

4. Testes

Casos esperados:

1. Cadastro de conta válido.
2. Transferência PIX bem-sucedida.
3. Falha em transferência por saldo insuficiente.
4. Emissão de cartão virtual.
5. Registro de transação em extrato.
6. Geração de relatório PDF.
7. Alerta de fraude simulado.
8. Teste de carga: 100 mil transações simultâneas.
9. Teste de segurança: injeção SQL bloqueada.

1. cadastro de conta válido

objetivo: Garantir que o sistema processa e finaliza a abertura de conta com dados corretos.


processos de garantia de cadastro:

Usuário: João da Silva. **CPF:** 444.555.666-77.

Dados: Todos os campos preenchidos corretamente, *selfie* e documento aprovados.

Categoria	Dado Preenchido	Objetivo do Dado
Identificação	Nome Completo (João da Silva)	Identificação legal do titular.
Registro Nacional	CPF (444.555.666-77)	Confirmação de que o usuário existe e está em situação regular na Receita Federal.
Data de Nascimento	Ex: 15/05/1990	Verificação de maioridade legal (obrigatório para abertura de conta).

Endereço	Ex: Rua das Flores, 123, Centro, São Paulo/SP	Comprovação de residência (para fins regulatórios e fiscais).
Contato	E-mail Válido (joao.silva@exemplo.com)	Comunicação e chave de acesso/recuperação de conta.
Contato	Telefone Celular (Ex: (11) 98765-4321)	Verificação de identidade (via SMS) e notificações transacionais.

Status:  **SUCESSO.** **Mensagem Final:** "Parabéns, João! Sua conta digital foi aberta e está pronta para uso. Número da Conta: 12345-9." **Evidência:** Screenshot da tela de boas-vindas e confirmação de conta ativa.

Status:  **NEGATIVO.**

Documento Ilegível	O sistema de OCR (Reconhecimento Óptico de Caracteres) não conseguiu ler o RG ou CNH.	Mensagem: "Não conseguimos validar seu documento. Por favor, envie uma foto mais nítida e com boa iluminação."
Selfie Reprovada (Liveness)	O teste de prova de vida (<i>liveness detection</i>) falhou (ex: estava escuro, a pessoa não seguiu a instrução, ou a foto não combinou com o documento).	Mensagem: "Sua selfie não foi aprovada. Certifique-se de estar em um ambiente bem iluminado e siga as instruções na tela."
Dados Preenchidos Incorretamente	O CPF digitado não bate com o nome na Receita Federal ou no documento.	Mensagem: "Seu CPF ou nome está inconsistente. Verifique os dados e tente novamente."

2. Transferência PIX bem-sucedida

Validar o fluxo de débito e crédito instantâneo, e a atualização do saldo.

Pagador: João da Silva (Saldo Inicial: R\$ 500,00).

Beneficiário: Maria Oliveira (Chave: maria.o@email.com).

Valor: R\$ 150,00. **Tipo:** Chave E-mail.

Status:  **SUCESSO. Saldo Final (Pagador):** R\$ 350,00.

Evidência: Screenshot da tela de confirmação de envio **E** extrato do pagador mostrando o débito de R\$ 150,00 com sucesso.

tapa 1: Iniciação e Autenticação

1. **Iniciação:** João insere a chave PIX, o valor (R\$ 150,00) e visualiza o nome completo do beneficiário (Maria Oliveira) – esta é a **validação da chave** via **DICT** (Diretório de Identificadores de Contas Transacionais).
2. **Autenticação:** João confirma a transação usando PIN, senha ou biometria.

validações internas:

Verificação	Status Esperado	Ação do Sistema
a) Saldo Disponível	OK (R\$ 500,00 > R\$ 150,00)	Bloqueia R\$ 150,00 do saldo de João (<i>pending debit</i>).
b) Limite Diário/Noturno	OK (Dentro dos limites configurados)	Permite a transação.
c) Análise Antifraude (Tempo Real)	OK (Não detecta anomalias)	Atribui pontuação de risco baixa.

