Política Institucional de PLD/FT

SX Digital Pay

Versão: 1.5
Data de Aprovação: 31/12/2025
Status: Em vigor

1. OBJETIVO

Esta política tem por objetivo estabelecer as diretrizes, princípios e procedimentos a serem adotados pela **SX Digital Pay** para prevenir e combater a utilização de sua plataforma para a prática dos crimes de lavagem de dinheiro (LD), ocultação de bens, direitos e valores, e financiamento do terrorismo (FT).

O documento visa garantir a conformidade com as leis e regulamentações vigentes, protegendo a reputação da instituição, seus acionistas, colaboradores, clientes (Users) e estabelecimentos comerciais (Merchants).

2. ABRANGÊNCIA

Esta política aplica-se a:

- Todos os administradores, diretores, colaboradores e prestadores de serviços da SX Digital Pay;
- Todos os processos de negócio, produtos e serviços oferecidos (PIX, Cartão de Crédito, Cotações/Câmbio);
- Relacionamentos com Clientes (Usuários Finais) e Estabelecimentos (Merchants).

3. FUNDAMENTAÇÃO LEGAL E REGULATÓRIA

Esta política foi elaborada em conformidade com:

- **Lei nº 9.613/1998:** Dispõe sobre os crimes de lavagem de dinheiro;
- **Lei nº 13.260/2016:** Disciplina o terrorismo e seu financiamento;
- **Circular BACEN nº 3.978/2020:** Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil;
- **Carta Circular BACEN nº 4.001/2020:** Relação de operações e situações que podem configurar indícios de lavagem de dinheiro.

4. GOVERNANÇA DE PLD/FT

4.1. Estrutura Organizacional

A SX Digital Pay mantém uma estrutura dedicada ou designa um Diretor Responsável, com as seguintes atribuições:

- Promover a cultura de conformidade e ética em toda a organização;
- Monitorar a aderência desta política e dos controles internos;
- Analisar operações atípicas e reportar indícios de suspeita à instituição financeira/banco de câmbio parceiro;
- Responder às requisições das autoridades competentes e parceiros bancários.

5. ABORDAGEM BASEADA EM RISCO (ABR)

A SX Digital Pay adota uma metodologia de Abordagem Baseada em Risco para identificar, avaliar e

mitigar os riscos de LD/FT associados aos seus clientes, produtos, canais de distribuição e jurisdições de atuação.

5.1. Classificação de Risco

Clientes e Merchants são classificados em níveis de risco (Baixo, Médio, Alto) com base em fatores como:

- Natureza da atividade econômica (para Merchants);
- Localização geográfica e sede;
- Volume, frequência e destino das transações;
- Perfil do usuário (ex: Pessoa Exposta Politicamente - PEP).

6. PROCEDIMENTOS DE CONHEÇA SEU CLIENTE (KYC E KYB)

O processo de aceitação segue um fluxo rigoroso de identificação e validação para garantir a integridade da base de usuários.

6.1. Cadastro de Usuários (Pessoa Física - KYC)

O onboarding de usuários (/user) exige:
1. **Coleta de Dados:** Nome completo, CPF, E-mail, Telefone, Endereço e Data de Nascimento.
2. **Verificação de Identidade (Didit ID):** Validação documental (RG/CNH) e liveness check (biometria facial).
3. **Triagem AML:** Verificação em listas globais de sanções (ONU, OFAC, etc.), pessoas procuradas e situação cadastral do CPF na Receita Federal.

6.2. Cadastro de Estabelecimentos (Pessoa Jurídica - KYB)

O onboarding de Merchants exige Due Diligence aprofundada:
1. **Dados do Negócio:** CNPJ (ou TaxID equivalente), Razão Social, Nome Fantasia e Ramo de Atividade (MCC).
2. **Identificação de Beneficiários Finais (UBO):** Identificação de todas as pessoas físicas que, em última instância, detêm, direta ou indiretamente, mais de 25% do capital social da empresa ou que exercem o controle efetivo da entidade.
3. **Verificação de Sócios e Diretores:** Triagem AML para todos os controladores e administradores.
4. **Aprovação Administrativa:** Status permanece PENDENTE até revisão manual por um ADMIN, garantindo que o modelo de negócio seja legítimo.

6.3. Identificação Digital e Registros de Acesso

Em alinhamento com a Política de Privacidade, a SX Digital Pay coleta e monitora dados técnicos de navegação e dispositivo, tais como endereço IP, geolocalização, fingerprint do dispositivo, data e hora de acesso e histórico de sessões. Essas informações compõem o perfil digital do usuário e são utilizadas como camada adicional de segurança para validação de identidade e detecção de acessos suspeitos.

6.4. Setores e Perfis Restritos (Política de Apetite a Risco)

A SX Digital Pay **não autoriza o credenciamento** de estabelecimentos que operem em setores de altíssimo risco ou fora do apetite regulatório:

- Exploração de jogos de azar, apostas (gambling/betting) e cassinos não regulamentados;

- Comércio ou intermediação de criptoativos/moedas virtuais (sem licença específica);
- Comércio de armas, munições ou substâncias ilícitas;
- Empresas com estruturas societárias excessivamente complexas que visem ocultar o beneficiário final.

