Métodos Modernos de Autenticação

Acesso crítico e práticas seguras

Professor Álvaro Gonçalves

Curso: Desenvolvimento de Software Multiplataforma

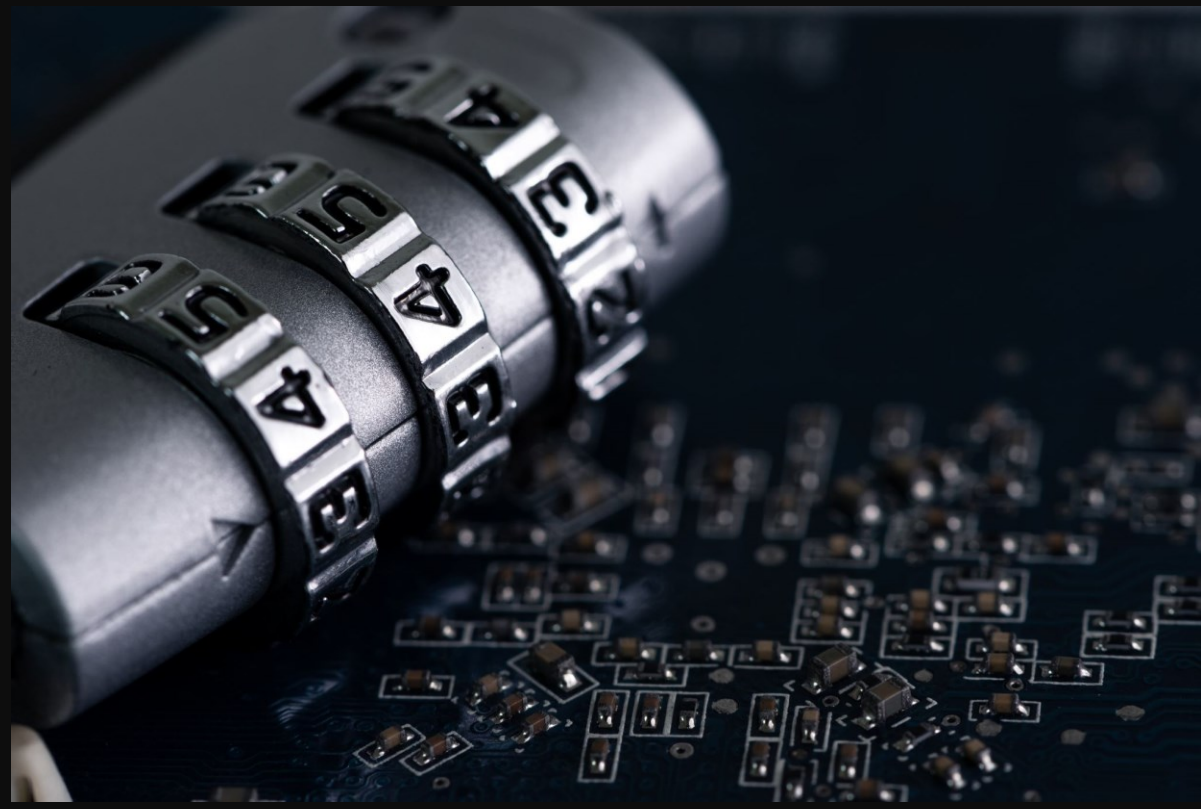
Fatec **Professor Francisco de Moura –** Jacareí, SP

Introdução

- Autenticação: validar identidade de usuários e dispositivos.
- Relevância em sistemas críticos (bancos, hospitais, cloud).
- Evolução: senhas → MFA → Zero Trust.

