

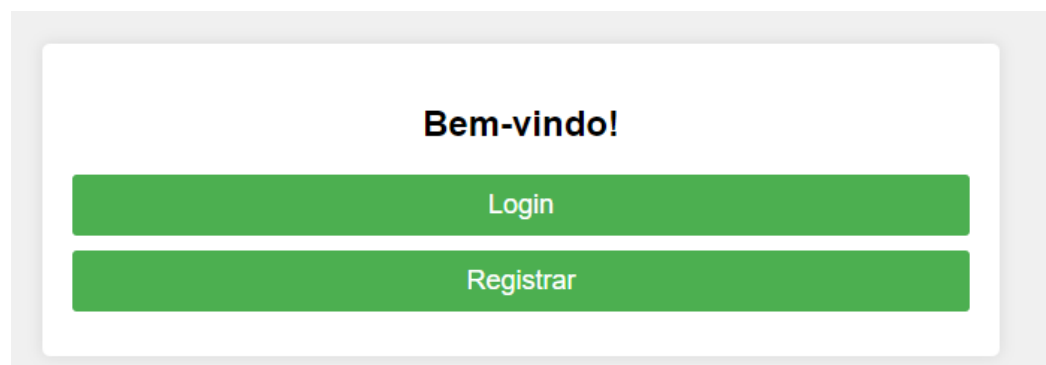
# Manual de Funcionamento - Metodologia STRIDE

Este manual descreve o funcionamento de uma aplicação, para sistema de gerenciamento de backups desenvolvida para objetivo é fornecer orientações claras sobre como utilizar a aplicação de maneira eficiente e segura.

## Uso da Aplicação

### Login e Autenticação:

- **Insira Nome de Usuário e Senha(forte):** Nome(Flávia), Senha(Flavia@569)
- **Para Registrar crie:** Nome de Usuário, E-mail e Senha
- **Caso necessário, utilize a autenticação de dois fatores para maior segurança.**



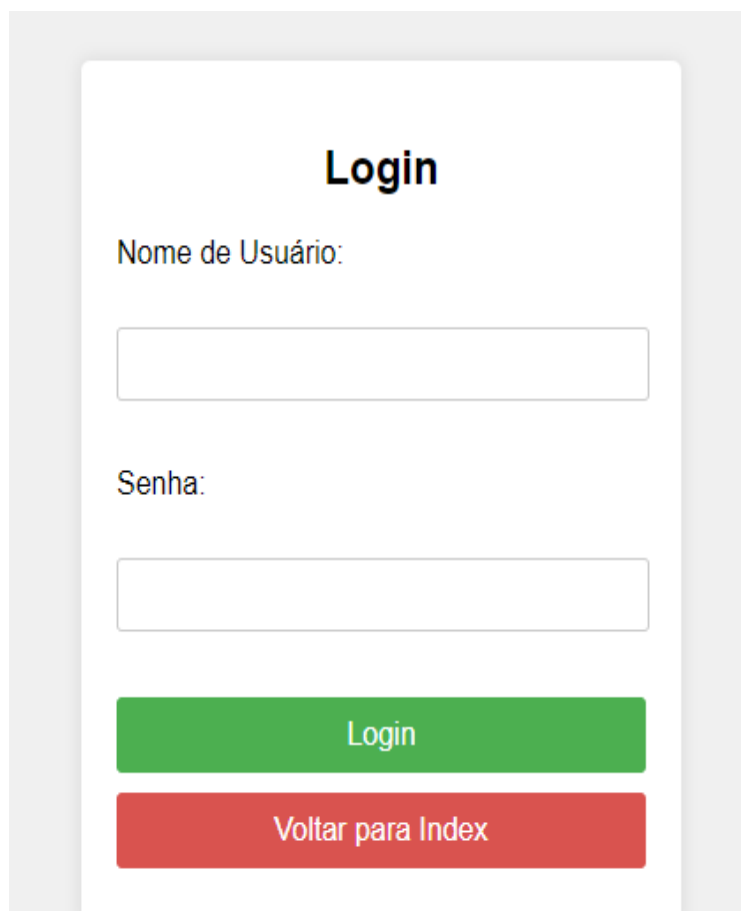
## Funcionalidades Principais

### A aplicação possui as seguintes telas:

- Login
- Registrar
- Autenticação em duas etapas onde o usuário irá receber um código
- Dashboard onde será possível criar Backup ou fazer Logout

**OBS:** Para melhor entendimento siga as instruções abaixo.

**1. Faça seu login ou registre-se:**

A login form interface with a white background and a light gray border. The title "Login" is centered at the top in bold black font. Below it, the label "Nome de Usuário:" is followed by a white text input field with a thin gray border. Further down, the label "Senha:" is followed by another white text input field with a thin gray border. At the bottom, there are two buttons: a green button with the text "Login" in white, and a red button with the text "Voltar para Index" in white.

