Metodologia de desenvolvimento
de novos sistemas e manutenções evolutivas

Especificação de Casos de Testes

IDENTIFICAÇÃO DO PROJETO

123456

Testes Para Logins

Equipe
Raffael Guideti Miello – 22013508-2
Gustavo Henrique – 22199398-2
Phelipe Barreto – 22079206-2
Vitor Hugo – 22021645-2
Luiz – Luiz Eduardo Viera Castilho - 23363456-2

Ago/2023

ESPECIFICAÇÃO DE CASOS DE TESTES

Premissas

- É esperado o ínicio dos testes conforme especificado no cronograma.
- É necessário que os ambientes de teste sejam criados e mantidos pelo time de Automação.
- O time de teste sera responsável por garantir que as condições/cenários de teste foram verificados e os resultados esperados estão de acordo. Os problemas devem ser reportados e resolvidos de acordo com os resultados esperados.
- Questões e problemas relacionados com a funcionalidade atual serão discutidos e um esforço para solução destes será feita pelo Líder do Projeto e o cliente antes da abertura do erro para o time de Automação.
- Os testes aqui especificados serão revistos e aprovados pelo cliente. Casos/Scripts de teste serão modificados se for preciso para acomodar os retestes.
- Apenas os requerimentos definidos no levantamento original aprovado pelo cliente são passíveis de teste.

Restrições

- Apenas os testes apontados descritos neste documento serão executados
- Caso outros testes sejam necessários, serão incluídos desde que em comum acordo entre o Líder de Projetos e o cliente, desde que claramente estejam endereçados como regras nos requisitos funcionais especificados.

ESPECIFICAÇÃO DE CASO DE TESTE			
Projeto	123456		
Caso de teste	Caso 001		
Tipo	Projeto		
Requisito funcional correspondente	RF003 – Login do Aplicativo		
Propósito	Realizar a validação das credenciais do cliente		
Descrição geral Este teste valida as credenciais de um cliente para que ele consiga realizar o login a partir de seu e-mail e senha, e também podendo recupera-lo caso não o possua			
Insumos para o caso de teste O usuário deve por suas credenciais nos campos informados, para realizar o login, caso esteja correto, ele tem acesso a informação, caso o contrário, informa que login ou senha estão errados, também possui a opção de "Esqueci minha senha"			
Roteiro para a realização do teste Pré-condições: O aplicativo está instalado e em execução no dispositivo Android do usuário. O usuário possui uma conta válida registrada no sistema. Fluxo principal: O usuário abre o aplicativo. O aplicativo exibe a tela de login, solicitando que o usuário insira suas credenciais (nome de usuário ou e-mail e senha). O usuário digita suas informações de login. O aplicativo valida as informações fornecidas pelo usuário e verifica a autenticidade do login com o sistema. Se as credenciais estiverem corretas e a autenticação for bem-sucedida, o aplicativo redireciona o usuário para a tela principal do aplicativo. Caso contrário, o aplicativo exibe uma mensagem de erro informando que as credenciais são inválidas ou que ocorreu um problema de autenticação. Fluxo alternativo: Se o usuário esquecer sua senha, ele pode selecionar a opção de recuperação de senha, onde o aplicativo enviará um e-mail com um link para redefinir a senha. Pós-condições: O usuário está autenticado no aplicativo e tem acesso aos recursos e funcionalidades específicas para usuários autenticados. Esse é um exemplo básico de um caso de uso para o login de um aplicativo Android. Na prática, pode haver outras considerações, como tratamento de erros, segurança e outras funcionalidades adicionais.			
Cenários de teste			
Objetivo específico		Especificação das entradas ou ações	Saídas esperadas
1	Realizar Login	Entrar com os dados de e-mail e senha do cliente	Que o cliente consiga ter acesso ao sistema.
2	Esqueci a Senha	Informar um e-mail ou numero para envio da mensagem automática	Que o cliente recupere a sua senha

Requisitos Funcionais:

RF[001] Cadastro de Clientes:

O sistema deve permitir que novos clientes se cadastrem fornecendo informações como nome completo, endereço de e-mail válido, senha segura e outras informações relevantes. As informações fornecidas devem ser armazenadas de forma segura no banco de dados do sistema.

