

POLÍTICA DE PLD/FTP

(Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa)

Sumário

1. OBJETIVO.....	3
2. GOVERNANÇA	3
3. ARCABOUÇO REGULAMENTAR	3
4. DEFINIÇÕES	4
5. PAPÉIS E RESPONSABILIDADES	5
6. AVALIAÇÃO DE NOVOS PRODUTOS, SERVIÇOS E TECNOLOGIAS	6
7. ABORDAGEM BASEADA EM RISCO (ABR).....	7
8. AVALIAÇÃO INTERNA DE RISCOS (AIR).....	7
9. AVALIAÇÃO DE EFETIVIDADE	8
10. TREINAMENTO E CAPACITAÇÃO	9
11. CONHEÇA SEU CLIENTE	9
12. CONHEÇA SEU COLABORADOR, PARCEIRO, PRESTADOR DE SERVIÇO E FORNECEDOR	9
13. BENEFICIÁRIO FINAL	10
14. MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS	10
15. SANÇÕES, LISTAS RESTRITIVAS E INDISPONIBILIDADE DE ATIVOS.....	11
16. PESSOA EXPOSTA POLITICAMENTE	11
17. SIGILO, CONFIDENCIALIDADE E RESTRIÇÃO DE ACESSO	11
18. GUARDA DE DOCUMENTOS E REGISTROS	11

1. OBJETIVO

O objetivo desta Política é estabelecer os princípios, diretrizes e procedimentos adotados pela Placarpay S.A. – Sociedade de Crédito, Financiamento e Investimento (“Instituição”) para prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP), de modo a assegurar a aderência à regulamentação aplicável e fortalecendo a integridade, a transparência e a governança do programa de PLD/FTP.

2. GOVERNANÇA

Esta Política é elaborada e revisada pela área de PLD/FTP, validada pelas áreas competentes e submetida à aprovação da Alta Administração, no mínimo anualmente ou em prazo inferior quando houver alterações regulatórias, mudanças relevantes no modelo de negócio, nos produtos, serviços, canais, tecnologias, estrutura operacional ou ambiente de risco da Instituição.

A Política deve contemplar, no mínimo, as diretrizes de identificação, qualificação e classificação de risco de clientes, beneficiários finais, funcionários, parceiros, prestadores de serviços terceirizados e fornecedores; os procedimentos de monitoramento, seleção, análise e comunicação de operações e situações suspeitas ao COAF; os critérios para avaliação de novos produtos, serviços, canais e tecnologias; a metodologia de Avaliação Interna de Riscos; a governança, responsabilidades, alçadas e reporte à Alta Administração; o programa de treinamento; a avaliação periódica de efetividade; e os procedimentos de guarda de documentos e informações, observados os prazos regulatórios aplicáveis.

3. ARCABOUÇO REGULAMENTAR

Esta Política baseia-se na Lei nº 9.613/1998, na Lei nº 13.810/2019 e nas normas emitidas pelos órgãos reguladores e fiscalizadores aplicáveis à Instituição, sem prejuízo e sem limitação a outras normas, legislações ou regulamentações que venham a ser aplicadas. O arcabouço normativo de referência inclui as regulamentações do Banco Central do Brasil sobre prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (PLD/FTP), bem como orientações e comunicações oficiais relacionadas a operações e situações que possam configurar indícios de ilícitos financeiros.

Lei nº 9.613/1998 - Dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores, bem como a prevenção da utilização do sistema financeiro para os ilícitos nela previstos, e institui o Conselho de Controle de Atividades Financeiras (COAF).

Lei nº 13.810/2019: Dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas (CSNU), incluindo a indisponibilidade de ativos de pessoas naturais, pessoas jurídicas e entidades, bem como a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados.

Resolução nº 44/2020: Estabelece os procedimentos para a execução, pelas instituições autorizadas a funcionar pelo Banco Central do Brasil, das medidas determinadas pela Lei nº 13.810/2019, incluindo aquelas relacionadas à indisponibilidade de ativos e ao cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, bem como à designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos correlacionados.

