

# Guia de Segurança Digital

## Documentação essencial sobre como proteger e evitar ataques cibernéticos

Proteger dados e evitar ataques envolve uma combinação de boas práticas, políticas de segurança e uso de tecnologias adequadas. Abaixo estão alguns pontos fundamentais que sustentam uma estrutura digital segura:

### Autenticação e Controle de Acesso

- Implemente autenticação segura para todos os usuários, utilizando senhas fortes e, quando possível, autenticação em dois fatores). Além disso, estabeleça níveis de permissão para que cada usuário acesse apenas o que é necessário, evitando brechas internas.

### Proteção de Dados, Criptografia e LGPD

- A segurança das informações é essencial para manter a integridade e a privacidade dos usuários. Aplique criptografia tanto para dados armazenados quanto para os transmitidos em rede, garantindo que informações confidenciais não possam ser lidas por terceiros, mesmo em caso de interceptação.
- Além disso, assegure o cumprimento da Lei Geral de Proteção de Dados (LGPD), armazenando dados pessoais de forma segura e apenas mediante consentimento, reforçando a responsabilidade e a transparência no uso das informações.

### Atualizações e Correções de Segurança

- Mantenha o sistema, bibliotecas e dependências sempre atualizados. Falhas conhecidas em versões antigas são uma das principais portas de entrada para ataques cibernéticos.

### Backup e Recuperação

- Estabeleça rotinas automáticas de backup e teste periodicamente os planos de recuperação. Em caso de falhas ou ataques, essa prática garante a restauração rápida dos dados e a continuidade do sistema.

## **Monitoramento e Logs**

- Implemente mecanismos de monitoramento contínuo e registro de logs. Isso permite identificar atividades suspeitas, detectar tentativas de invasão e agir de forma preventiva.
- 

## **Educação e Conscientização dos Usuários**

- A segurança não depende apenas de tecnologia, mas também de comportamento. Oriente a equipe e os usuários sobre boas práticas, como não compartilhar senhas, evitar links suspeitos e manter dispositivos protegidos.
- 

## **Testes e Auditorias de Segurança**

- Realize periodicamente testes de vulnerabilidade e auditorias para avaliar a eficácia das medidas implementadas. Ferramentas de pentest ajudam a detectar falhas antes que invasores as explorem.