HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor	Aprovado por
08/05/2025	1.0	Criação dos Cenários de Uso	ALLAN KARDEC DE JESUS FELIZ NAVEGANTES	
21/05/2025	1.1	Edição dos Cenários	EVERTON HIAN DOS SANTOS PINHEIRO	

Especificação de Cenários de Uso – Projeto NexSay

1 ESPECIFICAÇÃO DE CENÁRIOS DE USO

Caso de Uso: RF01 – Iniciar Nova Conversa

Como um Usuário
Eu posso iniciar uma nova conversa com um contato previamente adicionado.

Ocorre então:

1. O usuário acessa a lista de contatos.
2. O usuário seleciona um contato e opta por iniciar uma nova conversa.
3. O sistema valida o token JWT [RN01, RN05].
4. O sistema verifica se o contato existe e não está bloqueado [RN02].
5. O sistema cria uma nova conversa no banco de dados.
6. O sistema ativa o canal de comunicação via WebSocket [RN04].
7. O sistema registra a operação no log com timestamp, ID do usuário e IP [RN03].
8. O sistema retorna os dados da nova conversa com status 201 (Criado).

Contudo:
SE o contato não existir, ENTÃO o sistema retorna erro 404.
SE o contato estiver bloqueado, ENTÃO o sistema retorna erro 403 [RN02].
SE o JWT for inválido ou estiver ausente, ENTÃO o sistema retorna erro 401 [RN01].

Regras de Negócio Utilizadas:

RN01 – Apenas usuários autenticados com JWT válido podem iniciar conversas.
RN02 – O contato escolhido deve estar cadastrado e não pode estar bloqueado.
RN03 – Todas as ações sensíveis devem ser registradas no sistema de logs com timestamp, ID do usuário e IP.
RN04 – O canal de comunicação é ativado em tempo real via WebSocket após a criação da conversa.
RN05 – A autenticação de dois fatores (2FA) é obrigatória para abertura de sessão válida

Caso de Uso: RF02 – Enviar Mensagem de Texto

Como um Usuário
Eu posso enviar uma mensagem de texto em uma conversa ativa

Ocorre então:

1. O usuário acessa uma conversa existente.
2. O usuário digita a mensagem no campo apropriado.
3. O usuário confirma o envio da mensagem.
4. O sistema valida se o usuário pertence à conversa.
5. O sistema valida a sessão JWT [RN01].
6. O sistema verifica se a mensagem não está vazia ou inválida, conforme [RN06].
7. O sistema criptografa a mensagem antes de armazená-la, conforme [RN07].
8. O sistema armazena a mensagem criptografada.
9. O sistema emite a mensagem via WebSocket ao destinatário estiver online, conforme [RN08].
10. O sistema exibe a mensagem na interface do remetente com status “entregue”.
11. O sistema gera um log de envio conforme [RN09].

Contudo:
SE a conversa não existir, ENTÃO o sistema retorna erro 404.
SE o usuário não fizer parte da conversa, ENTÃO o sistema retorna erro 403.
SE a mensagem estiver vazia ou for inválida, ENTÃO o sistema retorna erro 422 [RN06].
SE ocorrer falha no envio via WebSocket, ENTÃO a mensagem será salva normalmente e o sistema tentará nova entrega posteriormente [RN08].

Regras de Negócio Utilizadas:

RN06 – A mensagem do usuário deve ser valida.

RN07 – Toda mensagem deve ser criptografada antes de ser armazenada.

RN08– A entrega da mensagem é feita via WebSocket, se o destinatário estiver online.

RN09 – Cada mensagem enviada gera um registro de log para auditoria.

Caso de Uso: RF03 – Visualizar Mensagens Novas

Como um Usuário
Eu posso visualizar mensagens novas recebidas

Ocorre então:

1. O usuário abre uma conversa.
2. O sistema verifica se há canal WebSocket ativo.
3. O sistema valida a sessão JWT. [RN01]
4. O sistema escuta o canal e exibe novas mensagens em tempo real [RN10].
5. O sistema registra o momento em que a mensagem é visualizada [RN11].
6. O sistema marca como "nova" apenas mensagens ainda não lidas destinadas ao usuário RN12.

Contudo:
SE não houver conexão com WebSocket, ENTÃO o sistema recorre ao polling REST e continua monitorando novas mensagens [RN10] e exibindo apenas as conversas antigas.

