SENAI Serviço Nacional de Aprendizagem Industrial

# Fundamentos de Segurança e Controle de Acesso

Capacitando profissionais para proteger ativos digitais no cenário atual da cibersegurança.

**Produzido por** MARCIO SCHOENFELDER

# O Tripé da Segurança da Informação: CID

A Segurança da Informação se baseia em três pilares essenciais: Confidencialidade, Integridade e Disponibilidade, garantindo que os dados estejam sempre seguros e acessíveis para quem precisa.

1

## Confidencialidade

Assegura que a informação seja acessível apenas por entidades autorizadas. **Protege contra acesso não autorizado**.

2

## Integridade

Garante que a informação seja precisa, completa e não alterada sem permissão. **Evita modificações indevidas**.

3

## Disponibilidade

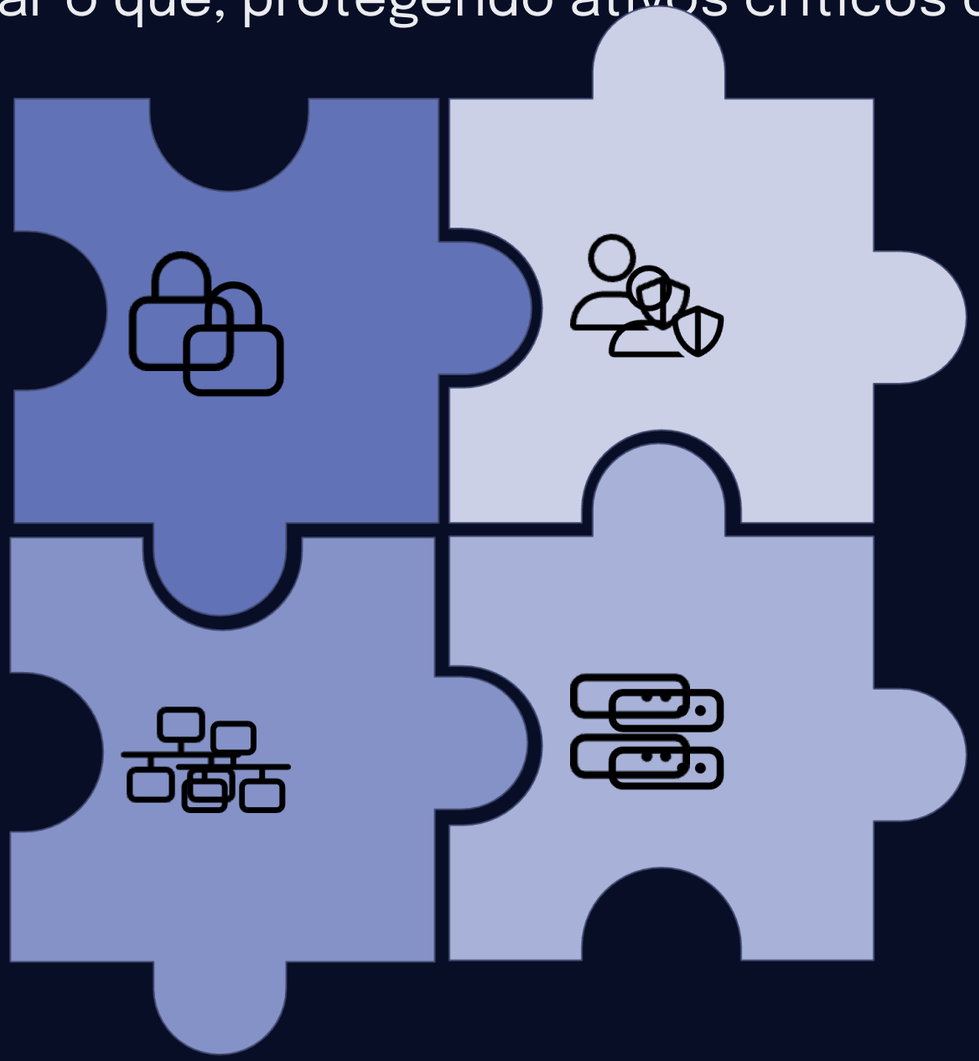
Garante que os usuários autorizados tenham acesso à informação e aos recursos quando necessário. **Mantém o acesso contínuo**.