Instrução Normativa nº 262/2022: Especifica e esclarece aspectos operacionais dos procedimentos estabelecidos na Resolução BCB nº 44, de 24 de novembro de 2020, para a execução de medidas determinadas pela Lei nº 13.810, de 8 de março de 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, bem como a designação nacional de pessoas investigadas ou acusadas de terrorismo, seu financiamento ou atos correlacionados.

Circular nº 3.978/2020 e alterações posteriores - Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil (BCB), visando à prevenção da utilização do sistema financeiro para a prática dos crimes de lavagem de dinheiro e de financiamento ao terrorismo e de financiamento da proliferação de armas de destruição em massa.

Carta Circular nº 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, ou de financiamento do terrorismo, devendo ser utilizada como referência para estruturação dos cenários, parâmetros e procedimentos de monitoramento, seleção, análise e comunicação ao COAF, sem prejuízo de outros indícios definidos pela Instituição com base em sua Avaliação Interna de Riscos.

4. DEFINIÇÕES

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

Lavagem de dinheiro (LD) - Qualquer atividade que tenha por finalidade ocultar ou disfarçar a origem ilícita de bens, direitos ou valores. O objetivo é processar ativos derivados de crimes para que eles pareçam legítimos, envolvendo atividades como conversão, transferência ou movimentação de recursos provenientes de infrações penais.

Financiamento do terrorismo (FT): Fornecimento, depósito, distribuição ou arrecadação de fundos ou bens, por qualquer meio, de forma direta ou indireta, com a intenção de serem utilizados ou com o conhecimento de que serão utilizados, integralmente ou em parte, para a prática de qualquer atividade terrorista.

Proliferação de Armas de Destruição em Massa (P): Fornecimento, disponibilização, intermediação, movimentação ou apoio financeiro, econômico ou material destinado, direta ou indiretamente, ao desenvolvimento, aquisição, fabricação, posse, transporte, transferência ou uso de armas nucleares, químicas ou biológicas, seus meios de entrega ou materiais relacionados, em desacordo com a legislação, regulamentação e sanções aplicáveis.

KYC – Know Your Customer: Termo em inglês que significa “Conheça Seu Cliente”.

KYP – Know Your Partner: Termo em inglês que significa “Conheça seu Parceiro”.

KYS – Know Your Supplier: Termo em inglês que significa “Conheça seu Fornecedor/Prestador de serviços”.

KYE – Know Your Employee: Termo em inglês que significa “Conheça seu Funcionário/Colaborador”.

PEP - Pessoa Exposta Politicamente: Pessoa natural que desempenha ou tenha desempenhado cargo, emprego ou função pública relevante no Brasil ou em país, território ou dependência estrangeira, bem como seus familiares e estreitos colaboradores, ou pessoas jurídicas das quais participem ou com as quais mantenham relacionamento relevante, sendo a condição de PEP aplicável durante o exercício da função e pelos 5 (cinco) anos seguintes à data em que a pessoa deixar de se enquadrar nas categorias previstas na regulamentação.

ABR - Abordagem Baseada em Risco: Controles proporcionais ao risco identificado. Quanto maior o risco, maior o nível de controle, análise, aprovação e monitoramento.

AIR - Avaliação Interna de Risco: Processo estruturado e periódico pelo qual a Instituição identifica, analisa e mensura os riscos de lavagem de dinheiro, financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP) inerentes às suas atividades.

EDD - Enhanced Due Diligence: Verificação aprofundada de antecedentes (*background checks*) utilizada para Clientes de maior risco.

Cliente: Considera-se cliente qualquer pessoa natural ou jurídica que mantenha relação de negócio com a Instituição, seja mediante a utilização de produtos de crédito, investimento ou serviços de pagamento, bem como seus representantes e procuradores.