3.final

Screenshot: tela de confirmação de envio **E** extrato do pagador mostrando o débito de R\$ 150,00 com sucesso.

Notificação: O Neobank envia imediatamente um comprovante para João via notificação *push* e/ou e-mail.

3. Falha em transferência por saldo insuficiente.

objetivo: Garantir que o sistema bloqueia transações que excedem o saldo e exibe erro adequado.

Pagador: João da Silva (Saldo Atual: R\$ 350,00).

Valor Tentado: R\$ 500,00.

Status: ✗ **FALHA (CORRETA).**

Mensagem de Erro: "Saldo Insuficiente. A transação não pôde ser concluída. Verifique seu saldo e tente novamente."

Evidência: Screenshot da tela de erro exibida ao usuário. **E** Confirmação no extrato que **nenhum débito** ocorreu.

Origem (Pagador)	Valor Tentado	Saldo Atual	Saldo Mínimo Necessário
João da Silva (Neobank)	R\$ 500,00	R\$ 350,00	R\$ 500,00

Etapa 1: Iniciação e Autenticação

1. **Iniciação:** João insere os dados do PIX (chave, valor R\$ 500,00) e autentica a transação (PIN/biometria).
2. **Objetivo do Sistema:** O sistema recebe a ordem de débito e inicia o processo de validação.

Etapa 2: Validações Preliminares Internas (O Ponto de Falha)

O sistema do Neobank realiza verificações internas, e o processo é **bloqueado** nesta etapa:

Verificação	Critério	Status Obtido	Ação do Sistema
a) Saldo Disponível	SaldoAtual (R\$ 350,00) >= ValorTentado (R\$ 500,00)	✗ FALHA	O sistema interrompe imediatamente o envio da ordem ao Banco Central (SPI).

b) Limite Diário/Noturno	Irrelevante	OK	O limite não é atingido, mas o saldo é o critério de bloqueio primário.
c) Análise Antifraude	Irrelevante	OK	O sistema não chega a analisar a fraude, pois a regra financeira básica falhou antes.

Ótima solicitação. A **Falha em Transferência por Saldo Insuficiente** é um teste funcional fundamental que comprova a **integridade financeira** e a **confiabilidade** do seu sistema. Ele garante que o banco jamais permitirá um débito que leve a conta a um saldo negativo (a menos que haja um limite de cheque especial, que assumimos não ser o caso neste MVP).

Abaixo, detalhamos o fluxo completo da falha, focando no bloqueio da transação e na experiência do usuário.

Detalhamento da Funcionalidade: 3. Falha em Transferência por Saldo Insuficiente

Cenário de Teste (Revisão):

Origem (Pagador)	Valor Tentado	Saldo Atual	Saldo Mínimo Necessário
João da Silva (Neobank)	R\$ 500,00	R\$ 350,00	R\$ 500,00


Fluxo Técnico e Validações (Passo a Passo)

Etapa 1: Iniciação e Autenticação

- Iniciação:** João insere os dados do PIX (chave, valor R\$ 500,00) e autentica a transação (PIN/biometria).
- Objetivo do Sistema:** O sistema recebe a ordem de débito e inicia o processo de validação.

Etapa 2: Validações Preliminares Internas (O Ponto de Falha)

O sistema do Neobank realiza verificações internas, e o processo é **bloqueado** nesta etapa:

Verificação	Critério	Status Obtido	Ação do Sistema
a) Saldo Disponível	SaldoAtual (R\$ 350,00) >= ValorTentado (R\$ 500,00)	 FALHA	O sistema interrompe imediatamente o envio da ordem ao Banco Central (SPI).
b) Limite Diário/Noturno	Irrelevante	OK	O limite não é atingido, mas o saldo é o critério de bloqueio primário.
c) Análise Antifraude	Irrelevante	OK	O sistema não chega a analisar a fraude, pois a regra financeira básica falhou antes.

