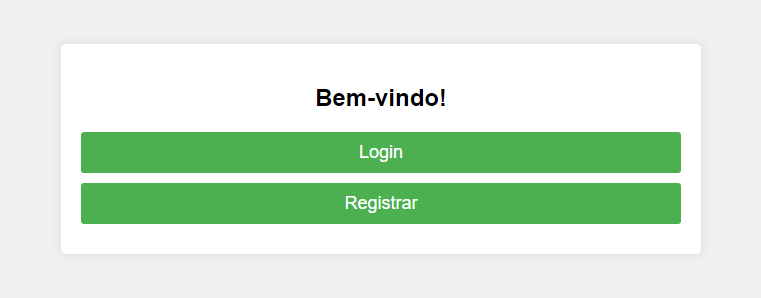
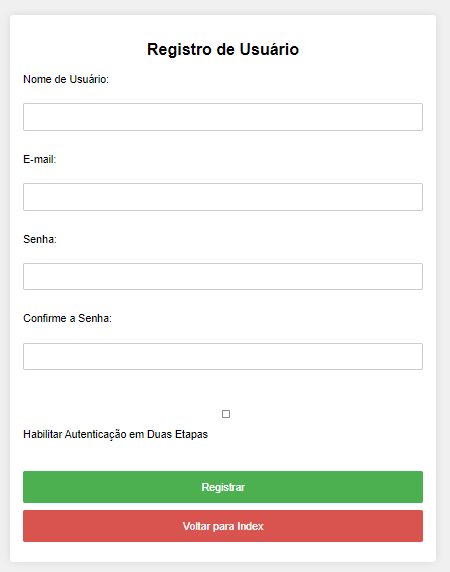
**MANUAL DE FUNCIONAMENTO DE APLICAÇÃO**

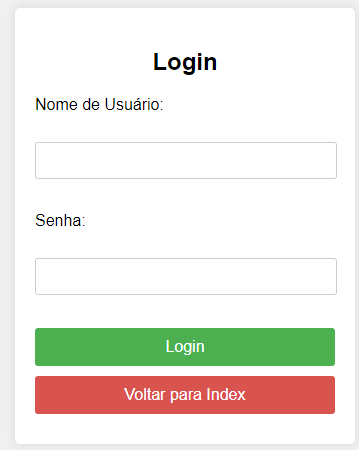
**Página Inicial:** No index.php temos a mensagem “Bem-vindo!” e duas opções para serem acessadas, sendo elas a área de Login e Registrar.



**Página de Registro:** No register.php temos os locais para serem preenchidos como, Nome de Usuário, E-mail, Senha e Confirme a Senha, além de um campo para ser preenchido opcionalmente que envolve a Autenticação de Duas Etapas.

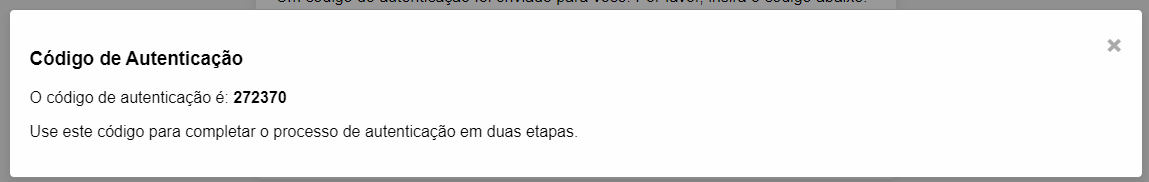
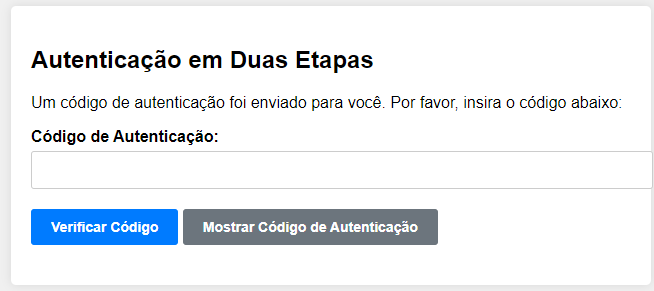


**Página de Login:** No login.php há dois campos que são necessários serem preenchidos para prosseguir a aplicação. Além da opção “Voltar para Index” que ao clicar te retorna para a página inicial.