Investidor: Pessoa física ou jurídica que aloca capital em produtos de captação da financeira, visando rentabilidade financeira em troca de prover os recursos necessários para o fomento das operações de crédito da instituição.

Colaboradores: Sócios, Diretores, Associados, Empregados, Estagiários e Menores Aprendizizes.

Beneficiário Final: Pessoa natural que, em última instância, direta ou indiretamente, possui, controla ou influencia significativamente uma pessoa jurídica, fundo, estrutura jurídica ou relacionamento, ou em nome da qual uma transação é conduzida, observados os critérios e percentuais definidos na regulamentação aplicável e nas normas internas da Instituição.

Influência significativa: Situação em que uma pessoa natural, ainda que não detenha o controle formal da pessoa jurídica, estrutura jurídica ou fundo de investimento, exerce influência relevante sobre suas decisões ou detém, direta ou indiretamente, mais de 25% (vinte e cinco por cento) do capital social, dos direitos de voto ou da participação aplicável, conforme os critérios estabelecidos na regulamentação vigente e nas normas internas da Instituição.

Operação Atípica: É a transação que apresenta inconsistência em relação ao perfil econômico, financeiro ou operacional do cliente, mas que ainda necessita de análise interna detalhada para identificação de sua real causa ou fundamentação econômica.

Operação Suspeita: É a operação, transação, comportamento ou situação que, após a análise aprofundada da atipicidade, apresenta fundados indícios de ilicitude ou incompatibilidade injustificada, gerando a obrigatoriedade de comunicação formal ao COAF.

5. PAPÉIS E RESPONSABILIDADES

Diretoria Executiva

A Diretoria Executiva é responsável por assegurar a estrutura, os recursos, a governança e o apoio institucional necessários à implementação e à efetividade do Programa de PLD/FTP, reafirmando seu compromisso com a integridade, a conformidade regulatória e a abordagem baseada em risco, competindo-lhe:

- Assegurar a independência, a autonomia e a disponibilização de recursos humanos, tecnológicos e financeiros adequados e suficientes para a função de PLD/FTP;
- Disseminar continuamente a cultura de conformidade e ética em toda a Instituição;
- Garantir que a atuação da Instituição seja pautada pela Abordagem Baseada em Risco (ABR);
- Apoiar integralmente as medidas preventivas e corretivas relacionadas à PLD/FTP;
- Aprovar e revisar, no mínimo anualmente, a presente Política de PLD/FTP; e
- Indicar formalmente ao Banco Central do Brasil o Diretor responsável pelo cumprimento das obrigações de PLD/FTP previstas na regulamentação vigente.

Comitê de PLD/FTP

Órgão deliberativo responsável pela avaliação e discussão de assuntos estratégicos, administrativos e operacionais relacionados à PLD/FTP. É de responsabilidade do Comitê:

- Deliberar sobre os casos identificados no processo de *onboarding* (conheça seu cliente/parceiro/colaborador) que apresentem risco crítico à reputação da Instituição, decidindo pela aprovação ou recusa do relacionamento;
- Avaliar e deliberar sobre os indícios de atipicidades identificadas durante o monitoramento de transações; e
- Definir parâmetros e limites de atuação, tais como o percentual de participação para identificação de beneficiários finais em casos específicos, observados os limites mínimos regulatórios.

Diretoria responsável por PLD/FTP

Compete ao Diretor formalmente indicado para a função de PLD/FTP:

- Assegurar a implementação, o monitoramento e o cumprimento das diretrizes estabelecidas nesta Política;
- Aprovar formalmente o documento de Avaliação Interna de Riscos (AIR) da Instituição;
- Dar ciência da Avaliação Interna de Riscos ao Comitê de Riscos, Auditoria Interna e à Diretoria Executiva;
- Avaliar e aprovar os relatórios regulatórios relativos à temática de PLD/FTP, bem como os respectivos planos de ação decorrentes destes; e
- Avaliar e aprovar as decisões sobre a comunicação ou não comunicação ao COAF das operações suspeitas apresentadas pela área de PLD/FTP.