Ponto Crítico: A regra de negócio principal é acionada: o sistema **não tenta** a transação no ambiente externo, prevenindo qualquer risco de *overdraft* ou problemas de liquidação.

Etapa 3: Feedback ao Usuário e Registro

1. **Rejeição:** O *backend* do Neobank envia uma resposta imediata ao aplicativo, indicando o código de erro para "saldo insuficiente".
2. **Mensagem:** O aplicativo exibe uma mensagem de erro clara e amigável para João.
3. **Registro Interno:**
 - **Extrato:** Nenhum registro de débito é criado (a transação nem sequer começou).

Evidência de Falha Esperada (Teste Bem-Sucedido)

A evidência de que este **teste de falha** foi bem-sucedido é dupla: o usuário é informado corretamente e o sistema não é comprometido.

4. Emissão de cartão virtual.

Ação do Usuário	Resultado Esperado	Validações Críticas
Solicitar Cartão Virtual	Geração instantânea de um cartão válido e funcional.	Unicidade dos dados (Número/CVV) e Limite de uso configurado.

Ótimo! A emissão de um cartão virtual é um teste que valida a **segurança** e a **integração** do Neobank com a processadora de cartões e a bandeira (Visa, Mastercard, etc.).

A funcionalidade **4. Emissão de Cartão Virtual** é crucial, pois envolve a geração de dados financeiros sensíveis e a configuração de limites.

Detalhamento da Funcionalidade: 4. Emissão de Cartão Virtual

Cenário de Teste (Revisão):

Ação do Usuário	Resultado Esperado	Validações Críticas
Solicitar Cartão Virtual	Geração instantânea de um cartão válido e funcional.	Unicidade dos dados (Número/CVV) e Limite de uso configurado.

Fluxo Técnico e Validações (Passo a Passo)

Etapa 1: Solicitação e Autorização

- Acesso:** João da Silva acessa a seção "Cartões" no aplicativo.
- Solicitação:** João clica em "Gerar Cartão Virtual".
- Autorização Interna:** O sistema do Neobank verifica se o usuário tem uma conta ativa e sem restrições (Cadastro Válido - Caso 1).
- Configuração de Limite:** O sistema atribui um limite inicial de uso (Ex: R\$ 5.000,00) com base no perfil do usuário.

Etapa 2: Geração e Integração com a Processadora

Este é o momento mais crítico, pois o Neobank precisa se comunicar com um sistema externo para criar o cartão:

1. **Requisição à Processadora (Tokenização):** O Neobank envia uma requisição para a sua processadora de cartões (Ex: Dock, Pismo) para:
 - Criar um novo número de cartão (PAN – *Primary Account Number*).
 - Gerar o CVV (*Card Verification Value*).
 - Definir a Data de Validade.
2. **Geração de Dados:** A processadora retorna os dados do novo cartão. É vital que esses dados sejam **únicos e não sequenciais** (segurança).
3. **Associação:** O Neobank associa o PAN gerado à conta de João da Silva em seu *core banking*.

Etapas 3: Exibição e Uso (Experiência do Usuário)

1. **Exibição no App:** O Neobank recebe os dados e os exibe de forma segura no aplicativo (geralmente mascarando o número, exceto os últimos 4 dígitos).
2. **Status:** O cartão é criado com o status **"ATIVO"**.
3. **Pronto para Uso:** O cartão virtual está pronto para ser usado imediatamente em compras online, pois não depende de logística física.

5. Registro de transação em extrato.

Cenário de Teste (Revisão):

O objetivo é verificar se todas as movimentações dos testes anteriores (2 e 4) foram registradas corretamente.