**Produzido por** MARCIO SCHOENFELDER

# Importância Vital do Controle de Acesso

O Controle de Acesso é a espinha dorsal da segurança da informação.

Ele regula quem pode acessar o quê, protegendo ativos críticos de ameaças internas e externas.




Produzido por MARCIO SCHOENFELDER

# Tipos de Controle de Acesso: Físico e Lógico

Para uma proteção abrangente, o controle de acesso é dividido em duas categorias principais, cada uma com seu papel distinto na segurança.

## Controle Físico


## Controle Lógico

# Modelos de Controle de Acesso

Diferentes modelos de controle de acesso são empregados para atender a necessidades específicas de segurança e governança em ambientes de TI.

1

DAC

Controle de Acesso Discricionário: O proprietário do recurso define as permissões.

2

MAC

Controle de Acesso Mandatório: Baseado em níveis de classificação de segurança.

3

RBAC

Controle de Acesso Baseado em Papéis: Permissões atribuídas a papéis, não a usuários.

4

ABAC

Controle de Acesso Baseado em Atributos: Acesso concedido com base em múltiplos atributos (usuário, recurso, ambiente).

**Produzido por** MARCIO SCHOENFELDER

# Mecanismos de Autenticação

A autenticação é o processo de verificar a identidade de um usuário, garantindo que apenas indivíduos legítimos possam acessar um sistema ou recurso.

## Senhas

Combinação de caracteres que o usuário deve conhecer para provar sua identidade.

## Tokens

Dispositivos físicos (tokens USB, cartões inteligentes) ou virtuais (aplicativos) que geram códigos temporários.

## Biometria

Verificação da identidade do usuário por características físicas únicas (impressão digital, reconhecimento facial, íris).

# Fatores de Autenticação

A segurança da autenticação é diretamente proporcional ao número e diversidade de fatores utilizados, dificultando acessos não autorizados.


## Fator Único

Autenticação baseada em um único fator (ex: apenas senha).


## Dois Fatores

Autenticação requer dois fatores diferentes (ex: senha + token).


## Múltiplos Fatores

Autenticação requer três ou mais fatores, oferecendo maior segurança.

A implementação de MFA é uma das práticas mais recomendadas atualmente para proteção de contas e sistemas.

