Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT)

Apostila de apoio

Sumário

Objetivos de aprendizagem

- Compreender o que é lavagem de dinheiro e financiamento do terrorismo, seus impactos e principais diferenças.
- Reconhecer métodos comuns utilizados em esquemas de PLD/FT e identificar sinais de alerta.
- Aplicar a abordagem baseada em risco para priorizar esforços de prevenção e detecção.
- Entender os elementos de um programa de compliance em PLD/FT: governança, políticas, KYC, monitoramento e auditoria.
- Estruturar análises e registros para monitoramento e reporte de operações suspeitas, respeitando privacidade e prazos internos.

Lavagem de dinheiro: conceito e impactos

Lavagem de dinheiro é o processo de ocultar ou disfarçar a origem de recursos obtidos de forma ilícita, de modo que passem a parecer provenientes de atividades legítimas. Na prática, isso permite que o dinheiro circule no sistema econômico com menor risco de detecção e com aparência regular.

Por que o tema importa

- Sustenta o crime organizado ao viabilizar a movimentação e o uso de recursos ilícitos.
- Pode distorcer mercados e preços (por exemplo, em setores de alto valor e baixa transparência).
- Aumenta riscos para instituições: reputação, sanções, perdas financeiras e restrições operacionais.

Sinais de alerta frequentes

- Movimentações incompatíveis com renda, patrimônio ou atividade declarada.
- Operações sem lógica econômica clara (vai-e-volta de valores, circularidade, interpostas pessoas).
- Uso intenso de espécie (dinheiro vivo) sem justificativa operacional.
- Estruturas societárias opacas ou complexas sem razão de negócio.
- Resistência em fornecer informações ou documentação mínima.

Financiamento do terrorismo: particularidades

No financiamento do terrorismo, recursos são direcionados para apoiar pessoas, redes ou organizações envolvidas em atividades terroristas. Um ponto importante é que, em muitos casos, os recursos podem ter origem lícita (por exemplo, doações ou negócios legais), o que torna a detecção mais complexa.

Diferenças práticas em relação à lavagem de dinheiro

- A origem dos recursos pode ser lícita, mas o destino é ilícito.
- O valor individual de uma transação pode ser baixo, porém recorrente ou fragmentado.
- Os fluxos podem usar múltiplos intermediários, rotas e instrumentos para reduzir rastreabilidade.

Pontos de atenção no monitoramento

- Transações para/desde jurisdições sensíveis, sem relação comercial consistente.
- Padrões de transferências recorrentes para múltiplos beneficiários sem justificativa clara.
- Uso de mecanismos de remessa e canais com menor transparência ou alto anonimato.
- Aderência a listas de sanções e listas de monitoramento, conforme política e obrigações aplicáveis.

Como os esquemas acontecem: fases e técnicas recorrentes

Fases típicas de um esquema

Muitos esquemas seguem uma lógica de entrada, dispersão e retorno ao mercado. As fases abaixo ajudam a entender a dinâmica e a desenhar controles mais eficazes.

- **Colocação:** Introdução de recursos no sistema financeiro ou econômico, com tentativas de reduzir suspeitas (por exemplo, fracionamento, depósitos em espécie, uso de intermediários).
- **Ocultação:** Criação de camadas de transações para confundir a origem: transferências sucessivas, trocas de ativos, múltiplas contas e contrapartes, estruturas em mais de um país.
- **Integração:** Reintrodução do dinheiro na economia como se fosse legítimo: investimentos, aquisição de bens, negócios formais e aparentes receitas regulares.

Técnicas comuns observadas no mercado

- Empresas de fachada e uso de interpostas pessoas para movimentar valores.
- Transações imobiliárias para misturar recursos, justificar entradas e elevar complexidade.
- Jogos de azar e apostas para converter dinheiro em “ganhos” aparentemente legítimos.
- Transferências internacionais aproveitando diferenças regulatórias entre jurisdições.
- Criptoativos e serviços digitais que podem aumentar a velocidade e reduzir transparência.