RF[002] Solicitar Recuperação da Senha:

Os usuários devem ter a opção de solicitar a recuperação de senha caso a tenham esquecido. Ao selecionar essa opção, o sistema deve solicitar o endereço de e-mail associado à conta. Depois de fornecido, o sistema enviará um e-mail contendo um link seguro para a página de redefinição de senha.

RF[003] Login:

O sistema deve permitir que os usuários acessem suas contas por meio do processo de login. Os usuários deverão inserir seu endereço de e-mail e senha. Após a verificação bem-sucedida das credenciais, o sistema permitirá o acesso à conta associada.

RF[004] Recuperação de E-mail:

Caso um usuário tenha esquecido o endereço de e-mail associado à sua conta, o sistema deve fornecer uma opção para recuperá-lo. Isso pode ser feito fornecendo informações adicionais de verificação, como nome completo e número de telefone, para confirmar a identidade do usuário e exibir o endereço de e-mail registrado.

RF[005] Redefinir Senha:

Após receber o link de redefinição de senha por e-mail ou após responder às perguntas de verificação, o sistema deve permitir que o usuário insira uma nova senha. A senha deve atender a critérios de segurança, como comprimento mínimo e combinação de caracteres, e deve ser confirmada digitando-a novamente.

RF[006] Notificar Sucesso ou Falha:

O sistema deve fornecer notificações claras aos usuários em relação às ações que eles executaram. Isso inclui notificações de sucesso após um cadastro bem-sucedido, notificações de falha durante o processo de login devido a credenciais inválidas e notificações de sucesso após a redefinição bem-sucedida da senha. As mensagens de erro devem ser informativas e orientar os usuários sobre os próximos passos, caso ocorram problemas.

Requisitos Não Funcionais:

RNF[001] Segurança de Dados:

A segurança de dados é um requisito crítico para garantir a proteção das informações dos usuários. O sistema deve utilizar criptografia de dados em repouso e em trânsito, utilizando algoritmos fortes e padrões de segurança reconhecidos. As senhas dos usuários devem ser armazenadas usando algoritmos de hash seguros e técnicas de "salting". Além disso, é necessário implementar medidas de segurança avançadas, como detecção de tentativas de login suspeitas, monitoramento de atividades de conta e prevenção contra ataques de força bruta.

RNF[002] Interface Amigável:

A interface do sistema deve ser projetada de forma a proporcionar uma experiência amigável e intuitiva para os usuários. Isso inclui o uso de elementos de design visualmente agradáveis, layout organizado e linguagem clara para orientar os usuários durante o processo de login e recuperação de senha. Os botões e campos de entrada devem ser de fácil identificação e uso, garantindo que os usuários possam interagir com o sistema sem dificuldades, independentemente de sua experiência técnica.

RNF[003] Tempo de Envio de E-mail:

O tempo de envio de e-mails é um requisito crucial para a eficácia do processo de recuperação de senha. O sistema deve garantir que os e-mails de recuperação de senha sejam enviados de maneira oportuna e consistente. Isso envolve a configuração de servidores de e-mail otimizados, implementação de filas de e-mail eficazes e a minimização de atrasos no processo de envio. O objetivo é que os usuários recebam o e-mail de recuperação em um período de tempo aceitável.

RNF[004] Tempo de Expiração do Link de Recuperação:

Para garantir a segurança das contas dos usuários, o sistema deve definir um tempo de expiração para os links de recuperação de senha enviados por e-mail. Esse período de tempo deve ser suficientemente longo para permitir que os usuários acessem o link e redefinam suas senhas com conveniência, mas também suficientemente curto para minimizar o risco de acessos não autorizados. O tempo de expiração deve ser comunicado claramente aos usuários durante o processo de recuperação.