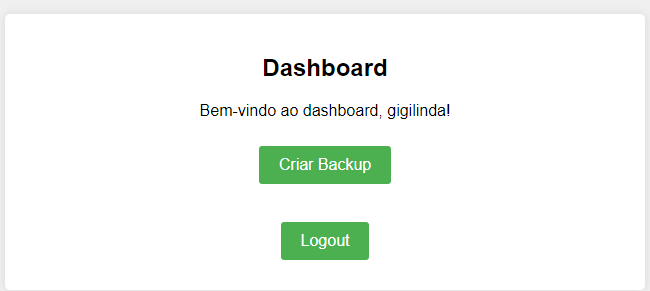


**Funcionalidade:** Sistema Login e registro de usuário utilizando autenticação multifatorial.

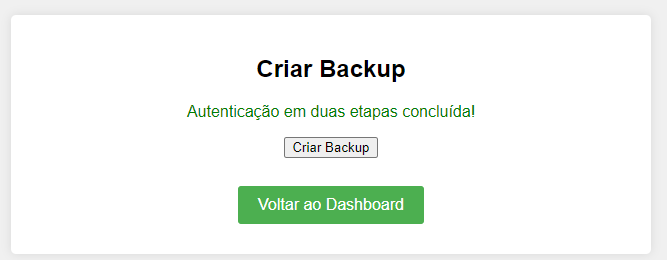
**Página de Autenticação:** Após realizar o registro e preencher o campo da autenticação de duas etapas, ao realizar o login será encaminhado para esta página. Onde para que possamos avançar temos que pegar o código solicitado, ele aparecerá ao escolher a opção “Mostrar Código de Autenticação”.



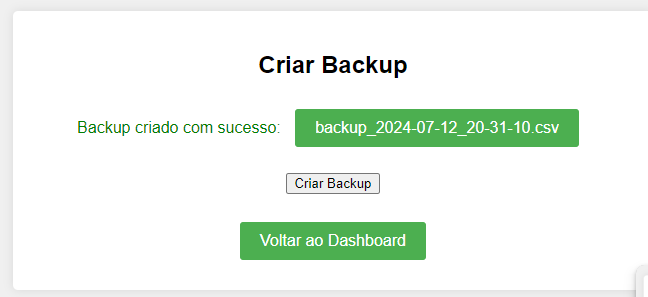
**Funcionalidade:** São usados modelos como **Spoofing (Falsificação), a qual** requer não apenas senha, mas também um segundo fator (como um código enviado) para evitar falsificação de identidade. Isso torna mais difícil para os invasores obterem acesso não autorizado, mesmo que conheçam a senha do usuário.



**Página do Dashboard:** No Dashboard temos duas opções, “Criar Backup” e “Logout”. Ao clicar na primeira opção irá te direcionar para outra página e a outra te voltará a página inicial



**Página do Backup:** Ao ser direcionado para a próxima página você terá duas alternativas, Criar Backup e Voltar ao Dashboard.



Depois de clicar em Criar backup, aparecerá um botão para que seja efetuado o download do backup local.

**O modelo Microsoft STRIDE de acordo com a aplicação:**

* **Tampering (Violação)**: Protege a integridade dos dados, mesmo se a senha for comprometida, pois o segundo fator é necessário para acesso.
* **Repudiation (Repúdio)**: Dificulta que usuários neguem transações autenticadas por dois fatores distintos.
* **Information Disclosure (Divulgação de Informação)**: Reduz a exposição de informações, pois o segundo fator não é facilmente acessível como a senha.
* **Denial of Service (Negação de Serviço)**: Ajuda a mitigar ataques de força bruta direcionados a senhas.
* **Elevation of Privilege (Elevação de Privilégio)**: Dificulta a elevação de privilégios ao exigir acesso ao segundo fator além da senha.

**Sugestões de melhorias na aplicação:**

* Opção para alterar a senha;
* Fazer a junção das páginas do dashboard e backup;

**Conclusão:** O desenvolvimento de aplicações seguras é crucial para proteger dados sensíveis, garantir a integridade dos sistemas e manter a confiança dos usuários. Práticas de segurança robustas previnem acessos não autorizados, fraudes e ataques cibernéticos, evitando perdas financeiras e danos á reputação. Implementar autenticação multifatorial, usar criptografia, realizar testes de segurança e educar desenvolvedores são medidas essenciais parar criar um ambiente digital confiável e conforme as regulamentações. Segurança no desenvolvimento é vital para a sustentabilidade e sucesso de qualquer organização na era digital.

**Nomes: Giovanna Esther, Matheus Coelho, Jessica Aníbal.**