Épico: Autenticação do Usuário

Descrição: Este épico utiliza o formato estrutural da plataforma Jira e se concentra na implementação da funcionalidade de autenticação de usuário para uma loja online de vendas de roupas. Compreende a criação de uma experiência de login e registro intuitiva e segura para os clientes, permitindo-lhes acessar os recursos do site, realizar compras e gerenciar suas informações pessoais.

Objetivos:

- Facilitar o acesso dos clientes ao site, proporcionando uma experiência de login simples e intuitiva.
- Garantir a segurança das contas dos clientes por meio de medidas robustas de autenticação e proteção de dados.
- Oferecer opções de registro para novos clientes, incentivando a expansão da base de usuários e aquisição de clientes.
- Personalizar a experiência do usuário, permitindo que os clientes gerenciem suas informações pessoais e preferências de conta.

Histórias de Usuário:

1. Login básico
2. Registro de novo usuário
3. Recuperação de senha
4. Verificação de e-mail
5. Login com autenticação social
6. Configurações de segurança da conta
7. Login com autenticação de dois fatores

1. História de usuário: Login básico

Requisitos:

- O sistema deve permitir que usuários registrados façam login usando seu nome de usuário e senha.

Critérios de aceitação:

- O usuário deve ser redirecionado para a página inicial após fazer login com sucesso.
- O sistema deve exibir uma mensagem de erro se o nome de usuário ou a senha estiverem incorretos.

Cenários BDD (Gherkin):

Funcionalidade: Login básico

I. Cenário: Login com sucesso
→ Dado que um usuário registrado possui um nome de usuário válido e uma senha válida
→ Quando o usuário faz login com seu nome de usuário e senha corretos
→ Então o usuário é redirecionado para a página inicial

II. Cenário: Login com senha incorreta
→ Dado que um usuário registrado possui um nome de usuário válido
→ Quando o usuário tenta fazer login com seu nome de usuário válido e uma senha incorreta
→ Então o sistema exibe uma mensagem de erro informando que a senha está incorreta

III. Cenário: Login com nome de usuário inválido
→ Dado que um usuário tenta fazer login com um nome de usuário inválido
→ Quando o usuário insere um nome de usuário que não está registrado no sistema
→ Então o sistema exibe uma mensagem de erro informando que o nome de usuário é inválido

2. História de usuário: Registro de novo usuário

Requisitos:

- O sistema deve permitir que novos usuários criem uma conta fornecendo um nome, endereço de e-mail e senha.

Critérios de aceitação:

- Após o registro bem-sucedido, o usuário deve receber um e-mail de verificação.
- O sistema deve validar se o endereço de e-mail fornecido é único e válido.

Cenários BDD (Gherkin):

Funcionalidade: Registro de novo usuário

I. Cenário: Registro bem-sucedido
→ Dado que um novo usuário preenche corretamente o formulário de registro com um nome, um endereço de e-mail único e uma senha
→ Quando o usuário envia o formulário de registro
→ Então o usuário recebe um e-mail de verificação

II. Cenário: Endereço de e-mail já em uso
→ Dado que um novo usuário preenche o formulário de registro com um endereço de e-mail que já está em uso
→ Quando o usuário tenta enviar o formulário de registro
→ Então o sistema exibe uma mensagem de erro informando que o endereço de e-mail já está em uso

III. Cenário: Endereço de e-mail inválido
→ Dado que um novo usuário preenche o formulário de registro com um endereço de e-mail inválido
→ Quando o usuário tenta enviar o formulário de registro
→ Então o sistema exibe uma mensagem de erro informando que o endereço de e-mail é inválido

3. História de usuário: Recuperação de senha

Requisitos:

- O sistema deve permitir que usuários solicitem a redefinição de sua senha fornecendo seu endereço de e-mail.

Critérios de aceitação:

- Após a solicitação de redefinição de senha, o usuário deve receber um e-mail com um link para redefinir sua senha.
- O sistema deve verificar se o endereço de e-mail fornecido pertence a uma conta válida.

Cenários BDD (Gherkin):

Funcionalidade: Recuperação de senha

I. Cenário: Solicitação de redefinição de senha bem-sucedida
→ Dado que um usuário deseja redefinir sua senha e fornece seu endereço de e-mail associado à sua conta
→ Quando o usuário envia a solicitação de redefinição de senha
→ Então o usuário recebe um e-mail com um link válido para redefinir sua senha

II. Cenário: Endereço de e-mail não associado a uma conta
→ Dado que um usuário deseja redefinir sua senha e fornece um endereço de e-mail que não está associado a uma conta no sistema
→ Quando o usuário envia a solicitação de redefinição de senha
→ Então o sistema exibe uma mensagem de erro informando que o endereço de e-mail não está associado a uma conta

III. Cenário: Endereço de e-mail inválido
→ Dado que um usuário deseja redefinir sua senha e fornece um endereço de e-mail inválido
→ Quando o usuário envia a solicitação de redefinição de senha
→ Então o sistema exibe uma mensagem de erro informando que o endereço de e-mail é inválido

4. História de usuário: Verificação de e-mail

Requisitos:

- O sistema deve enviar um e-mail de verificação para o endereço fornecido durante o registro.

Critérios de aceitação:

- O e-mail de verificação deve conter um link válido para ativar a conta do usuário.
- Após clicar no link de verificação, a conta do usuário deve ser ativada no sistema.

