📄 Documento de teste

Este documento tem como objetivo validar e assegurar a qualidade das User Stories que serão apresentadas.

1. User Stories

As User stories abaixo são funcionalidades do ponto de vista do usuário.

1. Como usuário mobile, quero fazer login no aplicativo para acessar de forma segura e rápida as funcionalidades exclusivas;

2. Como usuário mobile, quero redefinir minha senha para garantir a segurança da minha conta;

3. Como usuário mobile, quero criar uma nova conta para desfrutar de todos os recursos e benefícios exclusivos do aplicativo.

2. Critérios de aceitação

Os critérios de aceitação abaixo são condições específicas e mensuráveis que definem se a história do usuário é considerada completa e atende às expectativas do cliente ou do usuário.

2.1 Critérios em comum para todas as User stories:

Acessibilidade:

- As páginas devem ser acessíveis para usuários com deficiências, seguindo as diretrizes de acessibilidade mobile.

Eficiência no processo:

- O tempo máximo de carregamento deve ser inferior a 3 segundos para cada tela (login, cadastro e mudança de senha), proporcionando uma experiência ágil para o usuário.

Design e padronização:

- Os componentes das interfaces de login, cadastro e mudança de senha devem estar alinhados e seguir padrões estéticos consistentes.
- A disposição dos elementos nas telas devem ser intuitivas e proporcionar uma experiência visual agradável.

2.2 Login no aplicativo

Interface de Login:

- A tela de login deve apresentar campos distintos para inserção do nome de usuário e senha.
- Deve haver um botão claro e visível para acionar o processo de login.
- Deve existir uma opção para redirecionar o usuário para recuperação de senha e para cadastro.

Autenticação Valida:

- O sistema deve permitir o login apenas se o nome de usuário existir na base de dados.
- A senha fornecida deve ser correspondente a senha cadastrada na base de dados para aquele respectivo usuário.

Acesso seguro:

- A senha deve ser encriptada e armazenada de forma segura no banco de dados.

Feedback Visual:

- Após um login bem-sucedido, o usuário deve receber feedback visual para confirmar o acesso.
- Em caso de falha no login, o sistema deve apresentar uma mensagem de erro clara, indicando a natureza do problema.

2.3 Redefinir senha

Acesso à Recuperação de Senha:

- O usuário deve ter acesso fácil à opção de redefinição de senha a partir da tela de login.

Identificação do Usuário:

- O sistema deve solicitar informações de identificação, como e-mail ou nome de usuário, para garantir que o solicitante seja o legítimo proprietário da conta.

Envio Seguro do Link de Redefinição:

- O usuário deve receber um link seguro por e-mail contendo um token único para a redefinição.
- O link deve expirar após um período razoável para garantir segurança.
- Deve ser exibida uma mensagem indicando que um e-mail foi enviado com as instruções de redefinição.

Validação de Token de Redefinição:

- O sistema deve validar o token para garantir que seja único, válido e não expirado, caso contrário, apresentar uma mensagem de erro explicativa.

Senha Forte e Política de Segurança:

- O sistema deve exigir que a nova senha atenda a critérios de segurança, como comprimento mínimo, inclusão de caracteres especiais, letras maiúsculas e minúsculas, e números.

Confirmação de Redefinição:

- O sistema deve notificar o usuário de que a senha foi alterada com sucesso.

2.4 Cadastro de conta

Interface de Cadastro:

- O usuário deve ter acesso fácil à opção de cadastro a partir da tela de login.

- A página de cadastro deve conter campos para inserção do nome, e-mail, senha e data de nascimento.
- Deve existir um botão de "Cadastrar" na página.

Validação de Campos:

- Todos os campos (nome, e-mail, senha e data de nascimento) devem ser obrigatórios.
- O campo de e-mail deve aceitar apenas endereços de e-mail válidos e não cadastrados.
- A senha deve atender aos requisitos de segurança (por exemplo, tamanho mínimo, caracteres especiais).
- A data de nascimento deve ser inserida de acordo com o formato especificado.