Sinais de alerta por técnica

- Empresa com baixa atividade real, mas com movimentação financeira desproporcional.
- Compra/venda de ativos com valores incompatíveis ou sem justificativa de mercado.
- Movimentação internacional sem relação com fornecedores, clientes ou operação declarada.
- Conversões rápidas entre instrumentos financeiros sem propósito econômico aparente.
- Uso de múltiplas contas de terceiros com perfil financeiro inconsistente.

Abordagem baseada em risco e avaliação de risco

A abordagem baseada em risco orienta a instituição a aplicar controles proporcionais: maior rigor onde o risco é maior e processos mais simples onde o risco é menor. Isso torna o programa de PLD/FT mais eficiente e sustentável, especialmente quando há grande volume de clientes e transações.

Ciclo de gestão de risco em PLD/FT

- **Identificar riscos:** clientes, produtos/serviços, canais, contrapartes e geografias.
- **Avaliar e classificar:** definir critérios e pesos para chegar a um nível de risco (baixo, médio, alto) conforme metodologia interna.
- **Mitigar:** aplicar diligência, limites, aprovações e monitoramento adequados ao risco.
- **Monitorar continuamente:** revisar perfis e comportamentos; reclassificar quando houver mudança relevante.
- **Treinar pessoas:** capacitação adaptada ao papel de cada colaborador, com foco em detecção e escalonamento.

Fatores de risco: exemplos práticos

- **Cliente:** atividade econômica, histórico, estrutura societária, beneficiário final, perfil financeiro, volume e complexidade esperados.
- **Produto e serviço:** nível de anonimato, velocidade de liquidez, possibilidade de terceiros, complexidade contratual.
- **Canal:** abertura e movimentação remotas, intermediários, correspondentes, canais que reduzem contato direto.
- **Geografia:** jurisdições com lacunas regulatórias, alta incidência de crimes financeiros, sanções ou restrições relevantes.

Boas práticas de documentação

- Metodologia de risco documentada (critérios, pesos, fontes de informação e governança de revisão).
- Evidências de diligência e decisões registradas (por que foi classificado como alto risco, por exemplo).
- Histórico de revisões do perfil de risco e eventos que motivaram reclassificação.
- Rastreabilidade entre alertas, análises e decisões (o que foi visto, o que foi feito, por quê).

Estrutura de um programa de compliance em PLD/FT

Um programa de compliance em PLD/FT combina governança, políticas, processos e tecnologia para prevenir, detectar e responder a riscos. A efetividade do programa depende tanto do desenho quanto da execução no dia a dia.

Elementos essenciais

- Políticas e procedimentos claros, comunicados e atualizados.
- Controles internos e trilhas de auditoria (quem faz o quê, quando e como).
- Responsável por PLD/FT com autonomia e acesso à alta direção.
- Treinamento contínuo e adequado à função (linha de frente, operações, negócios, tecnologia, auditoria).
- Processo de KYC e diligências (simplificada, padrão e aprimorada).
- Monitoramento de transações e investigação de alertas, com critérios e evidências.
- Auditorias e revisões independentes para avaliar aderência e melhoria contínua.

Cultura e governança

- A alta direção apoia a política de PLD/FT e reforça comportamentos esperados.
- Metas e incentivos não estimulam “fechar os olhos” para riscos.
- Há canais de escalonamento e reporte interno sem retaliação.
- Indicadores (KPIs/KRIs) ajudam a enxergar efetividade, gargalos e qualidade das análises.

Conheça seu cliente (KYC) e avaliação prévia

KYC (Know Your Customer) reúne procedimentos para identificar e verificar clientes, compreender o propósito da relação comercial e definir o perfil de transações esperado. Um KYC bem feito reduz riscos, melhora a qualidade do monitoramento e dá base para decisões proporcionais.