RNF[005] Disponibilidade:

O sistema deve manter alta disponibilidade, garantindo que os usuários possam acessar a tela de login e as funcionalidades associadas sempre que precisarem. Isso envolve o uso de infraestrutura robusta, balanceamento de carga e monitoramento constante do sistema. Qualquer manutenção planejada deve ser comunicada antecipadamente aos usuários, e medidas de contingência devem estar em vigor para lidar com possíveis interrupções inesperadas.

RNF[006] Compatibilidade:

O sistema deve ser compatível com uma variedade de dispositivos e navegadores, garantindo uma experiência consistente para todos os usuários, independentemente de sua escolha de plataforma. A interface deve ser responsiva e adaptável a diferentes tamanhos de tela e resoluções. Além disso, o sistema deve ser compatível com diferentes sistemas operacionais e versões de navegadores populares, garantindo que os usuários possam acessá-lo sem problemas em suas configurações preferidas.

Ao considerar esses requisitos não funcionais, o sistema de autenticação pode ser projetado para oferecer segurança, usabilidade e desempenho eficazes, atendendo às necessidades dos usuários e cumprindo os padrões de qualidade.

Caso de Uso Descrito:

Ator Principal: Usuário

Pré-condições:
- O aplicativo está instalado e em execução no dispositivo Android do usuário.
- O usuário possui uma conta válida registrada no sistema.

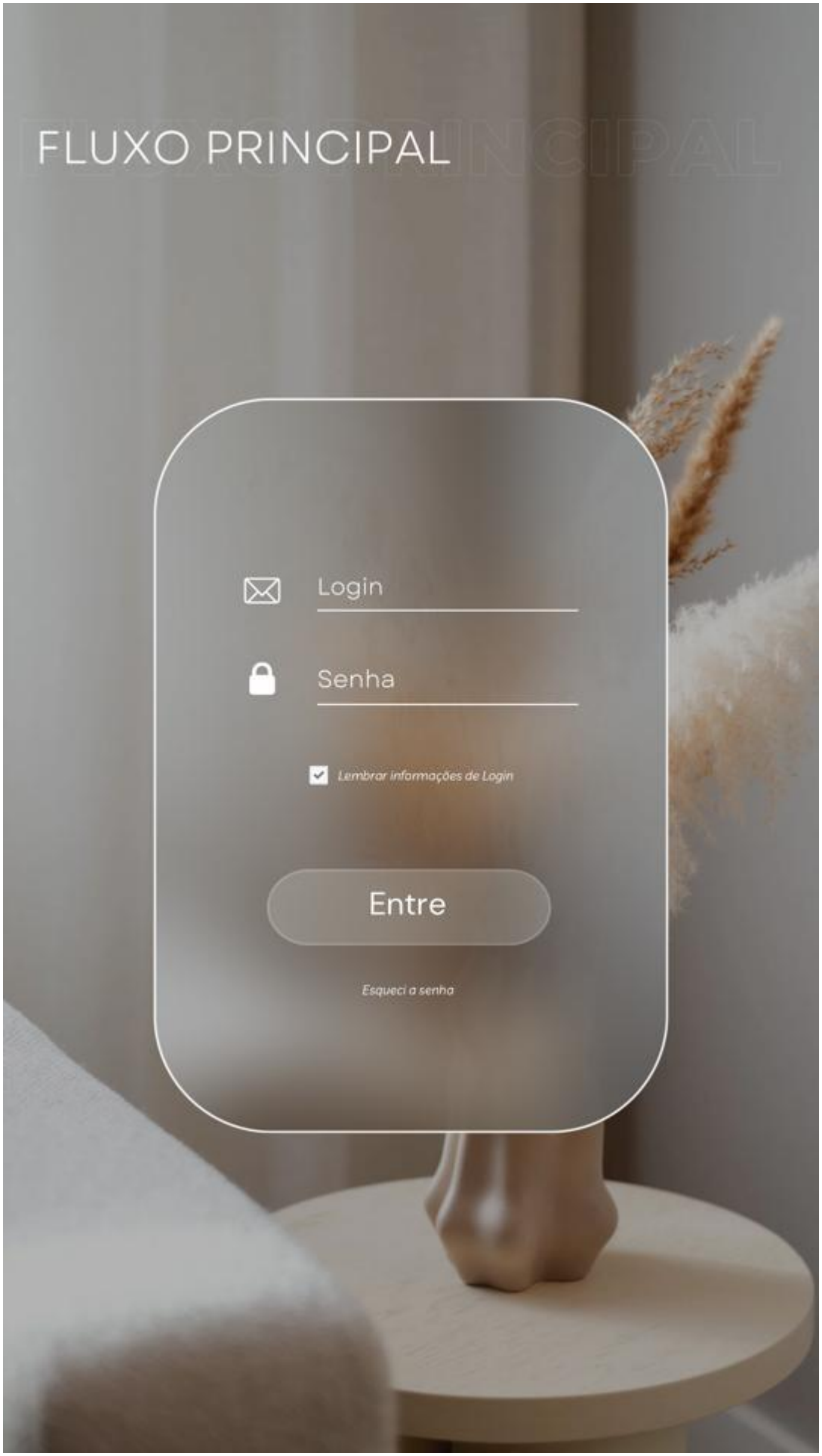
Fluxo Principal:
1. O usuário abre o aplicativo no dispositivo Android.
2. O aplicativo exibe a tela de login, apresentando campos para nome de usuário ou e-mail e senha.
3. O usuário digita suas credenciais de login nos campos apropriados.
4. O usuário pressiona o botão de login.
5. O aplicativo valida as informações inseridas pelo usuário.
6. O aplicativo envia as informações de login para o sistema de autenticação.
7. O sistema verifica a autenticidade das credenciais fornecidas.
8. Se as credenciais estiverem corretas e a autenticação for bem-sucedida, o aplicativo redireciona o usuário para a tela principal do aplicativo.
9. Caso contrário, o aplicativo exibe uma mensagem de erro na tela de login, informando que as credenciais são inválidas ou que ocorreu um problema de autenticação.