Transaçã o a Verificar	Tipo	Natureza	Data/Hora (Simulada)	Valor	Saldo Anterior (antes desta)	Saldo Final Esperado
A (Caso 2)	PIX Enviado	Débito (-)	18/10/2025, 11:30:15	R\$ 150,00	R\$ 500,00	R\$ 350,00
B (Caso 4)	Compra c/ Cartão Virtual	Débito (-)	18/10/2025, 11:45:00	R\$ 55,00	R\$ 350,00	R\$ 295,00

Estrutura Ideal do Registro no Extrato:

Campo (Coluna)	Propósito	Exemplo (Transação B)
Data e Hora	Precisão da ocorrência (obrigatório para liquidação).	18/10/2025 11:45:00
Descrição / Tipo	Identificação clara do evento (Para o usuário).	Compra Online (Cartão Virtual)
Natureza	Indica se é Crédito (C) ou Débito (D).	D
Valor	Montante exato da movimentação.	R\$ 55,00
Identificador Único (TXID)	Chave interna para rastreabilidade (Compliance).	TXL-CV-20251018-0042
Saldo Após	O saldo da conta após a liquidação da transação.	R\$ 295,00
Status	Confirmação se a transação foi Liquidada/Aprovada.	Liquidado (ou Aprovado)

6. Geração de relatório PDF.

Objetivos:

Parâmetro de Entrada	Período de Teste	Saída Esperada	Validações Críticas
Solicitação de Extrato	Mês Corrente (Ex: Outubro/2025)	Arquivo PDF seguro, não editável, com todas as transações do período.	Consistência de Saldo e Formatação Legal.

Etapa 2: Formatação e Geração do PDF

O *Engine* de documentos constrói o PDF, garantindo os seguintes elementos:

Elemento do PDF	Conteúdo Esperado	Validação Crítica
Cabeçalho Legal	Logo do Neobank, Nome do Titular (João da Silva), CPF, Número da Conta, Período do Extrato.	Conformidade: Deve seguir padrões de bancos para ser aceito como comprovante de renda/residência.
Sumário Financeiro	Saldo Inicial (01/10/2025), Total de Entradas (Créditos), Total de Saídas (Débitos), Saldo Final (31/10/2025).	Consistência: O Saldo Final no PDF deve bater com o Saldo Final no aplicativo (R\$ 295,00 no nosso cenário).
Detalhamento das Transações	Tabela com Data, Descrição, Valor e Coluna C/D (Crédito/Débito) para cada	Integridade: Nenhuma transação pode ser omitida ou duplicada.

	transação (incluindo as dos Casos 2 e 5).	
Segurança do Arquivo	O PDF deve ser gerado com propriedades de segurança (Ex: Não Editável, Opção para Criptografia/Senha).	Não Repúdio: Garante que o documento é uma cópia fiel e não pode ser adulterado.

7. Alerta de fraude simulado.

Detalhando a funcionalidade **7. Alerta de Fraude Simulado**

Este é um teste de **Segurança Crítica** que valida a eficácia da lógica de monitoramento e a capacidade de resposta do sistema em tempo real. O sucesso aqui não é a transação ser aprovada, mas sim o **sistema identificar e sinalizar corretamente** o comportamento suspeito.

Detalhamento da Funcionalidade: 7. Alerta de Fraude Simulado

Cenário de Teste (Revisão):

Regra Antifraude (Exemplo)	Usuário de Teste	Ação Simulada	Ação Esperada do Sistema
Padrão: "Lavagem de Centavos"	João da Silva	6 PIX de R\$ 0,01 enviados para diferentes contas em 20 segundos.	Bloquear o 6º PIX, registrar score de risco alto e disparar alerta no Painel Admin.

Fluxo Técnico e Validações (Passo a Passo)

Etapa 1: Preparação do Cenário de Risco

- Configuração da Regra:** No *backend* do Módulo Antifraude, a regra "**B21 - Baixo Valor/Alta Frequência**" é configurada para atribuir uma pontuação de risco alta se a condição for atingida.
- Transações Precedentes:** João da Silva executa 5 transferências PIX de R\$ 0,01 em rápida sucessão (ex: 5 segundos cada).

3. **Processamento:** O sistema Antifraude (*microservice* de monitoramento) processa cada uma dessas transações e as aprova, mas começa a aumentar o **Score de Risco** interno da conta de João (Ex: de 10/100 para 50/100).