Feedback de Cadastro:

- Após o cadastro bem-sucedido, o usuário deve receber uma mensagem de confirmação.
- Em caso de falha no cadastro, o usuário deve receber mensagens de erro específicas para orientar a correção dos campos.

Segurança e Privacidade:

- As informações sensíveis, como a senha, devem ser transmitidas de forma segura (usando HTTPS).
- Não deve ser possível cadastrar mais de uma conta com o mesmo endereço de e-mail.
- As informações de cadastro devem ser devidamente armazenadas nos servidores do aplicativo de forma segura.

3. Casos de teste

3.1 Casos de uso de Login

Caso de teste 1:

Título: Login bem-sucedido

Código: 001

Descrição: Este caso de teste visa verificar o comportamento do sistema quando um usuário realiza um login bem-sucedido.

Pré-condições: O usuário possui uma conta válida e ativa.

Passo de execução:
1. Acesse a página de login;
2. Insira um nome de usuário válido;
3. Insira uma senha válida;
4. Clique no botão de login.

Entrada:
1. Nome de Usuário: miguelsilva90
2. Senha: SenhaSegura123#

Saída esperada:
- O sistema deve autenticar o usuário com sucesso.
- O usuário deve ser redirecionado para a página inicial.

Critério de aceitação:
- O login deve ser bem-sucedido, fornecendo ao usuário acesso ao sistema.
- Não devem ocorrer mensagens de erro durante o processo de login.

Tempo de execução estimado: 2 minutos, incluindo o tempo para inserção de dados e redirecionamento.

Caso de teste 2:

Título: Login com credenciais inválidas

Código: 002

Descrição: Este caso de teste tem o objetivo de verificar como o sistema trata tentativas de login com credenciais inválidas.

Pré-condições: O usuário possui uma conta válida, mas as credenciais inseridas serão inválidas.

Passo de execução:
1. Acesse a página de login;
2. Insira um nome de usuário inválido;
3. Insira uma senha inválida;
4. Clique no botão de login.

Entrada:
1. Nome de Usuário: migelsilva90
2. Senha: Senhaegura123#

Saída esperada:
- O sistema deve exibir uma mensagem de erro informando que as credenciais são inválidas.
- O usuário não deve ser autenticado.
- O sistema não deve permitir o acesso à página interna.

Critério de aceitação:
- O sistema deve tratar corretamente credenciais inválidas, exibindo uma mensagem de erro apropriada.
- Não deve haver acesso concedido com credenciais inválidas.

Tempo de execução estimado: 2 minutos, incluindo o tempo para inserção de dados e exibição da mensagem de erro.

Caso de teste 3:

Título: Bloqueio de Conta temporário após Múltiplas Tentativas Falhas

Código: 003

Descrição: Este caso de teste tem como objetivo verificar se o sistema bloqueia a conta do usuário após um número específico de tentativas falhas de login.

Pré-condições:

- O sistema está operacional.
- A configuração do sistema permite bloqueio de conta após um número específico de tentativas falhas.

Passo de execução:

1. Acesse a página de login;
2. Insira um nome de usuário válido;
3. Insira uma senha inválida;
4. Repita o passo 3 por um número específico de vezes que resultaria no bloqueio da conta;
5. Tente realizar o login novamente com credenciais válidas.

Entrada:

1. Nome de Usuário: miguelsilva90
2. Senha: Senhaegura123#

Saída esperada:

- Após o número específico de tentativas falhas, a conta do usuário deve ser bloqueada.
- O sistema deve exibir uma mensagem informando sobre o bloqueio da conta.

Critério de aceitação:

- O sistema deve bloquear a conta após o número específico de tentativas falhas.
- O usuário deve ser notificado sobre o bloqueio da conta.

Tempo de execução estimado: 5 minutos, incluindo tentativas de login e espera pelo bloqueio.

3.2 Casos de uso de Mudança de senha

Caso de teste 1:

Título: Envio do link de redefinição

Código: 004

Descrição: Verificar se o sistema envia corretamente o link de redefinição de senha para o endereço de e-mail fornecido pelo usuário.

Pré-condições:
- O usuário deve ter uma conta registrada no sistema.
- O usuário deve estar conectado à internet.