**Login**

Nome de Usuário:

Senha:

Login

Voltar para Index

### Registro de Usuário

Nome de Usuário:

E-mail:

Senha:

Confirme a Senha:

☐

Habilitar Autenticação em Duas Etapas

Registrar

Voltar para Index

## 2. Faça sua autenticação:

### Autenticação em Duas Etapas

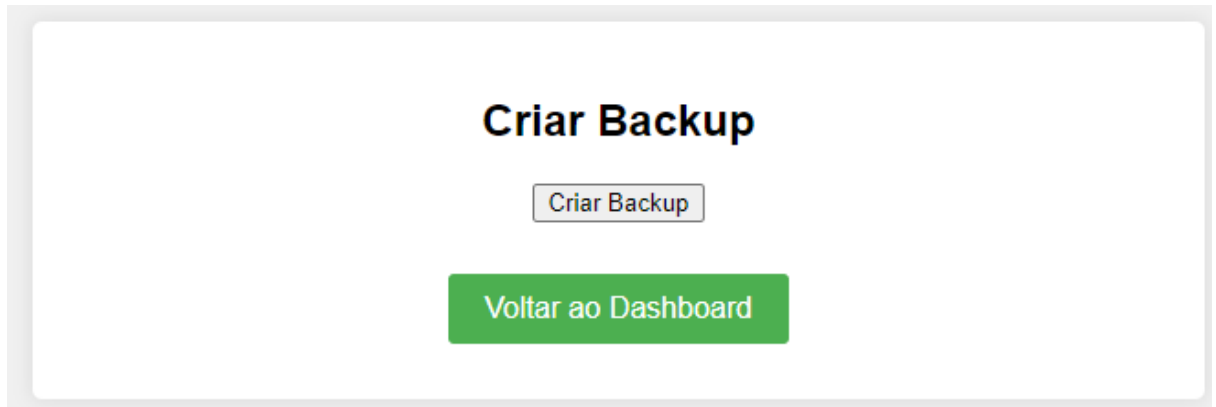
Um código de autenticação foi enviado para você. Por favor, insira o código abaixo:

Código de Autenticação:

Verificar Código

Mostrar Código de Autenticação

### 3. Crie seu Backup:



## Requisitos de Sistema

Para utilizar a aplicação é necessário:

- Dispositivo compatível (Computador, Notebook ou tablet ).
- Navegador web atualizado (Firefox, Chrome, Safari).
- Navegador web atualizado (Firefox, Chrome, Safari).

## Identificação dos Pontos de Atenção Utilizando a Metodologia STRIDE

### 1. Spoofing:

- utiliza um segundo fator de autenticação para fortalecer a segurança no login.
- Utilizar algoritmos de hashing robustos, como bcrypt, para armazenar senhas.

### 2. Tampering (Violação):

- Garante que todas as entradas do usuário sejam validadas e sanitizadas para evitar injeção de SQL e outros ataques de adulteração.

### **3. Repudiation (Repúdio):**

- Um usuário pode negar ter realizado uma ação específica, como alterar dados ou fazer login.
- Manter logs detalhados de todas as ações do usuário, incluindo tentativas de login, alterações de dados e acessos ao sistema, pois só é possível notar uma autenticação com o horário do sistema.

### **4. Information Disclosure (Divulgação de Informação):**

- Dados sensíveis podem ser expostos para usuários não autorizados, comprometendo a confidencialidade.
- Implementar controles rigorosos de acesso para garantir que apenas usuários autorizados possam acessar informações sensíveis.

### **5. Denial of Service (Negação de Serviço):**

- Um atacante não consegue sobrecarregar o sistema, tornando-o indisponível para os usuários legítimos.
- Possui as configurações do Apache e MySQL para lidar com grandes volumes de tráfego e prevenir DoS.

## **6. Elevation of Privilege (Elevação de Privilégio):**

- O sistema não permite ver o nome do usuário.
- Implementar RBAC para garantir que os usuários só possam executar ações permitidas por seu nível de acesso.
- Configurar as permissões de modo que os usuários só tenham acesso aos recursos necessários para suas funções.

## **Conclusão**

O sistema de gerenciamento de backups possui algumas melhorias a se fazer, para que isso seja resolvido será necessário implementar algumas mitigações propostas ou seja configurar algumas aplicações como fizemos na parte que configuramos diretrizes na parte do projeto e manter atualizações.