Informações mínimas que costumam ser necessárias

- Identificação e verificação de identidade (pessoa física e jurídica), com documentos e fontes confiáveis.
- Endereço e dados de contato atualizados.
- Atividade econômica e ocupação, incluindo fonte de renda e/ou faturamento.
- Propósito da conta e natureza do relacionamento: por que o cliente precisa do produto/serviço?
- Perfil transacional esperado: volumes, frequência, moedas, contrapartes, canais e regiões.

Erros comuns (e como evitar)

- Tratar o KYC como checklist burocrático, sem avaliar coerência do perfil.
- Aceitar declarações sem evidência quando o risco exige comprovação.
- Não atualizar dados após mudanças relevantes (atividade, renda, sócios, beneficiário final).
- Não registrar o racional de decisões de risco e exceções.

Diligência aprimorada e Pessoas Expostas Politicamente (PEPs)

Diligência aprimorada é o conjunto de medidas reforçadas aplicadas quando o risco é elevado. Ela costuma ser acionada para perfis como PEPs, estruturas complexas, operações atípicas sem justificativa econômica clara ou exposição a jurisdições sensíveis.

Quem pode ser considerado PEP

De forma geral, PEP é a pessoa que ocupa ou ocupou funções públicas relevantes e, por isso, pode ter maior exposição a riscos de corrupção, conflitos de interesse ou abuso de influência. Dependendo da regra aplicável, também podem ser incluídos familiares, representantes e pessoas com vínculo próximo.

Medidas típicas de diligência aprimorada

- Coleta de informações adicionais sobre origem do patrimônio e origem dos recursos.
- Validação reforçada do beneficiário final e de vínculos com terceiros.
- Aprovação por instância sênior antes de iniciar ou manter o relacionamento.
- Monitoramento contínuo com maior granularidade e revisão de perfil mais frequente.
- Consulta a bases, listas de sanções e fontes públicas, respeitando regras de privacidade e governança interna.

Equilíbrio entre diligência e privacidade

- Aplicar o mínimo necessário de dados para o objetivo de prevenção e conformidade.
- Registrar a finalidade e a base de decisão para cada coleta de informação adicional.
- Controlar acesso interno e retenção de dados conforme política e legislação.
- Revisar periodicamente a necessidade de manter informações sensíveis.

COAF e a inteligência financeira no Brasil

No Brasil, o COAF atua como unidade de inteligência financeira, recebendo e analisando comunicações de operações suspeitas provenientes de setores obrigados. A partir dessas comunicações, são produzidas informações de inteligência que podem apoiar investigações e ações de combate a crimes financeiros.

Como isso se conecta ao trabalho das instituições

- Manter processos para identificar e registrar operações atípicas e suspeitas.
- Comunicar às autoridades competentes conforme regras e prazos aplicáveis (sem "alertar" o cliente, quando houver vedação).
- Cooperar com solicitações e preservar evidências e trilhas de auditoria.
- Atualizar políticas e controles diante de novas tipologias e tecnologias.

Pontos de atenção

- Qualidade da comunicação: informações completas, objetivas e rastreáveis.
- Consistência com políticas internas e com a avaliação de risco do cliente.
- Governança para decisões sensíveis (quem aprova, quem envia, como é documentado).
- Proteção de dados e sigilo: acesso restrito e registro de uso.

Políticas corporativas de PLD/FT

Políticas de PLD/FT definem o padrão mínimo de conduta e controle dentro da instituição. Elas descrevem responsabilidades, critérios de risco, procedimentos de diligência, monitoramento, escalonamento e comunicação, além de governança de atualização.

O que uma política robusta costuma cobrir

- Escopo: quais produtos, clientes e operações são abrangidos e quais áreas participam.
- Papéis e responsabilidades: linha de frente, operações, compliance, riscos, jurídico, auditoria e tecnologia.
- Critérios de risco e gatilhos de diligência (incluindo diligência aprimorada quando aplicável).
- Regras de KYC, atualização cadastral e tratamento de beneficiário final.
- Monitoramento, investigação e critérios de encerramento de alertas (com rastreabilidade).
- Regras de retenção de evidências, sigilo e proteção de dados.
- Plano de treinamento e comunicação interna.
- Rotina de auditoria e revisão independente.

