Plano de Compliance, AML/PLD e Checklist LGPD (Brasil)

1. Estrutura do Programa de Compliance

A implementação de um Programa de Compliance robusto é essencial para a operação de uma Fintech no Brasil, dado o ambiente regulatório rigoroso do Banco Central (BCB) e a Lei Geral de Proteção de Dados (LGPD).

1.1. Governança e Papéis Chave

Papel	Responsabilidade Principal	Req
Compliance Officer (CO)	Responsável pela política geral de compliance, incluindo AML/PLD. Reporte direto ao Conselho/Diretoria.	Exig
Encarregado de Dados (DPO)	Atua como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).	LGP
Comitê de Compliance	Avaliação periódica de riscos, aprovação de políticas e monitoramento de performance.	Boa

1.2. Política de Compliance

A política deve ser formalizada e aprovada pela alta administração, cobrindo, no mínimo:

- Código de Conduta e Ética.
- Política de Prevenção à Lavagem de Dinheiro (PLD/AML).
- Política de Segurança da Informação.
- Política de Privacidade e Proteção de Dados (LGPD).
- Procedimentos para comunicação de violações e canais de denúncia.

2. Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/AML)

O programa de AML/PLD deve seguir as circulares e resoluções do Banco Central e do Conselho de Controle de Atividades Financeiras (COAF).

2.1. Know Your Customer (KYC)

O processo de KYC deve ser rigoroso e baseado em risco, conforme detalhado no SRS:

1. **Coleta de Dados:** Documentos de identificação (RG/CNH), CPF, comprovante de residência e dados biométricos (se aplicável).
2. **Validação:** Uso de ferramentas de OCR, validação em bases públicas (Receita Federal, Justiça Eleitoral) e prova de vida (*liveness check*).
3. **Screening:** Verificação de listas restritivas, sanções internacionais e listas de Pessoas Expostas Politicamente (PEP).
4. **Scoring de Risco:** Classificação do cliente (Baixo, Médio, Alto Risco) para definir o nível de monitoramento.

2.2. Monitoramento de Transações

- **Regras de Alerta:** Implementação de regras de monitoramento baseadas em volume, frequência, geolocalização e padrões de comportamento anormais (ex: transações noturnas, valores arredondados, pulverização de valores).
- **Thresholds:** Definição de limites de transação que, ao serem ultrapassados, geram alertas automáticos para análise manual.
- **Análise e Reporting (SAR):** Procedimento claro para análise de alertas e, se necessário, comunicação de Operações Suspeitas (SAR - *Suspicious Activity Report*) ao COAF.

3. Checklist de Conformidade com a LGPD (Lei nº 13.709/2018)

A conformidade com a LGPD é crítica, especialmente no tratamento de dados financeiros e biométricos.

Item de Conformidade	Status (A Fazer / Feito)	Detalhes e Ações
Base Legal	A Fazer	Mapear a base legal (Consentimento, Execução c Contrato, Obrigação Legal) para CADA tipo de tra de dados (KYC, Transação, Marketing).
Política de Privacidade	A Fazer	Elaborar e publicar a Política de Privacidade clar e em linguagem simples, detalhando dados cole finalidade e compartilhamento.
Consentimento	A Fazer	Implementar mecanismos granulares para coleta de consentimento (opt-in) para finalidades que r obrigação legal ou execução de contrato.
Direitos do Titular	A Fazer	Desenvolver um portal ou canal de atendimento titular possa exercer seus direitos: acesso, retific anonimização, bloqueio e exclusão (Art. 18).
DPIA/RIPD	A Fazer	Realizar o Relatório de Impacto à Proteção de Da Pessoais (RIPD/DPIA) para operações de alto risc processo de KYC e uso de biometria.
Segurança e Retenção	A Fazer	Definir e implementar políticas de retenção e de seguro de dados, garantindo a criptografia em re em trânsito.
DPO Designado	A Fazer	Nomear formalmente o Encarregado de Dados (I publicar seus dados de contato.
Resposta a Incidentes	A Fazer	Criar um Plano de Resposta a Incidentes de Segu (IRP) que inclua a comunicação à ANPD e aos titu caso de vazamento de dados.

4. Requisitos de Segurança e Certificações

O cumprimento de normas de segurança é um pilar do Compliance.

- **ISO 27001:** Considerar a certificação para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI).
- **PCI-DSS: Obrigatório** se a Fintech armazenar, processar ou transmitir dados de cartão (PAN). Caso contrário, utilizar parceiros certificados.
- **Testes de Segurança:** Realização de *Penetration Tests* (Pentest) anuais e após grandes mudanças no sistema.

5. Referências Regulatórias Oficiais

Para manter a conformidade, é imperativo consultar as fontes oficiais:

- **Banco Central do Brasil (BCB):** Normas sobre Instituições de Pagamento, PIX, e o *Regulatory Sandbox* 1.
- **Lei Geral de Proteção de Dados (LGPD):** Texto completo da Lei nº 13.709/2018 2.
- **COAF:** Regras e procedimentos para comunicação de operações suspeitas 3.

Referências