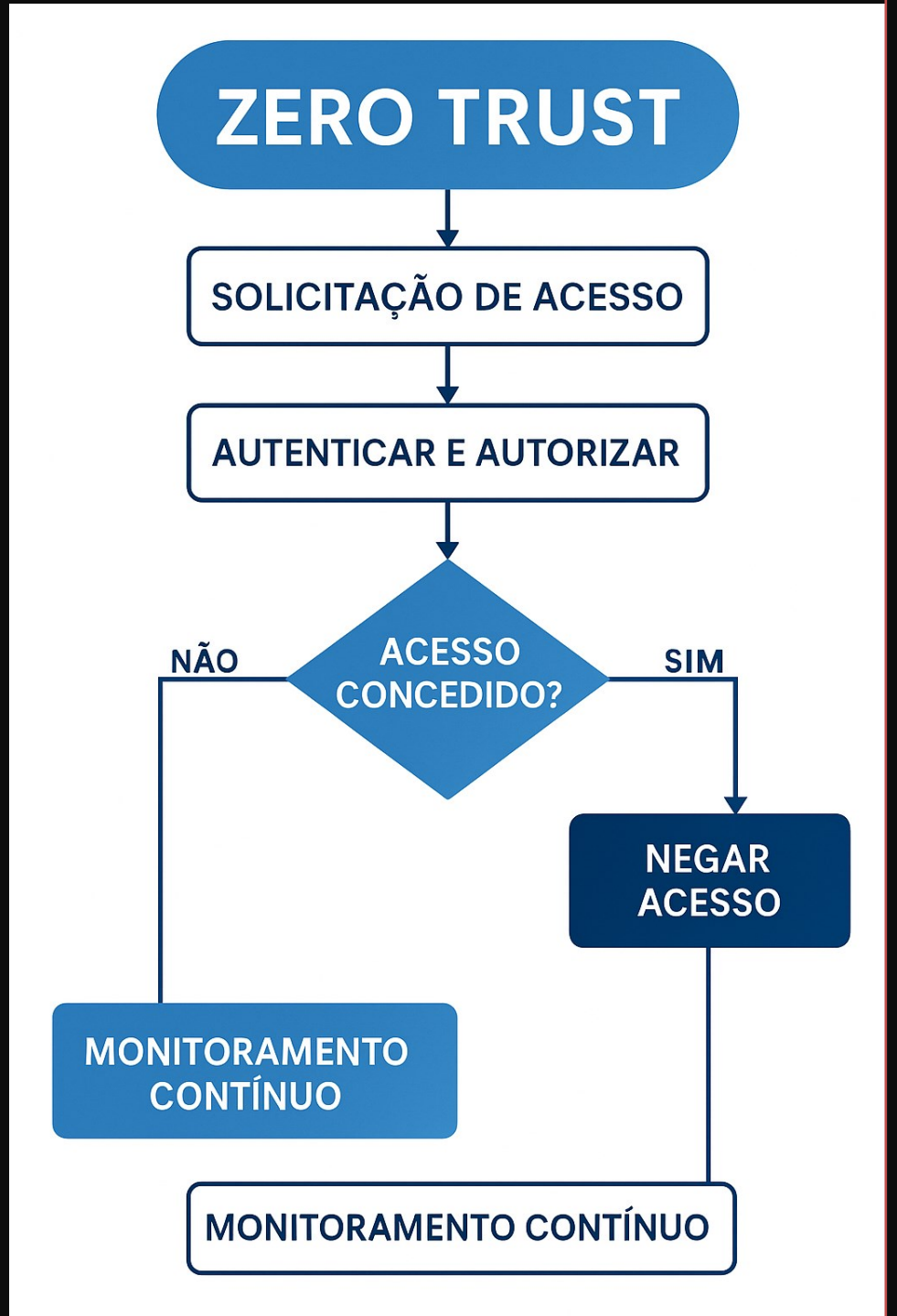
Por que autenticação robusta?

- Protege dados sensíveis.
- Previne acessos não autorizados.
- Reduz riscos de ataques (phishing, brute force).
- Atende conformidade (LGPD, GDPR, HIPAA).



Fluxograma Zero Trust

- 1. Solicitação de acesso.
- 2. Autenticação e autorização.
- 3. Acesso concedido?
- - Se SIM: permitir + monitorar continuamente.
- - Se NÃO: negar acesso.



Fatores de Autenticação

- Algo que você sabe (senha, PIN).
- Algo que você tem (token, celular).
- Algo que você é (biometria).
- Algo que você faz (padrões de uso).
- Localização (rede, geolocalização).

Métodos Modernos

- MFA e 2FA.
- Biometria avançada.
- Tokens FIDO2/U2F.
- SSO (Single Sign-On).
- OAuth 2.0 / OpenID Connect.
- Zero Trust.
- Passwordless.
- Autenticação adaptativa.

MFA e 2FA

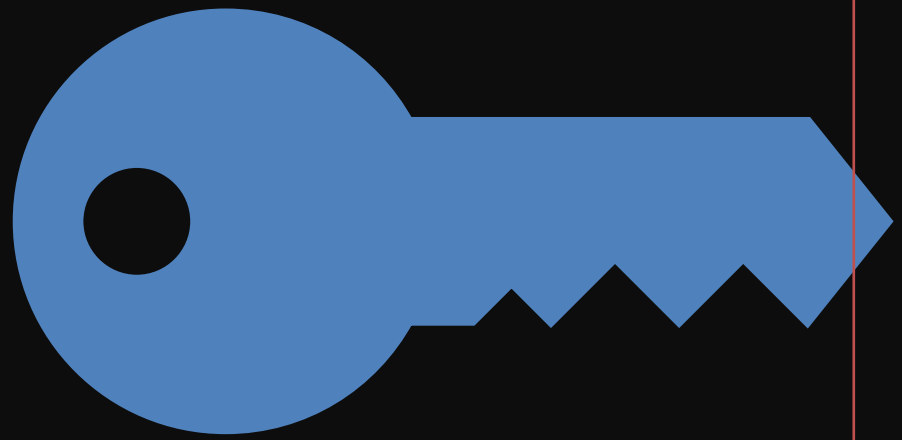
- Autenticação em múltiplos fatores (MFA) e dois fatores (2FA).
- Combina algo que você sabe (senha) + algo que você tem (token/celular).