Governança de atualização

- Calendário de revisão periódica (ou revisão acionada por evento: nova regra, nova tipologia, incidente).
- Controle de versão e registro de mudanças.
- Treinamento e comunicação quando houver atualização relevante.
- Teste de efetividade após mudanças importantes (regras, modelos, fluxos).

Monitoramento e reporte de operações suspeitas

Monitoramento é a prática de acompanhar transações e relacionamentos para identificar comportamentos atípicos e sinais de risco. Quando necessário, a análise evolui para investigação interna e comunicação às autoridades competentes, conforme regras aplicáveis.

Etapas comuns do processo

- Definição de regras e cenários de risco (baseados em tipologias, perfil do cliente e risco do produto).
- Geração de alertas (automação e/ou análise manual).
- Triagem: validar dados, eliminar falsos positivos óbvios, priorizar por risco.
- Investigação: reunir evidências, entender contexto, consultar histórico e contrapartes.
- Decisão e registro: encerrar com racional ou escalar para comunicação.
- Acompanhamento: monitoramento reforçado, revisão de perfil e melhorias de regras.

Qualidade da análise: perguntas-guia

- O comportamento faz sentido para a atividade e perfil declarado?
- Há mudanças abruptas em volume, frequência, contrapartes, regiões ou canais?
- Qual é a justificativa econômica? Existe documentação razoável?
- Há indícios de interposição de terceiros ou circularidade de valores?
- Quais evidências sustentam a conclusão (dados, documentos, logs, histórico)?

Desafios comuns (e como responder)

- Falsos positivos elevados: revisar regras, melhorar dados, calibrar limiares e priorização por risco.
- Privacidade e proteção de dados: aplicar minimização, controle de acesso e trilhas de auditoria.
- Cooperação internacional: garantir consistência de dados e rastreabilidade de contrapartes e jurisdições.
- Capacidade do time: automatizar triagem, padronizar relatórios e investir em treinamento.

Consequências da não conformidade

Falhas em PLD/FT podem gerar impactos financeiros, legais e reputacionais significativos. Além de multas e sanções, é comum haver restrições operacionais, necessidade de investimentos em controles e desgaste com clientes e parceiros.

Principais impactos

- Penalidades e sanções financeiras que afetam resultados e capital.
- Danos reputacionais com efeitos duradouros na confiança do mercado.
- Restrições operacionais, incluindo limitações de crescimento e exigências regulatórias adicionais.
- Aumento de custos com remediação (tecnologia, pessoas, consultorias, treinamentos).
- Litígios e compensações decorrentes de falhas de controle e governança.

Mentalidade preventiva

- Avaliar riscos de forma contínua e registrar mudanças de perfil.
- Investir em capacitação e cultura: a linha de frente é parte do controle.
- Revisar e testar periodicamente regras de monitoramento e fluxos de investigação.
- Tratar incidentes como fonte de aprendizado e melhoria, não apenas como “correção pontual”.

Casos práticos e lições aprendidas

Estudos de caso ajudam a enxergar padrões: onde os controles falham, como criminosos exploram lacunas e quais sinais surgem antes de um incidente relevante. O objetivo não é decorar casos, e sim reconhecer mecânicas recorrentes.

Padrões recorrentes em casos reais

- Uso de empresas de fachada e contrapartes em diferentes países para criar camadas de transações.
- Controles de clientes e transações insuficientes, principalmente em filiais, correspondentes ou canais menos supervisionados.
- Falhas de governança: exceções não documentadas, alertas ignorados, pressão comercial, baixa autonomia do compliance.
- Dificuldade de aplicar regras de forma consistente entre jurisdições e linhas de negócio.