6.5. Atualização Cadastral

Os dados cadastrais devem ser atualizados periodicamente ou sempre que houver suspeita de veracidade das informações, garantindo a fidedignidade do perfil do cliente.

7. MONITORAMENTO E SELEÇÃO DE OPERAÇÕES

7.1. Sinais de Alerta

São situações sujeitas a análise imediata:

- **Fracionamento (Smurfing):** Múltiplas transações de baixo valor para burlar limites;
- **Incompatibilidade Financeira:** Movimentação que diverge drasticamente do perfil de faturamento declarado ou presumido;
- **Transações de Passagem:** Recebimento de valores seguido de transferência rápida para terceiros, sem lógica comercial clara;
- **Uso de Cartões de Terceiros:** Pagamentos recorrentes utilizando cartões que não pertencem ao titular da conta.

7.2. Tratamento de Alertas

1. Geração de alerta pelo sistema (limites ou regras de comportamento).
2. Análise pela equipe de Compliance (Dossiê).
3. Solicitação de documentos comprobatórios (ex: Notas Fiscais, contratos) se necessário.
4. Decisão: Arquivamento fundamentado ou Reporte de Suspeita ao parceiro bancário.

8. SEGURANÇA E BLOQUEIOS

8.1. Limites Operacionais

A plataforma impõe limites baseados no nível de verificação e histórico do cliente. Limites para PIX e Cartão são monitorados em tempo real.

8.2. Bloqueio Cautelar

A SX Digital Pay pode realizar o bloqueio preventivo de contas ou saldos (userStatus = BANNED ou UNDER_REVIEW) sempre que houver suspeita de fraude, lavagem de dinheiro ou quando solicitado pela instituição financeira parceira.

8.3. Segurança da Informação e Compartilhamento de Dados

Para garantir a integridade das operações e reforçar a prevenção a ilícitos, são adotadas as seguintes práticas de segurança e compartilhamento:

- **Segurança Técnica:** Utilização de criptografia em trânsito (HTTPS/TLS) e armazenamento; dados críticos de cartão de crédito são processados via tokenização (Cielo) e protegidos com criptografia AES-256 no banco de dados.
- **Validação de Identidade e Biometria:** Compartilhamento de dados cadastrais e biométricos com

parceiros especializados (Didit) para realização de liveness check e validação documental antifraude.

• **Processamento de Pagamentos:** Compartilhamento estritamente necessário de dados transacionais com gateways (EFI Pay, Cielo) para execução de pagamentos, validação de segurança (ex: 3D Secure) e prevenção à lavagem de dinheiro.

• **Autoridades e Compliance:** Cooperação com autoridades governamentais, judiciárias e regulatórias (incluindo Banco Central), fornecendo dados quando exigido por lei, ordem judicial ou para investigação de fraudes e crimes financeiros.

9. REPORTE DE OPERAÇÕES SUSPEITAS

A SX Digital Pay, na qualidade de plataforma tecnológica de pagamentos, atua em colaboração com instituições financeiras e bancos de câmbio autorizados.

As operações identificadas como suspeitas pela nossa equipe de Compliance **serão reportadas à instituição financeira parceira**, que detém o acesso direto e a responsabilidade legal de comunicação ao **COAF (Conselho de Controle de Atividades Financeiras)** via SISCOAF.

Este reporte ocorre:

• Sem dar ciência ao cliente ou a terceiros (dever de sigilo);

• Acompanhado de todas as informações cadastrais e logs transacionais disponíveis.

10. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

Dada a natureza de alto risco das operações envolvendo PEPs, a SX Digital Pay adota uma postura restritiva:

• **Identificação:** Verificação obrigatória durante o onboarding via integração Didit e consultas a bases públicas.

• **Aprovação:** O credenciamento de Merchants cujo UBO seja PEP exige aprovação unânime da diretoria e aplicação de Medidas de Devida Diligência Reforçada (EDD).

• **Monitoramento:** Contas ligadas a PEPs sofrem monitoramento transacional mais rigoroso e frequente.

11. REGISTRO E ARMAZENAMENTO

Todos os registros de identificação (KYC/KYB), logs de transações (EFI/Cielo), análises de alertas e comunicações aos parceiros serão mantidos por um período mínimo de **10 (dez) anos**, contados a partir do primeiro dia do ano seguinte ao encerramento do relacionamento ou da conclusão da transação.

12. TREINAMENTO E CULTURA

A SX Digital Pay assegura que todos os colaboradores passem por treinamento de PLD/FT na admissão e anualmente. O programa abrange tipologias de crimes, identificação de alertas e procedimentos de reporte interno.

13. DISPOSIÇÕES GERAIS

O descumprimento das diretrizes desta política é considerado falta grave, sujeitando os responsáveis a sanções administrativas e desligamento, além de eventuais comunicações às autoridades policiais para apuração de responsabilidade criminal.

Esta política deve ser revisada anualmente ou sempre que houver mudanças significativas na legislação ou no modelo de negócio da empresa.