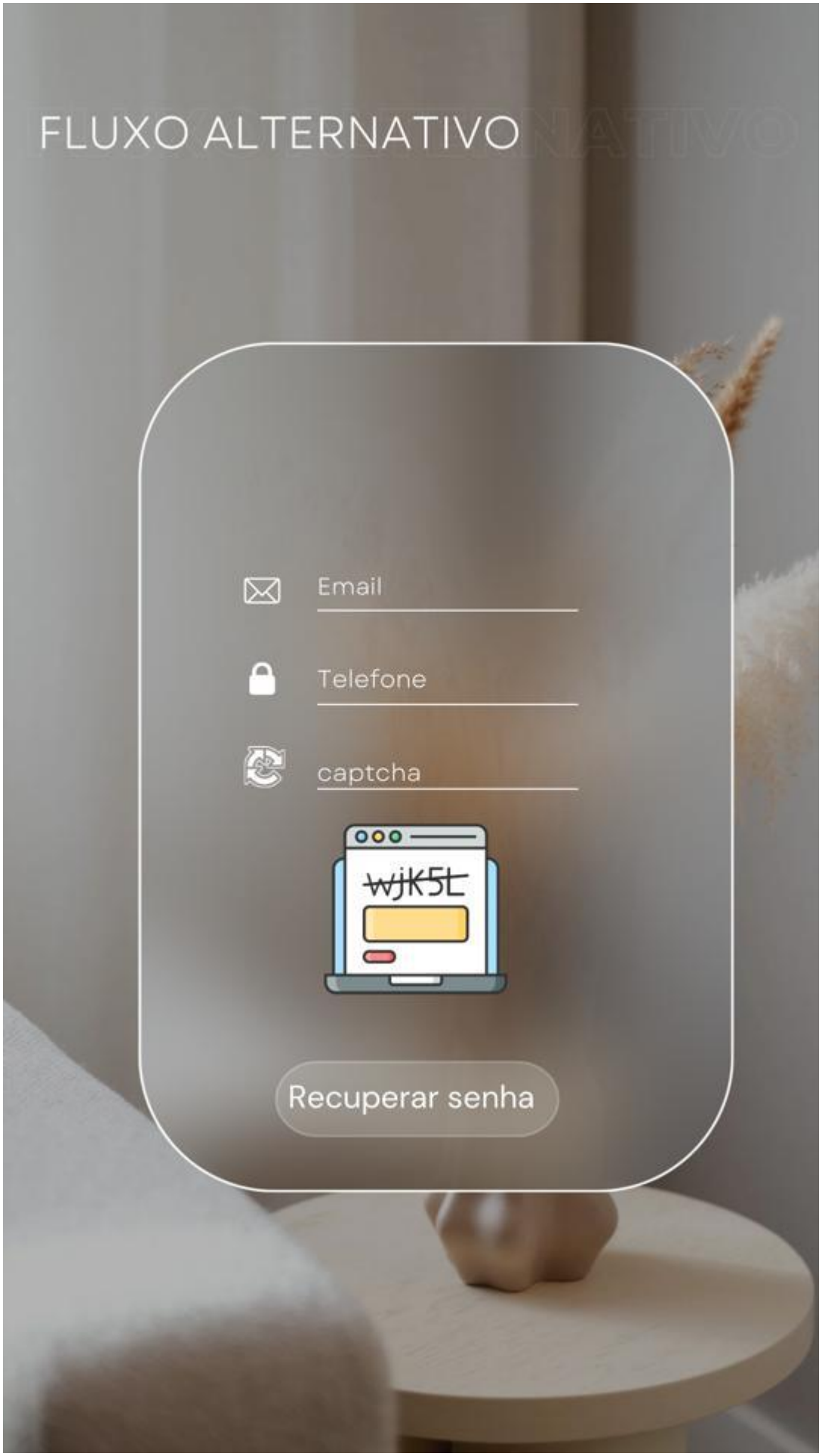
Fluxo Alternativo (Recuperação de Senha):
1. O usuário na tela de login seleciona a opção de recuperação de senha.
2. O aplicativo exibe uma tela para o usuário inserir seu endereço de e-mail.
3. O usuário insere seu endereço de e-mail registrado.
4. O usuário pressiona o botão de envio.
5. O aplicativo envia uma solicitação de recuperação de senha para o sistema.
6. O sistema gera um link de redefinição de senha e o envia para o endereço de e-mail fornecido.
7. O usuário recebe um e-mail com o link de redefinição de senha.
8. O usuário clica no link e é redirecionado para uma tela onde pode definir uma nova senha.

