# SEGURANÇA DA INFORMAÇÃO

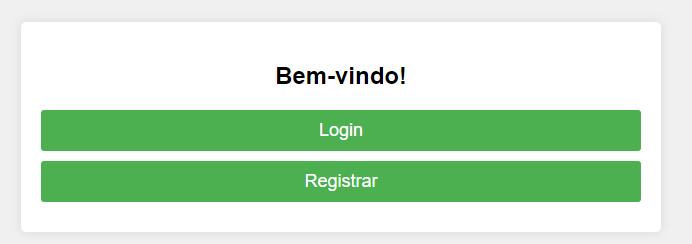
**Raphael Almeida, Carlos Eduardo, João Victor e Daniel Augusto**

# INTRODUÇÃO À APLICAÇÃO 2

# WEB E METODOLOGIA STRIDE

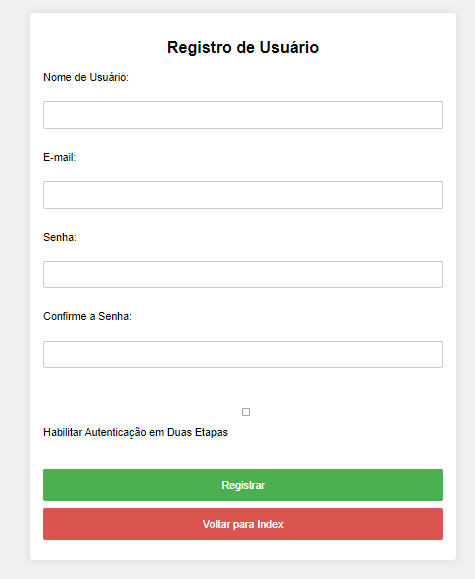
Esta aplicação web permite aos usuários registrar, fazer login, autenticar, gerenciar backups e acessar um painel administrativo. A segurança é crucial, e a metodologia STRIDE é usada para analisar e mitigar ameaças. STRIDE aborda Spoofing (falsificação), Tampering (adulteração), Repudiation (repúdio), Information Disclosure (divulgação de informações), Denial of Service (negação de serviço) e Elevation of Privilege (elevação de privilégios), garantindo um sistema mais seguro e confiável.

# INDEX 3



Aplicação começa com uma index com as opções de login e registrar, para o usuário poder utilizar a aplicação.

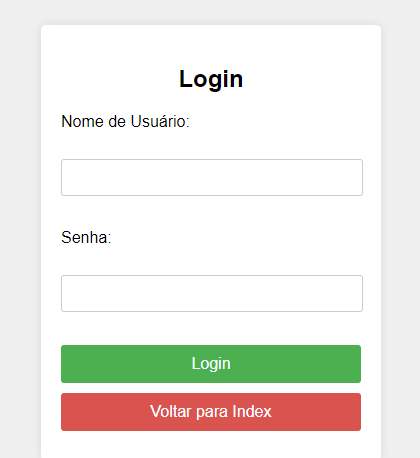
# REGISTER



No segundo passo o usuário registra com nome de usuário, e-mail valido, senha forte, e confirmar a senha.

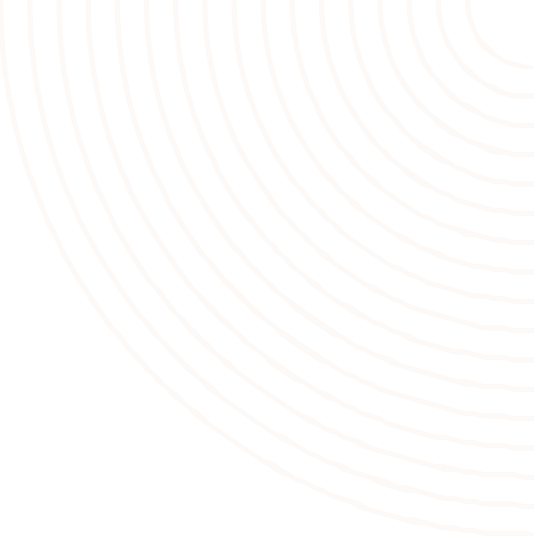
Essa senha precisa ter uma letra maiúscula um caractere especial e mínimo 8 caracteres

# LOGIN



Agora o usuário coloca seu nome de usuário e a senha que foi registrada para dar entrada no sistema

