

Especificação de Cenários de Uso – Projeto NexSay

1. Enviar Mensagem Direta

Quem usa: Usuário autenticado (com conta verificada no sistema)

Descrição do cenário:

Como um usuário comum, eu quero mandar uma mensagem para outro usuário, então acontece assim:

- O usuário acessa a tela de conversa com o contato.
- Ele digita a mensagem no campo de texto.
- Clica no botão “Enviar”.
- O sistema valida se a mensagem está preenchida e se o contato é válido.
- O sistema criptografa a mensagem com AES-256 e envia via WebSocket.
- O destinatário recebe a mensagem em tempo real.
- O sistema exibe: “Mensagem enviada com sucesso!”

E se algo der errado?

- Se o contato estiver bloqueado, aparece: “Você não pode enviar mensagens para este contato.”
- Se o campo da mensagem estiver vazio, aparece: “Digite algo antes de enviar!”
- Se houver erro de conexão, aparece: “Erro ao enviar mensagem. Tente novamente.”

Regras do sistema:

- A mensagem deve ter no máximo 1000 caracteres.
- Usuários bloqueados não podem enviar nem receber mensagens.
- As mensagens são criptografadas com AES-256.
- O envio só é permitido após autenticação com verificação em duas etapas (2FA ativa).

2. Adicionar Contato

Quem usa: Usuário autenticado

Descrição do cenário:

Como um usuário comum, eu quero adicionar outra pessoa aos meus contatos, então acontece assim:

- O usuário acessa o menu “Contatos”.
- Seleciona a opção “Adicionar novo contato”.

- Digita o número de telefone ou escaneia o QR Code.
- O sistema verifica se o número existe e se não está bloqueado.
- O sistema confirma a adição e exibe: “Contato adicionado com sucesso!”

E se algo der errado?

- Se o número for inválido ou não existir, o sistema mostra: “Contato não encontrado.”
- Se o número estiver bloqueado, o sistema mostra: “Você não pode adicionar este contato.”

Regras do sistema:

- O usuário deve estar autenticado com 2FA.
- Não é permitido adicionar contatos que já estejam bloqueados.
- O sistema valida o número com base no formato +DDDXXXXXXXXX.

3. Login com Verificação em Duas Etapas

Quem usa: Todos os usuários

Descrição do cenário:

Como um usuário do sistema, eu quero fazer login com segurança, então acontece assim:

- O usuário acessa a tela de login.
- Digita e-mail e senha.
- O sistema valida as credenciais.
- O sistema envia um código de verificação (2FA) para o e-mail ou app autenticador.
- O usuário insere o código recebido.
- O sistema valida o código.
- Ao sucesso, o usuário entra na conta e vê a mensagem: “Login realizado com sucesso!”

E se algo der errado?

- Se o e-mail ou senha estiverem incorretos: “Credenciais inválidas.”
- Se o código 2FA estiver errado ou expirado: “Código inválido ou expirado.”

Regras do sistema:

- A autenticação usa senhas criptografadas (hash com bcrypt).
- Todos os usuários devem ter 2FA ativado.
- Os tokens de acesso são JWT assinados e criptografados.
- O sistema gera alerta por e-mail a cada novo login.

4. Cadastro de Novo Usuário

Quem usa: Pessoa que ainda não possui conta no sistema

Descrição do cenário:

Como uma nova pessoa interessada em usar o sistema, eu quero me cadastrar com segurança, então acontece assim:

- O usuário acessa a tela de cadastro.
- Preenche nome, e-mail, senha e confirma os dados.
- O sistema envia um código de verificação (2FA) para o e-mail.
- O usuário insere o código recebido.
- O sistema valida o código e conclui o cadastro.
- O sistema exibe: “Cadastro realizado com sucesso!”

E se algo der errado?

- Se o código não for informado corretamente, aparece: “Código inválido ou expirado.”
- Se algum campo obrigatório não for preenchido, o sistema destaca os campos com erro.

Regras do sistema:

- A senha deve ter no mínimo 8 caracteres.
- O e-mail precisa ser único e válido.
- O cadastro só é finalizado após validação do código 2FA enviado ao e-mail.

5. Exclusão de Conta

Quem usa: Usuário autenticado

Descrição do cenário:

Como um usuário do sistema, eu quero excluir minha conta de forma segura, então acontece assim:

- O usuário acessa as configurações de conta.
- Seleciona a opção “Excluir conta”.
- O sistema envia um código de confirmação para o e-mail do usuário.
- O usuário insere o código na interface.
- O sistema valida o código e solicita confirmação final.
- Ao confirmar, o sistema remove os dados e exibe: “Conta excluída com sucesso.”

E se algo der errado?

- Se o código estiver errado ou expirado, aparece: “Código inválido ou expirado.”
- Se o usuário desistir do processo, nenhuma informação será removida.

Regras do sistema:

- A conta só pode ser excluída após a verificação do código enviado por e-mail.
- O sistema deverá manter logs de segurança mesmo após exclusão.
- O usuário precisa estar autenticado com 2FA para acessar essa opção.