



IAM

PAM

Andrei Ferraz Cesmigi
Analista de Segurança da Informação



IAM

Identity and Access Management

PAM

Privileged Access Management

Gerenciamento de Identidade e Acesso - IAM

- Autenticação
- Autorização
- Permissões



Autenticação - AuthN

Verifica Identidade

Multi-factor

SSO - Single Sign On

Autorização - AuthZ

Regras de acesso

Regras de não acesso

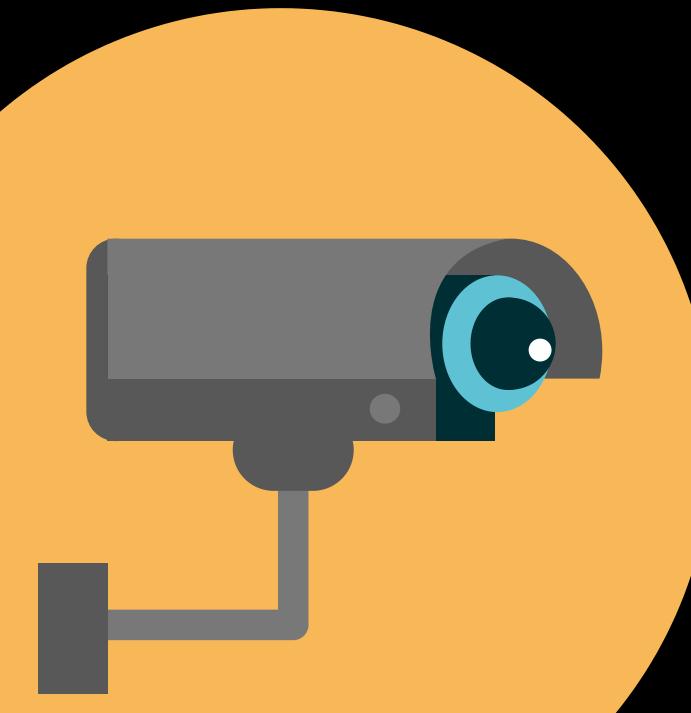


Persmissões

Quem logou?

Quem está logado?

O que este usuário pode fazer?



IAM - 2021

Serviços modernos de IAM permitem integrações com API's e garantir uma verificação ainda mais profunda e robusta da identidade real de seus clientes, mitigando ainda mais a falsidade ideológica e crimes de invasão por **engenharia social**.

SAML

Open Standard para troca de autenticação;

JWT

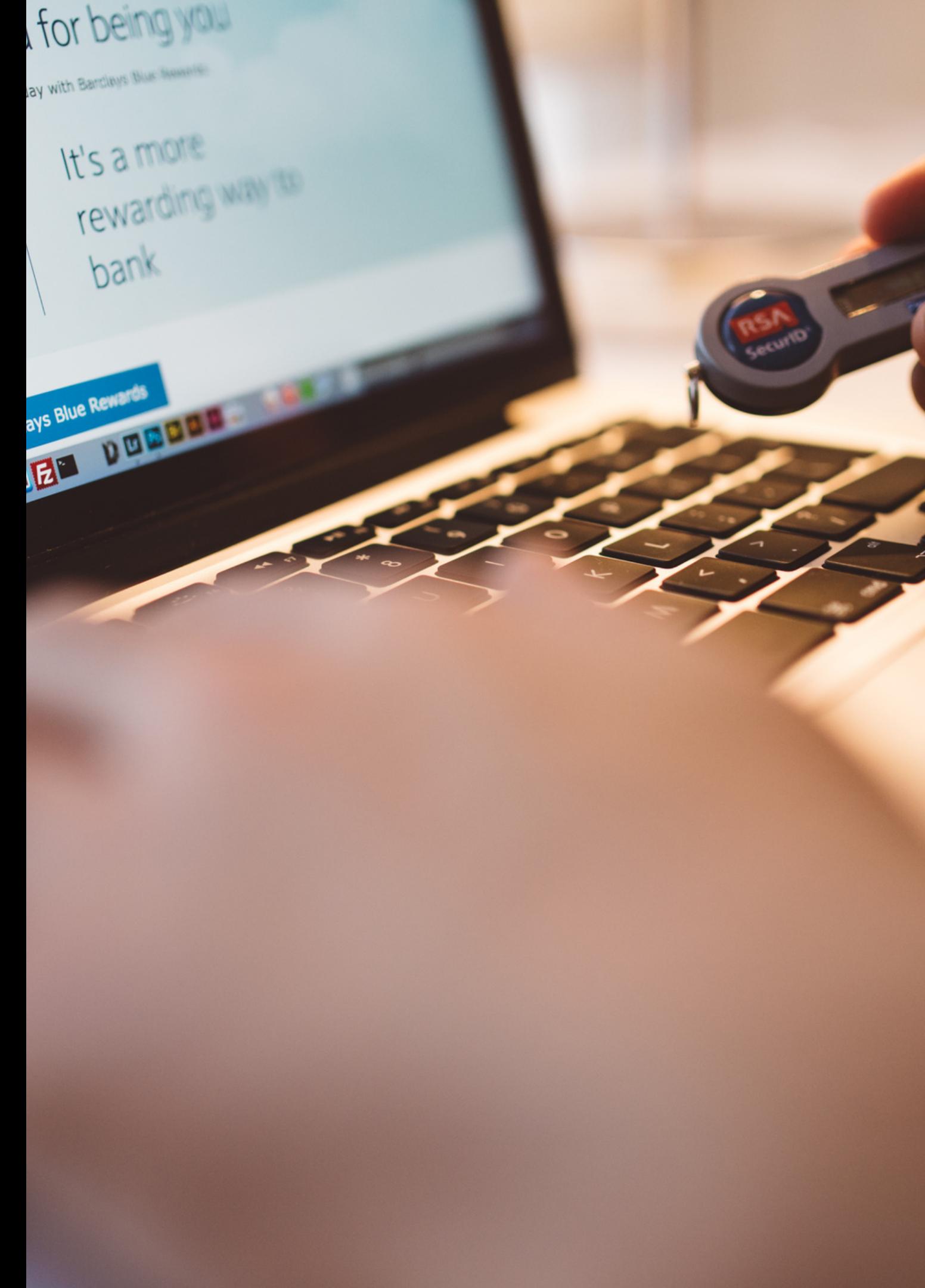
Jason Web Token;

USER - PASS

Usuário e Senha;

Gerenciamento de Acesso Privilegiado - PAM

- Super User;
- Root;
- Domain Administrative Account;
- Local Administrative Account;
- Secure Socket Shell Key;
- Emergency Account;
- Privileged Business User;
- Application Account;
- Service Account;
- SSH Key;
- Secret ...



Funcionamento



Primeiro, o usuário acessa um Vault, para certificação de autenticidade e autorização.

PAM

A ferramenta recebe o acesso direto do usuário e gera uma série de camadas complexas de segurança e controle.

Complex Password Password Storage

Senhas gigantes e
protegidas;

Encryption keys

Tudo encriptado e as chaves
armazenadas em locais
seguros e secretos;

Monitoramento Governança

Gravação, Monitoramento,
Controle e Relatórios;



Red Team

- Senhas fracas;
- Engenharia social;
- Desatualizações;
- Patches;
- Desinformação;
- CVE - Common Vulnerability Exposure;
- Zero Days;

...and so on...