

CNseg

PROGRAMA

EDUCAÇÃO EM SEGUROS

PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA E DE TECNOLOGIA DUAL (PLD/FTP)

REGULAÇÃO

CNseg

PROGRAMA

EDUCAÇÃO EM SEGUROS

PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E AO FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA E DE TECNOLOGIA DUAL (PLD/FTP)

REGULAÇÃO



Declaração de governança do documento

A nova edição deste livreto foi submetida à revisão técnica da Comissão de Governança e Compliance da Confederação Nacional das Seguradoras (CNseg), composta por executivos das associadas com ampla experiência na implementação de programas de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa e de Tecnologia Dual (PLD/FTP), em conjunto com a Superintendência de Acompanhamento Técnico da Confederação.

Esse processo assegura que o conteúdo reflita, de forma consistente, o arcabouço normativo vigente, as melhores práticas internacionais e os desafios operacionais enfrentados pelas entidades supervisionadas.

Ao integrar conhecimento regulatório, experiência prática e visão estratégica do setor, o material consolida-se como instrumento de apoio qualificado à governança, à gestão de riscos e à promoção de uma cultura de integridade alinhada às expectativas das autoridades supervisoras.

“Integridade é fazer a coisa certa, mesmo quando ninguém está olhando.”

C.S. Lewis

Sumário



Capítulo 1:

INTRODUÇÃO **8**

Da economia em espécie ao ambiente digital 9

Motivação da revisão: novos riscos em um ambiente digital 9

Relevância para o setor de seguros 11

Objetivo do livreto 11

Capítulo 2:

ESTRUTURA INSTITUCIONAL DA PREVENÇÃO **12**

Contexto geral 13

Marcos internacionais na evolução da prevenção 13

Coordenação e cooperação institucional 15

Principais organismos e referências institucionais 16

Autorregulação assistida: o Pacto Brasil pela Integridade Empresarial 19

Normas de PLD/FTP 21

Aspectos globais 21

Aspectos brasileiros 22

Fortalecimento do Combate aos Crimes Cibernéticos, Fraudes Digitais e Estruturas de Lavagem de Dinheiro 23

Novos instrumentos de combate às fraudes e seus impactos em PLD/FTP 25

Arcabouço regulatório no setor de seguros 26

Página da SUSEP sobre PLD/FTP: um recurso estratégico para o Setor 28

Capítulo 3:

CONCEITOS **30**

Tipificação do crime de lavagem de dinheiro na Lei nº 9.613/1998 31

Conceitos fundamentais em PLD/FTP 33

Etapas da lavagem de dinheiro 38

Dinâmica e variações operacionais 40
Como as empresas atuam na prevenção e no combate à LD/FT 41
Adequação a ambientes digitais e inovação tecnológica 42
Consequências e penalidades previstas na legislação 44
Responsabilização de pessoas físicas e jurídicas 44
Sanções administrativas 45
Abrangência do regime de PLD/FTP 45
Financiamento do terrorismo 46
Pessoas Politicamente Expostas ... 47
Como saber se um cliente é PEP? 48
Serviço CNseg: Sistema de Prevenção à Lavagem de Dinheiro (SIPLAV) 49
ASG e sua relação com PLD/FTP 49
Governança como elemento central 50
Ampliação da *due diligence* e visão de risco 51
Riscos emergentes e integridade de mercado 51
Padrões internacionais de divulgação e transparência 51

Capítulo 4:

Novas Tecnologias, Novos Modelos de Negócio e seus Impactos na PLD/FTP 52

Transformação digital e seus impactos na PLD/FTP 54
Impactos sobre os modelos de prevenção 54
Desafios regulatórios e necessidade de adaptação 55
Sociedades processadoras da ordem do cliente - SPOCs (art. 36-A do DL 73/66 – LC 213/2025) 57
Novas operações de cooperativas e proteção patrimonial mutualista (LC 213/2025) 58
PLD/FTP no Contexto de *Open Finance* e *Open Insurance* 61



Sumário

Capítulo 5:

Integração no combate à lavagem de dinheiro e os reflexos para o setor de seguros 64

Integração como resposta à complexidade crescente 65

Capacidades ampliadas pela integração 66

Implicações para o setor de seguros 66

Alinhamento internacional e consistência regulatória 67

Integração entre supervisão e PLD/FTP 67

Implicações para as estruturas internas 67

Outros órgãos reguladores 68

CVM 68

BACEN 69





Capítulo 6:

O Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa e de Tecnologia Dual (PLD/FTP) 72

Estrutura do Programa de PLD/FTP 73

Os papéis e responsabilidades das três linhas: prevenção como responsabilidade compartilhada ... 77

1ª linha: gestão do risco na origem 77

2ª linha: coordenação, supervisão e integração do risco ... 78

3ª linha: avaliação independente ... 79

Importância de conhecer os clientes e suas operações 80

Monitoramento de operações e a importância da compatibilidade 84

Listas impeditivas, restritivas e sanções: base estruturante do controle de PLD/FT 86

Monitoramento e seleção de operações 88

Comunicações ao Coaf 90

Importância de políticas e manuais 92

Avaliação Interna de Riscos 92

Auditoria 94

Relatório de Efetividade do Programa de PLD/FTP 95

Capítulo 7:

AVALIAÇÃO NACIONAL DE RISCOS (ANR) 96

Vulnerabilidade do setor de seguros 97

Evolução das comunicações de operações suspeitas e efeitos da mudança regulatória 98

Capítulo 8:

CONCLUSÃO 102

REFERÊNCIAS NORMATIVAS E INSTITUCIONAIS 104

Legislação Federal 104

Normativos da SUSEP e CNSP 104

Banco Central do Brasil (BCB) 105

Comissão de Valores Mobiliários (CVM) 105

Agência Nacional de Saúde Suplementar (ANS) 105

Superintendência Nacional de Previdência Complementar (Previc) 105

Organismos Internacionais 106

Órgãos e Instituições Nacionais .. 106

Sustentabilidade, Governança e Divulgação 106

INSTITUCIONAL 107





Introdução

Capítulo 1

Da economia em espécie ao ambiente digital

A PLD/FTP assumiu papel central na agenda regulatória e na gestão de riscos das instituições.

Esse movimento reflete a crescente sofisticação das práticas ilícitas, a digitalização dos serviços financeiros e a evolução dos modelos de negócio, fatores que ampliam a velocidade, a fragmentação e a complexidade das transações.

Nesse contexto, a atuação preventiva ultrapassa o cumprimento formal de obrigações normativas e passa a exigir a implementação de estruturas integradas de governança, gestão de riscos, controles internos e monitoramento contínuo, alinhadas a uma abordagem baseada em risco.

Motivação da revisão: novos riscos em um ambiente digital

Historicamente, o rastreamento de atividades ilícitas esteve fortemente associado à circulação de recursos em espécie, caracterizada por movimentações físicas, depósitos fracionados e padrões relativamente identificáveis.

A digitalização dos pagamentos transformou profundamente essa dinâmica. A adoção de transferências instantâneas, carteiras digitais, pagamentos por QR code, autenticação biométrica e contratação remota ampliou significativamente a eficiência do sistema financeiro, ao mesmo tempo em que introduziu novos riscos e desafios para a prevenção de ilícitos financeiros.

Nesse ambiente, as transações ocorrem em tempo real, frequentemente sem barreiras geográficas e com elevado grau de automação, exigindo mecanismos de controle mais sofisticados e baseados em dados. Estudos recentes indicam que instituições financeiras e entidades supervisionadas vêm priorizando investimentos em cibersegurança, prevenção de fraudes e validação digital de clientes, reconhecendo a necessidade de adaptação contínua diante da evolução tecnológica.

A prevenção à lavagem de dinheiro deixa, assim, de se limitar ao acompanhamento de fluxos financeiros tradicionais e passa a demandar a compreensão de padrões comportamentais, estruturas digitais e vulnerabilidades tecnológicas.



Organizações terroristas frequentemente operam de forma transnacional, utilizando múltiplas jurisdições e intermediários para fragmentar fluxos financeiros e dificultar sua identificação.

Essa transformação impacta igualmente o combate ao financiamento do terrorismo, que pode ocorrer por meio de transferências de pequeno valor, doações online, campanhas digitais e uso de plataformas de pagamento instantâneo ou redes informais de transferência de recursos. Diferentemente da lavagem de dinheiro, os recursos destinados ao terrorismo podem ter origem lícita, o que exige análise baseada no propósito das operações, no comportamento do cliente e em fatores contextuais.

Além disso, organizações terroristas frequentemente operam de forma transnacional, utilizando múltiplas jurisdições e intermediários para fragmentar fluxos financeiros e dificultar sua identificação. Nesse cenário, ganham relevância a cooperação internacional e o cumprimento de sanções financeiras direcionadas estabelecidas pelo Conselho de Segurança das Nações Unidas.

As Recomendações do Grupo de Ação Financeira (GAFI/FATF) estabelecem o padrão internacional para o enfrentamento desses riscos. Destacam-se, nesse contexto, a Recomendação 1 (abordagem baseada em risco), a Recomendação 6 (sanções financeiras direcionadas), a Recomendação 10 (identificação e verificação de clientes), a Recomendação 15 (novas tecnologias) e a Recomendação 16 (rastreamento de transferências eletrônicas).

Relevância para o setor de seguros

No setor de seguros, determinados produtos apresentam maior suscetibilidade à utilização em práticas de lavagem de dinheiro e financiamento do terrorismo, especialmente aqueles com componente financeiro e possibilidade de acumulação de valores elevados ou movimentação de recursos ao longo do tempo.

Entre esses produtos, podem ser citados os seguros de vida resgatáveis, os planos de previdência complementar aberta (Vida Gerador de Benefício Livre – VGBL; e Plano Gerador de Benefício Livre – PGBL), a capitalização e as operações com beneficiários designados, portabilidades, resgates antecipados e pagamentos de benefícios. Tais características podem ser utilizadas para a introdução, a movimentação ou a integração de recursos ilícitos, bem como para a transferência indireta de valores a terceiros.

Adicionalmente, operações envolvendo múltiplos beneficiários, interposição de pessoas ou estruturas contratuais complexas podem aumentar a dificuldade de identificação de padrões atípicos, exigindo análise mais aprofundada por parte das entidades supervisionadas.

Nesse contexto, a abordagem baseada em risco se mostra essencial, permitindo que as instituições identifiquem, avaliem e mitiguem continuamente suas exposições, ajustando políticas, procedimentos e controles à natureza, ao porte e à complexidade de suas operações.

Objetivo do livreto

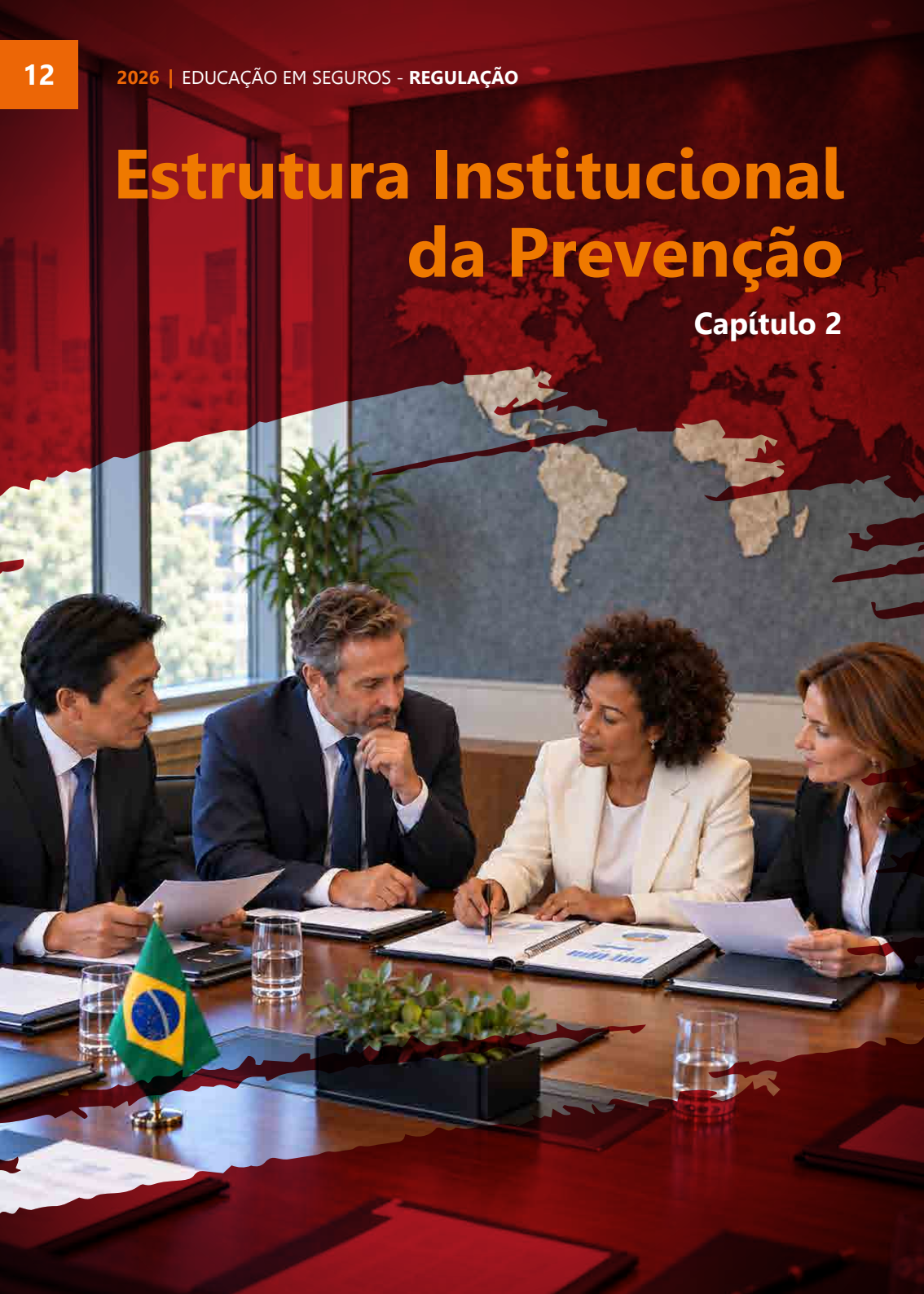
Diante desse cenário, este livreto tem como objetivo oferecer um referencial técnico e prático para apoiar as instituições na compreensão e no aprimoramento de seus programas de PLD/FTP.

Ao consolidar conceitos, diretrizes regulatórias e experiências do setor, o material busca contribuir para o fortalecimento da governança, da gestão de riscos e da efetividade dos controles, em consonância com os padrões internacionais e as expectativas das autoridades supervisoras.

Mais do que um instrumento informativo, trata-se de um material de apoio à atuação consistente e proporcional das entidades supervisionadas, reforçando o compromisso do setor de seguros com a conformidade, a integridade, a transparência e a confiança no sistema financeiro.

Estrutura Institucional da Prevenção

Capítulo 2



Contexto geral

A PLD/FTP consolidou-se como uma agenda prioritária nos âmbitos internacional e nacional, refletindo o reconhecimento de que a integridade dos sistemas financeiros depende de estruturas eficazes de regulação, supervisão e controle.

A crescente sofisticação das práticas ilícitas, associada à digitalização dos serviços financeiros e à natureza transnacional dos fluxos de recursos, exige respostas coordenadas entre diferentes jurisdições e setores econômicos. Nesse contexto, a atuação integrada entre organismos internacionais, autoridades nacionais e entidades supervisionadas é essencial para a efetividade das medidas de prevenção.

Marcos internacionais na evolução da prevenção

A estrutura atual de prevenção é resultado de um processo evolutivo impulsionado por convenções internacionais que consolidaram compromissos entre os países para o enfrentamento desses ilícitos.

Entre as iniciativas mais relevantes, destaca-se a Convenção de Viena (1988), considerada o marco inicial no enfrentamento da lavagem de dinheiro associada ao tráfico ilícito de entorpecentes. Os países signatários, incluindo o Brasil, assumiram o compromisso de tipificar essa conduta em seus ordenamentos jurídicos, estabelecendo as bases para a construção de legislações nacionais voltadas à prevenção desses ilícitos.

A partir desse marco, os modelos normativos evoluíram progressivamente, refletindo o aprimoramento do entendimento sobre a dinâmica do crime e a ampliação do conceito de infrações penais antecedentes.

Nos anos subsequentes, novas convenções e iniciativas internacionais foram desenvolvidas com o objetivo de fortalecer o sistema global de prevenção, ampliando seu escopo para abarcar outras formas de ilicitude, como a corrupção e o crime organizado transnacional, e consolidando uma abordagem mais integrada e abrangente no combate aos ilícitos financeiros.



Entre as principais iniciativas, destacam-se:

i. Convenção de Estrasburgo (1993) — convenção sobre a prevenção à lavagem de dinheiro — teve como objetivo estabelecer critérios para a apreensão e o confisco dos produtos do crime.

ii. Convenção Interamericana contra a Corrupção (1996) — primeiro movimento internacional de combate à corrupção — determinou não apenas medidas preventivas, mas também medidas punitivas em resposta aos atos de corrupção.

iii. Convenção da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) (1997) — entrou em vigor em 1999, tendo como principais objetivos combater e prevenir a corrupção de funcionários públicos estrangeiros.



O Brasil incorporou a Convenção ao seu ordenamento jurídico com a promulgação do Decreto Presidencial nº 3.678/2000 e comprometeu-se a criar uma Lei Anticorrupção. Apenas 13 anos depois, em 2013, surgiu a Lei Anticorrupção Brasileira (Lei nº 12.846/2013).

iv. Convenção Internacional para a Supressão do Financiamento do Terrorismo (1999) — estabeleceu a criminalização do financiamento do terrorismo e medidas para o rastreamento, o bloqueio e a cooperação internacional para a identificação de fluxos financeiros destinados a atividades terroristas.

v. Convenção de Palermo (2000) — Convenção das Nações Unidas contra o Crime Organizado Transnacional — entrou em vigor em 2003 e foi promulgada pelo Brasil em 2004.

vi. Convenção Interamericana contra o Terrorismo (2002) — visou prevenir o financiamento de atividades terroristas, reforçando o controle de fronteiras e aumentando a cooperação entre as forças policiais de diferentes países. O Brasil promulgou essa convenção em 2005.

vii. Convenção de Mérida (2003) — Convenção das Nações Unidas contra a Corrupção — entrou em vigor em 2005. Define os

procedimentos para a prevenção e a detecção de transferências de ativos oriundos de atos ilícitos, além de medidas para sua recuperação e métodos de cooperação internacional. Visa promover e intensificar as medidas de combate à corrupção, bem como fortalecer a integridade e a responsabilidade na gestão dos assuntos públicos. Por essa razão, prevê a figura da pessoa politicamente exposta (PEP). Foi promulgada pelo Brasil em 2006.

viii. Convenção de Varsóvia (2005) — ampliou os instrumentos internacionais para a prevenção à lavagem de dinheiro e ao financiamento do terrorismo, incluindo mecanismos de cooperação internacional e monitoramento de transações financeiras.

Em conjunto, essas convenções formaram a base do arcabouço internacional de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e de combate à corrupção, influenciando diretamente a legislação e os sistemas de controle dos países. A evolução desse regime demonstra uma transição de um enfoque restrito ao narcotráfico para um modelo abrangente, baseado em risco, cooperação internacional e monitoramento contínuo de fluxos financeiros ilícitos.

Coordenação e cooperação institucional

A efetividade dos padrões internacionais de PLD/FTP está diretamente associada à existência de mecanismos estruturados de coordenação e cooperação entre países, autoridades e instituições.

Nesse contexto, a atuação articulada entre organismos internacionais e autoridades nacionais é essencial para assegurar a convergência regulatória, a consistência das práticas de supervisão e a capacidade de resposta a riscos de natureza transnacional, dinâmica e tecnológica.

Os órgãos supervisores desempenham papel central nesse arranjo, sendo responsáveis por estabelecer diretrizes normativas, acompanhar o cumprimento das obrigações pelas instituições supervisionadas e promover ações de fiscalização e aplicação de normas (*enforcement*). Sua atuação busca assegurar a adoção de práticas de gestão de riscos compatíveis com os padrões internacionais e com o arcabouço normativo vigente.

No Brasil, essas diretrizes são internalizadas por autoridades reguladoras como o Banco Central do Brasil (BCB), a Comissão de Valores Mobiliários (CVM), a Superintendência de Seguros Privados (SUSEP), a Agência Nacional de Saúde Suplementar (ANS) e a Superintendência Nacional de

Previdência Complementar (Previc), que estabelecem normas específicas e exercem a supervisão das instituições sob sua competência, com base em uma abordagem proporcional ao risco.

No âmbito da inteligência financeira, o Conselho de Controle de Atividades Financeiras (Coaf) desempenha função central ao receber, analisar e disseminar comunicações de operações suspeitas, contribuindo para a produção de inteligência e para o suporte às autoridades competentes.

No setor de seguros, a atuação da SUSEP é complementada por sua articulação institucional com outros órgãos e por sua participação em instâncias de coordenação nacional, como a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA). Esse modelo integrado contribui para o alinhamento regulatório, o intercâmbio de informações e a atuação coordenada diante de riscos que ultrapassam os limites setoriais e jurisdicionais.

Principais organismos e referências institucionais

A estrutura de PLD/FTP é sustentada por um conjunto amplo de organismos internacionais, entidades de cooperação e instituições de referência, cujas diretrizes contribuem para a consolidação de padrões, o fortalecimento institucional e a disseminação de boas práticas.

Para fins de organização, destacam-se os principais organismos, agrupados conforme sua natureza de atuação:

a) Organismos internacionais de padronização e supervisão

- Grupo de Ação Financeira (GAFI/FATF): responsável pela definição de padrões internacionais por meio de suas 40 Recomendações, que orientam a estruturação dos sistemas nacionais de PLD/FTP e o monitoramento de sua efetividade.



- Associação Internacional de Supervisores de Seguros (*International Association of Insurance Supervisors* - IAIS): estabelece princípios globais de supervisão do setor de seguros, incluindo diretrizes relacionadas à governança, à gestão de riscos e à prevenção à lavagem de dinheiro.

