

POLÍTICA

SISTÊMICA

Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa - PLD/FTP

Área: Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo

Assunto: GIR – Risco de Conformidade e Compliance

Abrangência: Sistêmica





SUMÁRIO

01

Objetivo

02

Definições

03

Diretrizes

04

Base Regulatória

05

Vigência e Histórico de Aprovação



Este documento é extração da política de Prevenção à Lavagem de Dinheiro e ao Financiamento do terrorismo e da Proliferação de Armas de Destruição em Massa - PLD/FTP aprovada em 26/11/2025 pelo Conselho de Administração da SicrediPar.



1. Objetivo

Estabelecer as diretrizes para a Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD/FTP) aplicáveis a todos os níveis e Entidades do Sicredi - incluindo parceiros de negócio e prestadores de serviços terceirizados - em conformidade com a legislação e regulamentação vigentes e com as melhores práticas de mercado.



2. Definições



Lavagem de Dinheiro: Prática que visa ocultar ou disfarçar a origem ilícita de recursos, por meio da movimentação, transformação ou integração de bens, valores ou direitos provenientes de infrações penais.



Financiamento ao Terrorismo: Ato de direcionar recursos — lícitos ou ilícitos — para indivíduos, grupos ou ações com fins terroristas, com o objetivo de apoiar ou viabilizar atividades que representem ameaça à segurança nacional ou internacional.



Financiamento da Proliferação de Armas de Destruição em Massa: Envolve o fornecimento ou captação de recursos, por qualquer meio, com a finalidade de facilitar a produção, aquisição ou disseminação de armamentos capazes de causar danos em larga escala, como armas nucleares, químicas, biológicas ou similares.



3. Diretrizes

3.1. Prevenção.

3.1.1. Com o objetivo de mitigar os riscos de utilização indevida dos produtos e serviços para fins relacionados à LD/FTP, normativos, procedimentos e controles internos devem ser implementados e disseminados, contemplando no mínimo:

- a) **Promover e disseminar** a cultura de PLD/FTP em nível sistêmico, por meio de programas de treinamento e capacitação contínuos, adequado aos diferentes perfis de atividades desenvolvidas por colaboradores, prestadores de serviços terceirizados e funcionários dos correspondentes no país;
- b) **Definir procedimentos** voltados à avaliação e à análise prévia de novos produtos, serviços e tecnologias, sob a ótica de PLD/FTP, com o objetivo de garantir a segurança das operações em nível sistêmico e mitigar o risco de uso indevido para fins LD/FTP;
- c) **Realizar** Relatório de Avaliação Interna de Riscos (RAIR) sistêmico, devidamente formalizado em documento específico, com periodicidade compatível com a natureza, porte, complexidade e perfil de risco das atividades desenvolvidas, com o objetivo de identificar, mensurar e avaliar a probabilidade e o impacto dos riscos de utilização indevida dos produtos, serviços e canais de atendimento do Sicredi para fins de LD/FTP;
- d) **Desenvolver e implementar** processos de monitoramento, seleção, análise e comunicação de transações ou situações com indícios de LD/FTP;
- e) **Estabelecer** alçadas para deliberação sobre:
 - i) A comunicação ao Conselho de Controle de Atividades Financeiras (COAF) e/ou demais órgãos e reguladores, acerca de propostas, operações ou situações que apresentem indícios de LD/FTP;
 - ii) A continuidade de relacionamento com associados/clientes, parceiros de negócios ou prestadores de serviços terceirizados, nas hipóteses em que forem identificados indícios de comprometimento à reputação e/ou à imagem institucional do Sicredi.



- f) **Estabelecer** regras, procedimentos e controles de PLD/FTP suportados por sistemas de informação, adequados à natureza, complexidade e aos riscos inerentes às operações, produtos e serviços ofertados pelo Sicredi, observando o registro tempestivo, completo e fidedigno das operações;
- g) **Desenvolver e implementar** procedimentos e controles de PLD/FTP, aos associados/clientes, colaboradores, parceiros e prestadores de serviço terceirizados, com vistas a mitigar os riscos de danos à imagem e reputação, bem como prevenir à utilização de produtos e/ou serviços do Sicredi para fins LD/FTP;
- j) **Assegurar** a realização da avaliação anual de efetividade dos procedimentos, políticas e controles internos relacionados à PLD/FTP, com registro formal em relatório específico, contemplando, entre outros aspectos, a aplicação de testes de efetividade que permitam aferir a adequação, a consistência e a eficácia dos mecanismos adotados.
- k) **Assegurar** a realização de auditoria interna para verificar a aderência e a efetividade das políticas, procedimentos e controles internos de PLD/FTP, cujo escopo e periodicidade devem compor o programa de auditoria do Sicredi;

3.2. Relatório de Avaliação Interna de Riscos

3.2.1. O Relatório de Avaliação Interna de Riscos (RAIR) deve ser realizado, no mínimo, anualmente, com o objetivo de identificar, mensurar e avaliar os riscos de utilização dos produtos, serviços, canais de atendimento e operações do Sicredi para a prática de LD/FTP, conforme regulamentação vigente.