Regras de Negócio Utilizadas:

RN10 – As mensagens novas devem ser exibidas em tempo real via WebSocket, quando possível.

RN11 – O sistema deve registrar o momento em que o usuário visualiza a mensagem.

RN12 – Apenas mensagens destinadas ao usuário ainda não visualizadas devem ser marcadas como novas.

Caso de Uso: RF04 – Visualizar Mensagens Antigas

Como um Usuário
Eu posso visualizar mensagens antigas de uma conversa

Ocorre então:

1. O usuário rola a interface da conversa para cima.
2. O frontend envia uma requisição paginada para o histórico
3. O sistema valida a sessão JWT.[RN01]
4. O sistema valida se o usuário faz parte da conversa [RN14].
5. O sistema valida os parâmetros da requisição.
6. O sistema recupera o histórico criptografado do banco.
7. O sistema descriptografa as mensagens para os usuários participantes [RN14].

8. O sistema apresenta as mensagens em ordem cronológica, com paginação [RN13].
9. O sistema permite navegação contínua no histórico completo da conversa [RN15].

Contudo:
SE o usuário não fizer parte da conversa, ENTÃO o sistema retorna erro 403 [RN14].
SE houver erro de paginação (ex: parâmetros incorretos), ENTÃO o sistema retorna erro 400 com sugestão de parâmetros corretos.

Regras de Negócio Utilizadas:

RN13 – O sistema deve permitir a navegação por mensagens anteriores com paginação.

RN14 – As mensagens devem ser descriptografadas para os usuários participantes da conversa.

RN15 – O histórico completo da conversa deve estar disponível para os usuários autorizados.

Caso de Uso: RF05 – Apagar Mensagem Para Si

Como um Usuário
Eu posso apagar uma mensagem apenas do meu histórico de visualização

Ocorre então:

1. O usuário seleciona uma mensagem já recebida ou enviada.
2. O usuário clica na opção “Apagar”.
3. O sistema valida a sessão JWT e a participação do usuário na conversa [RN01].
4. A mensagem desaparece da interface do usuário, mas continua visível ao outro participante como “mensagem excluída” [RN17].[RN16]
5. O sistema registra a ação no log de auditoria [RN18].

Regras de Negócio Utilizadas:

RN16 – O usuário fica ciente da exclusão de mensagens do outro participante.

RN17 – A exclusão afeta o histórico de ambos os participantes.

RN18 – A ação de exclusão pessoal deve ser registrada nos logs de auditoria.

Caso de Uso: RF06 – Adicionar Novo Contato

Como um Usuário
Eu posso adicionar um novo contato à minha lista de contatos

Ocorre então:

1. O usuário acessa o menu de contatos.
2. O usuário seleciona a opção “pesquisar contato”.
3. O usuário informa o identificador único do novo contato (email/nome de usuário).
4. O sistema valida se o identificador informado corresponde a uma conta válida e existente [RN19].
5. O sistema verifica se o contato já está na lista do usuário [RN20].
6. O usuário aperta “adicionar contato”
7. O sistema adiciona o contato à lista e exibe confirmação [RN21].

Contudo:
SE o identificador informado não corresponder a uma conta válida, ENTÃO o sistema exibe mensagem de erro e retorna ao passo 3 [RN19].
SE o contato já estiver na lista, ENTÃO o sistema exibe a mensagem “adicionado” [RN20].

Regras de Negócio Utilizadas:

RN19 – O identificador do contato deve corresponder a uma conta registrada no sistema.

RN20 – Um mesmo contato não pode ser adicionado duas vezes.

RN21 – Ao adicionar um contato, o sistema deve registrar a nova associação entre os usuários.

Caso de Uso: RF07 – Bloquear Contato

Como um Usuário
Eu posso bloquear um contato para impedir futuras interações

Ocorre então:

1. O usuário acessa a lista de contatos.
2. O usuário seleciona o contato desejado.
3. O usuário aciona a opção “Bloquear contato”.
4. O sistema valida a sessão e a relação entre os usuários [RN22].
5. O sistema registra o bloqueio e impede novos envios de mensagens entre as partes [RN23].
6. O sistema atualiza o status do contato como “bloqueado” na interface do usuário [RN24].