- Comitê de Supervisão Bancária de Basileia (*Basel Committee on Banking Supervision* – BCBS): desenvolve padrões prudenciais e recomendações voltadas à solidez do sistema bancário internacional, amplamente adotadas como referência regulatória.

- Organização Internacional das Comissões de Valores (*International Organization of Securities Commissions* - IOSCO): promove o desenvolvimento, a integridade e a regulação dos mercados de valores mobiliários, com foco na harmonização de práticas entre jurisdições.

b) Organismos multilaterais e de cooperação internacional

- Organização das Nações Unidas (ONU): atua por meio de convenções, resoluções do Conselho de Segurança e programas especializados, estabelecendo diretrizes globais para o combate à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção.

- Fundo Monetário Internacional (FMI): contribui para a estabilidade financeira global e, desde os anos 2000, incorpora a agenda de PLD/FTP em suas avaliações e programas de assistência técnica.

- Banco Mundial: atua no apoio técnico e financeiro aos países, incluindo o fortalecimento de capacidades institucionais relacionadas à prevenção de ilícitos financeiros.

- Grupo Egmont: reúne unidades de inteligência financeira (*Financial Intelligence Units* - FIUs) para promover o intercâmbio seguro de informações e apoiar investigações transnacionais.

- Organização International de Polícia Criminal (*The Internacional Criminal Police Organization* - INTERPOL): apoia a cooperação policial internacional no combate ao crime organizado, incluindo lavagem de dinheiro e financiamento do terrorismo.

c) Organismos regionais e iniciativas de articulação

- *Grupo de Acción Financiera de Latinoamérica* (GAFILAT): promove a implementação das Recomendações do GAFI/FATF na América Latina e realiza avaliações mútuas dos países membros.

- ENCCLA: iniciativa brasileira que articula órgãos dos três Poderes e

entidades da sociedade civil para aprimorar políticas públicas e fortalecer a atuação coordenada no combate a ilícitos financeiros.

d) Referências de boas práticas e governança

- Comitê das Organizações Patrocinadoras da Comissão *Treadway* (*Committee of Sponsoring Organizations of the Treadway Commission* - COSO): referência global em controles internos, gestão de riscos e governança corporativa.

- Wolfsberg Group: desenvolve princípios e diretrizes para a prevenção à lavagem de dinheiro, especialmente em temas relacionados ao procedimento Conheça seu Cliente (*Know Your Customer* – KYC) e ao monitoramento de transações.

e) Autoridades e estruturas nacionais relevantes

- Coaf: unidade de inteligência financeira responsável por receber, analisar e disseminar comunicações de operações suspeitas, por meio de Relatórios de Inteligência Financeira (RIFs).

- SUSEP: responsável pela regulação e supervisão dos mercados de seguros, previdência complementar aberta, capitalização, resseguros e proteção patrimonial mutualista, além da atividade de corretagem de seguros, incluindo a implementação de normas de PLD/FTP.

- Conselho Nacional de Seguros Privados (CNSP): estabelece as diretrizes gerais da política de seguros privados no País.

- BCB e CVM: responsáveis pela regulação e supervisão de seus respectivos segmentos, com normativos específicos de PLD/FTP.

- PREVIC: responsável por licenciar, orientar, supervisionar e fiscalizar as Entidades Fechadas de Previdência Complementar (EFPC).

A atuação complementar desses organismos e instituições contribui para a consolidação de um sistema de prevenção robusto, baseado em padrões internacionais, cooperação institucional e supervisão efetiva. Esse arranjo é essencial para a mitigação de riscos associados a ilícitos financeiros e para a preservação da integridade e da estabilidade do sistema econômico.



Autorregulação assistida: o Pacto Brasil pela Integridade Empresarial

O Pacto Brasil pela Integridade Empresarial, iniciativa da Controladoria-Geral da União (CGU), constitui instrumento de promoção da ética, da transparência e da governança no ambiente corporativo brasileiro.

De adesão voluntária, o Pacto estabelece compromisso público das organizações com a prevenção da corrupção, o fortalecimento de programas de integridade e a adoção de práticas alinhadas às melhores referências nacionais e internacionais.

Inserido no contexto das políticas públicas de integridade privada, o Pacto busca fomentar uma cultura organizacional orientada à conformidade, à responsabilidade e à confiança, contribuindo para o fortalecimento do ambiente de negócios.



A adesão ocorre mediante assinatura de termo formal e preenchimento de instrumento de autoavaliação estruturada, que permite à organização analisar o grau de maturidade de seu programa de integridade.

Esse diagnóstico abrange, entre outros aspectos:

- comprometimento da alta administração (*tone at the top* – "tom que vem do topo");
- gestão de riscos de integridade;
- políticas e controles internos;
- canais de denúncia e mecanismos de apuração;
- ações de treinamento e comunicação;
- monitoramento e melhoria contínua.

É importante destacar que o Pacto não se configura como certificação governamental nem substitui auditorias regulatórias, tratando-se de mecanismo de autorregulação assistida voltado ao aprimoramento contínuo das práticas empresariais.

Para os mercados de seguros, previdência complementar aberta, capitalização e resseguros, a iniciativa apresenta relevância específica, considerando a natureza fiduciária das atividades e o nível de supervisão prudencial e comportamental exercido pela SUSEP.

As entidades supervisionadas já se submetem a um conjunto robusto de exigências relacionadas à governança corporativa, à gestão de riscos, aos controles internos e à PLD/FTP.

Nesse contexto, o Pacto atua como instrumento complementar, ao:

- reforçar o compromisso institucional com padrões de integridade;
- evidenciar alinhamento com diretrizes regulatórias e referências internacionais;
- estimular o aprimoramento contínuo dos programas de *compliance* (conformidade);
- contribuir para a mitigação de riscos reputacionais e operacionais.

A adesão ao Pacto dialoga com estruturas já consolidadas nas instituições supervisionadas, como:

- sistemas de gestão de riscos corporativos;
- programas de *compliance* e integridade;
- controles de prevenção de fraudes;
- mecanismos de PLD/FTP;
- políticas de conduta e governança.

Nesse sentido, o Pacto pode funcionar como instrumento de consolidação e demonstração dessas práticas, reforçando a transparência institucional e a consistência das estruturas de governança.

Embora não produza efeitos regulatórios diretos, a adesão ao Pacto pode contribuir para o fortalecimento da governança corporativa e da transparência das organizações, em linha com as expectativas de reguladores, investidores e demais partes interessadas (*stakeholders*).

Em um ambiente regulatório orientado à gestão de riscos e à conduta responsável, tais elementos reforçam a confiança no setor e contribuem para a integridade do sistema econômico.



Normas de PLD/FTP

Aspectos globais

Os primeiros marcos normativos relacionados à prevenção à lavagem de dinheiro remontam ao final da década de 1970. Um dos registros iniciais é a legislação italiana de 1978, editada em resposta à atuação de grupos terroristas, evidenciando, já naquele momento, a relação entre fluxos financeiros ilícitos e a criminalidade organizada.

Na década de 1980, os Estados Unidos avançaram de forma estruturada com a promulgação do *Money Laundering Control Act* (1986), que tipificou a lavagem de dinheiro como crime autônomo. Nos anos subsequentes, novas legislações foram editadas com o objetivo de aprimorar os mecanismos de prevenção, incluindo o *Money Laundering Suppression Act* (1994) e o *Money Laundering and Financial Crimes Strategy Act* (1998).

Os atentados de 11 de setembro de 2001 representaram um ponto de inflexão na agenda global, impulsionando a adoção de medidas mais abrangentes e rigorosas. Nesse contexto, destaca-se o *USA PATRIOT Act* (2001), que introduziu avanços relevantes, entre os quais:

- fortalecimento de políticas, procedimentos e controles internos;
- vedação à manutenção de relações com shell banks (bancos sem presença física);
- ampliação da cooperação e do intercâmbio de informações;
- expansão do rol de crimes relacionados à lavagem de dinheiro;
- ampliação dos poderes de bloqueio de ativos e monitoramento de transações;
- estímulo à comunicação de operações suspeitas, com proteção às instituições que realizam essas comunicações;
- reforço dos controles sobre operações financeiras de maior valor.

Na sequência, iniciativas como o *Intelligence Reform and Terrorism Prevention Act* (2004) contribuíram para consolidar a arquitetura institucional voltada à prevenção de ilícitos financeiros em nível global.

Esse processo evolutivo reflete o reconhecimento da necessidade de estruturas regulatórias capazes de responder a ameaças cada vez mais complexas, transnacionais e tecnologicamente sofisticadas.

Aspectos brasileiros

A evolução normativa da prevenção à lavagem de dinheiro no Brasil acompanhou o movimento internacional de ampliação do escopo do crime e de fortalecimento dos mecanismos de controle.

Inicialmente, as legislações de primeira geração restringiam a criminalização à lavagem de recursos provenientes do narcotráfico. Posteriormente, as leis de segunda geração passaram a considerar um rol específico de infrações penais antecedentes — modelo adotado pela Lei nº 9.613/1998, que representou o primeiro marco legal brasileiro sobre o tema.

A Lei nº 9.613/1998 estruturou os principais pilares do sistema nacional, ao estabelecer obrigações relacionadas à identificação de clientes, ao registro de operações, à comunicação de atividades suspeitas, à responsabilização administrativa e à criação do Coaf. Ainda que baseada em um rol taxativo de crimes antecedentes, essa legislação já refletia o reconhecimento da natureza transversal da lavagem de dinheiro.

Com a edição da Lei nº 12.683/2012, o ordenamento jurídico brasileiro passou a adotar o modelo de terceira geração, eliminando o rol taxativo de crimes antecedentes e permitindo que a lavagem de dinheiro tenha como origem qualquer infração penal. Essa alteração ampliou significativamente o alcance da legislação e alinhou o País às melhores práticas internacionais.

Além da ampliação conceitual, a reforma de 2012 fortaleceu o regime preventivo, com destaque para:

- ampliação do rol de pessoas obrigadas;
- aprimoramento dos mecanismos de cooperação institucional;
- reforço das obrigações de identificação, monitoramento e comunicação.

No âmbito das sanções internacionais, a Lei nº 13.810/2019 consolidou o regime de cumprimento de sanções impostas pelo Conselho de Segurança das Nações Unidas, estabelecendo a obrigatoriedade de indisponibilização de ativos de pessoas naturais e jurídicas designadas.

Essas medidas devem ser implementadas de forma imediata, sem necessidade de autorização judicial prévia ou de notificação ao titular dos ativos.

Nesse contexto, as entidades supervisionadas devem adotar mecanismos capazes de identificar, monitorar e bloquear, sem demora, ativos e operações envolvendo pessoas ou entidades sancionadas, abrangendo tanto a titularidade direta quanto a indireta.

Fortalecimento do Combate aos Crimes Cibernéticos, Fraudes Digitais e Estruturas de Lavagem de Dinheiro

O avanço da digitalização dos serviços financeiros, securitários e de pagamentos trouxe ganhos relevantes de eficiência, inclusão e conveniência para consumidores e instituições. Ao mesmo tempo, esse novo ambiente ampliou significativamente a sofisticação e a escala de atuação de organizações criminosas especializadas em fraudes eletrônicas, golpes digitais e mecanismos de ocultação de recursos ilícitos.

Nesse contexto, a publicação da Lei nº 15.397/2026 representa um marco relevante no fortalecimento da política nacional de prevenção e repressão aos crimes cibernéticos e às estruturas utilizadas para a lavagem de dinheiro no ambiente digital. A lei promove importante atualização do arcabouço penal brasileiro ao reconhecer que o combate à criminalidade financeira contemporânea exige atuação não apenas sobre o autor direto da fraude, mas também sobre toda a infraestrutura operacional e financeira que viabiliza a prática criminosa.

Entre os principais avanços trazidos pela nova legislação, destacam-se o endurecimento das penas relacionadas a fraudes eletrônicas, furtos mediante fraude digital, invasões de dispositivos informáticos e ataques contra serviços telemáticos e infraestruturas digitais essenciais. A legislação passa a reconhecer expressamente a gravidade de práticas realizadas mediante a utilização de redes sociais, aplicativos, engenharia social, programas maliciosos e mecanismos tecnológicos destinados à obtenção ilícita de recursos financeiros.

Especial relevância deve ser atribuída à tipificação específica da chamada "conta laranja", mecanismo amplamente utilizado em estruturas de fraude eletrônica e lavagem de dinheiro. A criminalização da cessão, da disponibilização ou do aluguel de contas bancárias para a movimentação de recursos ilícitos demonstra clara convergência entre a política criminal e os mecanismos regulatórios de PLD/FT.

Sob a perspectiva regulatória e de integridade financeira, a nova legislação reforça a importância de controles robustos de:

- KYC;
- monitoramento transacional;
- detecção de comportamentos atípicos;
- prevenção de fraudes;
- rastreamento de movimentações incompatíveis com o perfil econômico do cliente;
- identificação de contas utilizadas como instrumentos de circulação e ocultação de recursos ilícitos.



Nesse cenário, ganha ainda mais relevância a abordagem baseada em risco consolidada no setor supervisionado pela SUSEP, especialmente a partir da Circular SUSEP nº 612/2020, que promoveu importante evolução regulatória ao substituir modelos excessivamente prescritivos por mecanismos mais aderentes à efetiva gestão de riscos de lavagem de dinheiro, financiamento do terrorismo e fraude, preservada pela nova Resolução do Conselho Nacional de Seguros Privados (CNSP) nº 99, publicada em 2 de outubro de 2026 e em vigor a partir de 1º de janeiro de 2027.

A experiência recente demonstra que modelos regulatórios excessivamente formais e baseados em comunicações massificadas tendem a produzir elevado volume de registros com baixa efetividade operacional e reduzida capacidade investigativa. Em contrapartida, abordagens centradas em inteligência, segmentação de risco, monitoramento contínuo e análise contextual das operações contribuem para elevar significativamente a qualidade das comunicações encaminhadas às autoridades competentes.

Nesse sentido, o fortalecimento das estruturas de governança, integridade, segurança cibernética e monitoramento operacional passa a desempenhar papel estratégico não apenas para o atendimento regulatório, mas também para a proteção da estabilidade, da confiança institucional e da integridade do sistema financeiro e securitário nacional.

A evolução promovida pela Lei nº 15.397/2026 reforça, portanto, a necessidade de contínuo aperfeiçoamento da cooperação entre órgãos reguladores, instituições supervisionadas, unidades de inteligência financeira e autoridades de persecução penal, consolidando uma atuação coordenada no enfrentamento das novas dinâmicas da criminalidade digital e financeira.

Novos instrumentos de combate às fraudes e seus impactos em PLD/FTP

A Lei nº 15.397/2026 alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), promovendo o aumento das penas aplicáveis a diversos crimes patrimoniais, entre eles furto, roubo, estelionato e receptação, além de reforçar o tratamento penal de condutas relacionadas às fraudes praticadas em ambiente digital.

Embora não seja uma norma específica de PLD/FTP nem estabeleça novas obrigações diretas para as seguradoras e demais entidades supervisionadas, a Lei nº 15.397/2026 apresenta aspectos relevantes sob a perspectiva dos controles de prevenção. Entre eles, destacam-se o agravamento das penas aplicáveis às fraudes eletrônicas e a tipificação da cessão de contas bancárias para a movimentação de recursos relacionados a atividades criminosas, prática conhecida como utilização de "contas laranja".

Entre as principais alterações promovidas estão o aumento das penas para os crimes de furto, roubo, estelionato e receptação e o agravamento das penas relacionadas ao furto mediante fraude praticado por meio eletrônico ou informático e à fraude eletrônica. A lei também incluiu no art. 171, § 2º, inciso VII, do Código Penal a denominada "cessão de conta laranja", alcançando aquele que cede, de forma gratuita ou onerosa, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou provenientes dessa atividade.

A nova tipificação é especialmente relevante para o sistema de PLD/FTP, pois reconhece expressamente a utilização consciente de contas de terceiros como instrumento para a circulação de recursos relacionados à prática criminosa. Esse mecanismo pode dificultar a identificação da origem, da destinação e dos efetivos beneficiários dos valores, além de contribuir para o distanciamento dos recursos em relação ao crime que lhes deu origem.

É importante observar, contudo, que a cessão ou a utilização de conta de terceiro não configura, por si só, lavagem de dinheiro. A conta pode ser utilizada como instrumento para o recebimento ou a transferência dos recursos no próprio contexto da prática criminosa ou, em momento posterior, integrar operações destinadas a ocultar ou dissimular sua natureza, origem, localização, disposição, movimentação ou propriedade. A caracterização do crime de lavagem de dinheiro dependerá, portanto, das circunstâncias concretas e da presença dos elementos previstos na Lei nº 9.613/1998.

Sob a perspectiva de PLD/FTP, a inovação legislativa reforça a importância da análise não apenas da titularidade formal das contas envolvidas nas operações, mas também

da coerência entre as partes, da origem e da destinação dos recursos e da existência de justificativa econômica para a participação de terceiros.

Embora a Lei nº 15.397/2026 se refira especificamente à cessão de conta bancária, a dinâmica de utilização de terceiros para movimentar recursos pode contribuir para a avaliação de riscos relacionados a pagamentos, recebimentos e demais fluxos financeiros vinculados a produtos de seguros, previdência complementar aberta e capitalização. Situações envolvendo pagamentos realizados por terceiros, indicação de contas sem vínculo aparente com as partes da operação ou alterações atípicas de dados bancários, por exemplo, podem constituir elementos adicionais para análise no âmbito dos procedimentos de monitoramento e da abordagem baseada em risco.

Arcabouço regulatório no setor de seguros

Para dar cumprimento à legislação nacional, os órgãos reguladores passaram a editar normas específicas estabelecendo obrigações de PLD/FTP para as entidades sob sua supervisão.

No setor de seguros, a atuação da SUSEP está alinhada aos padrões internacionais definidos pela IAIS, especialmente aos *Insurance Core Principles* (Princípios Básicos dos Seguros — ICPs), que constituem referência global para a supervisão prudencial e a governança das seguradoras.

Destaca-se o ICP 22, que trata da prevenção à lavagem de dinheiro e ao financiamento do terrorismo, estabelecendo que o supervisor deve assegurar a implementação de controles efetivos baseados em risco, incluindo:

- identificação e verificação de clientes e beneficiários finais;
- monitoramento contínuo de operações;
- comunicação tempestiva de atividades suspeitas;
- estrutura adequada de governança e controles internos.

No Brasil, esses requisitos encontram respaldo, entre outros instrumentos, na Resolução SUSEP nº 99/2026, alinhada às Recomendações do Grupo de Ação Financeira (GAFI/FATF), que substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027.

Esse alinhamento abrange, entre outros aspectos:

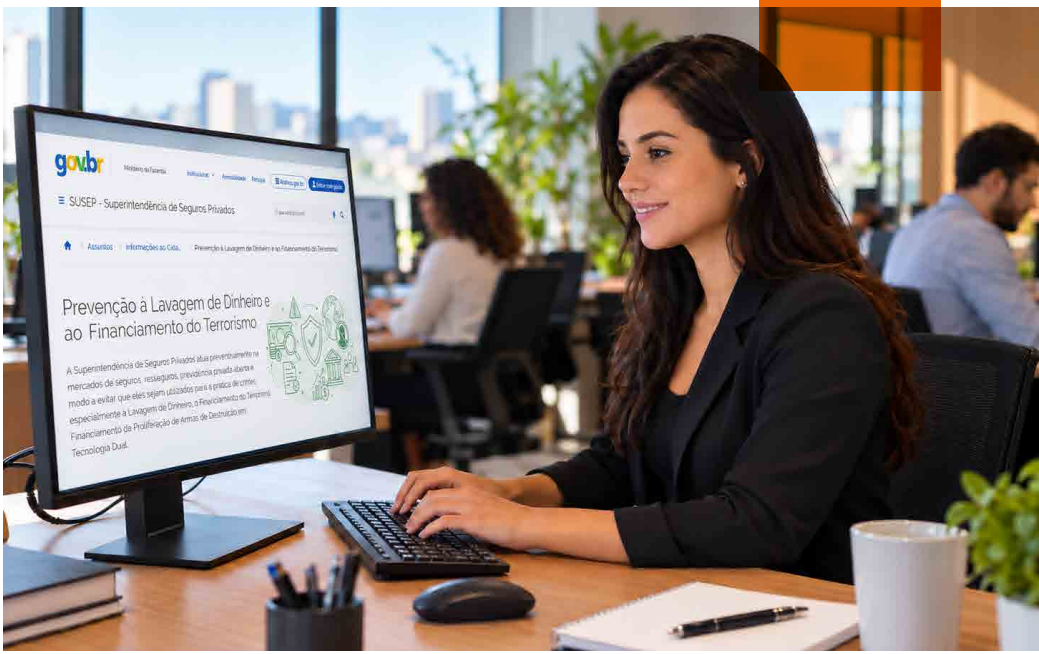
- abordagem baseada em risco;
- identificação e conhecimento de clientes e beneficiários finais;

- manutenção de registros;
- tratamento de PEP;
- avaliação de riscos associados a novas tecnologias;
- controles internos e programas de treinamento;
- comunicação de operações suspeitas;
- supervisão das instituições;
- cumprimento de sanções financeiras direcionadas.

Esse conjunto normativo evidencia a convergência entre padrões internacionais e regulamentação nacional, reforçando a necessidade de estruturas integradas de governança, controle e gestão de riscos pelas entidades supervisionadas.

A nova resolução exige a revisão e, quando necessário, a adequação das políticas, dos procedimentos e dos controles das instituições, de forma proporcional aos riscos identificados, para mitigar a utilização de seus produtos e serviços na prática de ilícitos financeiros.





Página da SUSEP sobre PLD/FTP: um recurso estratégico para o Setor
https://www.gov.br/susep/pt-br/assuntos/cidadao/pldftp

A SUSEP mantém em seu portal oficial uma página dedicada à PLD/FTP, concebida como um ponto de referência técnico-informacional para o setor supervisionado e demais interessados.