Biometria avançada

- Uso de características únicas como impressão digital, reconhecimento facial 3D, íris e voz.
- Alta segurança, mas requer proteção de dados biométricos.

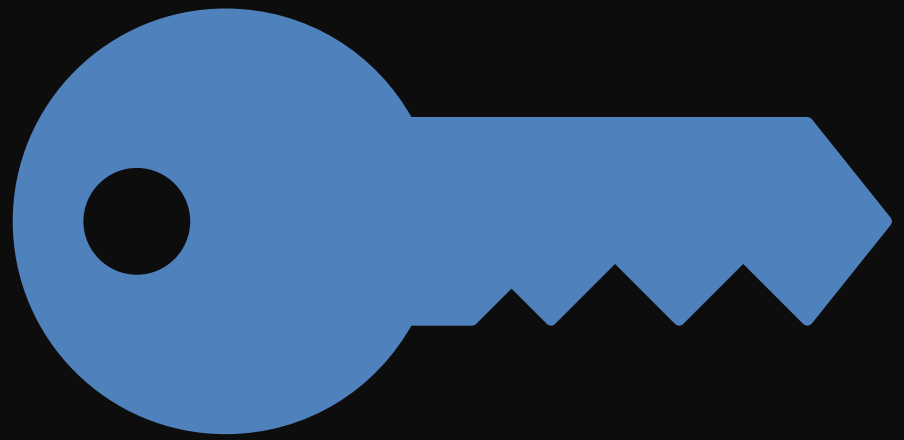
Tokens FIDO2/U2F

- Chaves de segurança físicas que validam o login sem depender apenas de senhas.
- Ex.: YubiKey, Titan Security Key.



SSO (Single Sign-On)

- Permite login único em vários sistemas.
- Exemplo: entrar no Google e ter acesso automático a Gmail, Drive e YouTube.



OAuth 2.0
OpenID Connect

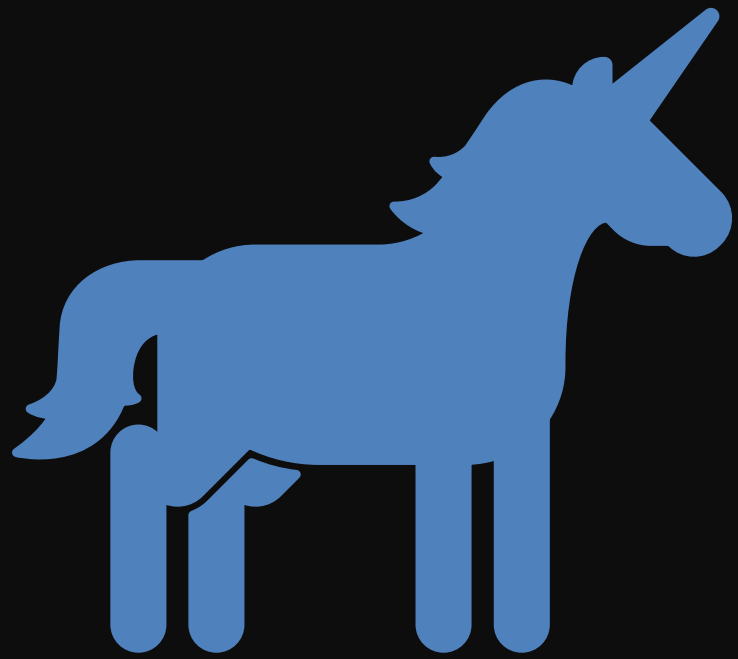
- Protocolos de autenticação e autorização.
- Permitem login via contas externas (Google, Facebook, Microsoft).

Zero Trust

- Modelo de segurança que nunca confia implicitamente em nenhum usuário ou dispositivo.
- Validação contínua do acesso e monitoramento de contexto.

Autenticação adaptativa

- Ajusta o nível de verificação conforme o risco.
- Ex.: exigir MFA apenas em logins suspeitos ou de locais desconhecidos.



Passwordless

- Elimina o uso de senhas.
- Autenticação via biometria, link mágico ou notificação push em aplicativo confiável.

Bibliotecas de Autenticação

Linguagem	Biblioteca	Funcionalidade	Implementação
Python	Flask-Login	Gerencia sessões	Fácil
Python	Flask-JWT-Extended	JWT em APIs REST	Médio
Node.js	Passport.js	OAuth, LDAP, social login	Médio
Node.js	NextAuth.js	Login social e JWT	Fácil
PHP	Laravel Breeze	Autenticação completa	Fácil
Java	Spring Security	OAuth2, JWT	Avançado

Conclusão

- Autenticação moderna vai além de senhas.
- MFA, biometria, tokens e Zero Trust são essenciais.
- Bibliotecas open source facilitam a prática.
- Equilibrar segurança e usabilidade é chave.