Ferramentas práticas

Roteiro rápido para análise de um alerta

- Confirmar dados básicos: cliente, produto, canal, valor, data, contrapartes e jurisdição.
- Comparar com o perfil esperado: o que mudou e desde quando?
- Buscar contexto: documentação, contratos, notas, e-mails internos, histórico de relacionamento.
- Avaliar sinais de alerta: coerência econômica, interposição de terceiros, circularidade, fragmentação.
- Registrar evidências e racional: o que foi observado, o que foi concluído, qual base (dados/documentos).
- Decidir encaminhamento: encerrar, monitorar reforçado, solicitar atualização cadastral, escalar para comunicação.

Checklist de qualidade do registro

- A narrativa está clara e objetiva (o que aconteceu, por que é relevante, o que foi feito).
- Há dados suficientes para reproduzir a análise (IDs, datas, valores, contrapartes, prints/logs quando aplicável).
- As fontes foram registradas (sistemas consultados, documentos recebidos, bases utilizadas).
- A decisão está justificada e alinhada à política (sem lacunas ou "achismos").
- Foram registradas ações de acompanhamento (se houver), com responsável e prazo.

Glossário essencial

- **Abordagem baseada em risco:** Estratégia que direciona controles e recursos conforme a exposição a risco, aplicando medidas proporcionais.
- **Alerta:** Sinal gerado por regra, modelo ou análise que indica possível atipicidade e exige triagem/investigação.
- **Beneficiário final:** Pessoa(s) que, em última instância, controla(m) ou se beneficia(m) de uma empresa ou operação, mesmo que indiretamente.
- **Diligência aprimorada:** Conjunto de medidas reforçadas aplicadas quando o risco é elevado, incluindo verificações adicionais e monitoramento intensificado.
- **Falso positivo:** Alerta que parece suspeito inicialmente, mas após análise é explicado por motivo legítimo.
- **KYC:** Processo de conhecer o cliente: identificar, verificar e entender propósito e perfil de transações.
- **Lista de sanções/monitoramento:** Bases que consolidam restrições e alvos de atenção (sanções, vigilância), usadas para triagem e monitoramento conforme política.
- **PEP:** Pessoa exposta politicamente: indivíduo com função pública relevante (conforme regra aplicável), que pode demandar diligência reforçada.
- **PLD/FT:** Prevenção à lavagem de dinheiro e ao financiamento do terrorismo.
- **Unidade de inteligência financeira:** Órgão que recebe e analisa comunicações e produz inteligência financeira para apoiar prevenção e combate a crimes financeiros.

Leituras e consultas recomendadas

Para aprofundamento, consulte a legislação e regulamentação aplicáveis ao seu setor, além de guias e recomendações de organismos internacionais e autoridades locais. As regras e listas de jurisdições/sanções podem mudar; use fontes oficiais atualizadas.

- Recomendações e relatórios do GAFI/FATF (tipologias e boas práticas).
- Normas e circulares do regulador aplicável ao seu segmento (ex.: financeiro, mercado de capitais, seguros, etc.).
- Políticas internas e manuais operacionais de PLD/FT da instituição.
- Guias de privacidade e proteção de dados aplicáveis ao tratamento de informações em compliance.

Órgão / Norma	Objetivo da norma
Congresso Nacional – Lei nº 9.613/1998	Define o crime de lavagem de dinheiro, cria o COAF e estabelece obrigações de prevenção e comunicação de operações suspeitas.
CMN – Resolução nº 4.595/2017	Estabelecer diretrizes gerais de PLD/FT no sistema financeiro com base na abordagem baseada em risco.
Banco Central do Brasil – Circular nº 3.978/2020	Regulamentar procedimentos operacionais de cadastro, monitoramento e comunicação de operações suspeitas ao COAF.
Banco Central do Brasil – Carta Circular nº 4.001/2020	Apresentar exemplos de situações e operações que podem configurar indícios de lavagem de dinheiro ou financiamento do terrorismo.
Comissão de Valores Mobiliários – Resolução CVM nº 50/2021	Dispor sobre deveres de PLD/FT no mercado de capitais, alinhando corretoras, distribuidoras e gestoras à Lei 9.613.