A página reúne informações institucionais e orientações práticas sobre o papel da SUSEP na prevenção de crimes financeiros nos mercados de seguros, resseguros, previdência complementar aberta e capitalização, com foco em evitar que tais segmentos sejam utilizados como instrumentos ou vetores para atividades ilícitas.

Principais componentes e utilidade da página:

Articulação Institucional sobre PLD/FTP: aborda o papel da SUSEP na integração com os demais órgãos do Sistema Brasileiro de Prevenção e Combate à Lavagem de Dinheiro, reforçando a necessidade de coordenação entre supervisão prudencial, unidades de inteligência financeira e órgãos de persecução penal.

Comunicados e orientações do GAFI/FATF: disponibiliza comunicados e materiais internacionais sobre melhores práticas, fortalecendo o alinhamento regulatório do Brasil aos padrões internacionais de governança e mitigação de riscos de PLD/FTP.

Avaliação Nacional de Riscos de PLD/FTP (ANR): conecta o setor segurador à avaliação nacional de riscos, permitindo a compreensão das ameaças, vulnerabilidades e exposições específicas que impactam o sistema financeiro e seus segmentos regulados.

Conteúdos educacionais e Glossário de termos de PLD/FTP: recursos como glossário, perguntas frequentes e materiais de contextualização técnica contribuem para o aprofundamento conceitual e operacional dos agentes do mercado.

Guia prático para Corretores e o Sistema SISCOAF: seções específicas abordam obrigações de comunicação, como as relativas a propostas e operações suspeitas e/ou atípicas, a utilização do Sistema de Controle de Atividades Financeiras (SISCOAF) e responsabilidades de corretores de seguros, ampliando a acessibilidade do tema a diferentes públicos.

A página de PLD/FTP da SUSEP representa uma ferramenta de referência contínua que:

- facilita a compreensão das exigências normativas e práticas de conformidade;
- disponibiliza recursos técnicos padronizados (glossário, perguntas frequentes, guias e normativos);
- conecta o setor segurador a diretrizes nacionais e internacionais de prevenção;
- apoia a implementação de programas robustos de governança, análise de riscos e controles internos;
- oferece material de suporte para a capacitação de profissionais e gestores.

Ao reunir conteúdos institucionais, normativos e operacionais em um único espaço, a SUSEP fortalece a transparência e o acesso ao conhecimento necessário para que as entidades supervisionadas implementem de forma eficaz seus programas de PLD/FTP, alinhando-se às boas práticas nacionais e internacionais.

Conceitos

Capítulo 3



Em um ambiente financeiro cada vez mais integrado e digitalizado, os riscos associados à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa assumem caráter transnacional e dinâmico.

A efetividade das medidas de prevenção depende da atuação coordenada entre instituições, reguladores e autoridades competentes, bem como da adoção de estruturas de controle capazes de acompanhar a evolução das práticas ilícitas.

Tipificação do crime de lavagem de dinheiro na Lei nº 9.613/1998

A Lei nº 9.613/1998, com redação dada pela Lei nº 12.683/2012, define como crime de lavagem de dinheiro a conduta de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.

A legislação estabelece, ainda, que incorre nas mesmas penas aquele que, com o propósito de conferir aparência de licitude a recursos de origem ilícita:

- os converte em ativos aparentemente lícitos;
- os adquire, recebe, troca, negocia, dá ou recebe em garantia, guarda, mantém em depósito, movimenta ou transfere;
- importa ou exporta bens com valores declarados em desacordo com os efetivamente praticados.

Sujeitam-se igualmente às mesmas penalidades aqueles que:

- utilizam, na atividade econômica ou financeira, bens, direitos ou valores provenientes de infração penal;
- participam de grupo, associação ou estrutura organizada, com conhecimento de que sua atividade, principal ou secundária, é direcionada à prática dos crimes previstos na referida lei.

No setor de seguros, essas condutas podem se materializar ao longo do ciclo de vida dos produtos, especialmente em operações que envolvem acumulação, movimentação e transferência de recursos.

Entre as situações de maior atenção, destacam-se:

- utilização de produtos com componente financeiro, como seguros de vida resgatáveis e planos de previdência (VGBL/PGBL), para a introdução ou a movimentação de recursos de origem ilícita;
- realização de contribuições/aportes relevantes incompatíveis com o perfil econômico do cliente, seguidos de resgates antecipados ou portabilidades;
- indicação de beneficiários interpostos ou sem vínculo aparente, com o objetivo de transferir recursos a terceiros;
- utilização de indenizações, benefícios ou devoluções de prêmio como mecanismo de reintegração de recursos ao sistema econômico formal;
- estruturas operacionais com múltiplos participantes, alterações frequentes de titularidade ou fragmentação de valores, com potencial de dificultar o rastreamento.

Essas situações evidenciam a necessidade de análise não apenas formal, mas também comportamental e econômica das operações, reforçando a importância da atuação preventiva baseada em risco.



A correta compreensão da tipificação legal constitui elemento fundamental para a estruturação de programas efetivos de PLD/FTP.

As entidades supervisionadas devem implementar controles proporcionais à sua exposição a riscos, incluindo:

- identificação e qualificação adequada de clientes e beneficiários;
- monitoramento contínuo de operações;
- definição de critérios para a detecção de situações atípicas;
- comunicação tempestiva de operações suspeitas.

No contexto atual, marcado pela intensificação das inovações tecnológicas, pela digitalização dos serviços financeiros e pelo surgimento de novos modelos de negócio, a identificação de operações suspeitas tende a se tornar mais complexa e menos evidente.



O uso de canais digitais, pagamentos instantâneos, estruturas descentralizadas e soluções baseadas em tecnologia amplia a velocidade, a fragmentação e a sofisticação das transações, reduzindo a eficácia de métodos tradicionais de detecção.

Nesse cenário, torna-se ainda mais relevante a adoção de processos estruturados, sustentados por uma abordagem baseada em risco, que incorporem:

- ferramentas analíticas;
- monitoramento contínuo;
- revisão periódica de parâmetros e critérios.

A análise integrada de aspectos operacionais, comportamentais e contextuais passa a ser elemento-chave para a efetividade dos mecanismos de prevenção, exigindo das entidades supervisionadas capacidade contínua de adaptação e aprimoramento de seus controles.

Conceitos fundamentais em PLD/FTP

A compreensão dos conceitos e das nomenclaturas relacionadas à PLD/FTP é essencial para a adequada identificação, avaliação e tratamento dos riscos, permitindo a adoção de medidas proporcionais à exposição das instituições.

A lavagem de dinheiro caracteriza-se por um conjunto de operações destinadas a ocultar ou dissimular a origem ilícita de bens, direitos ou valores, com o objetivo de integrá-los ao sistema econômico com aparência de legalidade.

O financiamento do terrorismo, por sua vez, consiste na provisão ou disponibilização de recursos, bens ou ativos com a finalidade de apoiar atividades terroristas, podendo tais recursos ter origem tanto lícita quanto ilícita.

Embora distintos em sua natureza, esses fenômenos apresentam significativa interseção operacional, na medida em que organizações criminosas e terroristas utilizam mecanismos semelhantes para ocultar a origem, o destino e os beneficiários dos recursos, dificultando sua identificação pelas autoridades.

A prática de lavagem de dinheiro não se limita ao uso de recursos em espécie, podendo envolver diferentes instrumentos financeiros, estruturas societárias e fluxos transacionais, nacionais ou internacionais.

De modo geral, quando uma atividade ilícita gera recursos, os envolvidos buscam utilizá-los sem revelar sua origem, empregando mecanismos como:

- dissimulação da origem dos recursos;
- alteração da forma dos ativos;
- utilização de intermediários;
- transferência para jurisdições ou estruturas menos transparentes.

As práticas podem variar desde operações simples até estruturas altamente sofisticadas, envolvendo múltiplas transações, diferentes agentes e elevada complexidade operacional.

Historicamente, as medidas de prevenção concentravam-se nas instituições financeiras tradicionais. Contudo, a evolução das normas internacionais — especialmente as Recomendações do GAFI/FATF — e, no Brasil, a alteração promovida pela Lei nº 12.683/2012 ampliaram significativamente o alcance das obrigações.

Esse movimento passou a abranger diversos setores econômicos suscetíveis ao uso indevido para a ocultação de recursos ilícitos, incluindo o mercado de seguros, previdência complementar aberta e capitalização.

De modo geral, o risco de utilização de produtos do setor de seguros para fins de lavagem de dinheiro ou financiamento do terrorismo tende a ser inferior ao observado em outros segmentos do sistema financeiro.

Produtos cuja liquidez depende exclusivamente da ocorrência de evento coberto (sinistro) apresentam menor suscetibilidade a esse tipo de prática.

Por outro lado, produtos com componente de acumulação financeira — como seguros de vida resgatáveis e planos de previdência complementar aberta — apresentam maior exposição ao risco, em razão da possibilidade de movimentação de recursos ao longo do tempo, por meio de aportes, resgates, portabilidades e pagamentos de benefícios.

Considerando a relevância econômica do setor, torna-se essencial que as entidades supervisionadas mantenham mecanismos eficazes de identificação da origem dos recursos, monitoramento de operações e comunicação de situações suspeitas.

A implementação de programas de PLD/FTP não se limita ao atendimento às obrigações regulatórias, mas constitui elemento fundamental para a proteção das instituições contra o uso indevido de seus produtos e serviços.

Esses programas contribuem para:

- a mitigação de riscos operacionais e reputacionais;
- a preservação da confiança de clientes e investidores;
- a integridade das relações contratuais;
- a estabilidade do sistema financeiro e econômico.

A seguir, apresentam-se os principais conceitos operacionais associados à PLD/FTP, fundamentais para a implementação de controles efetivos pelas entidades supervisionadas.

i. Lavagem de dinheiro: processo pelo qual recursos, bens ou valores provenientes de atividades ilícitas são ocultados ou dissimulados, de forma a aparentar origem lícita, podendo envolver múltiplas transações, utilização de intermediários e estruturas operacionais complexas.

ii. Financiamento do terrorismo: consiste na provisão, captação ou disponibilização de recursos, bens ou serviços com a finalidade de apoiar atividades terroristas, independentemente de sua origem ser lícita ou ilícita.

iii. Financiamento da proliferação de armas de destruição em massa: refere-se ao fornecimento, à movimentação ou à disponibilização de recursos destinados ao desenvolvimento, à aquisição, à produção ou à disseminação de armas nucleares, químicas ou biológicas, incluindo seus sistemas de entrega e materiais relacionados, frequentemente por meio de estruturas complexas destinadas a ocultar a finalidade das transações.

iv. Abordagem baseada em risco: princípio segundo o qual as instituições devem identificar, avaliar e compreender os riscos de PLD/FTP a que estão expostas, adotando medidas de prevenção e controle proporcionais ao nível desses riscos, com maior intensidade em situações de maior exposição.

v. Conheça seu Cliente (*Know Your Client* — KYC): conjunto de procedimentos destinados à identificação e à verificação da identidade dos clientes, à compreensão da natureza de suas atividades e da origem dos recursos e identificação do beneficiário final.

vi. Beneficiário final: pessoa natural que, isoladamente ou em conjunto, de forma direta ou indireta, possui, controla ou influencia significativamente uma pessoa jurídica ou outro tipo de estrutura análoga.

vii. Pessoa Politicamente Exposta (PEP): pessoa natural que ocupa ou tenha ocupado, nos cinco anos anteriores, funções públicas relevantes, inclusive no exterior, ou funções relevantes em organizações internacionais. Seus representantes, familiares e estreitos colaboradores também estão sujeitos às diligências previstas na norma. Base: arts. 4º, 24 e 33.

viii. Conheça seu Funcionário (*Know Your Employees* — KYE): procedimentos destinados à verificação da idoneidade e da adequação dos colaboradores, com o objetivo de prevenir riscos de fraude interna, conflitos de interesse e envolvimento em atividades ilícitas.

ix. Conheça seu parceiro (*Know Your Partner* — KYP): processo de obtenção e análise de informações sobre parceiros comerciais, fornecedores, intermediários e prestadores de serviços, com o objetivo de identificar e mitigar riscos associados ao relacionamento.

x. Monitoramento de operações: acompanhamento contínuo das operações realizadas por clientes e contrapartes, com o objetivo de identificar padrões atípicos ou suspeitos e viabilizar a adoção de medidas cabíveis, incluindo a comunicação às autoridades competentes.

xi. Comunicação ao Conselho de Controle de Atividades Financeiras (Coaf): obrigação de comunicar operações ou situações suspeitas ao Coaf, unidade de inteligência financeira responsável por analisar e disseminar informações para apoiar as autoridades competentes.

xii. Diligência prévia (*Due diligence*): processo de análise prévia e contínua de clientes, parceiros e operações, com o objetivo de identificar, avaliar e mitigar riscos de PLD/FTP e outros ilícitos.

xiii. Listas de sanções: procedimentos de consulta as listas de sanções aplicáveis e de monitoramento permanente das determinações do CSNU e de seus comitês de sanções, incluindo as emanadas do Conselho de Segurança das Nações Unidas, com o objetivo de prevenir relações com pessoas ou entidades sancionadas e assegurar o cumprimento de medidas de indisponibilidade de ativos. Base: art. 46, § 3º, I.

xiv. Treinamento e capacitação: processo contínuo de formação dos colaboradores, visando assegurar o conhecimento das obrigações regulatórias, a correta aplicação dos procedimentos internos e a capacidade de identificação de situações suspeitas.

xv. Governança e controles internos: conjuntos de políticas, procedimentos, estruturas organizacionais e mecanismos de controle destinados a assegurar a efetividade do programa de PLD/FTP e o cumprimento das obrigações legais e regulatórias.

xvi. Novas tecnologias e canais digitais: utilização de soluções tecnológicas para a oferta de produtos e serviços financeiros, incluindo canais remotos, pagamentos instantâneos e automação de processos, que, embora ampliem a eficiência e a inclusão, demandam avaliação contínua de riscos e adoção de controles adequados.

xvii. Tecnologia dual: tecnologia que pode ser utilizada legitimamente para fins civis/comerciais, mas que também pode ser empregada para fins militares ou para a produção de armas de destruição em massa.

Alinhamento regulatório: a Resolução SUSEP nº 99/2026 encontra-se alinhada às Recomendações do Grupo de Ação Financeira (GAFI/FATF), incorporando, entre outros, os seguintes princípios: abordagem baseada em risco, com diligência simplificada, padrão ou reforçada; identificação e verificação de clientes e beneficiários finais; diligência reforçada para pessoas expostas politicamente; monitoramento contínuo e comunicação de operações suspeitas; manutenção de registros; governança, controles internos e avaliação de sua efetividade; cumprimento de sanções financeiras direcionadas; prevenção ao financiamento da proliferação de armas de destruição em massa; e avaliação de riscos associados a novas tecnologias.

A adequada compreensão e aplicação desses conceitos constituem elementos essenciais para a efetividade dos programas de PLD/FTP, permitindo às instituições adotar medidas proporcionais aos riscos identificados e contribuir para a integridade do sistema financeiro e econômico.

Etapas da lavagem de dinheiro

A lavagem de dinheiro é tradicionalmente descrita em três fases principais: colocação, ocultação e integração. Esse modelo permanece válido como referência analítica e operacional, ainda que, no contexto atual, as transformações tecnológicas e a digitalização dos serviços financeiros tenham ampliado significativamente os mecanismos utilizados, permitindo operações mais rápidas, transnacionais e estruturalmente complexas.



1. Colocação

A colocação corresponde à introdução dos recursos de origem ilícita no sistema econômico ou financeiro.

Historicamente associada à inserção de dinheiro em espécie, essa fase passou a incorporar, de forma crescente, meios eletrônicos e digitais, incluindo transferências instantâneas, carteiras digitais, contas de pagamento, operações com criptoativos e a utilização de intermediários ou terceiros interpostos.

Além de depósitos e da aquisição de bens de alto valor, podem ser utilizados produtos financeiros e securitários com componente de acumulação — como planos de previdência complementar aberta, títulos de capitalização e seguros resgatáveis —, bem como podem ser adquiridos ativos de difícil rastreamento, como imóveis, obras de arte, participações societárias e ativos digitais.

A diversidade de instrumentos e a possibilidade de utilização de múltiplos canais aumentam a complexidade da identificação dessa fase, especialmente quando combinadas com estratégias de fragmentação de valores e uso de estruturas intermediárias.

2. Ocultação

Na fase de ocultação, o objetivo é dificultar o rastreamento da origem dos recursos por meio de operações destinadas à sua fragmentação, circulação e transformação.

Essa etapa pode envolver transferências sucessivas entre instituições e jurisdições, utilização de empresas de fachada, interposição de terceiros, operações com criptoativos, uso de plataformas digitais e de serviços financeiros não tradicionais, bem como mecanismos automatizados de movimentação de recursos.

A elevada velocidade das transações, a atuação em múltiplas jurisdições e a utilização de estruturas complexas contribuem para a dispersão dos valores e para a quebra da cadeia de evidências, dificultando o rastreamento dos recursos pelas autoridades e pelas próprias instituições.

3. Integração

A integração ocorre quando os recursos retornam ao sistema econômico formal com aparência de legitimidade.

Essa fase pode se materializar por meio de resgates de provisões acumuladas, de pagamento de benefícios previdenciários, do recebimento de indenizações securitárias, de devoluções associadas a produtos de capitalização ou da realização de operações comerciais aparentemente regulares.

Também podem ser utilizados mecanismos como a aquisição e a alienação de ativos financeiros e digitais, a distribuição de lucros por estruturas societárias utilizadas como fachada, investimentos em negócios legítimos ou outras operações que permitam a incorporação definitiva dos recursos à economia formal.

Nesse estágio, os valores já passaram por diversas transformações, o que dificulta significativamente a identificação de sua origem ilícita.

Dinâmica e variações operacionais



As fases da lavagem de dinheiro não ocorrem necessariamente de forma linear. Em muitos casos, podem se sobrepor, ocorrer simultaneamente ou, em determinados contextos, serem parcialmente suprimidas, especialmente em ambientes digitais caracterizados por alta velocidade e automação.

Essa dinâmica exige que os mecanismos de prevenção e detecção adotem uma abordagem estruturada e baseada em risco, com capacidade de identificar padrões complexos e acompanhar a evolução contínua das práticas ilícitas.

Muitos dos mecanismos utilizados na lavagem de dinheiro também podem ser empregados no financiamento do terrorismo e no financiamento da proliferação de armas de destruição em massa, ainda que esses fenômenos apresentem características próprias.

No financiamento do terrorismo, os recursos podem ter origem lícita e envolver valores relativamente baixos, obtidos por meio de doações, atividades comerciais legítimas ou arrecadações digitais, o que dificulta sua identificação com base em critérios tradicionais.

Já o financiamento da proliferação costuma estar associado a operações comerciais aparentemente regulares, especialmente no comércio internacional, incluindo a aquisição de bens de dupla utilização (civil e militar), frequentemente realizadas por meio de redes complexas de intermediação.

A digitalização dos serviços financeiros amplia esses riscos ao permitir transferências rápidas e transnacionais por meio de plataformas digitais, sistemas de pagamento instantâneo, carteiras eletrônicas e outros canais remotos.

Nesse contexto, torna-se essencial a adoção de mecanismos robustos de prevenção, incluindo:

- monitoramento baseado em risco;
- análise de padrões comportamentais e da finalidade das transações;
- verificação contínua de contrapartes e beneficiários;
- cumprimento de sanções financeiras direcionadas;
- cooperação entre instituições financeiras, reguladores e autoridades competentes.



Como as empresas atuam na prevenção e no combate à LD/FT

As empresas sujeitas às obrigações de PLD/FTP desempenham papel central na identificação e na mitigação de riscos e na comunicação de operações suspeitas, contribuindo para a integridade, a transparência e a estabilidade do sistema financeiro e econômico.

Nos termos da Lei nº 9.613/1998, essas entidades devem implementar mecanismos estruturados destinados à identificação, à avaliação e ao monitoramento de riscos, bem como à comunicação de indícios de ilícitos ao Coaf.

O Coaf, instituído pela referida lei, atua como unidade de inteligência financeira, sendo responsável por receber, examinar e identificar ocorrências suspeitas a partir das comunicações realizadas pelas pessoas obrigadas. Com base nessas informações, elabora e dissemina relatórios de inteligência financeira às autoridades competentes, como o Ministério Público, a Polícia Federal e outros órgãos de investigação. Ressalte-se que sua atuação como unidade de inteligência financeira não se confunde com a investigação criminal, sem prejuízo de suas competências de supervisão e de aplicação de sanções administrativas aos sujeitos sob sua competência

À luz do arcabouço regulatório vigente, as empresas devem estruturar seus programas de PLD/FTP com base na abordagem baseada em risco, de forma a assegurar que os controles adotados sejam compatíveis com a natureza, o porte, a complexidade e o perfil de exposição de suas operações.

Essa abordagem pressupõe a adoção de políticas, procedimentos e controles integrados, aplicáveis a toda a organização e extensivos a colaboradores, parceiros, prestadores de serviços e demais terceiros envolvidos em suas atividades.

Nesse contexto, destacam-se, entre os principais componentes do sistema de prevenção:

- identificação, qualificação e verificação de clientes e beneficiários finais;
- classificação de risco e definição de níveis de diligência proporcionais;
- monitoramento contínuo de operações e detecção de padrões atípicos;
- comunicação tempestiva de operações suspeitas ao Coaf;
- manutenção de registros e rastreabilidade das operações;
- capacitação contínua de colaboradores e disseminação da cultura de compliance;
- estabelecimento de estrutura de governança e controles internos compatíveis com o risco.

Adequação a ambientes digitais e inovação tecnológica

A crescente digitalização dos serviços financeiros, aliada à ampliação de canais remotos e ao surgimento de novos modelos de negócio, impõe desafios adicionais à efetividade dos mecanismos de prevenção.

Nesse cenário, os controles devem ser continuamente aprimorados para contemplar operações realizadas à distância, estruturas de intermediação, terceirizações e soluções baseadas em tecnologia, assegurando a adequada identificação de clientes, a verificação da identidade e o monitoramento de transações em ambientes digitais.