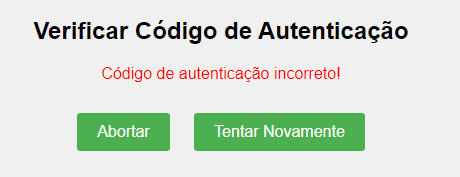
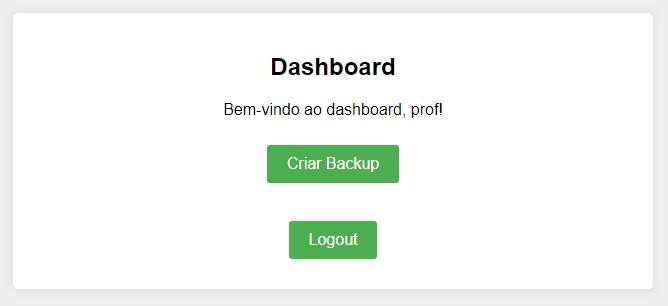
# AUTENTICAÇÃO 6



Na autentifica de duas etapas o usuário pode ver seu código clicando na opção mostrar código de autentificação, depois de copiar o código ele pode verificar e entrar na aplicação.

# CAMINHOS 7

Caso passe na autentificaçao pronto você esta no dashboard,tendo a opção de criar um backup e de logout

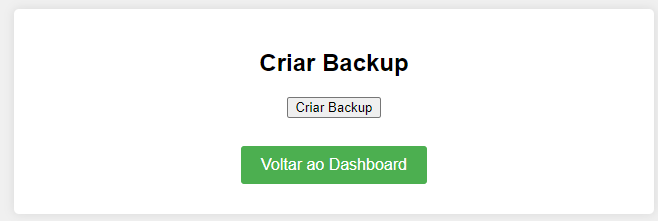


Caso não passe na autentificação o usuário terá a opção de abortar ou de tentar novamente a verificação

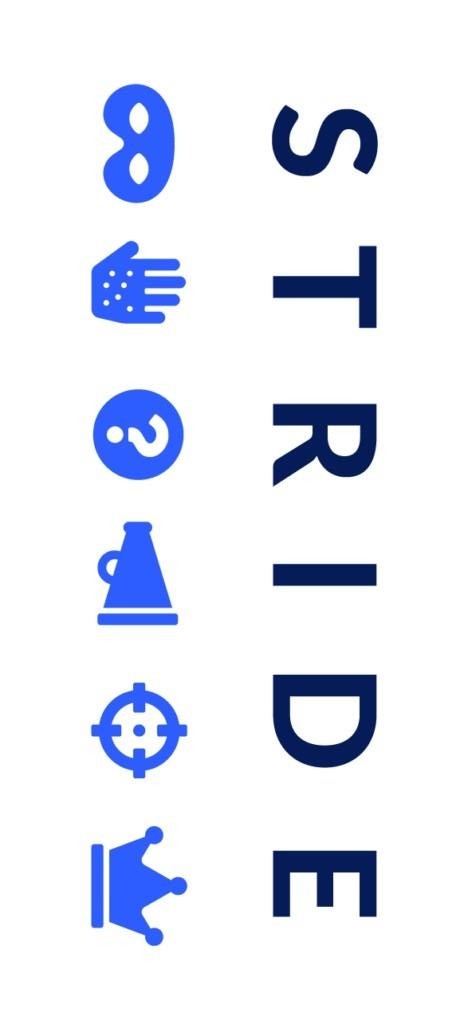
# CRIAR BACKUP

8

Por fim o usuário terá a opção de criar um arquivo de backup ou voltar ao dashboard.



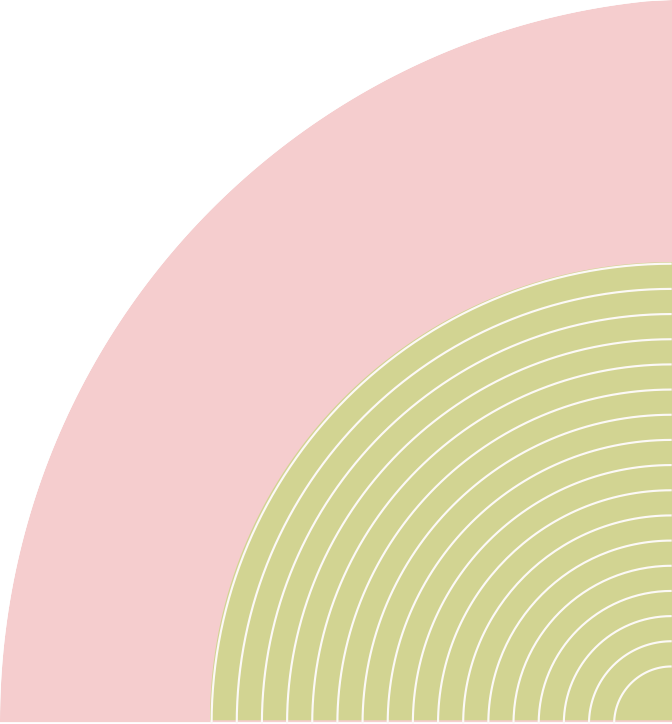
9



# O QUE É A METODOLOGIA STRIDE?

A metodologia STRIDE é uma abordagem estruturada para analisar e mitigar ameaças em sistemas de informação. Cada letra do acrônimo refere-se a uma categoria específica de ameaça.