Passo de execução:
1. Acesse a página de login do sistema;
2. Clique na opção "Esqueceu a senha";
3. Insira o endereço de e-mail associado à conta do usuário;
4. Envie a solicitação de redefinição de senha.

Entrada: Endereço de e-mail válido associado à conta do usuário. [miguel.silva@gmail.com]

Saída esperada: O sistema deve enviar um e-mail contendo um link de redefinição de senha para o endereço fornecido.

Critério de aceitação:
- O e-mail de redefinição de senha deve ser entregue ao endereço fornecido.
- O e-mail deve conter um link funcional que direcione o usuário para a página de redefinição de senha.

Tempo de execução estimado: 3 minutos, considerando a inserção do e-mail e a chegada do link.

Caso de teste 2:

Título: Validação de token de redefinição

Código: 005

Descrição: Verificar se o sistema valida corretamente o token de redefinição de senha antes de permitir que o usuário crie uma nova senha.

Pré-condições: O usuário solicitou a redefinição de senha e recebeu o e-mail com o link contendo o token de redefinição.

Passo de execução:

1. Abra o e-mail de redefinição de senha;
2. Clique no link de redefinição de senha fornecido;
3. O sistema deve direcionar o usuário para uma página de validação de token;
4. Insira o token.

Entrada: Token de redefinição de senha recebido por e-mail. [A5H6F9]

Saída esperada:

- O sistema deve exibir uma página de validação de token.
- Caso o token seja válido, o sistema deve permitir ao usuário criar uma nova senha.
- Caso o token seja inválido ou expirado, o sistema deve fornecer uma mensagem de erro apropriada.

Critério de aceitação:

- O usuário deve ser capaz de validar com sucesso o token de redefinição de senha.
- O sistema deve permitir que o usuário crie uma nova senha após a validação bem-sucedida.
- Mensagens de erro devem ser exibidas de forma clara e informativa em caso de token inválido ou expirado.

Tempo de execução estimado: 5 minutos

Caso de teste 3:

Título: Expiração de link de redefinição

Código: 006

Descrição: Verificar se o sistema expira corretamente o link de redefinição de senha após um período determinado.

Pré-condições:
- O usuário solicitou a redefinição de senha e recebeu o e-mail com o link contendo o token de redefinição.
- O link ainda não expirou.

Passo de execução:
1. Aguarde até que o link de redefinição atinja o tempo limite de expiração;
2. Clique no link de redefinição de senha fornecido no e-mail.

Entrada: Não se aplica

Saída esperada:
- Caso o link ainda esteja dentro do prazo de validade, o sistema deve permitir ao usuário prosseguir para a página de redefinição de senha.
- Caso o link tenha expirado, o sistema deve exibir uma mensagem informando que o link expirou e solicitar ao usuário que faça uma nova solicitação de redefinição de senha.

Critério de aceitação:
- O sistema deve expirar corretamente o link de redefinição de senha após o tempo determinado.
- O usuário deve ser notificado de forma adequada em caso de link expirado.

Tempo de execução estimado: 10 minutos.

3.3 Casos de uso de Cadastro

Caso de teste 1:

Título: Cadastro bem-sucedido

Código: 007

Descrição: Verificar se o sistema realiza o cadastro de um novo usuário com sucesso

Pré-condições: O usuário não possui uma conta pré-existente no sistema.

Passo de execução:
1. Acesse a página de registro do sistema;
2. Preencha os campos obrigatórios, incluindo nome, e-mail, senha e data de nascimento;
3. Envie o formulário de cadastro clicando no botão "Sign up".

Entrada:
1. Nome: miguelsilva90
2. E-mail: miguel.silva@gmail.com
3. Senha: SenhaSegura123#
4. Data nascimento: 15/03/1990

Saída esperada: O sistema deve exibir uma mensagem de confirmação indicando que o cadastro foi concluído com sucesso.

Critério de aceitação:
- O cadastro do novo usuário deve ser realizado sem erros.
- Os dados do novo usuário, incluindo nome, e-mail, senha e data de nascimento, devem ser armazenados corretamente no sistema.
- O usuário deve ser redirecionado para a página inicial ou de login após o cadastro bem-sucedido.