Adicionalmente, pode contribuir para esse processo a incorporação de ferramentas analíticas e mecanismos de monitoramento em tempo real, capazes de identificar padrões comportamentais e transacionais complexos, bem como a realização de revisões periódicas dos critérios de detecção à luz das novas tipologias de risco.

Os mecanismos de PLD/FTP devem abranger tanto operações tradicionais quanto digitais, considerando a crescente integração entre diferentes segmentos do sistema financeiro e a atuação de múltiplos agentes em cadeias de valor cada vez mais complexas.

A efetividade desses controles depende não apenas de sua formalização, mas

também de sua aplicação consistente, da adequada governança e da capacidade de adaptação contínua das instituições diante da evolução dos riscos.

Nesse contexto, as diretrizes regulatórias e as boas práticas já estabelecem um conjunto de medidas específicas a serem observadas pelas entidades supervisionadas, conforme detalhado a seguir:

- **Avaliação interna de risco:** metodologia que baliza toda a análise de PLD/FTP, com o objetivo de mensurar e tratar os diferentes riscos de utilização dos produtos e serviços para a prática dos crimes de lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa;

- **Políticas, instruções normativas e manuais de procedimentos internos:** documentação obrigatória que formaliza as diretrizes corporativas e os controles de PLD/FTP;

- **Programas "Conheça seu cliente, funcionário, prestador de serviço, parceiro e fornecedor":** constituem instrumentos utilizados pelas empresas para avaliar se clientes, funcionários, prestadores de serviços, parceiros e fornecedores apresentam riscos relacionados à PLD/FTP;

- **Identificação e acompanhamento de PEPs e de seus representantes, familiares e estreitos colaboradores:** procedimentos para identificar essas condições e aplicar diligência reforçada contínua às operações e às relações de negócio abrangidas pelo art. 33. A condição de PEP não implica sanção ou impedimento automático;

- **Monitoramento e comunicação de operações suspeitas:** procedimentos destinados a selecionar situações consideradas suspeitas, com base em critérios previamente definidos e na análise de profissionais capacitados, bem como a comunicar essas situações ao Coaf, quando cabível;

- **Aculturamento sobre PLD/FTP:** processo de disseminação da cultura de prevenção aos riscos de PLD/FTP nas empresas, por meio de treinamentos, ações de comunicação e iniciativas de conscientização dirigidas a clientes, funcionários, prestadores de serviços, parceiros e fornecedores;

- **Avaliação de efetividade:** avaliação anual, documentada em relatório, da efetividade das políticas, dos procedimentos e dos controles internos de PLD/FTP, incluindo testes, indicadores e identificação de deficiências;

- **Canal de denúncias:** mecanismo adotado pelas empresas para a recepção de denúncias relacionadas a desvios de conduta e atos ilícitos, incluindo situações relacionadas à lavagem de dinheiro e ao financiamento do terrorismo.

Consequências e penalidades previstas na legislação

A observância das obrigações relacionadas à PLD/FTP é elemento essencial para a mitigação de riscos legais, operacionais e reputacionais, bem como para a preservação da integridade das operações das instituições.

No ordenamento jurídico brasileiro, a matéria é disciplinada principalmente pela Lei nº 9.613/1998, que define o crime de lavagem de dinheiro e estabelece mecanismos de prevenção e repressão. A prática desse crime sujeita os responsáveis à pena de reclusão de 3 a 10 anos, além de multa, podendo haver aumento da pena em circunstâncias específicas, como sua prática reiterada, por intermédio de organização criminosa ou por meio da utilização de ativo virtual.

Responsabilização de pessoas físicas e jurídicas

A responsabilização decorrente do descumprimento das obrigações de prevenção não se limita às pessoas físicas diretamente envolvidas. As pessoas jurídicas sujeitas às obrigações legais e regulatórias também podem ser submetidas a sanções administrativas, especialmente quando:

- são utilizadas como instrumento para a prática de ilícitos;
- deixam de implementar controles e procedimentos adequados de prevenção;
- apresentam falhas relevantes em seus mecanismos de governança e monitoramento.

Nesses casos, além de eventual responsabilização civil e penal de administradores, podem ser aplicadas sanções administrativas pelos órgãos supervisores.



Sanções administrativas

A legislação prevê um conjunto de penalidades aplicáveis às organizações que descumpram as obrigações de PLD/FTP, entre as quais se destacam:

- advertência;
- multa pecuniária, observados os limites e critérios previstos na legislação;
- inabilitação temporária de administradores;
- suspensão do exercício de atividades;
- cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento.

Essas medidas evidenciam a necessidade de implementação de estruturas robustas de governança, controles internos e gestão de riscos, compatíveis com o porte e a complexidade das operações.

Abrangência do regime de PLD/FTP

Ainda que a Lei nº 9.613/1998 não contemple expressamente determinadas figuras introduzidas por marcos legais mais recentes — como as operações de proteção patrimonial mutualista e as sociedades processadoras de ordens do cliente, previstas na Lei Complementar nº 213/2025 —, isso não implica sua exclusão do regime de prevenção.

O art. 9º, parágrafo único, inciso VIII, da referida lei estabelece que também se sujeitam às obrigações de PLD/FTP as demais entidades cujo funcionamento dependa de autorização de órgãos reguladores dos mercados financeiro, de capitais e de seguros.

Considerando que tais entidades passam a depender de autorização e supervisão da SUSEP, resta caracterizado seu enquadramento no rol de pessoas obrigadas, devendo implementar mecanismos adequados de gestão e controle de riscos.

Da mesma forma, o CNSP disciplinou a matéria em âmbito infralegal, com o objetivo de assegurar a adequada implementação de políticas, procedimentos e controles internos voltados à prevenção e ao combate à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa, em consonância com a regulamentação editada pela SUSEP, Circular SUSEP nº 612/2020, que será revogada pela recente Resolução SUSEP nº 99.2026 a partir de 1º de janeiro de 2027.

Esse arcabouço normativo confere maior clareza quanto às obrigações das entidades supervisionadas, reforçando a necessidade de estruturas de governança e mecanismos de controle

compatíveis com os riscos inerentes às operações do setor.

Nesse contexto, destacam-se, entre outros, os seguintes dispositivos:

- Resolução CNSP nº 491/2026, art. 135;
- Resolução CNSP nº 429/2021, art. 6º e Anexo II — requisitos de governança, sigilo de dados e informações e segurança cibernética.

Esses normativos consolidam diretrizes que orientam a atuação das supervisionadas, promovendo maior uniformidade regulatória e fortalecendo a efetividade dos mecanismos de prevenção no âmbito dos mercados de seguros, previdência complementar aberta e capitalização.

Financiamento do terrorismo

No que se refere ao financiamento do terrorismo, a Lei nº 13.260/2016 estabelece a tipificação do crime de terrorismo, bem como os procedimentos investigativos e processuais aplicáveis.

As penas associadas são significativamente mais severas, podendo alcançar reclusão de 12 a 30 anos, além das sanções aplicáveis a crimes correlatos.

Diferentemente da lavagem de dinheiro, o financiamento do terrorismo pode envolver recursos de origem lícita, frequentemente em valores reduzidos, o que dificulta sua identificação por meio de critérios tradicionais de materialidade.



Pessoas Politicamente Expostas

Consideram-se Pessoas Expostas Politicamente (PEPs) as pessoas naturais que ocupem ou tenham ocupado, nos cinco anos anteriores, cargos, empregos ou funções públicas relevantes, no Brasil ou no exterior, assim como funções relevantes em organizações internacionais, conforme o art. 4º da Resolução SUSEP nº 99/2026.

No Brasil, enquadram-se como PEPs, entre outros, detentores de mandatos eletivos federais; ministros de Estado; ocupantes de cargos de natureza especial e DAS nível 6 ou equivalentes; determinadas autoridades do Poder Judiciário, do Ministério Público e dos Tribunais de Contas; presidentes e tesoureiros nacionais de partidos políticos; e autoridades estaduais, distritais e municipais expressamente relacionadas na norma.

No exterior, incluem-se chefes de Estado ou de governo, políticos e ocupantes de cargos governamentais de escalões superiores, oficiais generais, membros de escalões superiores do Poder Judiciário, executivos de escalões superiores de empresas públicas e dirigentes de partidos políticos. A definição também abrange dirigentes de escalões superiores de entidades de direito internacional público ou privado.

A verificação deve abranger tanto a condição de PEP quanto a de seu representante, familiar ou estreito colaborador. Independentemente de autodeclaração negativa, a instituição deve recorrer a informações públicas disponíveis ou consultar bases de dados públicas ou privadas sobre PEPs, adotando ao menos uma dessas providências, conforme o art. 24.

Nos termos do art. 33, operações e propostas envolvendo PEPs, seus familiares, representantes, estreitos colaboradores ou pessoas jurídicas de que participem são consideradas de alto risco e devem ser submetidas continuamente à diligência reforçada. As medidas mínimas incluem a autorização prévia de alçadas superiores para estabelecer ou prosseguir com a relação de negócios e a obtenção e a validação de informações adicionais, quando disponíveis, sobre a identidade do cliente, o beneficiário final, a estrutura societária e a origem dos recursos.

A condição de PEP não implica irregularidade, mas exige maior nível de diligência, controle e governança para prevenir a lavagem de dinheiro, o financiamento do terrorismo e o financiamento da proliferação de armas de destruição em massa.

A Resolução SUSEP nº 99/2026 entra em vigor em 1º de janeiro de 2027, quando substitui a Circular SUSEP nº 612/2020.

Como saber se um cliente é PEP?

A verificação da condição de Pessoa Exposta Politicamente (PEP) deve observar o art. 24 da Resolução SUSEP nº 99/2026. Independentemente de autodeclaração negativa do cliente, a instituição deve adotar pelo menos uma das seguintes providências:

- recorrer a informações públicas disponíveis; ou
- consultar bases de dados públicas ou privadas sobre PEPs.

A declaração do cliente pode complementar a verificação, mas não substitui essas consultas. Os procedimentos também devem verificar se o cliente é representante, familiar ou estreito colaborador de PEP.

Identificado o enquadramento, as operações e as relações de negócio devem ser submetidas continuamente à diligência reforçada, nos termos do art. 33. Esse acompanhamento deve considerar as operações realizadas, a atualização cadastral e eventuais dúvidas sobre a veracidade ou a adequação das informações.

As medidas mínimas incluem a autorização prévia de alçadas superiores para estabelecer ou prosseguir com a relação de negócios e a obtenção e a validação de informações adicionais, quando disponíveis, sobre a identidade do cliente, o beneficiário final, a estrutura societária e a origem dos recursos.

A Resolução SUSEP nº 99/2026 entra em vigor em 1º de janeiro de 2027, quando substitui a Circular SUSEP nº 612/2020.



Serviço CNseg: Sistema de Prevenção à Lavagem de Dinheiro (SIPLAV)

Diante da crescente complexidade dos riscos associados à lavagem de dinheiro e ao financiamento do terrorismo, bem como da intensificação das exigências regulatórias e da necessidade de atuação coordenada entre as instituições do setor, torna-se fundamental dispor de ferramentas institucionais que promovam padronização, eficiência e confiabilidade nos processos de prevenção.

O SIPLAV assume papel estratégico ao oferecer um serviço centralizado de apoio às entidades associadas, fortalecendo a capacidade do mercado de seguros, previdência e capitalização de cumprir suas obrigações legais e regulatórias, reduzir assimetrias informacionais e aprimorar a gestão de riscos de PLD/FTP.

Trata-se de solução desenvolvida para apoiar o cumprimento das obrigações previstas na Circular SUSEP nº 612/2020, que será substituída pela Resolução SUSEP nº 99/2026 a partir de 1º de janeiro de 2027, especialmente quanto à verificação da condição de Pessoa Exposta Politicamente (PEP) e de seus representantes, familiares e estreitos colaboradores. Por meio de uma base única, consolidada e periodicamente atualizada com dados públicos, o SIPLAV permite consultas ágeis e padronizadas, fornecendo subsídios para a avaliação de risco e a aplicação de diligência reforçada.

Ao centralizar informações relevantes — incluindo vínculos familiares e societários —, o sistema contribui para maior eficiência operacional e maior consistência nos controles internos. Sua utilização não afasta a responsabilidade de cada entidade pela atualização cadastral, pelo monitoramento contínuo das operações e das relações de negócio e pela adoção das demais medidas exigidas pela regulamentação.

ASG e sua relação com PLD/FTP

A agenda Ambiental, Social e Governança (ASG) relaciona-se diretamente com a PLD/FTP, especialmente no que se refere à gestão integrada de riscos e ao fortalecimento de padrões de integridade corporativa.

A integração entre PLD/FTP e critérios ASG contribui para elevar o nível de governança, transparência e gestão de riscos das organizações, fortalecendo sua capacidade de prevenir o uso indevido de suas operações para fins ilícitos.

Organizações que adotam critérios ASG tendem a orientar suas decisões de investimento e de relacionamento com contrapartes que observem práticas compatíveis com a sustentabilidade, a ética, a transparência e a

A convergência entre sustentabilidade, integridade e conformidade regulatória consolida-se como elemento essencial para a perenidade dos negócios e para a estabilidade do sistema econômico



responsabilidade social, reduzindo a exposição a entidades envolvidas em corrupção, ilícitos financeiros, violações de direitos humanos ou outras condutas incompatíveis com esses princípios.

Ao demandar estruturas decisórias mais robustas, controles internos consistentes e divulgação qualificada de riscos, esses referenciais ampliam a confiança de investidores, reguladores e da sociedade, ao mesmo tempo em que reduzem a exposição a riscos legais, reputacionais e financeiros.

A convergência entre sustentabilidade, integridade e conformidade regulatória consolida-se como elemento essencial para a perenidade dos negócios e para a estabilidade do sistema econômico.

Governança como elemento central

Sob a perspectiva da governança — eixo estruturante do ASG —, a adoção de políticas robustas de *compliance*, controles internos, transparência e prestação de contas contribui diretamente para a mitigação dos riscos de lavagem de dinheiro e de financiamento de atividades ilícitas.

Empresas com estruturas frágeis de governança apresentam maior vulnerabilidade a fraudes, corrupção e uso indevido de suas operações por organizações criminosas, evidenciando a relevância da governança como primeira linha de defesa no contexto de PLD/FTP.

Ampliação da *due diligence* e visão de risco

A incorporação de critérios ASG fortalece os processos de *due diligence* aplicáveis a clientes, parceiros, fornecedores e investimentos, ampliando a capacidade de identificação de riscos ao longo da cadeia de valor.

Essa abordagem permite capturar, de forma mais abrangente, riscos associados a:

- sanções internacionais;
- crime organizado;
- exploração ambiental ilegal;
- tráfico de pessoas;
- financiamento de atividades ilícitas ou extremistas.

Dessa forma, a análise ASG expande a visão tradicional de *compliance*, incorporando dimensões reputacionais, sociais e ambientais que podem indicar maior probabilidade de exposição a ilícitos.

Riscos emergentes e integridade de mercado

A integração de critérios ASG também contribui para a antecipação de riscos regulatórios e de sanções, especialmente em setores, produtos ou jurisdições de maior exposição.

Adicionalmente, o crescimento da demanda por produtos e investimentos sustentáveis exige atenção a riscos específicos, como o *greenwashing* ou a utilização indevida de instrumentos financeiros rotulados como "verdes" para a ocultação de fluxos ilícitos, o que reforça a necessidade de mecanismos de verificação e controle consistentes.

Padrões internacionais de divulgação e transparência

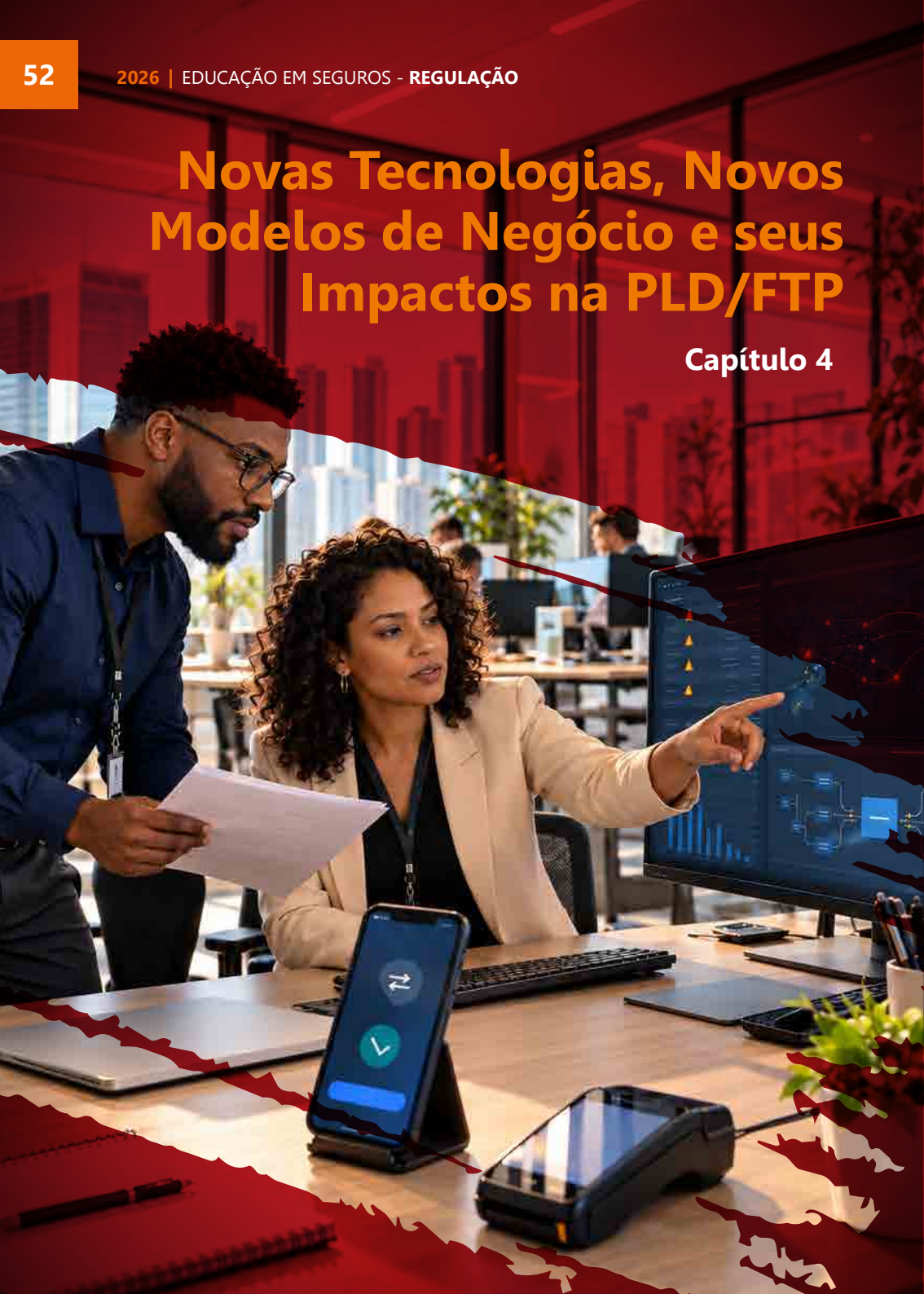
A integração entre ASG e gestão de riscos corporativos é reforçada pela adoção de padrões internacionais de divulgação de sustentabilidade, como o IFRS S1 (Requisitos Gerais para Divulgação de Informações Financeiras Relacionadas à Sustentabilidade) e o IFRS S2 (Divulgações Relacionadas ao Clima), emitidos pelo *International Sustainability Standards Board* (ISSB).

No Brasil, esses referenciais foram incorporados como CBPS 1 e CBPS 2, estabelecendo diretrizes para a divulgação consistente, comparável e auditável de riscos e oportunidades relacionados à sustentabilidade, incluindo aspectos de governança, controles internos e gestão de riscos.

Embora não tratem especificamente de PLD/FTP, esses padrões reforçam a transparência e a responsabilidade corporativa ao exigir maior qualidade das informações, robustez dos processos decisórios e alinhamento entre estratégia, riscos e desempenho.

Novas Tecnologias, Novos Modelos de Negócio e seus Impactos na PLD/FTP

Capítulo 4



A PLD/FTP permanece como um dos pilares da integridade do sistema financeiro e, em particular, do mercado segurador, de previdência e capitalização brasileiro.

Entretanto, a intensificação da digitalização dos serviços financeiros, a emergência de novos modelos de negócio e a ampliação do número de agentes no ecossistema vêm alterando de forma relevante a dinâmica de riscos, impondo desafios adicionais à efetividade dos mecanismos tradicionais de prevenção.

Adicionalmente, a evolução recente do arcabouço regulatório e institucional — em especial, com a introdução de novos atores e estruturas operacionais pela Lei Complementar nº 213/2025 — evidencia a necessidade de revisão crítica dos modelos de identificação, monitoramento e controle adotados pelas instituições.

A atuação de sociedades processadoras da ordem do cliente, o desenvolvimento de arranjos baseados em intermediação tecnológica e a ampliação de estruturas como cooperativas e entidades de proteção patrimonial mutualista introduzem novos vetores de risco, especialmente no que se refere à fragmentação de responsabilidades, à circulação de dados e à rastreabilidade das operações.

Essas transformações ocorrem em paralelo ao fortalecimento das diretrizes internacionais, em especial das recomendações do GAFI/FATF, que reforçam a necessidade de abordagens baseadas em risco, proporcionais e adaptáveis à evolução das tipologias de ilícitos financeiros.

O movimento de aprimoramento regulatório conduzido pela SUSEP reflete a crescente complexidade do ambiente supervisionado, demandando das entidades maior capacidade de adaptação, integração de controles e utilização de instrumentos tecnológicos para a prevenção, a detecção e a comunicação de operações suspeitas.