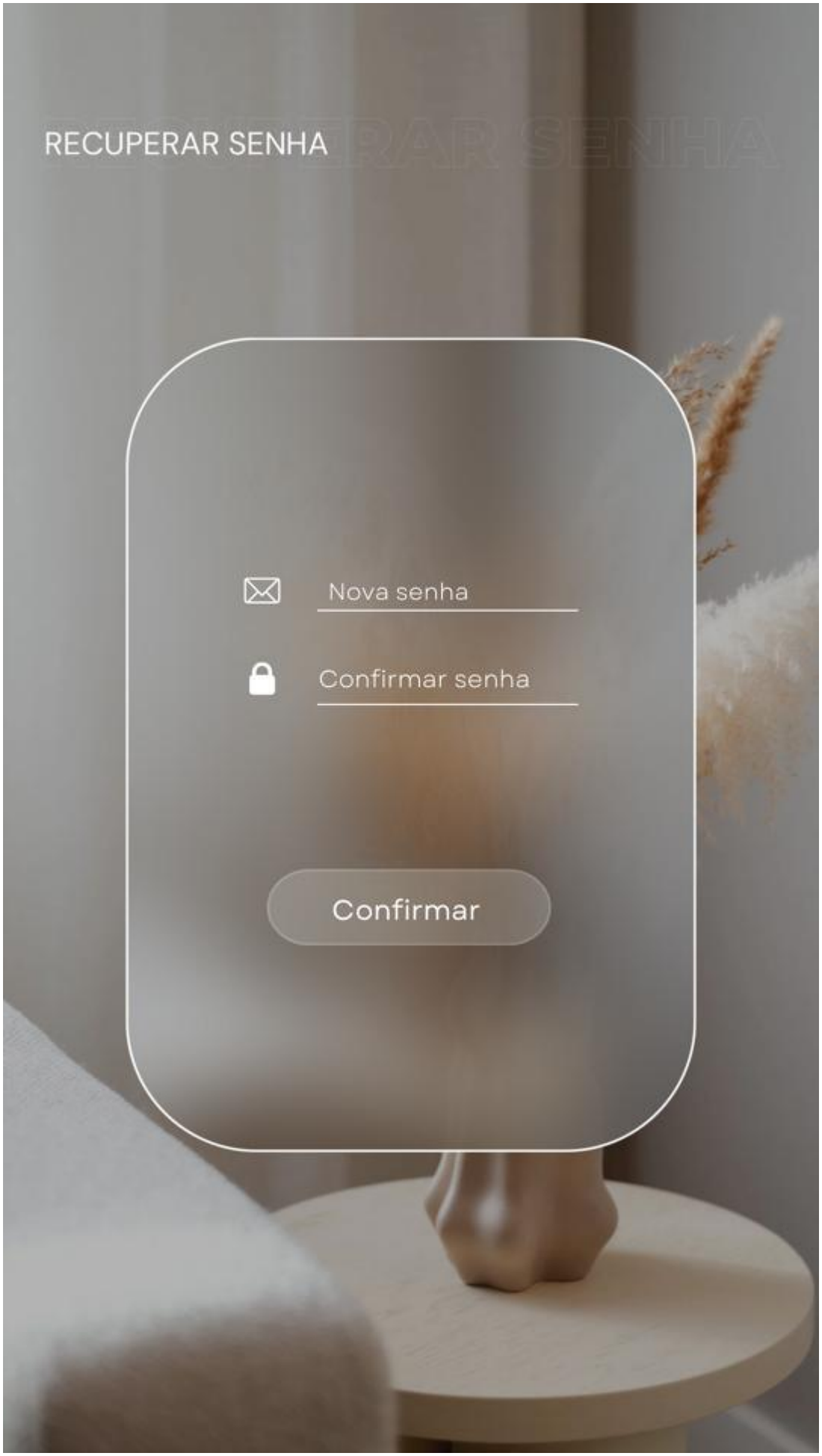
Pós-condições:
- Se o login for bem-sucedido, o usuário está autenticado no aplicativo e tem acesso aos recursos e funcionalidades específicas para usuários autenticados.

Fluxo de Exceção:
- Se o aplicativo não puder se conectar ao servidor de autenticação devido a problemas de rede, uma mensagem de erro será exibida, informando ao usuário para verificar sua conexão com a Internet.
- Se o usuário inserir credenciais incorretas ou um formato de e-mail inválido, o aplicativo exibirá uma mensagem de erro pedindo ao usuário para verificar os dados inseridos.
- Se o usuário solicitar a recuperação de senha, mas o sistema não conseguir enviar o e-mail de recuperação, uma mensagem de erro instruirá o usuário a tentar novamente mais tarde.

Figuras Exemplares:


FLUXO PRINCIPAL
Login
Senha
Lembrar informações de Login
Entre
Esqueci a senha


FLUXO ALTERNATIVO
Email
Telefone
captcha
wjK5L
Recuperar senha


RECUPERAR SENHA
Nova senha
Confirmar senha
Confirmar