# METODOLOGIA STRIDE E SUAS DIVISÕES



10

**1-Spoofing (Falsificação)**

**O que é**:Entidade maliciosa assume identidade de outra para acesso não autorizado.

**Mitigações:Autenticação Multifator (MFA):**Foi implementado um segundo fator de autenticação para fortalecer a segurança no login.

**Controle de Sessão:** Utiliza tokens de sessão seguros e configurá-los para expirar após um período de inatividade.

**Hashing Seguro de Senhas:** Utiliza algoritmos de hashing robustos, como bcrypt, para armazenar senhas.

# METODOLOGIA STRIDE E SUAS DIVISÕES 11

## Tampering (Adulteração)

Injection

**O que é:** Modificação não autorizada de dados ou sistemas.

**Mitigações: Validação e Sanitização de Dados:** Aaplicaçao garante que todas as entradas do usuário sejam validadas e sanitizadas para evitar injeção de SQL e outros ataques de adulteração.

**Prepared Statements: A** aplicaçao utiliza consultas preparadas com bind\_param para interações com o banco de dados, prevenindo SQL

1. **Repudiation (Repúdio)**

**O que é:** Usuário nega ter realizado uma ação

específica.

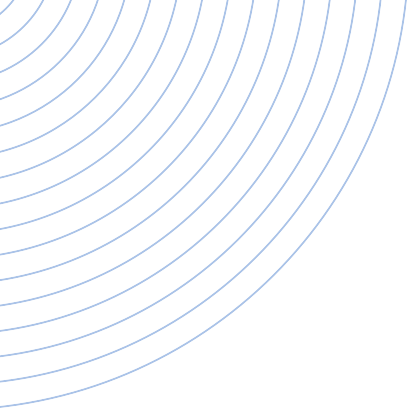
**Falha:** O sistema não registra quantos backups um usuário fez, nem quem fez.

**Mitigação:** Logs auditáveis e seguros, assinaturas digitais, sistemas de registro imutáveis.

# METODOLOGIA STRIDE E SUAS 12

DIVISÕES

## Information Disclosure (Divulgação de Informações)



**O que é:**Acesso não autorizado a informações sensíveis.

**Falha:** Todos os usuários entram com controle total da aplicação podendo vazar informações sensíveis

**Mitigação:** Criptografia de dados, controle de acesso baseado em funções (RBAC), mascaramento de dados, monitoramento e alertas.

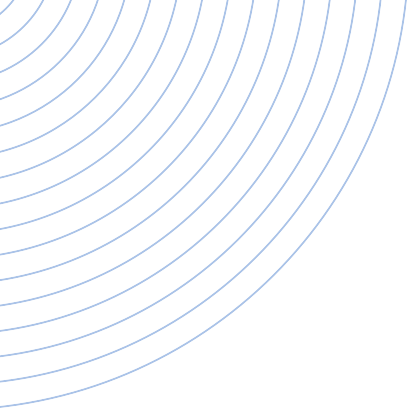
1. **Denial of Service (Negação de Serviço)**

**O que é:**Ataques que visam tornar sistemas ou serviços indisponíveis.

**Mitigações:Limites de Taxa (Rate Limiting):**Foi implementado limites de taxa para requisições ao servidor, prevenindo ataques de negação de serviço.

**Configuração do Servidor:** A aplicação faz a configuração do Apache e MySQL para lidar com grandes volumes de tráfego e prevenir DoS.

# METODOLOGIA STRIDE E SUAS 13



DIVISÕES

## Elevation of Privilege (Elevação de Privilégios)

**O que é:** Usuário obtém níveis de acesso maiores do que os autorizados.

**Falha:** É possível um usuário se auto elevar na aplicação, pois todos entram com o controle máximo da aplicação.

**Mitigações: Controle de Acesso Baseado em Funções (RBAC):** Implementar RBAC para garantir que os usuários só possam executar ações permitidas por seu nível de acesso.

**Princípio do Menor Privilégio:** Configurar as permissões de modo que os usuários só tenham acesso aos recursos necessários para suas funções.

# CONCLUSÃO

A segurança é um aspecto crítico para qualquer aplicação web especialmente aquelas que lidam com dados sensíveis e funções Administrativas. Implementar medidas adequadas de mitigação para ameaças comuns pode ajudar a proteger a integridade confidencialidade e disponibilidade da aplicação e dos dados dos usuários.