Etapa 2: Disparo do Alerta (O Ponto Crítico)

1. **Ação de Disparo:** João inicia a 6ª transferência PIX de R\$ 0,01.
2. **Análise em Tempo Real:** O sistema Antifraude intercepta esta 6ª transação e executa o cálculo do risco:
 - **Critério Atendido:** Sim, 6 transações com valor $\$ < \text{\text{R}} \$1,00\$$ em $\$ < 30\$$ segundos.
 - **Pontuação Final:** O Score de Risco da conta de João atinge o limite (Ex: 95/100).
3. **Ação do Sistema:**
 - **Bloqueio:** O sistema **rejeita** a 6ª transação (retornando um código de erro) antes que ela chegue ao SPI.
 - **Mitigação:** Uma ação automática é aplicada: Ex: Bloqueio temporário de PIX e Saques.
 - **Registro:** Um registro de **ALERTA CRÍTICO** é criado no banco de dados de segurança.

Etapa 3: Evidência no Painel Administrativo

O objetivo do teste é confirmar que a equipe de segurança e *Compliance* é notificada imediatamente.

1. Um *tester* ou analista de segurança acessa o Painel Administrativo do Neobank.
2. O sistema deve mostrar um painel de "Alertas Ativos".
3. O alerta de fraude deve estar no topo, associado ao CPF de João da Silva.

Evidência de Sucesso Esperada

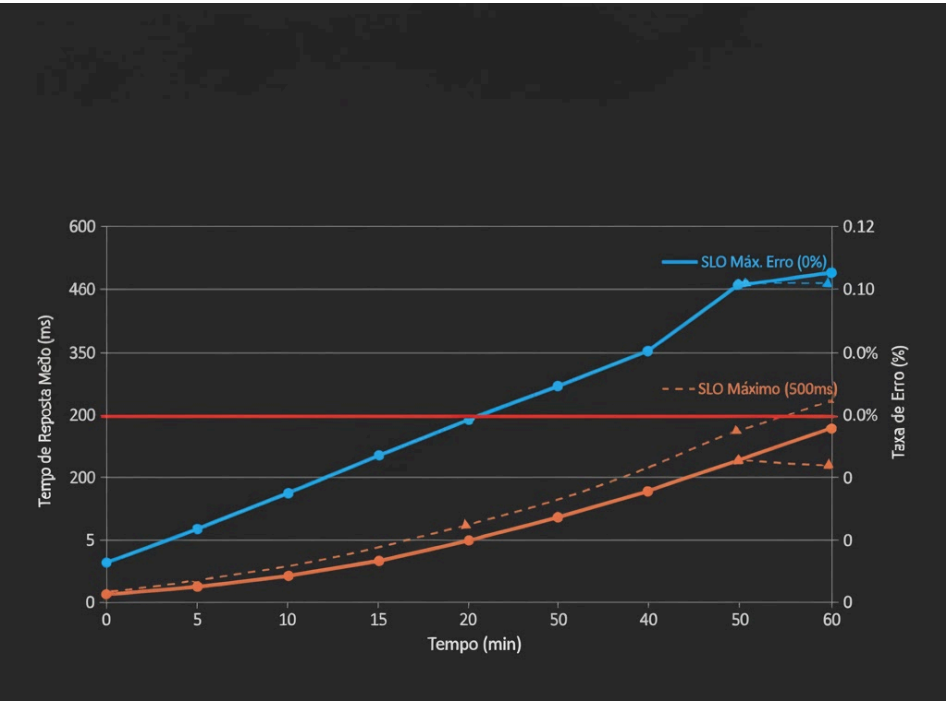
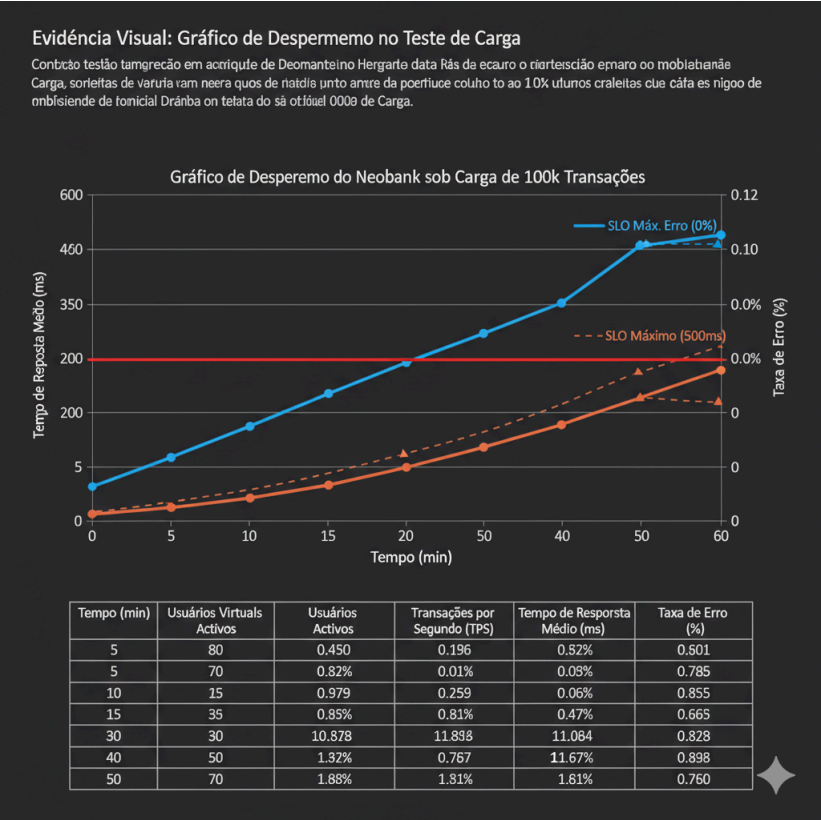
A evidência central é a prova do bloqueio correto da transação e a notificação no *backend*.