Diante desse cenário, o presente capítulo tem por objetivo analisar os impactos dessas transformações sobre os mecanismos de PLD/FTP, explorando, sob perspectiva técnica e operacional:

- os novos vetores de risco associados à digitalização e à inovação;
- os desafios decorrentes da atuação de novos agentes e estruturas;
- as implicações para a governança, os controles internos e o monitoramento de operações;
- a necessidade de evolução dos modelos tradicionais de prevenção.

Mais do que descrever mudanças, busca-se, neste capítulo, contribuir para a compreensão dos ajustes necessários à manutenção da efetividade dos programas de PLD/FTP em um ambiente caracterizado por maior complexidade, velocidade e interconectividade.

Transformação digital e seus impactos na PLD/FTP

A aceleração da transformação digital tem produzido impactos estruturais sobre os mecanismos de PLD/FTP, alterando não apenas os instrumentos disponíveis para o controle, mas também a própria dinâmica de risco enfrentada pelas instituições.

A digitalização dos serviços financeiros e securitários, aliada ao uso de inteligência artificial, análise de grandes volumes de dados (*big data*), computação em nuvem e modelos de negócio baseados em plataformas, ampliou significativamente a capacidade de processamento, monitoramento e detecção de padrões atípicos.

Ao mesmo tempo, essas transformações introduzem novos vetores de risco, especialmente em contextos caracterizados por:

- elevada velocidade e volume de transações;
- multiplicidade de canais digitais e pontos de acesso;
- fragmentação de responsabilidades entre diferentes agentes;
- maior dependência de terceiros e de infraestruturas tecnológicas compartilhadas.

Nesse ambiente, a rastreabilidade das operações e a identificação de responsabilidades tornam-se mais complexas, exigindo maior integração entre sistemas, bases de dados e estruturas de controle.

Impactos sobre os modelos de prevenção

A incorporação de tecnologias avançadas permite ganhos relevantes de eficiência e precisão, incluindo:

- monitoramento contínuo e em tempo quase real;
- uso de modelos analíticos para a identificação de padrões comportamentais;
- automação de processos de detecção e triagem de alertas.

Entretanto, esses avanços também trazem desafios relevantes, como:

- dependência da qualidade e da integridade dos dados;
- risco de vieses em modelos automatizados;
- necessidade de calibragem constante para evitar falsos positivos e negativos;
- complexidade na explicabilidade das decisões automatizadas (*model explainability*).

Esses fatores reforçam a necessidade de estruturas de governança tecnológica e de validação de modelos compatíveis com o nível de risco das operações.

Desafios regulatórios e necessidade de adaptação

No Brasil, a SUSEP estabeleceu, por meio da Circular nº 612/2020, um arcabouço normativo principiológico, orientado pela proporcionalidade e pela abordagem baseada em risco. A Resolução SUSEP nº 99/2026 atualiza esse arcabouço e substituirá a Circular a partir de 1º de janeiro de 2027.

A evolução tecnológica e o surgimento de novos arranjos operacionais, especialmente aqueles baseados em intermediação digital e compartilhamento de infraestrutura, exigem adaptação contínua das supervisionadas para assegurar a efetividade da prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa.

Nesse contexto, destacam-se:

- atualização dos critérios de monitoramento conforme a evolução dos riscos;
- integração entre controles tecnológicos, governança e gestão de riscos;
- definição clara de responsabilidades entre os agentes envolvidos;
- aplicação de diligência simplificada, padrão ou reforçada, proporcional ao risco identificado;
- avaliação da efetividade das políticas, dos procedimentos e dos controles internos;
- alinhamento entre inovação, regulação e supervisão.

Atualização normativa: publicada em 1º de outubro de 2026, a Resolução SUSEP nº 99/2026 inclui expressamente em seu alcance as administradoras de operações de proteção patrimonial mutualista, as sociedades seguradoras de propósito específico e as sociedades processadoras de ordem do cliente (SPOCs), mantendo as cooperativas de seguros entre os sujeitos obrigados.

A norma explicita a prevenção ao financiamento da proliferação de armas de destruição em massa, detalha os níveis de diligência conforme o risco e disciplina o aproveitamento de procedimentos de identificação, qualificação e classificação de clientes realizados por entidades do mesmo conglomerado ou sistema cooperativo, preservando a responsabilidade individual. Também reorganiza as exigências de informações sobre residência e sede e exige indicadores quantitativos e qualitativos na avaliação de efetividade.



A Confederação Nacional das Seguradoras (CNseg), por meio de sua Comissão de Governança e *Compliance*, contribuiu para a Consulta Pública nº 2/2026. Com a publicação da resolução, as entidades devem avaliar e implementar as adequações necessárias para sua entrada em vigor.

A Instrução Normativa SUSEP nº 40, de 30 de setembro de 2026, atualiza os procedimentos internos para comunicação de operações e situações suspeitas ao Conselho de Controle de Atividades Financeiras (Coaf). A norma complementa a atuação regulatória da Autarquia: enquanto a Resolução SUSEP nº 99/2026 disciplina as obrigações de PLD/FTP das entidades supervisionadas, a Instrução Normativa organiza o tratamento e o encaminhamento das informações pelos servidores da SUSEP.

A atualização adapta os procedimentos estabelecidos em 2015 ao ambiente eletrônico da Autarquia, prevendo tramitação em processos específicos e sigilosos, concentração da documentação no mesmo processo e definição do fluxo de análise pelas áreas responsáveis. A apreciação passa a contar com o Comitê de Supervisão Integrada (CSINT), que reúne diferentes áreas de supervisão antes da deliberação sobre a comunicação ao Coaf. Essas medidas buscam conferir maior agilidade e segurança ao fluxo interno, preservando o sigilo das informações.

Sociedades processadoras da ordem do cliente – SPOCs (art. 36-A do DL 73/66 – LC 213/2025)

A Lei Complementar nº 213/2025 reforçou a base legal da supervisão das sociedades processadoras de ordem do cliente pela SUSEP, entidades já disciplinadas pela Resolução CNSP nº 429/2021.

Essas entidades operam predominantemente em ambiente digital (*Open Insurance*), atuam no processamento de ordens diretas dos clientes e processam grande volume de dados e transações em tempo quase real. Diferentemente do modelo tradicional centrado na relação direta seguradora–cliente ou seguradora-corretor-cliente, esse arranjo cria um novo tipo de relação com o consumidor, mais mediada por plataformas tecnológicas e menos dependente de interações presenciais. Do ponto de vista da PLD/FTP, esse modelo apresenta oportunidades e riscos:

Oportunidades

- Maior capacidade de rastreamento digital de operações;
- Uso de ferramentas analíticas avançadas para a identificação de padrões suspeitos;
- Integração de bases de dados para a melhoria de KYC e do monitoramento contínuo.

Riscos e Desafios

- Possível diluição de responsabilidades entre diferentes agentes da cadeia;
- Dependência de terceiros para a coleta e o tratamento de dados sensíveis;
- Necessidade de governança clara sobre compartilhamento, armazenamento e uso de informações pessoais;
- Potencial aumento de riscos cibernéticos e de vazamento de dados.

Novas operações de cooperativas e proteção patrimonial mutualista (LC 213/2025)

A Lei Complementar nº 213/2025 introduziu mudanças relevantes na estrutura do mercado segurador brasileiro ao reconhecer e disciplinar modelos que, embora não se enquadrem formalmente como contratos de seguro tradicionais, apresentam funcionalidades econômicas análogas, especialmente no que se refere à proteção contra riscos patrimoniais.

A introdução de cooperativas e operações de proteção patrimonial mutualista representa um avanço relevante na diversificação do mercado, mas também amplia a complexidade do ambiente de riscos.

A efetividade dos mecanismos de PLD/FTP dependerá da capacidade de adaptação das novas instituições e do regulador a essas novas estruturas, assegurando que a inovação ocorra de forma compatível com a integridade, a transparência e a estabilidade do sistema.



As cooperativas organizam-se para oferecer aos seus membros mecanismos de proteção financeira contra determinados riscos, com regras de cobertura que, na prática, se aproximam da lógica securitária.

Embora possuam natureza jurídica distinta daquela das seguradoras, essas entidades podem:

- administrar recursos destinados à cobertura de eventos futuros e incertos;
- definir critérios de elegibilidade e pagamento de benefícios;
- estruturar mecanismos de mutualização de riscos entre os cooperados.

Essa aproximação funcional com o seguro tradicional amplia a relevância dessas entidades no sistema financeiro ampliado, ao mesmo tempo em que demanda a aplicação de mecanismos de supervisão e controle compatíveis com os riscos envolvidos.

Já as operações de proteção patrimonial mutualista baseiam-se no princípio da solidariedade entre participantes, que contribuem para um fundo comum destinado a suportar prejuízos individuais quando ocorrem eventos previamente definidos.

Nesse modelo:

- o risco não é transferido a uma seguradora, mas compartilhado entre os membros;
- as contribuições podem variar conforme a sinistralidade;
- os pagamentos dependem da disponibilidade de recursos no fundo coletivo;
- a gestão pode envolver estruturas associativas ou entidades organizadoras.

Embora juridicamente distintas dos contratos de seguro, essas operações reproduzem efeitos econômicos semelhantes, especialmente no que se refere à proteção patrimonial e à circulação de recursos financeiros.

A introdução desses modelos amplia o espectro de entidades sujeitas a riscos de utilização indevida para fins de lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

Isso ocorre porque tais estruturas podem envolver:

- captação e gestão de recursos de múltiplos participantes;
- fluxos financeiros recorrentes e potencialmente fragmentados;



- intermediação por entidades com diferentes níveis de maturidade de governança;
- menor padronização operacional em comparação com o mercado segurador tradicional.

Nesse contexto, a aplicação de mecanismos de PLD/FTP torna-se essencial, especialmente no que se refere a:

- identificação e qualificação de participantes;
- verificação da origem dos recursos;
- monitoramento de contribuições e pagamentos;
- rastreabilidade das operações;
- comunicação de situações suspeitas.

A ausência ou a fragilidade desses controles pode criar vulnerabilidades relevantes, tanto do ponto de vista regulatório quanto reputacional.

Se, por um lado, a expansão dessas estruturas traz consigo riscos específicos, por outro, quando adequadamente estruturados e supervisionados, esses modelos também apresentam oportunidades relevantes:



Riscos associados aos novos modelos

- Fragmentação de responsabilidades: múltiplos agentes envolvidos na gestão, na intermediação e na operação;
- Assimetria de controles: diferentes níveis de maturidade em governança e compliance;
- Dificuldade de rastreabilidade: fluxos financeiros pulverizados entre diversos participantes;
- Potencial uso indevido de estruturas coletivas para a dissimulação da origem dos recursos;
- Arbitragem regulatória: utilização desses modelos como alternativa a estruturas mais reguladas.

Oportunidades e ganhos estruturais

- Ampliação do acesso a mecanismos de proteção patrimonial;
- Maior inclusão financeira;
- Diversificação de soluções de gestão de risco;
- Estímulo à inovação no setor segurador;
- Desenvolvimento de modelos mais flexíveis e adaptados a nichos específicos.

A incorporação desses modelos ao ambiente regulado impõe desafios relevantes à supervisão e à implementação de controles de PLD/FTP, especialmente no que se refere à definição de responsabilidades, à padronização de procedimentos e à integração de informações.

PLD/FTP no Contexto de *Open Finance* e *Open Insurance*

O *Open Finance* e o *Open Insurance* ampliam as possibilidades de inovação e eficiência, mas também introduzem desafios estruturais para os mecanismos de PLD/FTP.

A efetividade desses sistemas dependerá da capacidade das instituições e dos reguladores de adaptar seus modelos de controle a um ambiente caracterizado por maior interconectividade, fragmentação operacional e velocidade transacional, assegurando que a abertura do sistema ocorra de forma compatível com a integridade, a transparência e a estabilidade do mercado.

A implementação dos ecossistemas de *Open Finance* e *Open Insurance* representa uma mudança estrutural na prestação de serviços financeiros e securitários, baseada no compartilhamento padronizado de dados, mediante consentimento do cliente, na interoperabilidade entre instituições e na atuação distribuída de múltiplos participantes ao longo da cadeia de valor.

Esse modelo pretende ampliar a concorrência, a inovação e a personalização de produtos, mas também altera de forma relevante a dinâmica de riscos associados à PLD/FTP.

A ampliação do ecossistema, com a entrada de *fintechs*, *insurtechs*, agregadores de dados e, no caso do *Open Insurance*, das SPOCs, introduz um modelo operacional distribuído, no qual diferentes agentes passam a desempenhar funções complementares na iniciação, no processamento e na execução de operações. Nesse contexto, surgem desafios relevantes, como:

- fragmentação de responsabilidades entre participantes;
- assimetria informacional entre iniciadores e detentores dos produtos;
- dificuldade de consolidação de dados para análise de risco;
- limitação da visão integral da jornada do cliente e da transação.

Essa configuração pode dificultar a verificação da origem dos recursos, a identificação do beneficiário final e o monitoramento consolidado das operações.



A integração por meio de Interface de Programação de Aplicações (*Application Programming Interface* – APIs), aliada à contratação remota e à execução quase instantânea de transações, reduz o tempo disponível para análises preventivas e amplia a capacidade de dispersão rápida de recursos.

Adicionalmente, o uso de identidades digitais, credenciais compartilhadas ou comprometidas e a atuação de intermediários tecnológicos podem permitir o acesso a múltiplas instituições sem presença física, aumentando a exposição a:

- fraudes estruturadas;
- utilização de "laranjas";
- ocultação da titularidade efetiva dos recursos.

No setor de seguros, embora determinados produtos apresentem, em geral, menor risco intrínseco, a digitalização amplia a complexidade operacional das transações, especialmente em operações como:

- contratação remota;
- indicação de beneficiários;
- pagamento de prêmios;
- resgates e portabilidades;
- pagamento de benefícios.

A atuação de iniciadores externos e intermediários tecnológicos pode reduzir a visibilidade das instituições sobre o contexto econômico das operações, dificultando a identificação de incoerências e padrões atípicos.

A interconectividade e a capacidade de movimentação rápida de recursos também ampliam a exposição a riscos associados ao financiamento do terrorismo, especialmente por meio de transferências de baixo valor e alta frequência, e ao financiamento da proliferação, frequentemente vinculado a operações comerciais complexas envolvendo múltiplas jurisdições.

Por outro lado, o acesso ampliado a dados estruturados e o uso de ferramentas analíticas avançadas podem fortalecer significativamente a capacidade de identificação de riscos, desde que acompanhados de:

- governança adequada sobre dados e modelos;
- integração entre sistemas e bases de informação;
- definição clara de responsabilidades entre participantes;
- mecanismos de compartilhamento seguro de informações.

Mais uma vez, a abordagem baseada em risco é ponto-chave e deve evoluir para considerar não apenas o cliente, mas também:

- os participantes envolvidos na operação;
- os canais utilizados;
- a arquitetura da transação no ecossistema aberto.

A evolução desses modelos reforça o papel do regulador na definição de um arcabouço que assegure clareza na atribuição de responsabilidades, padrões mínimos de governança, segurança da informação e mecanismos eficazes de supervisão.

A definição de responsabilidades entre participantes, especialmente novos entrantes como as SPOCs, torna-se elemento central para evitar lacunas que possam ser exploradas para fins ilícitos.

Integração no combate à lavagem de dinheiro e os reflexos para o setor de seguros

Capítulo 5



O cenário contemporâneo de PLD/FTP evidencia que o enfrentamento do crime financeiro não pode ser conduzido de forma isolada ou segmentada. A crescente sofisticação das estruturas ilícitas — frequentemente transnacionais, digitalizadas e operando por meio de múltiplos agentes — impõe a necessidade de integração estruturada entre órgãos reguladores, autoridades de investigação, unidades de inteligência financeira e o setor privado.

Nesse contexto, a efetividade do sistema de PLD/FTP depende da atuação coordenada de todos os seus participantes. A integração institucional não substitui a responsabilidade individual das entidades supervisionadas, mas amplia a capacidade coletiva de prevenção, detecção e resposta a ilícitos financeiros.

Em um ambiente caracterizado por elevada interconectividade, digitalização e fragmentação operacional, a integração — entre instituições, sistemas e autoridades — consolida-se como elemento crítico para a preservação da integridade e da estabilidade do sistema financeiro e securitário.

Integração como resposta à complexidade crescente

A evolução recente do sistema financeiro e securitário, marcada pela digitalização, pela interoperabilidade entre instituições e pela atuação distribuída de participantes (potencializada por ecossistemas como *Open Finance* e *Open Insurance*), ampliou significativamente a complexidade das operações e a fragmentação das responsabilidades.

Nesse ambiente, esquemas ilícitos tendem a explorar:

- lacunas entre diferentes regimes regulatórios;
- assimetrias informacionais entre participantes;
- descontinuidade de controles ao longo da cadeia de valor;
- velocidade e dispersão das transações digitais.

Dessa forma, a integração institucional deixa de ser apenas um mecanismo de cooperação e passa a ser elemento essencial para recompor a visão consolidada dos riscos.

Capacidades ampliadas pela integração

A coordenação entre autoridades prudenciais, órgãos de persecução penal, unidades de inteligência financeira e entidades supervisoras fortalece a capacidade do sistema de PLD/FTP de:

- compartilhar informações relevantes de forma tempestiva e estruturada;
- harmonizar critérios e metodologias de avaliação de risco;
- identificar padrões complexos e interinstitucionais de movimentação ilícita;
- coordenar ações de supervisão, investigação e responsabilização.

Essa atuação integrada é particularmente relevante em ambientes caracterizados por alta interconectividade e múltiplos intermediários.

Implicações para o setor de seguros

Para o setor de seguros, os reflexos dessa integração são diretos e estruturantes.

Em primeiro lugar, intensifica-se a exigência quanto à qualidade, à consistência e à rastreabilidade das informações reportadas às autoridades. Os sistemas internos devem ser capazes de produzir dados íntegros, auditáveis e alinhados às expectativas de supervisão e inteligência financeira.

Em segundo lugar, a ampliação da cooperação institucional eleva o nível de diligência esperado sobre toda a cadeia operacional. Isso inclui intermediários, parceiros comerciais, prestadores de serviços tecnológicos e novos agentes introduzidos por modelos digitais.

Nesse contexto, a responsabilidade das entidades supervisionadas não se limita à sua estrutura interna, mas se estende à governança de terceiros e à compreensão integrada das operações realizadas em ambientes distribuídos.

Alinhamento internacional e consistência regulatória

A consolidação de uma abordagem interinstitucional reforça a necessidade de alinhamento contínuo com padrões internacionais, especialmente aqueles estabelecidos pelo GAFI/FATF.

A aderência a esses parâmetros contribui para:

- reduzir riscos sistêmicos;
- fortalecer a credibilidade regulatória;
- assegurar consistência entre diferentes jurisdições;
- mitigar exposições reputacionais associadas a falhas de prevenção.

Integração entre supervisão e PLD/FTP

No setor segurador, a evolução regulatória recente — caracterizada pela digitalização, pelo aumento da circulação de dados e pela introdução de novos modelos operacionais — torna ainda mais relevante a articulação entre:

- supervisão prudencial;
- supervisão de conduta;
- mecanismos de PLD/FTP.

Falhas em qualquer desses eixos tendem a se propagar de forma sistêmica, especialmente em ambientes interconectados.

Implicações para as estruturas internas

O fortalecimento da integração institucional deve ser acompanhado por uma evolução equivalente nas estruturas internas das entidades supervisionadas, por meio de:

- programas robustos de governança e compliance;
- gestão integrada de riscos (incluindo riscos operacionais, tecnológicos e de PLD/FTP);
- mecanismos claros de comunicação interna e externa;
- estruturas de controle capazes de operar em ambientes digitais e distribuídos;
- cultura organizacional orientada à integridade e à prevenção.

Outros órgãos reguladores

CVM

Em 22 de dezembro de 2025, foi disponibilizada atualização relevante no âmbito do mercado de capitais, com o objetivo de contemplar as alterações introduzidas pela Resolução CVM nº 175, que reformulou o marco regulatório dos fundos de investimento no Brasil. A atualização dos guias de prevenção à lavagem de dinheiro e proteção de dados de cotistas, promovida no âmbito da autorregulação da Associação Brasileira das Entidades dos Mercados Financeiros (ANBIMA), reforça a centralidade da governança, da diligência e da responsabilidade dos participantes da cadeia de distribuição e gestão de recursos.

Entre as principais mudanças, destaca-se a ampliação das responsabilidades do gestor, que passa a assumir papel mais ativo na condução de diligências para a contratação de distribuidores, além de reforçar seus deveres de monitoramento e supervisão contínua. Trata-se de movimento alinhado às melhores práticas internacionais recomendadas pelo GAFI/FATF, com ênfase na abordagem baseada em risco e na responsabilização clara dos agentes econômicos ao longo da cadeia operacional.

Outro ponto relevante foi a expansão da lista de bases e sites sugeridos para consulta de instituições ou pessoas vinculadas ao financiamento do terrorismo e à proliferação de armas de destruição em massa. A ampliação dessas referências demonstra o fortalecimento do monitoramento preventivo e a incorporação de parâmetros internacionais mais rigorosos no sistema brasileiro.

O movimento observado no âmbito da CVM guarda importante paralelismo com o setor segurador. Assim como no mercado de capitais, o setor de seguros também vem experimentando maior complexidade na cadeia de distribuição; crescente participação de intermediários digitais e novos agentes; ampliação de responsabilidades de governança e controles internos; e ênfase na abordagem baseada em risco e na responsabilização proporcional dos participantes.

No contexto da Resolução SUSEP nº 99/2026, que substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027, e das inovações trazidas pela Lei Complementar nº 213/2025, observa-se uma convergência regulatória: diligência na identificação, qualificação e acompanhamento de parceiros e prestadores de

serviços; clareza na definição de responsabilidades; aplicação de controles proporcionais ao risco; e alinhamento às recomendações do GAFI. A nova resolução também contempla expressamente as administradoras de operações de proteção patrimonial mutualista e as sociedades processadoras de ordem do cliente (SPOCs), além de incorporar às políticas, aos procedimentos e aos controles internos a prevenção ao financiamento da proliferação de armas de destruição em massa.