Área de PLD/FTP

À área de PLD/FTP, compete o suporte técnico e a operacionalização do programa de conformidade da Instituição, sendo responsável por:

- A elaboração, manutenção e implantação de uma Política eficaz de PLD/FTP;
- Executar as rotinas de monitoramento de transações e a triagem de alertas de operações atípicas, estruturando os dossiês para deliberação; e
- Conduzir e supervisionar os processos de *due diligence* (KYC, KYP, KYS, KYE), submetendo à aprovação conforme as alçadas estabelecidas;

Auditoria Interna

Compete à Auditoria Interna avaliar de forma independente, periódica e sistemática a aderência, a consistência e a efetividade desta Política e dos controles internos de PLD/FTP, reportando seus achados e recomendações diretamente à Diretoria Executiva.

Colaboradores e terceiros

Todos os colaboradores, administradores e prestadores de serviços terceirizados da Instituição são responsáveis por:

- Conduzir os negócios em estrita observância à legislação vigente de PLD/FTP;
- Cumprir integralmente as diretrizes do Código de Conduta Ética e desta Política;
- Comunicar tempestivamente à área de PLD/FTP qualquer operação, comportamento ou situação atípica que possa configurar indício de ilícito financeiro.

6. AVALIAÇÃO DE NOVOS PRODUTOS, SERVIÇOS E TECNOLOGIAS

A Instituição estabelece como diretriz fundamental que nenhum novo produto, serviço, funcionalidade, canal de distribuição ou nova tecnologia será lançado, disponibilizado ao mercado ou implementado operacionalmente sem a prévia e formal avaliação do seu potencial risco de utilização para a prática de Lavagem de Dinheiro, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa (PLD/FTP).

Governança e Alçada de Aprovação

Compete à área de PLD/FTP realizar a avaliação dos riscos relacionados a novos produtos, serviços, ou tecnologias e emitir parecer técnico fundamentado, podendo recomendar a aprovação, a aprovação condicionada à implementação de medidas mitigadoras ou a não aprovação da iniciativa. Nos casos em que o parecer técnico da área de PLD/FTP for desfavorável, a iniciativa deverá ser submetida à avaliação e à deliberação da alçada competente, conforme a estrutura de governança interna, podendo o Comitê de PLD/FTP ou o Diretor responsável aprovar, aprovar condicionadamente ou rejeitar a iniciativa, desde que a decisão seja devidamente fundamentada, formalizada e acompanhada das medidas de mitigação e dos controles aplicáveis.

Fica vedado o lançamento ou a implementação de qualquer iniciativa que possua parecer desfavorável da área de PLD/FTP e não tenha sido submetida à avaliação e aprovada pela alçada competente, ou que não tenha obtido aprovação formal do Diretor responsável, quando aplicável.

A implementação de novos produtos, serviços, funcionalidades, canais de distribuição ou tecnologias dependerá da conclusão da avaliação de risco, da adoção das medidas mitigadoras eventualmente definidas e da aprovação pela alçada competente, observados os procedimentos internos de governança.

7. ABORDAGEM BASEADA EM RISCO (ABR)

A Instituição estabelece uma Abordagem Baseada em Risco (ABR) estruturada para identificar, analisar, compreender, mitigar e monitorar os riscos de lavagem de dinheiro, financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP).

A metodologia aplicada garante que as ações de prevenção e mitigação sejam proporcionais aos riscos identificados desde o processo de *onboarding* (identificação e qualificação), estendendo-se pela manutenção do relacionamento e pelo monitoramento transacional. Os parâmetros de ponderação, variáveis e limites de tolerância a riscos são consolidados formalmente no documento de Avaliação Interna de Risco (AIR).

