

Especificação de Requisitos de Software (SRS) - Fintech Digital MVP

1. Introdução

1.1. Objetivo do Documento

Este documento detalha a Especificação de Requisitos de Software (SRS) para a **Fintech Digital**, um projeto de instituição de pagamento focado em conta digital para Pessoa Física (PF). O objetivo é fornecer uma base técnica e funcional clara para o desenvolvimento do Produto Mínimo Viável (MVP), garantindo que todas as funcionalidades e requisitos não-funcionais críticos sejam endereçados.

1.2. Escopo do Projeto (MVP)

O escopo inicial (MVP) se concentra na entrega de uma **conta digital completa para PF** com as seguintes funcionalidades essenciais:

1. Abertura de conta e Onboarding (KYC).
2. Dashboard de conta (saldo, extrato).
3. Transferências PIX (envio e recebimento).
4. Cartão virtual para compras online.
5. Suporte in-app.

1.3. Definições e Acrônimos

Acrônimo	Definição
SRS	Especificação de Requisitos de Software
MVP	Produto Mínimo Viável
PF	Pessoa Física
KYC	Know Your Customer (Conheça Seu Cliente)
AML/PLD	Anti-Money Laundering/Prevenção à Lavagem de Dinheiro
LGPD	Lei Geral de Proteção de Dados Pessoais
PIX	Sistema de Pagamentos Instantâneos do Banco Central do Brasil
SLA	Service Level Agreement (Acordo de Nível de Serviço)

2. Visão Geral do Produto

2.1. Público-Alvo

Pessoas Físicas (PF) com idade superior a 18 anos, bancarizadas ou desbancarizadas, que buscam uma solução digital, rápida e de baixo custo para gerenciar suas finanças diárias, com foco em transferências instantâneas (PIX) e compras online (cartão virtual).

2.2. Proposta de Valor

Oferecer uma conta digital **simples, segura e 100% gratuita** para o público PF, com foco na experiência do usuário e na conformidade regulatória brasileira (PIX e LGPD).

3. Requisitos Funcionais

ID	Módulo	Requisito Funcional	Descrição
RF01	Onboarding/KYC	Cadastro de Usuário	O usuário deve conseguir iniciar o cadastro com nome, e-mail, celular e CPF.
RF01.01	Onboarding/KYC	Verificação KYC	O sistema deve realizar a verificação documental e validação em bases públicas para aprovação.
RF01.02	Onboarding/KYC	Aceite de Termos	O usuário deve aceitar os Termos de Uso, Política de Privacidade e consentimentos LGPD para concluir o cadastro.
RF02	Gestão da Conta	Dashboard	O usuário deve visualizar o saldo atualizado e o histórico de movimentações.
RF02.01	Gestão da Conta	Extrato Detalhado	Deve ser possível filtrar o extrato por período, tipo de transação e valor.
RF03	Transferências	Envio PIX	O usuário deve conseguir enviar PIX usando CPF/CNPJ, Telefone, E-mail, Chave Aleatória ou Chave Bancária (TED).
RF03.01	Transferências	Recebimento PIX	O usuário deve conseguir receber PIX via chave estática/dinâmica.
RF03.02	Transferências	Comprovante	O sistema deve gerar comprovante digital para todas as transações.
RF04	Cartão Virtual	Emissão de Cartão	O usuário deve conseguir gerar um cartão virtual (ou pré-pago) para uso imediato em compras.
RF04.01	Cartão Virtual	Gestão do Cartão	O usuário deve conseguir bloquear e desbloquear o cartão virtual a qualquer momento via app.
RF05	Suporte	Suporte In-App	O aplicativo deve oferecer uma seção de chat para atendimento ao cliente.
RF06	Administrativo	Painel de Compliance	O sistema deve fornecer um painel administrativo para gerenciamento de usuários, aprovação de KYC e relatórios de compliance (AML/PLD).

4. Requisitos Não-Funcionais

4.1. Performance e Escalabilidade

- **Escalabilidade:** A arquitetura deve ser projetada para suportar um crescimento de 10.000 para 1.000.000 de usuários ativos (planejamento de *horizontal scaling*).
- **Performance:** A latência de API deve ser **inferior a 200ms** para endpoints críticos (ex.: consulta de saldo, envio de PIX).
- **Disponibilidade (SLA):** Os serviços core (transferências, consulta de saldo) devem ter uma disponibilidade mínima de **99.9%** (equivalente a menos de 8h e 45min de *downtime* por ano).