A metodologia empregada na avaliação, bem como os impactos decorrentes de alterações nos níveis de risco, encontra-se devidamente descritos no referido relatório.

3.3. Avaliação de Efetividade e Plano de Ação

3.3.1. Anualmente, serão realizados testes e verificações para avaliar a efetividade da política, dos procedimentos e dos controles internos de PLD/FTP. Os testes devem ser devidamente registrados em relatório específico, e as fragilidades identificadas devem ser objeto de um plano de ação para correção das deficiências.



3.4. Avaliação de Produtos e Serviços

3.4.1. O Sicredi adota procedimentos para identificar, avaliar e classificar o risco de utilização de produtos, serviços e tecnologias para a prática de lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa, bem como estabelece controles e medidas mitigadoras compatíveis com os riscos identificados;

3.5. Fortalecimento das Estratégias de Integridade

3.5.1. Conheça Seu Associado/Cliente: O Sicredi deve adotar procedimentos que assegurem o conhecimento adequado dos associados e/ou clientes desde a proposição para o início do relacionamento, seja ele iniciado de maneira presencial ou não.

3.5.2. Conheça Seu Colaborador: O Sicredi deve adotar procedimentos que permitam o conhecimento e o monitoramento contínuo de todas as pessoas colaboradoras.

3.5.3. Conheça Seu Parceiro: A aceitação de parceiros deve estar condicionada à verificação da existência e efetividade de políticas, procedimentos e controles de PLD/FTP, especialmente quando se tratar de pessoas obrigadas por regulamentação.

3.5.4. Conheça Seu Fornecedor e Prestador de Serviços Terceirizado: O processo de avaliação de fornecedores e prestadores de serviços terceirizados deve contemplar diretrizes que assegurem a integridade das relações comerciais. Devem ser adotados controles que mitiguem o vínculo com empresas envolvidas em atos ilícitos, contribuindo para a preservação da imagem, reputação e conformidade da instituição no âmbito da PLD/FTP.

3.6. Cultura Organizacional

3.6.1. A cultura organizacional voltada à PLD/FTP deve ser promovida de forma contínua entre colaboradores, parceiros e prestadores de serviços terceirizados, com foco na conscientização, responsabilidade e conduta ética.

3.7. Governança de PLD/FTP

3.7.1. A governança de PLD/FTP no Sicredi é estruturada de forma sistêmica, abrangendo as empresas do Centro Administrativo Sicredi (CAS), as Centrais e as Cooperativas. O Conselho de Administração, os Comitês de Auditoria, Riscos e Compliance, a Diretoria Executiva e o



Comitê de Diretores Executivos são responsáveis por definir, aprovar e acompanhar políticas e normas, assegurando a conformidade regulatória e o alinhamento com as melhores práticas.

3.8. Intercâmbio de Informações

3.8.1. No Sicredi, o intercâmbio de informações relacionadas PLD/FTP é conduzido de forma estruturada, segura e colaborativa entre as entidades, incluindo cooperativas singulares, Centrais, Banco Cooperativo Sicredi e áreas corporativas. Esse fluxo é essencial para garantir a efetividade das ações de prevenção e o alinhamento sistêmico às diretrizes regulatórias e às melhores práticas de mercado.

3.9. Guarda de Documentos e Informações

3.9.1. O Sicredi deve manter a guarda de documentos e informações conforme os prazos definidos pela regulamentação vigente.



4. Base Regulatória

Lei nº 9.613/98.

Lei nº 105/01.

Lei nº 13.260/16.

Circ. BCB nº 3.978/20.

Carta Circ. BCB nº 4.001/20.

Res. CVM nº 50/21.

Res. CVM nº 35/21.

Res. CVM nº 62/22.

Circ. SUSEP nº 612/20.

Lei nº 13.810/19.



5. Vigência e Histórico de Aprovação

DATA	DESCRIÇÃO	APROVADOR
15/08/2023	3ª versão – Atualização do documento	Conselho de Administração em 15/08/2023 no Voto nº 008/2023.
26 e 27/11/2025	4ª versão – Atualização do documento	Conselho de Administração em 26 e 27/11/2025 no Voto nº 50/2025.

Este documento deve ser atualizado minimamente a cada 02 (dois) anos, ou extraordinariamente, a qualquer tempo.

Este documento é extração da política de Prevenção à Lavagem de Dinheiro e ao Financiamento do terrorismo e da Proliferação de Armas de Destruição em Massa - PLD/FTP aprovada em 26/11/2025 pelo Conselho de Administração da SicrediPar.