Tempo de execução estimado: 3 minutos

Caso de teste 2:

Título: Cadastro com e-mail existente

Código: 008

Descrição: Verificar se o sistema impede o cadastro de um novo usuário com um endereço de e-mail que já está em uso.

Pré-condições: Um usuário já está cadastrado no sistema.

Passo de execução:

1. Acesse a página de registro do sistema;
2. Preencha os campos obrigatórios, incluindo nome, e-mail, senha e data de nascimento, utilizando um endereço de e-mail já existente no sistema;
3. Envie o formulário de cadastro clicando no botão "Sign up".

Entrada:

1. Nome: miguelsilva90
2. E-mail: miguel.silva@gmail.com
3. Senha: SenhaSegura123#
4. Data nascimento: 15/03/1990

Saída esperada: O sistema deve exibir uma mensagem de erro indicando que o endereço de e-mail já está em uso.

Critério de aceitação:

- O sistema deve impedir o cadastro de um novo usuário com um endereço de e-mail já existente.
- A mensagem de erro deve ser clara e informativa.

Tempo de execução estimado: 3 minutos

Caso de teste 3:

Título: Dados armazenados no servidor

Código: 009

Descrição: Verificar se os dados do usuário, incluindo nome, e-mail, senha e data de nascimento, são armazenados de forma segura no

servidor.

Pré-condições: O usuário realizou com sucesso o cadastro no sistema.

Passo de execução:

1. Acesse a base de dados do servidor onde os dados do usuário são armazenados;
2. Verifique se as informações do usuário, como nome, e-mail, senha e data de nascimento, estão armazenadas de forma segura, utilizando métodos adequados de criptografia para senhas e dados sensíveis.

Entrada: Não se aplica

Saída esperada: Os dados do usuário devem estar armazenados de forma segura, utilizando métodos adequados de criptografia para garantir a confidencialidade das informações.

Critério de aceitação:

- Os dados do usuário devem ser armazenados de maneira segura, garantindo a proteção contra acesso não autorizado.
- Senhas devem ser armazenadas de forma criptografada e não devem ser recuperáveis em texto claro.

Tempo de execução estimado: O tempo estimado para a execução deste caso de teste é de 10 minutos, considerando a análise da estrutura de armazenamento no servidor.

4. Report de bug

Título: Registro de Conta com email Duplicado Associado a Outro Usuário

Identificação: 001

Tester: Ana Beatriz de Araújo

Comportamento observado: Quando um usuário tenta criar uma nova conta no sistema utilizando um endereço de e-mail que já está associado a outro usuário, o sistema permite a conclusão do processo de registro, resultando em dois usuários diferentes compartilhando o mesmo endereço de e-mail.

Comportamento Esperado: Ao tentar criar uma nova conta no sistema com um endereço de e-mail que já está associado a outro usuário, o sistema deve exibir uma mensagem de erro específica indicando que o endereço de e-mail já está em uso, não permitir que o usuário conclua o registro e orientar o usuário sobre a necessidade de utilizar um endereço de e-mail único.

Passos para reprodução:

1. Acesse a página de registro.
2. Insira um e-mail que já esteja associado a outra conta existente.
3. Complete os demais campos obrigatórios.
4. Clique no botão "Cadastrar".

Ambiente de teste: Versão app 2.1, tipo de dispositivo Iphone 11 IOS 17.4

Dados de Entrada:

1. Nome: miguelsilva90
2. E-mail: miguel.silva@gmail.com
3. Senha: SenhaSegura123#
4. Data nascimento: 15/03/1990

Risco: A criação de contas associadas ao mesmo e-mail pode resultar em uma violação da privacidade, pois informações pessoais podem ser acessadas por usuários não autorizados. Um usuário mal-intencionado pode explorar essa falha para criar contas adicionais com o mesmo e-mail, levando a atividades maliciosas, como roubo de identidade ou uso indevido de informações.

Severidade: Alta

Prioridade: Alta

Data de identificação: 08/03/2024

Imagem e vídeo: E*m um ambiente de teste real registrar imagem e vídeo*