Contudo:
SE o contato não existir ou já estiver bloqueado, ENTÃO o sistema exibe mensagem informativa e finaliza o fluxo [RN22], [RN23].
SE houver falha na sessão do usuário (ex: JWT inválido), ENTÃO o sistema exige novo login.

Regras de Negócio Utilizadas:

RN22 – O usuário só pode bloquear contatos com os quais já tenha uma interação registrada.

RN23 – O sistema deve impedir comunicação entre usuários após o bloqueio.

RN24 – O status de bloqueio deve ser refletido na interface do usuário e registrado internamente.

Caso de Uso: RF08 – Ver Lista de Contas

Como um Usuário
Eu posso visualizar a lista de contatos adicionados na minha conta

Ocorre então:

1. O usuário acessa o menu de contatos.
2. O sistema valida a sessão do usuário.
3. O sistema busca todos os contatos associados à conta do usuário [RN26].
4. O sistema exibe a lista de contatos em ordem alfabética ou de interação recente [RN27].

Contudo:
SE não houver contatos na lista, ENTÃO o sistema exibe a mensagem “Nenhum contato encontrado” [RN26].
SE houver falha de sessão, ENTÃO o sistema solicita nova autenticação [RN25].

Regras de Negócio Utilizadas:

RN26 – A lista de contatos deve refletir apenas os contatos ativos associados ao usuário.

RN27 – A exibição da lista deve seguir critérios de ordenação predefinidos (ex: ordem alfabética ou atividade).

Caso de Uso: RF09 – Ver Informações Básicas de Contatos

Como um Usuário
Eu posso visualizar informações básicas dos meus contatos

Ocorre então:

1. O usuário acessa a lista de contatos.
2. O usuário seleciona um contato da lista.
3. O sistema valida a sessão e a existência da relação entre os usuários [RN28].
4. O sistema exibe as informações básicas do contato, como nome, status, última atividade e foto [RN29].

Contudo:
SE o contato não for encontrado, ENTÃO o sistema exibe erro e retorna à lista [RN28].
SE houver falha na sessão JWT, ENTÃO o sistema solicita nova autenticação [RN28].

Regras de Negócio Utilizadas:

RN28 – Apenas contatos válidos e previamente adicionados podem ter seus dados acessados.

RN29 – O sistema deve exibir apenas informações públicas e permitidas por política de privacidade.

Caso de Uso: RF10 – Cadastrar Usuários

Como um Usuário
Eu posso criar uma nova conta no sistema

Ocorre então:

1. O usuário acessa a tela de cadastro.
2. O usuário preenche os campos obrigatórios (nome, e-mail, senha etc.).
3. O sistema valida os dados informados [RN30].
4. O sistema verifica se o e-mail já está cadastrado.
5. O sistema armazena os dados criptografados e cria o perfil do usuário [RN31].
6. O sistema envia uma mensagem de confirmação por e-mail [RN05].
7. O sistema exibe mensagem de sucesso e direciona o usuário para a tela de login.

Contudo:

SE o e-mail já estiver cadastrado, ENTÃO o sistema exibe erro e solicita outro e-mail.

SE houver falha na validação dos dados, ENTÃO o sistema exibe erro e destaca os campos inválidos [RN30].

Regras de Negócio Utilizadas:

RN30 – Todos os dados obrigatórios devem ser preenchidos corretamente.

RN31 – As senhas devem ser armazenadas de forma segura e criptografada.

Caso de Uso: RF11 – Autenticar Usuários

Como um Usuário
Eu posso fazer login no sistema com minhas credenciais

Ocorre então:

1. O usuário acessa a tela de login.
2. O usuário informa e-mail e senha.
3. O sistema valida os dados [RN33].
4. O sistema envia um código para o e-mail do usuário [RN05]
5. **O usuário digita esse código no campo da interface**
6. O sistema gera um token JWT para a sessão ativa [RN34].
7. O sistema redireciona o usuário à interface principal.

Contudo:

SE o e-mail ou senha estiverem incorretos, ENTÃO o sistema exibe erro genérico de autenticação.

SE a conta estiver desativada ou não confirmada, ENTÃO o sistema bloqueia o login e informa o motivo.

Regras de Negócio Utilizadas:

[RN33] – O sistema deve validar as credenciais de acesso.