**Produzido por** MARCIO SCHOENFELDER

# Autenticação vs. Autorização

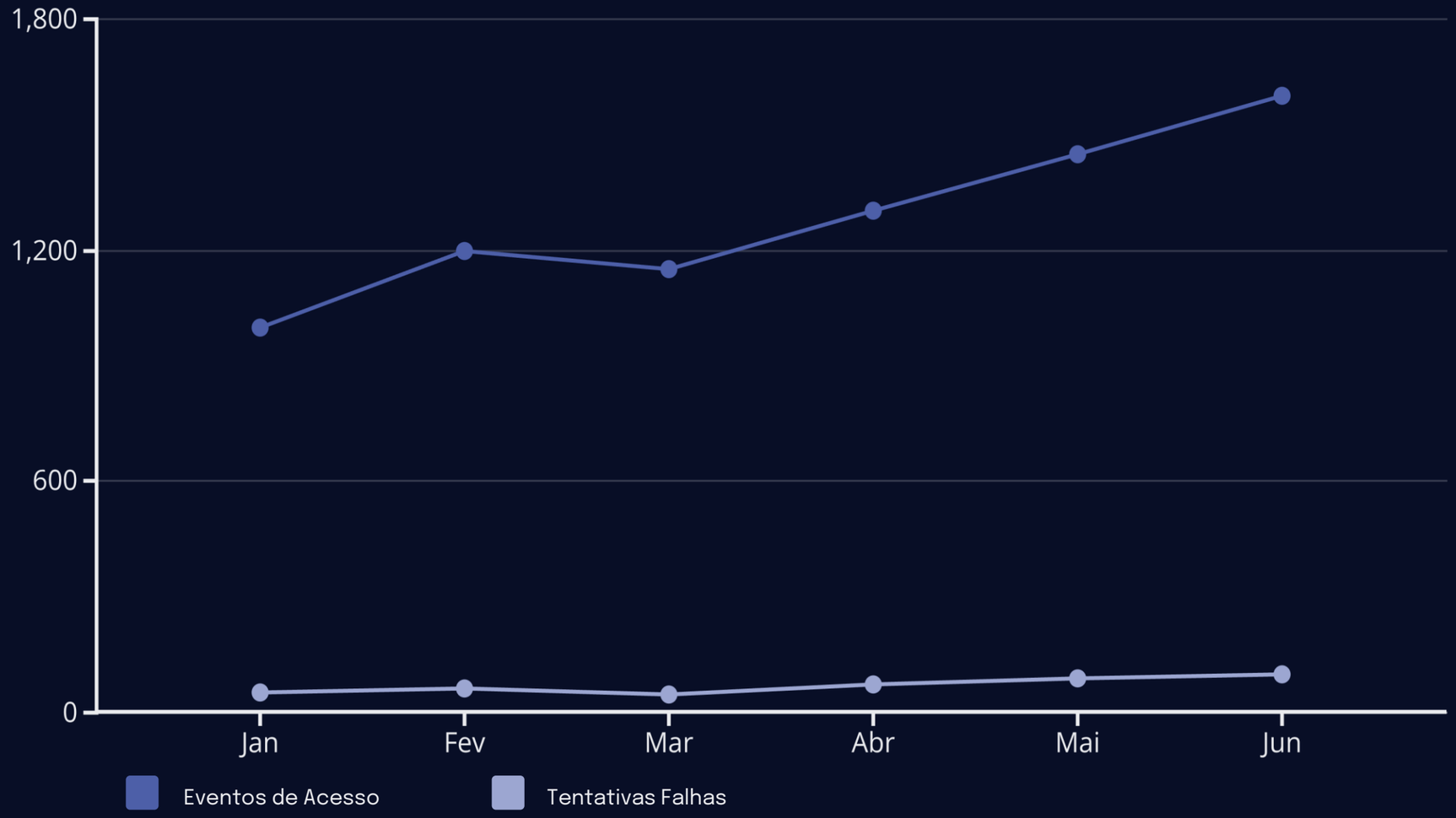
Embora frequentemente confundidos, autenticação e autorização são processos distintos e complementares na segurança de sistemas.

## Autenticação


## Autorização

# Auditoria e Logs de Acesso

A auditoria e o registro de logs são cruciais para monitorar atividades, detectar anomalias e responder a incidentes de segurança de forma eficaz.



# Boas Práticas e o Princípio do Menor Privilégio

Adotar boas práticas de segurança e o princípio do menor privilégio são fundamentais para minimizar riscos e fortalecer o controle de acesso.

## 1 Princípio do Menor Privilégio

Conceder apenas as permissões mínimas necessárias para que um usuário ou sistema realize suas tarefas. **Minimiza a superfície de ataque**.

## 2 Senhas Fortes e Únicas

Usar senhas complexas e diferentes para cada serviço/sistema. Considerar o uso de geradores e gerenciadores de senhas.

## 3 MFA em Todo Lugar

Habilitar autenticação multifator sempre que possível, adicionando uma camada extra de segurança.

## 4 Revisão Periódica de Acessos

Auditar e ajustar as permissões de acesso regularmente para garantir que estejam alinhadas às necessidades atuais.

**Produzido por** MARCIO SCHOENFELDER