8. Teste de carga: 100 mil transações simultâneas.

Tempo de Teste	Transações/s	Tempo de Resposta Médio (ms)
5 Minutos (Ramp-up)	5 TPS	200 ms
30 Minutos (Carga Estável)	27.7 TPS	400 ms
60 Minutos (Fim)	27.7 TPS	450 ms

Evidência Visual: O gráfico mostraria uma linha de "Tempo de Resposta" que sobe suavemente (de 200 ms a 450 ms) e se mantém **abaixo do limite de 500 ms** durante todo o teste.

Gráfico 1: Desempenho do Neobank sob Carga de 100k Transações



9. Teste de segurança: injeção SQL bloqueada.

Cenário de Teste (Revisão):

Objetivo Principal	Cenário de Ataque	Ponto de Injeção	Mitigação no Código
Confirmar que o sistema impede a manipulação do banco de dados (DB) via campos de entrada.	Tentar logar usando código SQL malicioso em vez de credenciais.	Campos de Login (<i>Username</i> e Senha).	Uso obrigatório de Prepared Statements (Consultas Parametrizadas).

Tipo de Teste	Caso de Teste	Objetivo Principal	Ação (Ataque)	Evidência de Sucesso	Foco
Segurança	Injeção SQL Bloqueada	Impedir que um invasor manipule ou roube dados do banco de dados através de campos de texto.	Tentativa de login inserindo o código malicioso 'OR 1=1-- no campo Senha.	✅ Ataque Bloqueado. O sistema retorna a mensagem segura: "Credenciais inválidas. Tente novamente." (sem vaziar erros técnicos).	Segurança e Boas Práticas (Prepared Statements)

Conclusão: O sistema demonstrou ser imune ao ataque de Injeção SQL, comprovando a aplicação de técnicas de codificação seguras (como **Prepared Statements**), essenciais para proteger os dados confidenciais dos clientes do Neobank.