Metodologia de avaliação e classificação de risco

Para materializar a ABR, a Instituição utiliza uma Matriz de Classificação de Risco que avalia e segmenta as contrapartes e os elementos operacionais nos níveis de risco: Baixo, Médio, Alto e Crítico. A classificação resultante da Matriz de Risco determina a intensidade e a frequência dos controles aplicados ao longo da relação com a Instituição:

- **Risco Baixo:** Permite a adoção de procedimentos de Diligência Simplificada na coleta de informações cadastrais e monitoramento com parâmetros regulares de periodicidade.
- **Risco Médio:** Aplicação de procedimentos de Diligência Padrão, com validação documental ordinária e monitoramento sistêmico recorrente.
- **Risco Alto ou Crítico:** Exige, obrigatoriamente, a aplicação de Diligência Reforçada, incluindo a exigência de comprovações adicionais de origem de recursos, monitoramento transacional intensificado e ritos de aprovação por alçadas superiores (ou Comitê) para o início ou manutenção do relacionamento.

Manutenção da classificação de risco

A Instituição garante que a classificação de risco das contrapartes seja mantida atualizada. A periodicidade do processo de renovação está vinculada ao nível de risco atribuído na matriz:

- **Perfis de Risco Alto e Crítico:** Atualização cadastral e revisão de risco prioritárias, realizadas em ciclos curtos e contínuos (no máximo anuais) ou tempestivamente diante de eventos geradores de alerta.
- **Perfis de Risco Médio e Baixo:** Atualização cadastral em ciclos mais espaçados, conforme cronograma interno estabelecido em Manual de Procedimentos, observando o limite máximo admitido pela regulamentação vigente.

A classificação de risco também é atualizada extraordinariamente sempre que identificadas atipicidades no monitoramento transacional ou alterações societárias/caadstrais relevantes que desenquadm o perfil original da contraparte.

8. AVALIAÇÃO INTERNA DE RISCOS (AIR)

A Avaliação Interna de Risco (AIR) é o instrumento formal pelo qual a Instituição identifica, analisa, mensura e compreende os riscos de utilização de suas estruturas, produtos, serviços, canais e relacionamentos para lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa (PLD/FTP).

Seus resultados orientam a Abordagem Baseada em Risco (ABR), assegurando que políticas, procedimentos, controles, monitoramentos e medidas mitigadoras sejam proporcionais aos riscos identificados.

Em conformidade com a regulamentação vigente, a AIR considera a probabilidade de ocorrência e a magnitude dos impactos financeiro, regulatório, jurídico, reputacional e socioambiental. A avaliação abrange, no mínimo, os riscos relacionados aos clientes e demais contrapartes; ao modelo de negócio, porte, estrutura e áreas geográficas de atuação da Instituição; às operações, transações, produtos, serviços, canais de distribuição e novas tecnologias; e às atividades desempenhadas por funcionários, parceiros, prestadores de serviços terceirizados e fornecedores.

A AIR deve ser documentada, aprovada pelo Diretor responsável por PLD/FTP e submetida à ciência da Diretoria Executiva e dos órgãos de governança competentes, conforme a estrutura vigente da Instituição. Sua revisão ocorrerá na periodicidade mínima exigida pela regulamentação aplicável, ou em prazo inferior diante de alterações relevantes no perfil de risco, no modelo de negócio, nos produtos, serviços, processos, canais, tecnologias ou no ambiente regulatório, hipótese em que a versão atualizada deverá seguir o mesmo rito de aprovação e ciência.

9. AVALIAÇÃO DE EFETIVIDADE

A Instituição avaliará anualmente a efetividade da sua Política, dos procedimentos operacionais e dos sistemas de controles internos voltados à Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLD/FTP), com data-base de 31 de dezembro do ano-calendário correspondente.

O relatório de Efetividade deve conter informações que descrevam:

- a metodologia adotada na avaliação de efetividade;
- os testes aplicados;
- a qualificação dos avaliadores; e
- as deficiências identificadas.