Assim como a Resolução CVM nº 175 consolidou no mercado de capitais a figura do gestor como agente central de governança e diligência, no setor de seguros cresce a expectativa de que seguradoras e demais supervisionadas adotem postura ativa na relação com intermediários, correspondentes, processadores e demais parceiros de negócio, especialmente em ambientes digitais.

Esse alinhamento intersetorial fortalece a posição do Brasil perante avaliações internacionais e contribui para reduzir assimetrias regulatórias entre segmentos financeiros, promovendo maior coerência sistêmica na prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

BACEN

Os recentes acontecimentos envolvendo riscos tecnológicos, incidentes cibernéticos e vulnerabilidades operacionais reforçaram a centralidade da governança de terceiros no sistema financeiro. Nesse contexto, o BCB publicou a Resolução BCB nº 498, estabelecendo novos requisitos para o credenciamento e a atuação dos Prestadores de Serviços de Tecnologia da Informação (PSTIs), entidades aptas a prestar serviços de processamento de dados às instituições financeiras e demais instituições autorizadas a funcionar pelo BCB para acesso à Rede do Sistema Financeiro Nacional (RSFN).

A norma consolida um movimento regulatório claro: a tecnologia deixou de ser mero suporte operacional e passou a ser elemento crítico de risco sistêmico, exigindo estrutura robusta de governança, gestão de riscos e mecanismos de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FTP).

Além disso, atribui às instituições contratantes a responsabilidade de assegurar que os PSTIs contratados estejam plenamente aderentes à

regulamentação, reforçando o dever de diligência e monitoramento contínuo.

A Resolução BCB nº 498 deixa explícita a exigência de que os PSTIs mantenham mecanismos estruturados de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, além de controles robustos para a mitigação de riscos operacionais, cibernéticos e de fraude.

Esse movimento reforça três tendências regulatórias relevantes:

1. responsabilização ampliada de terceiros críticos;

2. elevação do padrão mínimo de governança tecnológica;

3. integração entre risco operacional, risco cibernético e risco de PLD/FTP.

O recado regulatório é inequívoco: terceirização não significa transferência de responsabilidade.

O setor de seguros vive momento semelhante, especialmente com:

- a crescente digitalização das operações;
- a entrada de novos agentes tecnológicos, como as sociedades processadoras de ordem do cliente;
- a ampliação do uso de plataformas e intermediários digitais;
- a necessidade de compartilhamento de dados em estruturas como Sistema de Registro de Operações (SRO) e *Open Insurance*.

A Resolução SUSEP nº 99/2026, que substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027, reforça a articulação entre governança, gestão de riscos e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa. A norma inclui expressamente as sociedades processadoras de ordem do cliente (SPOCs) em seu alcance e estabelece procedimentos de identificação, qualificação e classificação de risco de funcionários, parceiros e prestadores de serviços terceirizados.

Também prevê a avaliação dos riscos associados à utilização de novas tecnologias e atribui à diretoria e ao conselho de administração, quando existente, a responsabilidade por prover estrutura de governança e recursos humanos, financeiros e tecnológicos adequados. A indicação de um diretor responsável por PLD/FTP não afasta a responsabilidade dos demais diretores em suas respectivas áreas de competência.

Nesse contexto, a evolução tecnológica exige atenção contínua a:

- critérios de seleção, contratação e acompanhamento de terceiros, proporcionais aos riscos identificados;
- definição clara de responsabilidades e prevenção de conflitos de interesses;
- integração entre controles tecnológicos e gestão de riscos de PLD/FTP;
- qualidade, integridade e atualização das informações utilizadas nas diligências;
- avaliação da efetividade dos controles, com indicadores quantitativos e qualitativos.

A experiência do Banco Central indica tendência regulatória de aproximação entre supervisão prudencial, supervisão tecnológica e supervisão de PLD/FTP, reconhecendo que falhas tecnológicas podem gerar impactos reputacionais, operacionais e financeiros equivalentes aos riscos tradicionais.

A imposição de capital mínimo, auditorias externas, certificações internacionais e seguros obrigatórios demonstra que o BCB passou a tratar determinados prestadores tecnológicos como infraestruturas críticas.

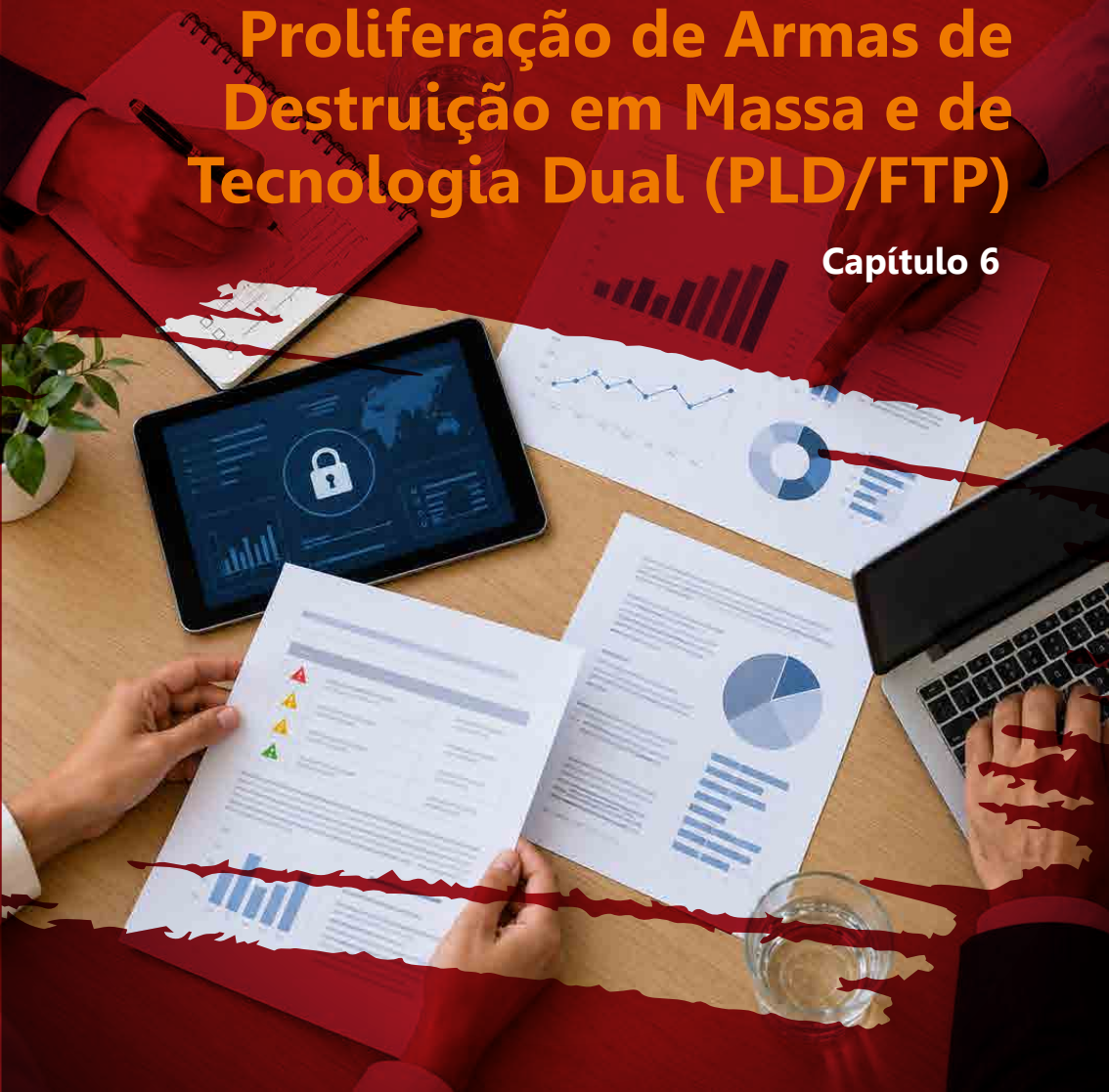
No setor de seguros, à medida que novos modelos de negócio ampliam a intermediação digital e o trânsito de grandes volumes de dados sensíveis, torna-se relevante avaliar se estruturas equivalentes de governança e diligência sobre terceiros tecnológicos não deveriam seguir direção semelhante.

A convergência entre as práticas de governança, gestão de riscos e diligência nos segmentos supervisionados por BCB, pela CVM e pela SUSEP pode contribuir para reduzir assimetrias e fortalecer a efetividade da prevenção a ilícitos financeiros. A efetividade dessa convergência depende, contudo, na implementação dos controles e da capacidade de demonstrar os resultados alcançados.



O Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa e de Tecnologia Dual (PLD/FTP)

Capítulo 6



Estrutura do Programa de PLD/FTP

O programa de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP) deve integrar a governança corporativa e estar alinhado ao sistema de controles internos e à estrutura de gestão de riscos da instituição. Sua organização deve considerar as características das operações, os objetivos estratégicos e os requisitos regulatórios aplicáveis. A adoção de uma política única no âmbito de um conglomerado ou sistema cooperativo é permitida, desde que contemple as especificidades das operações de cada entidade.

Para as pessoas sujeitas[1] à regulamentação da SUSEP, o art. 5º da Resolução SUSEP nº 99/2026 determina o desenvolvimento e a implementação de políticas, procedimentos e controles internos efetivos, destinados à identificação, à avaliação, ao controle e ao monitoramento dos riscos de envolvimento em lavagem de dinheiro e financiamento do terrorismo e da proliferação de armas de destruição em massa. Esses mecanismos devem abranger os produtos comercializados, as negociações privadas, as operações de compra e venda de ativos e as demais práticas operacionais. A resolução substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027.

A Avaliação Interna de Riscos deve orientar a aplicação de diligência simplificada, padrão ou reforçada, com procedimentos e controles proporcionais aos riscos identificados.

Se, no passado, a prevenção à lavagem de dinheiro estava fortemente associada ao rastreamento de fluxos financeiros tradicionais — muitas vezes vinculados a dinheiro em espécie e movimentações físicas —, o cenário atual é substancialmente distinto e mais complexo.

A digitalização dos serviços financeiros, a ampliação de modelos de negócio baseados em plataformas, o uso intensivo de dados e a crescente interdependência entre instituições transformaram profundamente a dinâmica dos riscos. Hoje, os fluxos financeiros são predominantemente digitais, instantâneos, descentralizados

[1] Art. 2º Sujeitam-se às obrigações previstas nesta Resolução as sociedades seguradoras, as sociedades de capitalização, as entidades abertas de previdência complementar - EAPC, os resseguradores locais, os resseguradores admitidos, as corretoras de resseguro, os corretores de seguros pessoas naturais ou jurídicas, as sociedades seguradoras de propósito específico, as sociedades cooperativas de seguros, as administradoras de operações de proteção patrimonial mutualista e as sociedades processadoras de ordem do cliente - SPOC.

e, muitas vezes, operados por múltiplos participantes ao longo de uma mesma cadeia.

Nesse novo ambiente, a prevenção à lavagem de dinheiro e ao financiamento do terrorismo deixa de ser uma atividade centrada apenas na análise de transações e passa a exigir uma compreensão ampla de ecossistemas operacionais complexos.

O ambiente atual impõe um desafio claro: programas de PLD/FT estáticos tendem rapidamente à obsolescência.

A velocidade das transformações tecnológicas, a entrada de novos atores, a ampliação das cadeias operacionais e o aumento da sofisticação dos ilícitos exigem uma abordagem dinâmica, integrada e prospectiva.

Mais do que atender a requisitos regulatórios, a efetividade dos programas dependerá da capacidade das instituições de:

- antecipar riscos emergentes;
- antecompreender sua posição na cadeia de valor;
- anteintegrar diferentes dimensões de risco;
- anteadaptar continuamente seus controles.

Nesse cenário, a prevenção à lavagem de dinheiro deixa de ser uma função isolada e passa a ocupar papel central na sustentabilidade, na integridade e na resiliência das instituições e do próprio mercado.

Diante desse contexto, os programas de PLD/FT precisam evoluir para evitar obsolescência e perda de efetividade. Entre as principais implicações, destacam-se:

1 Revisão da Avaliação Interna de Riscos

- consideração dos riscos associados a clientes, beneficiários de produtos de acumulação, ao modelo de negócio, à área geográfica de atuação, às operações, aos produtos, aos serviços, aos canais de distribuição, às novas tecnologias e às atividades de funcionários, parceiros e prestadores de serviços terceirizados;

- revisão a cada dois anos e sempre que ocorrerem alterações significativas nos perfis de risco, conforme o art. 15 da Resolução SUSEP nº 99/2026.

2 Integração entre áreas

- PLD/FT, tecnologia, cibersegurança, fraude e riscos operacionais;
- atuação coordenada e compartilhamento de informações.

3 Ampliação do escopo de monitoramento

- não apenas clientes, mas também terceiros, fluxos operacionais e interações sistêmicas;
- análise de comportamento e padrões, e não apenas de eventos isolados.

4 Fortalecimento da governança sobre terceiros

- *due diligence*, monitoramento contínuo e definição clara de responsabilidades;
- rastreabilidade das operações ao longo da cadeia.

5 Uso de tecnologia e analytics

- automação de controles;
- uso de dados para a identificação de padrões e anomalias;
- integração de bases internas e externas.

6 Capacidade de resposta rápida

- adaptação ágil a mudanças regulatórias e operacionais;
- revisão de políticas e controles sem necessidade de ciclos longos.

7 Avaliação da efetividade

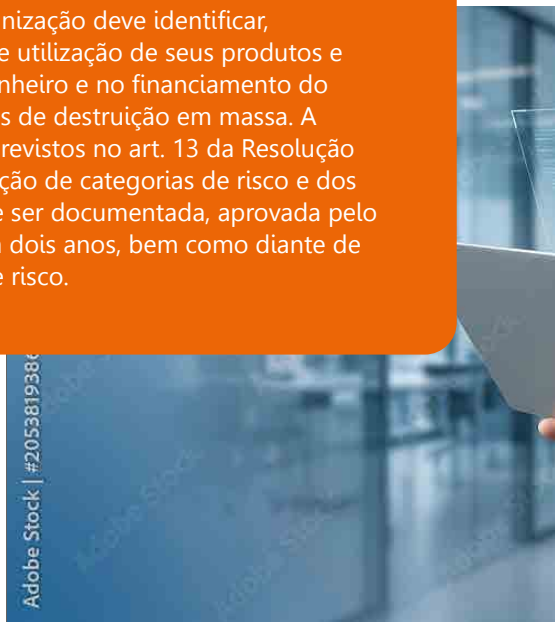
- avaliação anual das políticas, dos procedimentos e dos controles internos, documentada em relatório;
- utilização de indicadores quantitativos e qualitativos para avaliar os procedimentos de monitoramento, detecção, seleção, análise e comunicação de operações ou situações suspeitas;
- identificação de deficiências e acompanhamento das medidas e dos prazos para sua correção.

Diante desse cenário de maior complexidade operacional, intensificação do uso de tecnologia, ampliação da cadeia de terceiros e evolução constante das agendas regulatórias, torna-se ainda mais evidente que a estrutura do programa de PLD/FT deve ser sólida, dinâmica e alinhada à realidade de riscos da instituição.

Nesse contexto, destacam-se duas ações estruturantes que devem compor a governança do programa de prevenção à lavagem de dinheiro e ao financiamento do terrorismo:

Comprometimento da alta administração: a alta administração deve exercer papel ativo na definição do direcionamento estratégico do programa, assegurando o adequado "tone at the top"[2], e seu alinhamento ao sistema de controles internos e à estrutura de gestão de riscos. Nos termos dos arts. 6º e 11 da Resolução SUSEP nº 99/2026, esse comprometimento envolve a efetividade e a melhoria contínua das políticas, dos procedimentos e dos controles, além da provisão de recursos humanos, financeiros e tecnológicos adequados. A indicação de um diretor responsável por PLD/FTP não afasta a responsabilidade dos demais diretores em suas respectivas áreas de competência.

Avaliação interna de Riscos: a organização deve identificar, compreender e mensurar os riscos de utilização de seus produtos e serviços na prática de lavagem de dinheiro e no financiamento do terrorismo e da proliferação de armas de destruição em massa. A avaliação deve considerar os perfis previstos no art. 13 da Resolução SUSEP nº 99/2026 e orientar a definição de categorias de risco e dos respectivos níveis de diligência. Deve ser documentada, aprovada pelo diretor responsável e revisada a cada dois anos, bem como diante de alterações significativas nos perfis de risco.



[2] "Tone at the top" é uma expressão muito usada em governança corporativa, *compliance*, auditoria, controles internos e gestão de riscos. A ideia é que a postura e o exemplo dado pela alta administração da organização influenciam a cultura, os comportamentos e a forma como as regras são cumpridas.

Os papéis e responsabilidades das três linhas: prevenção como responsabilidade compartilhada

A prevenção à lavagem de dinheiro e ao financiamento do terrorismo deixou de ser uma função isolada e passou a exigir uma atuação integrada de toda a organização. Em um ambiente marcado pela digitalização, pela utilização intensiva de tecnologia, pela entrada de novos atores e pela ampliação da terceirização de atividades, os riscos não se concentram mais apenas nas operações internas, mas se distribuem ao longo de toda a cadeia de valor.



Nesse contexto, cada área, instância e nível hierárquico possui responsabilidade direta na identificação, na avaliação e na mitigação desses riscos. A efetividade do programa depende da capacidade da organização de atuar de forma coordenada, garantindo que decisões operacionais, tecnológicas e comerciais estejam alinhadas aos princípios de PLD/FT.

O modelo das três linhas de defesa permanece como referência para a estruturação dessa governança, mas sua aplicação exige evolução para incorporar a complexidade atual dos modelos de negócio, a interdependência entre sistemas e a atuação de terceiros.

1ª linha: gestão do risco na origem

A primeira linha é composta pelas áreas de negócio, operações, tecnologia e canais de distribuição — incluindo, cada vez mais, ambientes digitais e interfaces com terceiros.

Essas áreas estão diretamente expostas aos riscos e, portanto, são responsáveis por sua gestão no nível mais granular. Isso inclui não apenas as transações realizadas internamente, mas também aquelas originadas, processadas ou suportadas por parceiros, plataformas e prestadores de serviços.

Suas principais responsabilidades incluem:

- implementar, no dia a dia, políticas e procedimentos de PLD/FT, garantindo sua aderência às operações reais;
- incorporar controles nos fluxos operacionais e sistemas, incluindo soluções digitais e automatizadas;
- identificar e avaliar riscos associados a produtos, canais, tecnologias e terceiros envolvidos na operação;
- monitorar transações e comportamentos, considerando o uso de ferramentas tecnológicas e *analytics*;
- assegurar a qualidade, a integridade e a rastreabilidade das informações utilizadas nos processos;
- reportar tempestivamente situações suspeitas ou inconsistentes à segunda linha.

A primeira linha passa a ter papel crítico também na gestão de riscos associados a terceiros e na utilização de soluções tecnológicas, sendo responsável por garantir que a operação funcione de forma segura desde a sua origem.

2ª linha: coordenação, supervisão e integração do risco

A segunda linha — composta pelas áreas de *compliance*, controles internos, PLD/FT e gestão de riscos — tem o papel de estruturar, coordenar e supervisionar o sistema de prevenção.

Sua atuação deve evoluir de um modelo predominantemente normativo para uma abordagem integrada, capaz de dialogar com áreas de tecnologia, segurança da informação, prevenção a fraudes e gestão de terceiros.

Entre suas principais responsabilidades, destacam-se:

- definir políticas, diretrizes e procedimentos de PLD/FT alinhados à estratégia e ao perfil de risco da instituição;
- conduzir a Avaliação Interna de Riscos, incorporando riscos tecnológicos, cibernéticos, operacionais e de terceiros;
- estabelecer critérios para classificação de risco de clientes, operações, produtos e parceiros;
- monitorar a efetividade dos controles implementados pela primeira linha;
- atuar de forma integrada com áreas de tecnologia e cibersegurança na identificação de padrões de risco;

- apoiar as áreas de negócio na implementação de controles proporcionais e eficazes;
- realizar comunicações obrigatórias aos reguladores e reportar à alta administração.

A segunda linha assume, portanto, papel central na integração das diversas agendas de risco, garantindo coerência e consistência em um ambiente cada vez mais complexo e dinâmico.



3ª linha: avaliação independente

A terceira linha, representada pela auditoria interna e, em alguns casos, por estruturas independentes de gestão de riscos, é responsável por avaliar de forma independente a adequação e a eficácia do programa de PLD/FT.

Em um cenário de maior complexidade tecnológica e operacional, sua atuação deve considerar não apenas a conformidade formal, mas a efetividade dos controles diante de riscos emergentes.

Suas principais responsabilidades incluem:

- avaliar a robustez do programa de PLD/FT, incluindo sua aderência ao perfil de risco da instituição;
- testar a eficácia dos controles implementados na primeira e na segunda linhas, incluindo aqueles relacionados a sistemas, tecnologia e terceiros;
- verificar a integração entre PLD/FT, cibersegurança, prevenção a fraudes e gestão de riscos operacionais;
- identificar fragilidades estruturais e oportunidades de melhoria;
- reportar de forma independente à alta administração e aos órgãos de governança.

A terceira linha desempenha papel fundamental na identificação de lacunas que, em ambientes altamente interconectados, podem não ser evidentes no dia a dia operacional.

Importância de conhecer os clientes e suas operações

O processo de aceitação de clientes deve observar os requisitos de identificação, qualificação e classificação estabelecidos pelo regulador. Sua efetividade depende de uma abordagem estruturada e baseada em risco, que permita compreender o cliente, a natureza da relação de negócio e os riscos associados às operações.

Para as pessoas sujeitas à regulamentação da SUSEP, o art. 21 da Resolução SUSEP nº 99/2026 estabelece procedimentos de identificação que contemplem, no mínimo, clientes, beneficiários, terceiros e beneficiários finais. A resolução substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027.

Esses procedimentos devem ser compatíveis com os perfis de risco do cliente e do beneficiário de produtos de acumulação, com a natureza da relação de negócio, com a política de PLD/FTP e com a Avaliação Interna de Riscos.