Cenários BDD (Gherkin):

Funcionalidade: Verificação de e-mail

I. Cenário: Registro bem-sucedido e recebimento do e-mail de verificação
→ Dado que um novo usuário se registra com sucesso fornecendo um endereço de e-mail válido
→ Quando o usuário conclui o registro
→ Então o sistema envia um e-mail de verificação para o endereço fornecido

II. Cenário: Tentativa de clicar no link de verificação após expiração
→ Dado que um usuário se registrou recentemente e recebeu um e-mail de verificação
→ Quando o usuário tenta clicar no link de verificação após um determinado período
→ Então o sistema exibe uma mensagem informando que o link de verificação expirou

III. Cenário: Ativação bem-sucedida da conta após clicar no link de verificação
→ Dado que um usuário recebeu um e-mail de verificação e clicou no link
→ Quando o usuário clica no link de verificação
→ Então a conta do usuário é ativada com sucesso no sistema

5. História de usuário: Login social

Requisitos:

- O sistema deve permitir que usuários façam login usando suas credenciais de mídia social.

Critérios de aceitação:

- Os usuários devem ser capazes de associar suas contas de mídia social com suas contas no site.
- Os usuários devem ser redirecionados para o site após fazer login com sucesso usando mídia social.

Cenários BDD (Gherkin):

Funcionalidade: Login social

I. Cenário: Login usando conta do Facebook pela primeira vez
→ Dado que um usuário deseja fazer login usando sua conta do Facebook pela primeira vez
→ Quando o usuário seleciona a opção de login via Facebook e autoriza o acesso ao site
→ Então o usuário é redirecionado para o site e sua conta de mídia social é associada à sua conta no site

II. Cenário: Login usando conta do Google já associada
→ Dado que um usuário deseja fazer login usando sua conta do Google
→ E o usuário já possui uma conta associada ao site usando a mesma conta de mídia social
→ Quando o usuário seleciona a opção de login via Google
→ Então o usuário é redirecionado para a página inicial do site

III. Cenário: Tentativa de login com conta de mídia social não associada
→ Dado que um usuário deseja fazer login usando uma conta de mídia social não associada ao site
→ Quando o usuário seleciona a opção de login via mídia social e tenta fazer login
→ Então o sistema exibe uma mensagem de erro informando que a conta de mídia social não está associada a uma conta no site

6. História de usuário: Configurações de segurança da conta

Requisitos:

- O sistema deve permitir que usuários atualizem sua senha e outras configurações de segurança da conta.

Critérios de aceitação:

- As atualizações de senha devem ser aplicadas com sucesso e refletidas imediatamente.
- Os usuários devem ser notificados por e-mail sobre qualquer alteração nas configurações de segurança da conta.

Cenários BDD (Gherkin):

Funcionalidade: Configurações de segurança da conta

I. Cenário: Atualização bem-sucedida da senha
→ Dado que um usuário deseja atualizar sua senha
→ Quando o usuário insere uma nova senha que atende aos critérios de segurança
→ E confirma a atualização da senha
→ Então a senha é atualizada com sucesso e refletida imediatamente
→ E o usuário recebe uma notificação por e-mail confirmando a alteração

II. Cenário: Tentativa de atualização de senha com senha inválida
→ Dado que um usuário deseja atualizar sua senha
→ Quando o usuário insere uma nova senha que não atende aos critérios de segurança
→ E tenta confirmar a atualização da senha
→ Então o sistema exibe uma mensagem de erro informando que a nova senha não atende aos critérios de segurança

III. Cenário: Alteração bem-sucedida nas configurações de segurança
→ Dado que um usuário deseja alterar suas configurações de segurança da conta
→ Quando o usuário realiza as alterações desejadas
→ E confirma as alterações
→ Então as configurações são atualizadas com sucesso e refletidas imediatamente
→ E o usuário recebe uma notificação por e-mail informando sobre a alteração

7. História de usuário: Login com autenticação de dois fatores (2FA)

Requisitos:

- O sistema deve oferecer suporte à autenticação de dois fatores para usuários que optarem por ativar essa opção.

Critérios de aceitação:

- Os usuários devem poder ativar e desativar a autenticação de dois fatores em suas configurações de conta.
- Após ativar a autenticação de dois fatores, os usuários devem ser solicitados a fornecer um código de autenticação além de suas credenciais habituais durante o login.

Cenários BDD (Gherkin):

Funcionalidade: Login com autenticação de dois fatores (2FA)

I. Cenário: Ativação bem-sucedida da autenticação de dois fatores
→ Dado que um usuário deseja aumentar a segurança de sua conta
→ Quando o usuário ativa a autenticação de dois fatores em suas configurações de conta
→ Então durante o login, além de suas credenciais habituais, o usuário é solicitado a fornecer um código de autenticação

II. Cenário: Desativação bem-sucedida da autenticação de dois fatores
   → Dado que um usuário deseja desativar a autenticação de dois fatores em suas configurações de conta
   → Quando o usuário desativa essa opção
   → Então durante o login, o usuário não é mais solicitado a fornecer um código de autenticação além de suas credenciais habituais

III. Cenário: Tentativa de login com código de autenticação incorreto
   → Dado que um usuário tem a autenticação de dois fatores ativada
   → Quando o usuário faz login e fornece suas credenciais habituais e um código de autenticação incorreto
   → Então o sistema exibe uma mensagem de erro informando que o código de autenticação fornecido é incorreto