Além disso, deve conter, no mínimo, a avaliação:

- dos procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
- dos procedimentos de monitoramento, seleção, análise e comunicação ao COAF, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas;
- da governança da Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
- das medidas de desenvolvimento da cultura organizacional voltadas à Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
- dos programas de capacitação periódica de pessoal;
- dos procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados; e
- das ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do Banco Central do Brasil.

O Relatório Anual de Efetividade será encaminhado para ciência e avaliação da Auditoria Interna e da Diretoria Executiva da Instituição até o dia 31 de março do ano seguinte ao da data-base.

Relatório de acompanhamento

Diante de eventuais deficiências ou oportunidades de melhoria identificadas no Relatório de Efetividade, a Instituição elaborará e executará um Plano de Ação específico destinado a sanar os apontamentos, estabelecendo medidas corretivas, prazos e responsáveis. O acompanhamento da implementação das medidas mitigadoras será formalizado por meio de Relatório de Acompanhamento, com registro do andamento, eventuais atrasos, justificativas e decisões de escalonamento quando necessário.

O plano de ação e o respectivo relatório de acompanhamento devem ser encaminhados para ciência e avaliação da Auditoria Interna e da Diretoria Executiva até o dia 30 de junho do ano seguinte ao da data-base do Relatório de Efetividade.

10. TREINAMENTO E CAPACITAÇÃO

A Instituição adota programa contínuo e obrigatório de capacitação em PLD/FTP para colaboradores, administradores e demais públicos definidos conforme exposição ao risco. A capacitação será realizada, no mínimo, anualmente, e os novos colaboradores deverão concluir o treinamento inicial de integração em até 30 (trinta) dias contados da admissão. O conteúdo, a profundidade e a metodologia dos treinamentos observarão as responsabilidades de cada público, as áreas de maior exposição e os resultados da Avaliação Interna de Riscos, podendo incluir trilhas digitais, sessões práticas, treinamentos direcionados e capacitações especializadas.

A gestão integral e o controle de eficácia do programa de capacitação competem à área de Compliance, que deve monitorar a adesão para garantir a participação de cem por cento do público-alvo requerido no ciclo anual. O aproveitamento dos participantes é verificado mediante testes de avaliação aplicados ao término do treinamento.

Todas as evidências geradas nesse processo, tais como relatórios de conclusão, listas de presença de sessões presenciais, materiais didáticos utilizados e notas obtidas nas avaliações, devem ser mantidas organizadas e arquivadas em conformidade com o prazo legal de guarda de documentos, servindo como comprovação técnica e formal para auditorias internas, independentes e fiscalizações dos órgãos reguladores.

11. CONHEÇA SEU CLIENTE

A Instituição adota procedimentos de identificação, qualificação, classificação e atualização cadastral de clientes, investidores, representantes, procuradores e beneficiários finais antes do início e durante a manutenção do relacionamento. Esses procedimentos devem observar a abordagem baseada em risco, incluindo coleta e validação de informações cadastrais, verificação de beneficiário final, identificação de Pessoas Expostas Politicamente e seus relacionados, avaliação de listas restritivas, sanções, mídias desabonadoras e jurisdições de maior risco, bem como aplicação de diligência reforçada para clientes classificados como de maior risco. A ausência, inconsistência ou insuficiência de informações necessárias poderá impedir o início, a continuidade ou a ampliação do relacionamento com a Instituição.

12. CONHEÇA SEU COLABORADOR, PARCEIRO, PRESTADOR DE SERVIÇO E FORNECEDOR

A Instituição adota procedimentos contínuos visando identificar, qualificar e monitorar seus colaboradores, parceiros de negócios, prestadores de serviços e fornecedores ao longo de todo o relacionamento profissional e contratual. Essas medidas têm como objetivo mitigar riscos associados à lavagem de dinheiro, ao financiamento do terrorismo e da proliferação de armas de destruição em massa, a fraudes, a conflitos de interesse, a sanções e a demais atos ilícitos.