4.2. Segurança

- **Criptografia:** Todos os dados sensíveis devem ser armazenados com criptografia AES-256 (em repouso) e toda a comunicação deve ser protegida por TLS 1.2+ (em trânsito).
- **Gestão de Chaves:** Chaves criptográficas sensíveis (ex.: chaves de PIX, chaves de API) devem ser gerenciadas por um HSM (Hardware Security Module) ou serviço equivalente (ex.: AWS Secrets Manager / Vault).
- **Autenticação:** O acesso ao aplicativo deve usar autenticação forte (MFA/2FA) e o acesso administrativo deve ser rigorosamente controlado com 2FA obrigatório.
- **Testes:** O sistema deve passar por *pentest* (teste de intrusão) antes do lançamento (*go-live*).

4.3. Compliance e Regulatório

- **AML/PLD:** O sistema deve incorporar regras de monitoramento de transações e *screening* de Pessoas Expostas Politicamente (PEP) em tempo real, conforme requisitos do Banco Central.
- **LGPD:** O sistema deve garantir o controle de consentimento, anonimização de dados quando solicitada e a figura do Encarregado (DPO) definida e acessível.
- **PCI-DSS:** Se houver armazenamento, processamento ou transmissão de dados de cartão (PAN), o sistema deve ser compatível com PCI-DSS ou utilizar um provedor certificado.

5. Casos de Uso e Fluxos

5.1. Fluxo de Onboarding / KYC (RF01)

1. **Início:** Usuário baixa o app e inicia o cadastro (`/api/v1/signup`).
2. **Coleta de Dados:** Coleta de dados básicos e documentos (RG/CNH, selfie).

3. **Processamento:** O sistema executa OCR nos documentos, valida o CPF/CNPJ na Receita Federal e verifica o risco (PEP/AML).
4. **Decisão:**
 - **Aprovado:** Provisionamento da conta e notificação ao usuário.
 - **Revisão:** Criação de um caso para análise manual no Painel de Compliance (RF06).
 - **Recusado:** Notificação de recusa ao usuário.

5.2. Fluxo de Transferência PIX (RF03)

1. **Início:** Usuário informa a chave PIX de destino e o valor no app.
2. **Validação:** O sistema verifica saldo, limites diários/mensais e regras AML/PLD em tempo real.
3. **Execução:** O sistema envia a requisição de pagamento ao provedor de PIX/SPI.
4. **Confirmação:** Recebe o *callback* de confirmação/falha do provedor.
5. **Registro:** Atualiza o saldo do usuário, registra a transação no extrato e envia o comprovante.
6. **Idempotência:** O sistema deve usar uma `idempotency_key` (cabeçalho ou campo) para garantir que a mesma requisição de pagamento não seja processada duas vezes.

6. Especificação de APIs (Exemplo Mínimo)

Endpoint	Método	Descrição	Exemplo de P
<code>/v1/payments/transfer</code>	POST	Cria uma nova transferência PIX/TED.	<pre>{ "from_accou "to_account_k "currency":"BR</pre>
<code>/v1/accounts/{id}/balance</code>	GET	Consulta o saldo atual da conta.	N/A
<code>/v1/accounts/{id}/statement</code>	GET	Consulta o extrato da conta.	<code>?start_date=20</code>
<code>/v1/cards/virtual</code>	POST	Solicita a emissão de um novo cartão virtual.	N/A

Padrões de API:

- **Autenticação:** OAuth2 (JWT access + refresh tokens).
- **Versionamento:** Uso de `/v1/` no prefixo.

- **Logs de Auditoria:** Todas as requisições devem gravar `tracer_id` , usuário, ação, timestamp, IP e resultado.

7. Requisitos Legais/Compliance (Resumo)

Os requisitos legais e de compliance detalhados no guia original devem ser incorporados como critérios de aceitação.

- **Regulação BCB:** O sistema deve estar em conformidade com as regras para Instituições de Pagamento (IP) e as normas de operação do PIX.
- **AML/PLD:** Implementação de política formal de Prevenção à Lavagem de Dinheiro, incluindo monitoramento de transações e *thresholds* de reporte.
- **LGPD:** Implementação de mecanismos para controle de consentimento, direito de acesso e exclusão de dados.

8. Critérios de Aceitação (Exemplos)

1. O usuário deve conseguir completar o fluxo de KYC em menos de 5 minutos, desde o início do cadastro até a aprovação da conta (se não cair em análise manual).
2. Uma transação PIX deve ser concluída e refletida no saldo em até 10 segundos em 95% dos casos.
3. O Painel de Compliance (RF06) deve permitir a geração de relatórios de todas as transações acima de R\$ 10.000,00 em um período de 24 horas.
4. O bloqueio/desbloqueio do cartão virtual deve ser instantâneo.