Avaliação e classificação de risco

A instituição deve estabelecer critérios documentados para avaliar e classificar os riscos, considerando, entre outros aspectos:

- perfil dos clientes e dos beneficiários de produtos de acumulação;
- modelo de negócio e área geográfica de atuação;
- operações, produtos, serviços e canais de distribuição, inclusive digitais;
- utilização de novas tecnologias;
- atividades de funcionários, parceiros e prestadores de serviços terceirizados;
- condição de Pessoa Exposta Politicamente (PEP) ou de seu representante, familiar ou estreito colaborador;
- exposição a países ou territórios classificados pelo GAFI como não cooperantes ou com deficiências estratégicas;
- presença em listas de sanções do Conselho de Segurança das Nações Unidas (CSNU);
- demais fatores relevantes identificados na Avaliação Interna de Riscos.

A metodologia pode utilizar pesos e outros critérios de ponderação, desde que preserve o tratamento obrigatório das situações previstas na regulamentação. Nos termos do art. 13, as categorias de risco devem permitir a aplicação de:

Diligência simplificada: procedimentos e controles menos rigorosos e abrangentes para situações de menor risco, preservados os requisitos mínimos;

Diligência padrão: procedimentos e controles correspondentes ao nível padrão de diligência;

Diligência reforçada: procedimentos e controles mais rigorosos e abrangentes para situações de maior risco.

A simplificação não afasta a identificação do cliente nem o monitoramento das operações. Também é vedada a dispensa integral das medidas mínimas de identificação do cliente e, quando aplicável, do respectivo beneficiário final.

Identificação e acompanhamento de PEPs

A verificação deve abranger tanto a condição de PEP quanto a de seu representante, familiar ou estreito colaborador. Independentemente de autodeclaração negativa, a instituição deve recorrer a informações públicas disponíveis ou consultar bases de dados públicas ou privadas, adotando pelo menos uma dessas providências, conforme o art. 24.

As operações e as relações de negócio envolvendo PEPs, seus familiares, representantes, estreitos colaboradores ou pessoas jurídicas de que participem são consideradas de alto risco e devem ser submetidas continuamente à diligência reforçada, nos termos do art. 33.

Na diligência simplificada, a norma exige a revisão de toda a base cadastral de clientes pelo menos uma vez ao ano para identificar pessoas que possam ter se tornado PEPs. Nas situações previstas no art. 35, como renovação do contrato, pagamento de indenização ou benefício e cancelamento com devolução de prêmio, essa verificação deve ser realizada quando tiverem transcorrido mais de seis meses desde a última revisão da base.

As especificidades da instituição orientam a implementação dos controles, mas não afastam as medidas mínimas exigidas pela regulamentação.

Intermediários e compartilhamento de procedimentos

A participação de corretores e de outros intermediários deve ser considerada na avaliação dos riscos e na definição de responsabilidades. A utilização de terceiros para obtenção de informações cadastrais não afasta a responsabilidade da entidade pelo cumprimento de suas obrigações.

O art. 17 permite o aproveitar de procedimentos de identificação, qualificação e classificação de clientes realizados por instituições do mesmo conglomerado ou sistema cooperativo. Esse aproveitamento exige compartilhamento formal, integridade, atualização e rastreabilidade das informações, consideração dos riscos de cada entidade, diligências adicionais, quando necessárias, e definição de papéis e responsabilidades.

A norma também prevê tratamento específico para corretores de seguros com faturamento bruto anual inferior a R$ 12 milhões no exercício precedente, resseguradores admitidos e SPOCs, conforme as condições do art. 48.

Qualidade das informações e diligências

A efetividade do processo de "Conheça Seu Cliente" (KYC) depende de informações suficientes e confiáveis para compreender o perfil do cliente, avaliar sua capacidade financeira e verificar a compatibilidade entre os produtos contratados e as operações realizadas.

Os procedimentos devem contemplar, conforme os requisitos aplicáveis:

1. identificação do cliente e das demais pessoas abrangidas pela norma;
2. no caso de pessoa jurídica, identificação de controladores até o nível de pessoa natural, dos principais administradores, dos procuradores e dos beneficiários finais;
3. qualificação do cliente, incluindo informações sobre residência ou sede e capacidade financeira;
4. verificação da condição de PEP e de seus representantes, familiares e estreitos colaboradores;
5. verificação de sanções e determinações de indisponibilidade de ativos;
6. verificação e validação das informações, com intensidade compatível com o nível de diligência e as possibilidades de simplificação previstas na norma.



Como medidas complementares, a instituição pode adotar pesquisas reputacionais, incluindo menções negativas em fontes idôneas, e consultas a outras listas relevantes, conforme os riscos identificados. Essas práticas devem ser diferenciadas dos requisitos mínimos expressamente previstos na regulamentação.

Nas situações de alto risco previstas no art. 33, a diligência reforçada deve incluir a autorização prévia de alçadas superiores para estabelecer ou prosseguir com a relação de negócios, além da obtenção e da validação de informações adicionais, quando disponíveis, sobre a identidade do cliente, o beneficiário final, a estrutura societária e a origem dos recursos.

Monitoramento e governança

A prevenção não se encerra na aceitação do relacionamento. A qualificação do cliente deve ser reavaliada de forma permanente, por meio de diligências contínuas, e a classificação de risco deve ser revista sempre que houver alterações no perfil do cliente ou na natureza da relação de negócio.

Os procedimentos devem permitir identificar mudanças relevantes nas informações cadastrais, no comportamento do cliente e nas características das operações, orientando a atualização dos controles e a adoção das medidas cabíveis.

A governança deve definir responsabilidades e alçadas de decisão, observando as autorizações obrigatórias para as situações de alto risco previstas na norma. Mecanismos de duplo controle e da validação independente podem ser adotados como práticas complementares, conforme a estrutura e a exposição ao risco da instituição.

O cumprimento das determinações de indisponibilidade de ativos deve ser imediato e não se submete à abordagem baseada em risco.

Monitoramento de operações e a importância da compatibilidade

O monitoramento de operações e de relações de negócio constitui atividade essencial à prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP). Consiste no acompanhamento contínuo e na análise de operações e propostas, individualmente ou em conjunto, para identificar situações atípicas ou suspeitas.

A Resolução SUSEP nº 99/2026, que substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027, disciplina esse processo e estabelece níveis de diligência proporcionais aos riscos identificados.

Em um ambiente de crescente digitalização, múltiplos canais de distribuição e participação de terceiros, o monitoramento exige uma abordagem dinâmica e integrada, capaz de relacionar informações cadastrais, características das operações e comportamento dos envolvidos.

A análise da compatibilidade financeira permite avaliar se as operações são coerentes com a capacidade financeira do cliente, a natureza de suas atividades e seu histórico de relacionamento. A qualificação deve incluir informações sobre renda, no caso de pessoa natural, ou faturamento, no caso de pessoa jurídica, observadas as regras de verificação e validação aplicáveis a cada nível de diligência.

Essa análise deve considerar a evolução do perfil do cliente, a natureza da relação de negócio e a interação com produtos, canais e terceiros. A automação e as ferramentas analíticas podem apoiar a identificação de padrões e desvios, desde que seus critérios sejam adequados aos riscos e sua efetividade seja avaliada.

Entre os sinais de atenção que podem orientar o monitoramento, destacam-se:

- operações incompatíveis com a capacidade financeira ou com as atividades do cliente;
- valores ou frequência de operações discrepantes do histórico de relacionamento;
- estruturas complexas ou participação de múltiplos intermediários sem justificativa aparente;
- operações envolvendo jurisdições de maior risco;
- uso de canais digitais de forma inconsistente com o comportamento esperado;
- indícios de fraude, uso indevido de credenciais ou movimentações financeiras associadas;
- pagamentos a beneficiários sem aparente relação com o contratante.

Esses sinais devem ser analisados em conjunto com as informações disponíveis e o contexto da operação. Sua ocorrência, isoladamente, não comprova a prática de um ilícito. Também devem ser observadas as situações para as quais a regulamentação determina diligência reforçada ou comunicação automática ao Coaf.

A crescente interdependência entre operações, tecnologia e terceiros exige que o monitoramento considere o contexto das transações, incluindo a atuação de parceiros, prestadores de serviços e plataformas. A integração entre áreas de negócio, compliance, controles internos, tecnologia, prevenção a fraudes e gestão de riscos contribui para uma análise abrangente e tempestiva.

Nos termos do art. 36 da Resolução SUSEP nº 99/2026, quando a análise indicar atipicidade ou indícios da ocorrência de crime, a comunicação ao Coaf deve ser realizada em até 24 horas, contadas da conclusão da análise ou do conhecimento da condição assim enquadrada, preservado o sigilo.

A efetividade do monitoramento deve ser avaliada por meio de indicadores quantitativos e qualitativos, conforme o art. 43, com identificação de deficiências e acompanhamento das medidas de correção.

O monitoramento contínuo, proporcional ao risco e apoiado em informações confiáveis fortalece a capacidade de prevenção, a governança e a segurança das operações.



Listas impeditivas, restritivas e sanções: base estruturante do controle de PLD/FT

A utilização de listas e bases de referência constitui instrumento relevante dos programas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP). Essas fontes apoiam a identificação de riscos e o cumprimento de restrições legais. É necessário distinguir as informações que exigem diligência reforçada, como a condição de Pessoa Exposta Politicamente (PEP), das determinações que impõem a indisponibilidade de ativos ou outros impedimentos legais.

A instituição deve estabelecer procedimentos de consulta aplicáveis a clientes, beneficiários, parceiros, prestadores de serviços e demais partes relacionadas, conforme os requisitos regulatórios e os riscos identificados. As consultas devem integrar os processos de aceitação e acompanhamento dos relacionamentos. Para as determinações de indisponibilidade de ativos do Conselho de Segurança das Nações Unidas (CSNU), o monitoramento deve ser permanente e permitir o cumprimento imediato, independentemente dos ciclos de revisão cadastral.

Os procedimentos devem contemplar fontes que permitam:

- verificar a condição de PEP e de seu representante, familiar ou estreito colaborador;
- identificar a exposição a países ou territórios classificados pelo GAFI como não cooperantes ou com deficiências estratégicas;
- identificar pessoas, entidades e ativos sujeitos às determinações de indisponibilidade do CSNU ou de seus comitês de sanções.

Listas de sanções estrangeiras, como a *Specially Designated Nationals and Blocked Persons List* (SDN), podem complementar os controles, conforme a exposição internacional, as obrigações aplicáveis e a política da instituição. Sua utilização não deve ser confundida com a obrigatoriedade de cumprimento das determinações do CSNU prevista na legislação brasileira.

A Resolução SUSEP nº 99/2026, que substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027, determina, em seu art. 46, o cumprimento imediato e sem aviso prévio das resoluções do CSNU ou das designações de seus comitês de sanções que imponham a indisponibilidade de ativos, nos termos da Lei nº 13.810/2019, sem prejuízo das determinações judiciais previstas nessa lei.

O cumprimento dessas medidas não se submete à abordagem baseada em risco. Diferentemente da identificação de PEPs ou de outros fatores que exigem diligência reforçada, a determinação de indisponibilidade impõe uma obrigação vinculante.

Além das listas de caráter obrigatório, a instituição pode e deve desenvolver listas e critérios complementares, com base em sua experiência, perfil de risco e características de seus modelos de negócio. Entre os principais elementos que podem ser considerados, destacam-se:

- histórico de mídia negativa e informações reputacionais;
- características dos produtos e serviços operacionalizados;
- atividade econômica e setor de atuação;
- capacidade econômico-financeira;
- exposição geográfica, incluindo regiões de maior risco.

Em um ambiente marcado pela digitalização, pela atuação em cadeia e pela participação crescente de terceiros, a efetividade desses controles depende também da capacidade de integrá-los aos sistemas e processos da instituição. Isso inclui:

- automação das consultas em bases atualizadas;
- integração com processos de *onboarding* e monitoramento contínuo;
- cobertura de múltiplos pontos da cadeia (clientes, parceiros, prestadores e plataformas);
- atualização tempestiva das listas e reprocessamento da base.

As listas de sanções, em especial, desempenham papel estratégico no contexto global de combate ao financiamento do terrorismo, ao buscarem restringir o acesso de indivíduos e entidades ao sistema financeiro e viabilizar o congelamento de ativos. Nesse sentido, sua correta implementação não apenas assegura conformidade regulatória, mas contribui diretamente para a integridade do sistema e para a mitigação de riscos sistêmicos.

Diante disso, a gestão de listas impeditivas e restritivas deve ser tratada como função crítica, integrada à governança de PLD/FT, capaz de responder de forma rápida e eficaz a mudanças no ambiente regulatório e nas estruturas de risco.

Monitoramento e seleção de operações

O monitoramento e a seleção de operações constituem elementos centrais dos programas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, permitindo a identificação tempestiva de transações atípicas, suspeitas ou incompatíveis com o perfil do cliente e com a natureza das operações.

Em um ambiente caracterizado pela digitalização, pela execução de operações em tempo real e pela participação de múltiplos agentes ao longo da cadeia, esse processo exige uma abordagem contínua, integrada e orientada por risco, que considere não apenas as transações isoladas, mas também o contexto em que são realizadas.

O monitoramento consiste no acompanhamento das operações e das relações de negócio para identificar padrões, desvios e situações que mereçam atenção. A seleção corresponde à identificação de operações ou situações que, conforme os parâmetros estabelecidos, devem ser encaminhadas para análise. Esses procedimentos podem abranger propostas e operações em diferentes etapas, inclusive antes ou depois de sua realização. A seleção, por si só, não implica bloqueio ou suspensão da transação.

Operações complexas ou com maior exposição ao risco podem exigir diligências adicionais e avaliação prévia à sua conclusão, conforme os requisitos aplicáveis e os critérios da instituição. Eventuais restrições, suspensões ou recusas devem observar a legislação, a regulamentação e os fundamentos pertinentes, distinguindo-se das medidas obrigatórias de indisponibilidade de ativos.

A definição da criticidade do monitoramento deve considerar, de forma combinada:

- o nível de risco atribuído ao cliente ou à contraparte;
- as características do produto ou serviço envolvido;
- o canal de distribuição utilizado, incluindo meios digitais;
- a participação de terceiros ou intermediários na operação;
- o contexto geográfico e regulatório.

Determinadas operações, especialmente aquelas mais complexas ou com maior exposição a riscos — como operações internacionais ou que envolvam múltiplos intermediários —, podem demandar diligências adicionais e análise prévia, conforme os requisitos aplicáveis e os critérios da instituição, com base em parâmetros estruturados que contemplem requisitos regulatórios, listas de sanções, restrições legais e informações reputacionais.

O processo de monitoramento e de seleção deve abranger a identificação de situações atípicas, tais como:

- transações incompatíveis com o perfil econômico-financeiro do cliente;
- movimentações com valores ou frequência fora do padrão histórico;
- operações realizadas em horários, localidades ou canais incomuns;
- uso de estruturas complexas ou participação de múltiplos agentes sem justificativa econômica clara;
- indícios de integração entre fraude, uso indevido de credenciais e movimentações financeiras subsequentes;
- operações envolvendo jurisdições ou contrapartes classificadas como de maior risco.

Para garantir a efetividade desse processo, alguns elementos são fundamentais:

- definição de critérios objetivos: estabelecimento de parâmetros claros para identificação de operações atípicas, considerando valores, frequência, geografia, produtos, canais e padrões de comportamento;
- uso da tecnologia: adoção de soluções adequadas aos riscos e à estrutura da instituição, que podem incluir análise de dados, inteligência artificial e monitoramento em tempo real, capazes de identificar padrões complexos e comportamentos não evidentes;



- análise contextual e histórica: avaliação das operações à luz do histórico do cliente, de seu perfil de risco e do contexto em que a transação ocorre, evitando análises isoladas e desconectadas da realidade operacional;
- verificação e aprofundamento: realização de diligências adicionais quando identificadas situações suspeitas, incluindo solicitação de informações complementares, análise documental e avaliação da finalidade econômica da operação;
- documentação e rastreabilidade: registro estruturado de todas as análises realizadas, critérios utilizados e decisões adotadas, assegurando transparência, consistência e capacidade de auditoria.

A crescente interdependência entre tecnologia, operações e terceiros amplia a complexidade desse processo. Transações podem ser originadas em uma interface digital, processadas por prestadores de tecnologia e liquidadas por diferentes agentes, o que exige que o monitoramento seja capaz de capturar riscos ao longo de toda a cadeia.

Nesse contexto, a integração entre áreas — especialmente PLD/FT, tecnologia, cibersegurança, prevenção a fraudes e gestão de riscos — torna-se essencial para garantir uma visão abrangente e tempestiva das operações.

Mais do que um requisito regulatório, o monitoramento e a seleção de operações representam um mecanismo crítico de proteção da instituição, permitindo não apenas a identificação de ilícitos, mas também a mitigação de riscos operacionais, reputacionais e sistêmicos em um ambiente cada vez mais dinâmico e interconectado.



Comunicações ao Coaf

O Coaf, ao divulgar seu Relatório Integrado de Gestão com os resultados de 2025, reforça o avanço da inteligência financeira no Brasil e a crescente sofisticação dos mecanismos de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa.

As comunicações realizadas pelos entes obrigados possuem papel estratégico. Constituem a principal fonte de insumo para a produção de relatórios de inteligência e para o apoio às autoridades de investigação e persecução penal. Esse fluxo de informações — estruturado, tempestivo e de qualidade — é fundamental para a identificação de padrões, conexões e tipologias cada vez mais complexas, especialmente em um ambiente marcado por digitalização, novos modelos de negócio e atuação em cadeia.

Nesse contexto, a comunicação ao Coaf deixa de ser apenas uma obrigação regulatória e assume caráter estratégico, exigindo das instituições capacidade analítica, integração de dados e alinhamento entre áreas, de modo a assegurar que operações suspeitas sejam identificadas, analisadas e reportadas de forma consistente e tempestiva.

Essa diretriz se materializa, no setor de seguros, nas obrigações estabelecidas

na Resolução SUSEP nº 99/2026, que substituirá a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027. A norma vincula diretamente o processo de monitoramento e seleção de operações à necessidade de reporte ao Coaf. O monitoramento não tem como finalidade apenas a identificação de situações atípicas, mas também o atendimento ao dever legal de comunicação, sendo esse um dos seus objetivos centrais.

O art. 36, § 2º, da Resolução SUSEP nº 99/2026 determina que as comunicações ao Coaf sejam realizadas em até 24 horas, contadas da conclusão da análise que indique atipicidade ou indícios da ocorrência de crime, ou do conhecimento de condição assim enquadrada. O art. 38 exige comunicação negativa anual, até o último dia útil de março, caso não tenham sido efetuadas, no ano civil anterior, as comunicações de transações ou propostas de transações previstas no art. 36. Já o art. 36, § 3º, inciso VI, determina que as comunicações sejam realizadas na forma definida pelo Coaf, sem que seja dada ciência a qualquer pessoa, inclusive aos envolvidos.

Adicionalmente, determinadas operações devem ser comunicadas independentemente de análise subjetiva, conforme critérios objetivos definidos na norma, reforçando que o processo de comunicação não se limita a julgamentos discricionários, mas também incorpora obrigações automáticas baseadas em parâmetros regulatórios.

As comunicações realizadas pelos entes obrigados possuem papel estratégico. Constituem a principal fonte de insumo para a produção de relatórios de inteligência e para o apoio às autoridades de investigação e persecução penal.

Nesse ambiente, marcado por operações digitais, múltiplos intermediários e crescente complexidade dos fluxos financeiros, a qualidade das comunicações ao Coaf passa a depender diretamente da robustez dos processos de monitoramento, da integração entre áreas e do uso de tecnologia para análise de dados em larga escala.

Dessa forma, identificar, analisar e comunicar deixam de ser etapas isoladas e passam a constituir um processo contínuo e integrado, em consonância com a **Resolução SUSEP nº 99/2026**. A efetividade do programa de PLD/FTP depende da capacidade da instituição de transformar dados em análises consistentes e, quando cabível, em comunicações ao Coaf qualificadas e tempestivas.

Importância de políticas e manuais

Todo procedimento relacionado à PLD/FTP deve estar formalmente estabelecido, documentado e atualizado em políticas, manuais e normativos internos, abrangendo não apenas a área de compliance, mas também as áreas operacionais diretamente envolvidas nos processos de relacionamento com clientes e execução de operações.

A mera formalização documental, contudo, não é suficiente para assegurar a efetividade do programa. É indispensável a implementação de um plano estruturado de comunicação e treinamento contínuo, com periodicidade definida e adequada ao nível de risco, garantindo que todos os colaboradores — especialmente aqueles expostos a funções críticas — compreendam suas responsabilidades e estejam aptos a aplicar os procedimentos estabelecidos.

Adicionalmente, os critérios, os parâmetros de monitoramento, as alçadas decisórias, os papéis e as responsabilidades, bem como o tratamento de exceções, devem estar refletidos de forma consistente na Avaliação Interna de Risco de PLD/FTP da instituição. Essa avaliação deve ser documentada e aprovada pelo diretor responsável, com encaminhamento para ciência ao comitê de risco e ao comitê de auditoria, quando houver, à diretoria e ao conselho de administração, se existente.

Avaliação Interna de Riscos

As empresas devem compreender de forma clara os riscos de PLD/FTP inerentes às suas operações, de modo a estruturar seus controles e mecanismos de prevenção de forma proporcional a esses riscos. Nesse contexto, a abordagem baseada em risco pressupõe a adoção de medidas mais rigorosas para situações de maior exposição e, de forma complementar, a possibilidade de aplicação de medidas simplificadas quando os riscos forem reduzidos.

A correta implementação dessa abordagem permite a alocação mais eficiente de recursos, direcionando



esforços para os pontos de maior criticidade e contribuindo para a efetividade e a sustentabilidade do sistema de PLD/FTP.