Antes de qualquer admissão, celebração de contrato ou início das atividades operacionais, será realizada análise prévia de risco do candidato, parceiro, prestador de serviços ou fornecedor, conforme os procedimentos de diligência aplicáveis. A área de PLD/FTP realizará a análise e emitirá parecer técnico contendo a conclusão obtida com base nas verificações realizadas, a classificação de risco e as recomendações pertinentes. Os casos classificados como de Risco Alto ou Crítico, ou que apresentem apontamentos relevantes, deverão ser submetidos à aprovação da alçada competente, incluindo o Diretor responsável, conforme a estrutura de governança e os critérios internos estabelecidos. A ausência, inconsistência ou insuficiência das informações necessárias poderá impedir o início, a continuidade ou a ampliação do relacionamento com a Instituição.

A Instituição realiza análises periódicas de sua base de colaboradores, parceiros, prestadores de serviços e fornecedores para o acompanhamento contínuo e a devida atualização de sua classificação de risco. A frequência e a profundidade dessas reavaliações consideram a natureza do vínculo, a criticidade operacional e o enquadramento de risco da parte ao longo de todo o seu relacionamento com a Instituição.

13. BENEFICIÁRIO FINAL

Os procedimentos de identificação e qualificação de pessoas jurídicas exigem a análise e o mapeamento da cadeia de participação societária, até a identificação da pessoa natural caracterizada como seu beneficiário final. Considera-se beneficiário final a pessoa natural que, em última instância, direta ou indiretamente, possui, controla ou influencia significativamente a pessoa jurídica, estrutura jurídica ou fundo de investimento, ou em nome da qual uma transação é conduzida, observados os critérios e percentuais definidos na regulamentação aplicável e nas normas internas da Instituição.

Caracteriza-se a influência significativa quando a pessoa natural detém mais de 25% (vinte e cinco por cento) do capital social ou dos direitos de voto, ou exerce a preponderância nas deliberações sociais, independentemente do percentual de participação societária mantido.

Compete à área demandante a obtenção e apresentação de documentação oficial, válida e atualizada que comprove, de forma clara e rastreável, toda a árvore de controle societário, abrangendo contratos sociais, estatutos, atas, regulamentos, livros societários, declarações de custódia e organogramas assinados, conforme a natureza jurídica da contraparte e as especificidades detalhadas nos manuais e procedimentos operacionais de PLD/FTP.

14. MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

A Instituição adota procedimentos de monitoramento, seleção, análise e tratamento destinados à identificação de operações e situações que possam indicar a utilização da Instituição para a prática de lavagem de dinheiro, financiamento do terrorismo, financiamento da proliferação de armas de destruição em massa, descumprimento de sanções ou outras atividades ilícitas.

Os procedimentos e cenários de monitoramento são definidos com base na Avaliação Interna de Risco e na Política de PLD/FTP, considerando a classificação de risco do cliente, o canal utilizado, a presença de Pessoas Expostas Politicamente (PEPs) ou seus familiares e estreitos colaboradores, além de operações oriundas ou destinadas a jurisdições com deficiências estratégicas em PLD/FTP.

O monitoramento contínuo das operações, movimentações e comportamentos de clientes e demais contrapartes é realizado com o objetivo de identificar situações atípicas ou incompatíveis com o perfil de risco estabelecido.

As operações ou situações que, após análise, apresentarem indícios de lavagem de dinheiro, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa devem ser comunicadas ao COAF, nos prazos e na forma estabelecidos pela regulamentação vigente. A decisão de comunicação ou de não comunicação deve ser formalmente documentada, com registro dos fundamentos da análise, das evidências consideradas, da alçada responsável, da data da decisão, do prazo regulatório aplicável e da rastreabilidade do processo decisório.

É vedado aos colaboradores, administradores, parceiros e prestadores de serviços comunicar ao cliente, contraparte ou terceiro envolvido a existência de análise interna, investigação, deliberação ou comunicação ao COAF, devendo ser preservado o sigilo das informações relacionadas ao processo de PLD/FTP.