[RN34] – Toda sessão autenticada deve gerar um token JWT válido.

Caso de Uso: RF12 – Recuperação de Senha e Redefinição Segura

Como um Usuário
Eu posso redefinir minha senha em caso de esquecimento

Ocorre então:

1. O usuário acessa a opção “Esqueci minha senha”.
2. O sistema envia um código de recuperação ao e-mail informado [RN35].
3. O usuário digita esse código no campo da interface.
4. O usuário digita a nova senha [RN36].
5. O sistema atualiza a senha criptografada no banco de dados.
6. O sistema exibe confirmação da redefinição.

Contudo:

SE o e-mail não estiver cadastrado, ENTÃO o sistema exibe mensagem genérica sem confirmar a existência do e-mail.

Se o código estiver errado o sistema envia a mensagem “código inválido”

Regras de Negócio Utilizadas:

RN35 – A autenticação de dois fatores (2FA) é obrigatória para a alteração de senha do usuário

RN36 – A nova senha deve seguir critérios mínimos de segurança (número mínimo de caracteres, complexidade etc.).

Caso de Uso: RF13 – Excluir Conta

Como um Usuário
Eu posso excluir permanentemente minha conta do sistema

Ocorre então:

1. O usuário acessa as configurações da conta.
2. O usuário solicita a exclusão da conta e confirma a ação.
3. O sistema solicita autenticação para confirmação junto a reentrada da senha[RN38].
4. O sistema valida a solicitação e remove os dados pessoais do usuário conforme [RN37].
5. O sistema encerra todas as sessões e revoga o token JWT.
6. O sistema exibe mensagem de confirmação e redireciona para a tela inicial.

Contudo:

SE a senha estiver incorreta, ENTÃO o sistema cancela a operação e exibe erro.

SE houver falha técnica na exclusão, ENTÃO o sistema exibe mensagem de erro e registra o incidente.

Regras de Negócio Utilizadas:

RN37 – A exclusão de conta deve seguir diretrizes de privacidade, removendo dados pessoais e encerrando sessões ativas.

RN38 – A autenticação de dois fatores (2FA) é obrigatória para a exclusão da conta do usuário

1 REGRAS DE NEGÓCIO

ID	REGRA DE NEGÓCIO
RN01	Apenas usuários autenticados com JWT válido podem iniciar conversas
RN02	O contato escolhido deve estar cadastrado e não pode estar bloqueado
RN03	Todas as ações sensíveis devem ser registradas no sistema de logs com timestamp, ID do usuário e IP
RN04	O canal de comunicação é ativado em tempo real via WebSocket após a criação da conversa
RN05	A autenticação de dois fatores (2FA) é obrigatória para abertura de sessão válida
RN06	A mensagem do usuário deve ser válida
RN07	Toda mensagem deve ser criptografada antes de ser armazenada
RN08	A entrega da mensagem é feita via WebSocket, se o destinatário estiver online
RN09	Cada mensagem enviada gera um registro de log para auditoria
RN10	As mensagens novas devem ser exibidas em tempo real via WebSocket, quando possível
RN11	O sistema deve registrar o momento em que o usuário visualiza a mensagem
RN12	Apenas mensagens destinadas ao usuário ainda não visualizadas devem ser marcadas como novas
RN13	O sistema deve permitir a navegação por mensagens anteriores com paginação
RN14	As mensagens devem ser descriptografadas para os usuários participantes da conversa
RN15	O histórico completo da conversa deve estar disponível para os usuários autorizados
RN16	O usuário fica ciente da exclusão de mensagens do outro participante
RN17	A exclusão afeta o histórico de ambos os participantes
RN18	A ação de exclusão pessoal deve ser registrada nos logs de auditoria
RN19	O identificador do contato deve corresponder a uma conta registrada no sistema
RN20	Um mesmo contato não pode ser adicionado duas vezes
RN21	Ao adicionar um contato, o sistema deve registrar a nova associação entre os usuários
RN22	O usuário só pode bloquear contatos com os quais já tenha uma interação registrada
RN23	O sistema deve impedir comunicação entre usuários após o bloqueio
RN24	O status de bloqueio deve ser refletido na interface do usuário e registrado internamente
RN26	O sistema deve retornar todos os contatos associados ao usuário