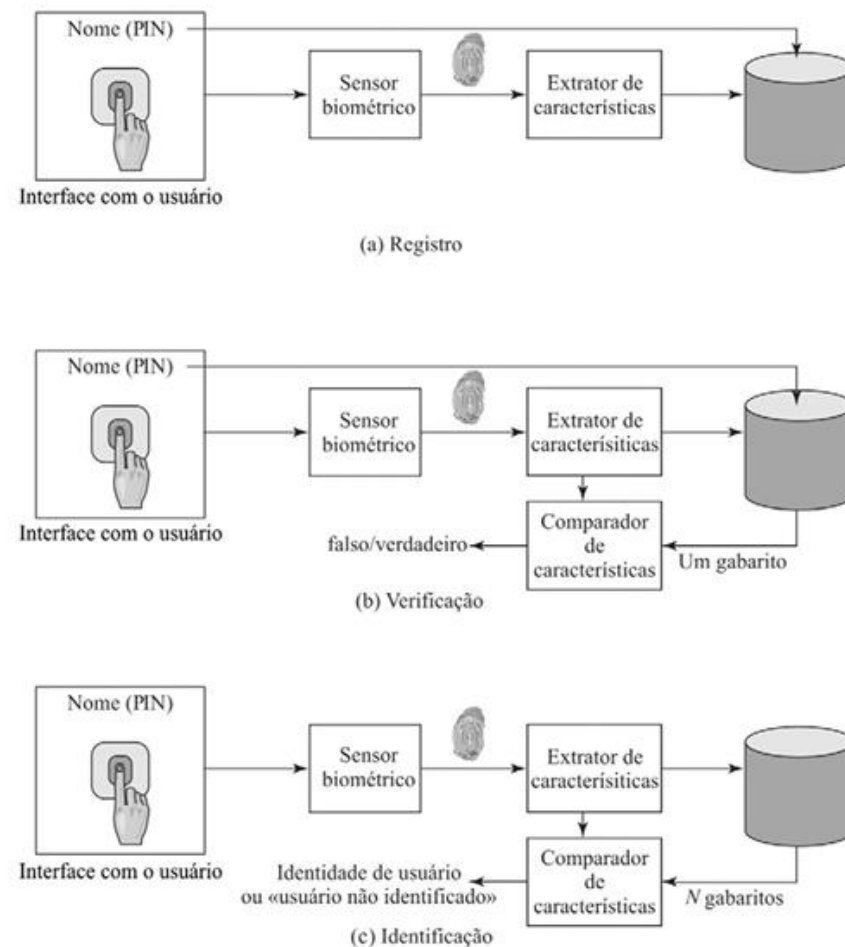
# O que o usuário é/faz: biometria

## Processo:

- Dados armazenados em banco de dados para comparação posterior



# O que o usuário é/faz: biometria



**FIGURA 3.6** Sistema biométrico genérico O registro cria uma associação entre um usuário e as características biométricas desse usuário. Dependendo da aplicação, a autenticação de usuário envolve verificar se um usuário alegado é o usuário real ou identificar um usuário desconhecido.



# O que o usuário é/faz: biometria

## Biometria (Vulnerabilidades):

- **Reprodução de dados biométricos**
  - Ex.: dedo de borracha, foto de alta resolução de olhos ou da face;
- **Roubo de dados em trânsito:** interceptação durante comunicação entre sensor e sistema;
- **Ataque de repetição:** reutilização de dados biométricos capturados para autenticação;
- **Roubo da base de informações biométricas:** base de dados do TSE (eleição);
- **Criação de objetos falsos:** dispositivos ou lentes que simulam a leitura biométrica correta. Ex.: lente para leitura de íris;
- **Revogação** é um desafio: um dedo ou outra informação biométrica revogada não é facilmente substituível.

# O que o usuário é/faz: biometria

## Biometria (Contramedidas):

- **Contra falsificações:**
  - **Sensores de alta acurácia:** dificultam a criação de réplicas.
  - **Combinação de sensores:** verificam presença real (ex.: temperatura da pele, profundidade da íris).
  - **Monitoramento dos sensores:** evita apresentação de artefatos como fotos ou impressões falsas.
- **Proteção de dados:**
  - Transmissão segura: canal de comunicação criptografado e protegido fisicamente.
  - Armazenamento seguro: módulo de registros protegido fisicamente e logicamente contra acesso indevido

# Ataques, autenticadores e defesas

**Tabela 3.4** Alguns ataques potenciais, autenticadores suscetíveis e defesas típicas

Ataques	Autenticadores	Exemplos	Defesas típicas
<b>Ataque a cliente</b>	Senha	Adivinhação, busca exaustiva	Grande entropia; tentativas limitadas
	Token	Busca exaustiva	Grande entropia; tentativas limitadas; roubo de objeto requer presença
<b>Ataque a sistema</b>	Biométrico	Falsa correspondência	Grande entropia; tentativas limitadas
	Senha	Roubo de texto às claras, busca em dicionário, busca exaustiva	Uso de hash; grande entropia; proteção de banco de dados de senhas
	Token	Roubo de código de acesso	Mesmas da senha; código de acesso de uso único
	Biométrico	Roubo de gabarito	Captura de dispositivo de autenticação; desafio/resposta
<b>Escuta, roubo e cópia</b>	Senha	“Olhar sobre os ombros” (“shoulder surfing”)	Diligência do usuário para proteger segredo; diligência do administrador para revogar rapidamente senhas comprometidas; autenticação multifator
	Token	Roubo, falsificação de hardware	Autenticação multifator; token resistente ou que evidencie falsificação
	Biométrico	Cópia (spoofing) da biometria	Detecção de cópia no dispositivo de captura e autenticação do dispositivo de captura
<b>Repetição</b>	Senha	Repetição de resposta roubada para senha	Protocolo de desafio/resposta
	Token	Repetição de resposta roubada para código de acesso	Protocolo de desafio/resposta; código de acesso de uso único
	Biométrico	Repetição de resposta roubada para gabarito biométrico	Detecção de cópia no dispositivo de captura e autenticação do dispositivo de captura via protocolo de desafio/resposta
<b>Cavalo de Troia</b>	Senha, token, biometria	Instalação de cliente falso ou dispositivo de captura	Autenticação de cliente ou dispositivo de captura dentro do perímetro de segurança confiável
<b>Negação de service</b>	Senha, token, biometria	Bloqueio após várias autenticações fracassadas	Multifator com token

# Dúvidas?



# Referências Bibliográficas

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. 2. ed., 8. tiragem. Rio de Janeiro: [s.n.], 2018.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. *Segurança dos sistemas de informação: gestão estratégica da segurança empresarial*. 1. ed. Lisboa; V. N. Famalicão: Centro Atlântico, 2003. ISBN 972-8426-66-6.

STALLINGS, William; BROWN, Lawrie. *Segurança de computadores: princípios e práticas*. 2. ed. Tradução Arlete Simille Marques. Rio de Janeiro: Elsevier, 2014. ISBN 978-85-352-6449-4.