A Avaliação Interna de Riscos (AIR) constitui elemento central desse modelo, ao permitir a identificação, mensuração e classificação dos riscos associados às atividades desenvolvidas, aos produtos ofertados e às transações realizadas. Com base nessa avaliação, as empresas devem definir e implementar medidas adequadas de prevenção, detecção e mitigação, compatíveis com o perfil de risco identificado.

A AIR deve ser conduzida de forma estruturada, com base em critérios objetivos e metodologias consistentes, e envolver as áreas relevantes da organização, especialmente aquelas expostas a maior risco. Sua governança deve assegurar rastreabilidade, documentação adequada e validação pelos níveis apropriados de gestão.



Como instrumento de apoio, destaca-se a utilização de matriz de risco, que permite consolidar e classificar os riscos a partir de diferentes dimensões, tais como perfil de clientes, produtos e serviços, canais de distribuição, localização geográfica e natureza das operações. A partir dessa análise, é possível estabelecer níveis de risco e orientar a aplicação de controles proporcionais.

Os resultados da AIR devem subsidiar, de forma direta, a definição de políticas, procedimentos e controles internos, incluindo, entre outros, processos de *due diligence* de clientes e parceiros, monitoramento de operações, definição de alçadas decisórias e programas de treinamento.

Por fim, a AIR não deve ser tratada como exercício pontual, mas como um processo contínuo e dinâmico, sujeito a revisões periódicas e atualizações sempre que houver alterações relevantes no perfil de risco da empresa, em suas operações ou no ambiente regulatório. A manutenção desse processo, aliada à observância das orientações dos órgãos reguladores e supervisores, é essencial para assegurar a aderência às normas de PLD/FTP e a efetividade do sistema de controles.

Auditoria

O programa de PLD/FTP deve ser abrangido pelo plano anual da auditoria interna, quando existente, para verificar o cumprimento da Resolução SUSEP nº 99/2026 em todos os seus aspectos (art. 5º V).

A auditoria interna exerce papel fundamental nesse processo, ao atuar de forma independente na verificação da aderência das práticas da instituição às políticas internas e às normas regulatórias aplicáveis, bem como na avaliação da capacidade dos controles existentes de mitigar os riscos identificados.

Nesse contexto, a atuação da auditoria interna deve contemplar, entre outros aspectos:

- avaliação da existência, adequação e efetividade dos controles internos destinados à prevenção e à detecção de operações suspeitas;
- verificação da conformidade com políticas, procedimentos internos e regulamentação aplicável em matéria de PLD/FTP;
- realização de testes e revisões independentes para aferir a efetividade dos controles implementados;
- análise da estrutura organizacional, incluindo a clareza na definição de papéis, responsabilidades e segregação de funções;
- identificação de fragilidades, lacunas e oportunidades de aprimoramento na gestão de riscos.

Ao fornecer uma visão independente e imparcial, a auditoria interna contribui para o fortalecimento do programa de PLD/FTP, permitindo a identificação tempestiva de deficiências e a implementação de ações corretivas e preventivas.

Por fim, os resultados das avaliações realizadas pela auditoria interna devem ser devidamente reportados à alta administração, com recomendações claras, acompanhadas de planos de ação, assegurando a melhoria contínua dos processos e o alinhamento com as melhores práticas e exigências regulatórias.



Relatório de Efetividade do Programa de PLD/FTP

As empresas devem elaborar, com periodicidade anual e data-base em 31 de dezembro, o Relatório de Efetividade do programa de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP), com o objetivo de avaliar a adequação e a efetividade das políticas, dos procedimentos e dos controles implementados, conforme o **art. 42 da Resolução SUSEP nº 99/2026**.

O relatório deve contemplar, no mínimo, os elementos exigidos pelo art. 43, incluindo a descrição da metodologia adotada, os testes realizados, a qualificação dos avaliadores, as deficiências identificadas e os indicadores quantitativos e qualitativos que permitam avaliar a efetividade dos procedimentos de monitoramento, detecção, seleção, análise e comunicação de operações ou situações suspeitas.



A avaliação de efetividade deve ser conduzida de forma estruturada e documentada, permitindo demonstrar a consistência dos critérios adotados e a robustez das conclusões apresentadas, em linha com o perfil de risco da instituição.

O Relatório de Efetividade deve ser encaminhado para ciência até 31 de março do ano subsequente à data-base, ao comitê de auditoria, quando houver, à diretoria e ao conselho de administração, se existente, conforme o **art. 42, § 2º**.

Adicionalmente, o relatório deve conter recomendações objetivas para o tratamento de eventuais deficiências identificadas, acompanhadas de planos de ação e cronogramas para sua implementação. Deve, ainda, apresentar o acompanhamento das providências adotadas em relação a deficiências apontadas em ciclos anteriores, permitindo a avaliação da evolução do programa ao longo do tempo, bem como a manifestação do diretor responsável, com compromisso quanto à correção de eventuais deficiências, conforme o **art. 43, incisos V e VII**.

Por fim, o Relatório de Efetividade deve ser compreendido como instrumento central de governança do programa de PLD/FTP, contribuindo para o monitoramento contínuo, a melhoria dos controles internos e o alinhamento com as exigências regulatórias.

AVALIAÇÃO NACIONAL DE RISCOS (ANR)

Capítulo 7



Na última revisão das recomendações (finalizada em 2012), o GAFI/FATF estabeleceu um marco importante na forma como a lavagem de dinheiro, o financiamento do terrorismo e o financiamento da proliferação de armas de destruição em massa devem ser prevenidos e combatidos, consagrando a chamada "abordagem baseada no risco", mecanismo em que os países, as autoridades competentes e o setor privado devem identificar, avaliar e compreender os riscos de PLD/FTP a que estão expostos e, posteriormente, adotar, de acordo com os riscos identificados, medidas proporcionais e adequadas para mitigá-los.

Uma ANR é uma boa prática que permite ao País determinar medidas preventivas mais eficazes e fazer uma melhor alocação de recursos, que passam a ser direcionados com base no nível dos riscos identificados, de modo a mitigar fluxos financeiros ilícitos, configurando-se como um passo imprescindível de preparação para a avaliação mútua do Brasil pelo GAFI/FATF.

Nesse contexto, em 2020, foi instituído o Grupo de Trabalho de Avaliação Nacional de Riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa pelo Decreto nº 10.270, de 6 de março de 2020. Este grupo de trabalho foi coordenado pelo Coaf em conjunto com representantes do Ministério da Justiça e do BCB. O diagnóstico foi consolidado na primeira Avaliação Nacional de Riscos, publicada em 2021.

A ANR identificou e catalogou os maiores riscos de lavagem de dinheiro, de financiamento do terrorismo e da proliferação existentes. O processo da ANR exigiu a identificação das atividades criminosas que geram maior lucratividade, uma avaliação das vulnerabilidades dos setores financeiro e privado à lavagem de dinheiro, a avaliação dos controles previstos, das fraquezas do sistema de persecução penal e da eficácia da prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação já existentes.

A primeira ANR está disponível para consulta ao público em geral. Seus resultados devem ser levados em conta por todo o mercado no momento de avaliar seus riscos internos de lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa.

Vulnerabilidade do setor de seguros

Os setores supervisionados pela SUSEP foram considerados como de vulnerabilidade ponderada baixa aos riscos de lavagem de dinheiro e financiamento do terrorismo, de acordo com a Avaliação Setorial de Riscos (ASR) realizada pelo órgão. Apesar disso, são considerados de maior risco e estão no foco de atenção da supervisão os setores de previdência com acumulação, como o PGBL e o VGBL, e os produtos de capitalização.

Evolução das comunicações de operações suspeitas e efeitos da mudança regulatória

A análise histórica das comunicações de operações suspeitas por setor evidencia uma mudança estrutural relevante no comportamento do mercado segurador brasileiro, diretamente associada à evolução do arcabouço regulatório de PLD/FTP.

No período anterior à Circular SUSEP nº 612/2020, o setor operava sob normas predominantemente prescritivas, que induziam a uma abordagem mais formalista na identificação e na comunicação de operações suspeitas. Nesse período, observa-se um volume expressivo de comunicações oriundas do mercado segurador, que, em determinados anos, representaram parcela significativamente elevada do total do sistema financeiro, chegando a atingir percentuais superiores a 80% e, em casos extremos, mais de 90% do total de comunicações.

Adicionalmente, a relação entre o volume de comunicações do setor segurador e aquele proveniente do sistema bancário apresentava distorções relevantes, com proporções que, em alguns momentos, superaram múltiplas vezes o volume registrado por instituições tradicionalmente mais expostas a riscos de lavagem de dinheiro. Esse comportamento é indicativo de um modelo de sobrecomunicação, caracterizado por baixa seletividade e, consequentemente, menor efetividade na geração de informações úteis para fins de inteligência financeira.



Regulador	BACEN	BACEN	SUSEP		RELAÇÃO	
Setor Econômico	Bancos	Cooperativa de Crédito	Mercado Segurador	Total de Comunicações de todos os setores	SUSEP/ Total de comunicações	SUSEP/BACEN (Bancos + Cooperativas de Crédito)
2008	15.332	961	**305.477**	**361.467**	**85%**	**1875%**
2009	18.711	2.281	**1.391.778**	**1.458.034**	**95%**	**6630%**
2010	23.415	3.111	**256.255**	**536.269**	48%	**966%**
2011	31.533	3.016	**332.539**	**559.118**	59%	**963%**
2012	28.983	8.707	**467.479**	**773.981**	60%	**1240%**
2013	36.011	7.288	**125.265**	**418.747**	30%	**289%**
2014	36.668	11.483	**45.244**	**190.433**	24%	94%
2015	47.395	13.120	**47.799**	**298.027**	16%	79%
2016	56.389	19.938	**53.602**	**319.942**	17%	70%
2017	63.176	29.236	**59.492**	**326.603**	18%	64%
2018	77.772	35.057	**60.851**	**434.256**	14%	54%
2019	118.473	45.287	**85.091**	**351.154**	24%	52%
2020	248.878	50.787	**85.532**	**863.238**	10%	29%
2021	437.192	55.153	**61.603**	**1.270.064**	5%	13%
2022	703.745	56.043	**387.558**	**1.938.204**	20%	51%
2023	990.507	62.124	**377.959**	**2.250.576**	17%	36%
2024	1.164.960	77.478	**482.493**	**2.574.781**	19%	39%
2025	1.199.641	109.580	**655.508**	**3.104.191**	21%	50%

Os valores podem sofrer alteração conforme atualização da data-base.

FONTE: CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS (COAF). *Coaf em Números*. Brasília, DF: Coaf, 31 dez. 2020. Atualizado em 3 ago. 2026. Disponível em: https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/coaf-em-numeros-1

A publicação da Circular SUSEP nº 612/2020, com efeitos práticos a partir de 2021, representa um marco na evolução desse modelo, ao introduzir de forma estruturada a abordagem baseada em risco. A nova regulamentação desloca o foco do cumprimento estritamente formal para a análise substancial das operações, priorizando a materialidade, o contexto e a qualidade das comunicações. A **Resolução SUSEP nº 99/2026**, que substituirá a Circular a partir de 1º de janeiro de 2027, mantém essa orientação e explicita a aplicação de diligência simplificada, padrão ou reforçada, conforme os riscos identificados.

Como reflexo dessa mudança, observa-se, a partir de 2021, uma redução significativa da participação relativa do setor segurador no total de comunicações, bem como uma aproximação mais consistente em relação ao sistema bancário, que permanece como principal concentrador de riscos e de reportes no sistema. Esse movimento não indica redução na capacidade de controle, mas, sim, um aumento da seletividade e da qualidade das comunicações realizadas.

Nos períodos mais recentes, verifica-se crescimento no volume absoluto de comunicações no setor segurador, fenômeno compatível com a ampliação da proteção securitária e a expansão do setor. Contudo, mesmo diante desse crescimento, a participação relativa do setor permanece em patamares

Nos períodos mais recentes, verifica-se crescimento no volume absoluto de comunicações no setor segurador, fenômeno compatível com a ampliação da proteção securitária e a expansão do setor.





significativamente inferiores aos observados no período pré-2020, especialmente quando comparada ao sistema bancário.

Essa estabilidade relativa reforça a interpretação de que o setor segurador mantém menor exposição estrutural a riscos de PLD/FTP, ao mesmo tempo em que evidencia evolução na maturidade de seus mecanismos de identificação, monitoramento e reporte de operações suspeitas.

A trajetória observada indica uma transição de um modelo caracterizado por elevado volume e baixa efetividade para um sistema mais alinhado à abordagem baseada em risco, no qual a qualidade da informação e a aderência ao perfil de risco das operações assumem papel central. Esse movimento contribui para o aprimoramento da efetividade do sistema de PLD/FTP como um todo, ao reduzir ruídos informacionais e fortalecer a utilidade das comunicações para fins de inteligência e investigação.

Como conclusão, os dados indicam que a evolução do arcabouço regulatório e a adoção da abordagem baseada em risco vêm produzindo resultados consistentes, com maior alinhamento entre o volume de comunicações e o perfil efetivo de risco do setor. A combinação entre redução de distorções históricas, aumento da qualidade das informações reportadas e manutenção de níveis proporcionais de exposição reforça que o mercado segurador, de previdência e capitalização tem avançado na direção adequada, consolidando mecanismos de PLD/FTP mais eficientes, proporcionais e aderentes às melhores práticas internacionais.



Conclusão

Capítulo 8

A evolução do arcabouço regulatório, a crescente sofisticação dos riscos e a intensificação da transformação digital dos serviços financeiros consolidam a PLD/FTP como um dos pilares estruturantes da governança, da gestão de riscos e da integridade institucional das organizações.

Nesse ambiente, a efetividade dos mecanismos de prevenção deixa de ser aferida exclusivamente pela aderência formal às normas e passa a ser mensurada pela capacidade das instituições de identificar, avaliar e mitigar riscos de forma dinâmica, consistente e proporcional. A adoção da abordagem baseada em risco, alinhada às Recomendações do GAFI/FATF, exige estruturas capazes de integrar dados, aplicar inteligência analítica, revisar continuamente parâmetros de monitoramento e assegurar a rastreabilidade das operações em ambientes cada vez mais digitais, descentralizados e interconectados.

Adicionalmente, o fortalecimento da agenda de PLD/FTP está diretamente associado à qualidade das informações produzidas e reportadas, à governança dos modelos de detecção, à integração entre áreas de risco, controles internos, *compliance*, prevenção a fraudes e tecnologia, e à capacidade de interação eficiente com unidades de inteligência financeira e autoridades supervisoras. Nesse contexto, a supervisão tende a evoluir para modelos cada vez mais orientados à efetividade, com maior ênfase em evidências, testes de aderência, validação de controles e avaliação de resultados.

É nesse cenário que se destaca o papel institucional da CNseg. Ao liderar a produção deste material técnico, a Confederação contribui para a consolidação de entendimentos, a redução de assimetrias interpretativas e o alinhamento do setor às melhores práticas regulatórias e internacionais. A atuação da Comissão de Governança e *Compliance*, composta por especialistas com experiência prática na implementação de programas de PLD/FTP, assegura que o conteúdo reflita não apenas os requisitos normativos, mas também os desafios operacionais e as soluções adotadas no âmbito das entidades supervisionadas.

A construção coletiva deste livreto — integrando perspectiva regulatória, visão técnica e experiência de mercado — fortalece sua função como instrumento de referência para o setor, apoiando o aprimoramento contínuo dos programas de PLD/FTP, a evolução das estruturas de controle e a qualificação dos processos decisórios.

Mais do que promover conformidade, a iniciativa reforça a capacidade do setor segurador de atuar de forma preventiva, coordenada e tecnicamente estruturada frente a riscos cada vez mais complexos. Ao fomentar uma cultura orientada à integridade, à transparência e à gestão qualificada de riscos, a CNseg contribui diretamente para a robustez do sistema financeiro, a proteção dos mercados e o fortalecimento da credibilidade do Brasil no cenário internacional.

Rererências Normativas e Institucionais

Legislação Federal

Lei nº 9.613/1998 – Lei de Lavagem de Dinheiro – Dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores e cria o Conselho de Controle de Atividades Financeiras (Coaf).

Lei nº 12.683/2012 – Altera a Lei nº 9.613/1998 para ampliar e tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro.

Lei nº 13.810/2019 – Dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.

Decreto-Lei nº 73/1966 – Lei do Seguro Privado – Dispõe sobre o Sistema Nacional de Seguros Privados, disciplina as operações de seguros e resseguros e as operações de proteção patrimonial mutualista e dá outras providências.

Lei Complementar nº 213/2025 – Dispõe sobre sociedades cooperativas de seguros, operações de proteção patrimonial mutualista e sociedades processadoras da ordem do cliente e altera a Lei Complementar nº 126, de 15 de janeiro de 2007.

Normativos da SUSEP e CNSP

Resolução SUSEP nº 99/2026 — Regulamenta as Leis nº 9.613/1998 e nº 13.810/2019 no âmbito dos mercados supervisionados pela SUSEP, estabelecendo políticas, procedimentos e controles internos de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa. Substitui a Circular SUSEP nº 612/2020 a partir de 1º de janeiro de 2027.

Resolução CNSP nº 491/2026 – Operação Patrimonial Mutualista.

Resolução CNSP nº 492/2026 – Cooperativas de Seguros.

Resolução CNSP nº 429/2021 – Sociedades Processadoras da Ordem do Cliente.

Banco Central do Brasil (BCB)

Circular BCB nº 3.978/2020 – Dispõe sobre política, procedimentos e controles internos de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

Carta Circular n° 4.001/2020 – Divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf).

Resolução BCB nº 498/2025 – Disciplina os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI.

Comissão de Valores Mobiliários (CVM)

Resolução CVM nº 50/2021 – Dispõe sobre PLD/FTP no âmbito do mercado de valores mobiliários.

Agência Nacional de Saúde Suplementar (ANS)

Resolução Normativa ANS nº 529/2022 – Dispõe sobre a identificação de clientes, a manutenção de registros e prevê relação de operações e situações que podem configurar indícios de ocorrência dos crimes previstos na Lei nº 9.613/1998.

Superintendência Nacional de Previdência Complementar (Previc)

Resolução Previc nº 23/2023 (alterada pela Resolução Previc nº 25/2024) – Estabelece procedimentos para a aplicação das normas relativas às atividades desenvolvidas pela Superintendência Nacional de Previdência Complementar, bem como normas complementares às diretrizes do Conselho Nacional de Previdência Complementar e do Conselho Monetário Nacional.

Organismos Internacionais

Grupo de Ação Financeira – GAFI/FATF

Grupo de Acción Financiera de Latinoamérica – GAFILAT

International Association of Insurance Supervisors – IAIS

Insurance Core Principles – ICPs/IAIS

Office of Foreign Assets Control – OFAC

Conselho de Segurança das Nações Unidas – Sanções

Organização das Nações Unidas – ONU

Organização para a Cooperação e Desenvolvimento Econômico – OCDE

Banco Mundial e Fundo Monetário Internacional – FMI

Órgãos e Instituições Nacionais

Conselho de Controle de Atividades Financeiras – Coaf

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro – ENCCLA

Controladoria-Geral da União – CGU

Pacto Brasil pela Integridade Empresarial

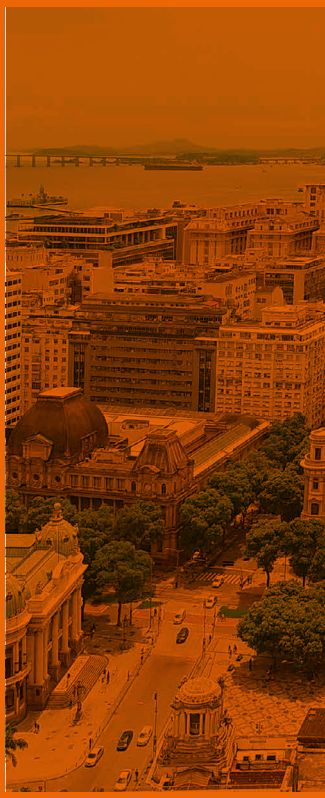
Sustentabilidade, Governança e Divulgação

CBPS 1 e CBPS 2 – CFC

Institucional

A prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa no mercado segurador, de previdência e capitalização brasileiro insere-se em um esforço contínuo, de natureza global, voltado ao fortalecimento da integridade dos sistemas financeiros e à mitigação de práticas ilícitas cada vez mais sofisticadas.

Diante da exposição do setor a esses riscos, torna-se essencial que as supervisionadas adotem programas de PLD/FTP robustos, proporcionais ao seu porte, perfil de risco e complexidade operacional, sustentados por governança efetiva, controles consistentes e monitoramento contínuo.



Mais do que atender a exigências regulatórias, a efetividade desses programas é elemento central para a preservação da confiança no setor, contribuindo para a mitigação de riscos legais, regulatórios e reputacionais, bem como para a proteção da própria atividade seguradora como instrumento de desenvolvimento econômico e social.

Ao longo deste material, buscou-se evidenciar que a identificação, a prevenção e a comunicação de situações atípicas dependem, em grande medida, da atuação diligente e consciente de todos os envolvidos. Nesse contexto, a responsabilidade é compartilhada e exige engajamento transversal, capacitação contínua e alinhamento com as melhores práticas nacionais e internacionais.

Assim, ao fortalecer seus mecanismos de prevenção e controle, as instituições não apenas asseguram a conformidade com a legislação vigente, mas também reafirmam seu compromisso com a ética, a transparência e a integridade — valores essenciais para a sustentabilidade do setor e para o atendimento às expectativas das autoridades supervisoras e da sociedade.

Revisão 2026:

Comissão de Controles Internos da CNseg

Superintendência de Acompanhamento Técnico da CNseg

Grupo de trabalho técnico de PLD/FTP da CNseg











Rio de Janeiro
Rua Senador Dantas, 74 - 16 andar
Centro / CEP 20031 - 205
Tel. 21 2510-7777

Brasília
SCN Quadra 1 bl C
Brasília / CEP 7011-902
Tel. 61 3424-9337 / Fax. 61 3328-1904



PROGRAMA

EDUCAÇÃO EM SEGUROS

cnseg.org.br



CNseg

Confederação Nacional das Seguradoras