Quando aplicável, a Instituição deve realizar a comunicação de não ocorrência ao COAF, nos prazos e na forma estabelecidos pela regulamentação vigente, mantendo evidência formal da avaliação e do envio.

15. SANÇÕES, LISTAS RESTRITIVAS E INDISPONIBILIDADE DE ATIVOS

A Instituição deve manter procedimentos de consulta, monitoramento e tratamento de apontamentos em listas restritivas, sancionatórias, nacionais e internacionais, incluindo resoluções do Conselho de Segurança das Nações Unidas, observando os procedimentos de indisponibilidade de ativos, comunicação às autoridades competentes e registro das evidências de análise e decisão.

16. PESSOA EXPOSTA POLITICAMENTE

A Instituição deve manter procedimentos para identificação, qualificação, classificação, aprovação, monitoramento e revisão periódica de clientes, beneficiários finais, representantes, procuradores, contrapartes ou relacionados classificados como Pessoas Expostas Politicamente (PEP). Considera-se PEP a pessoa natural que desempenha ou tenha desempenhado cargo, emprego ou função pública relevante no Brasil ou em país, território ou dependência estrangeira, bem como seus familiares e estreitos colaboradores, ou pessoas jurídicas das quais participem ou com as quais mantenham relacionamento relevante, sendo a condição de PEP aplicável durante o exercício da função e pelos 5 (cinco) anos seguintes à data em que a pessoa deixar de se enquadrar nas categorias previstas na regulamentação.

17. SIGILO, CONFIDENCIALIDADE E RESTRIÇÃO DE ACESSO

Todas as informações, relatórios, pareceres e dossiês de análise de risco elaborados pela área de PLD/FTP possuem classificação de segurança Confidencial.

É expressamente proibido o compartilhamento, envio ou disponibilização dos dossiês de PLD/FTP, sejam parciais ou conclusivos, com as áreas demandantes do negócio, parceiros externos ou quaisquer outros terceiros não autorizados. A área de PLD/FTP informará às áreas solicitantes tão somente o parecer conclusivo e as recomendações de alçada, preservando o sigilo dos critérios detalhados, das fontes de pesquisa e das ferramentas de inteligência utilizadas.

O acesso integral aos dossiês restringe-se estritamente à própria equipe de PLD/FTP, aos Diretores Executivos e ao Comitê de PLD/FTP, garantindo-se o fornecimento, mediante registro e controle, aos órgãos reguladores (Banco Central do Brasil, COAF) e à Auditoria Interna/Independente, quando formalmente requisitado.

18. GUARDA DE DOCUMENTOS E REGISTROS

A Instituição manterá à disposição do Banco Central do Brasil e dos demais órgãos competentes os cadastros, documentos comprobatórios, dossiês de *due diligence*, relatórios de análise transacional, registros das operações realizadas, evidências de monitoramento, decisões de comunicação ou não comunicação, relatórios de efetividade e demais informações relacionadas aos procedimentos de PLD/FTP pelos prazos mínimos e observados os marcos iniciais de contagem estabelecidos na legislação e na regulamentação vigentes, conforme a natureza das informações, dos documentos e dos registros.

* * * * *

REGISTRO DAS ALTERAÇÕES

Versão	Data Vigência	Item / Resumo da Alteração	Motivo	Área Responsável	Data Vencimento
01	15/06/2020	Novo documento	Elaboração do documento	PLD/FTP	23/06/2022
02	23/05/2022	Leiaute do documento e atualização de conteúdo	Revisão Periódica	PLD/FTP	23/05/2023
03	21/09/2023	Atualização de conteúdo	Revisão Geral	PLD/FTP	21/09/2024
04	02/09/2026	Reestruturação do documento como um todo	Revisão Periódica	PLD/FTP	02/09/2028

Em caso de dúvidas sobre o conteúdo deste documento, contate a área responsável.

Qualquer outro assunto em relação à publicação deste documento, fale com a área de Compliance.