Elaboração: Departamento de PLD/FTP	Validação: Departamento de Compliance	Aprovação: CAD
Data aprovação: 25/03/2025	Validade: 24/03/2026	Versão: 05

SUMÁRIO

1. OBJETIVO

Esta Política tem por objetivo estabelecer princípios, diretrizes, procedimentos e responsabilidades compatíveis com os negócios e porte do Banco Semear S.A.; de forma a garantir que a Instituição atue de forma responsável e eficaz na Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa ("PLD/FTP"), minimizando os riscos financeiros, jurídicos, reputacionais e socioambientais, e protengendo a Instituição, seus clientes e o sistema financeiro como um todo.

2. APLICAÇÃO

Esta Política é aplicável a todos os colaboradores, prestadores de serviços, correspondentes bancários e parceiros do Banco Semear S.A..

3. REFERÊNCIA

Novas referências normativas que impactem os processos de PLD/FTP serão adotadas de forma imediata às práticas da Instituição, tomando como base as referências a seguir, sem se restringir a elas, assegurando a contínua conformidade regulatória e a efetividade dos controles, sem a necessidade de revisões constantes desta Política.

a) **Carta-Circular 4.001, de 29 de janeiro de 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 ao terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf);

b) **Circular 3.978, de 23 de janeiro de 2.020** - Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática 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, previsto na Lei nº 13.26, de 16 de março de 2016;

c) **Instrução Normativa BCB nº 262, de 31 de março de 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;

d) **Instrução Normativa RFB 2119, de 06 de dezembro de 2022** – Dispõe sobre o Cadastro Nacional da Pessoa Jurídica no âmbito da Secretaria Especial da Receita Federal do Brasil;

e) **Lei 13.810, de 8 de março de 2019** - 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, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados; e revoga a Lei nº 13.170, de 16 de outubro de 2015;

f) **Lei 13.974, de 7 de janeiro de 2020** - Dispõe sobre o Conselho de Controle de Atividades Financeiras (Coaf), de que trata o art. 14 da Lei nº 9.613, de 3 de março de 1998;

g) **Lei 14.478, de 21 de dezembro de 2022** - Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições;

h) **Lei 9.613, de 03 de março de 1.998** - Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências;

i) **Lei nº 13.260, de 16 de março de 2.016** - Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013;

j) **Resolução 4.753, de 26 de setembro de 2.019** - Altera e consolida as normas relativas à abertura, manutenção e movimentação de contas de depósitos;

k) **Resolução BCB 131, de 20 de agosto de 2021** - Consolida as normas sobre o rito do processo administrativo sancionador, a aplicação de penalidades, o termo de compromisso, as medidas acautelatórias, a multa cominatória e o acordo administrativo em processo de supervisão, previstos na Lei nº 13.506, de 13 de novembro de 2017, e os parâmetros para a aplicação das penalidades administrativas previstas na Lei nº 9.613, de 3 de março de 1998;

l) **Resolução BCB 44, 24 de novembro de 2020** - Estabelece procedimentos para a execução pelas instituições autorizadas a funcionar pelo Banco Central do Brasil das 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, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;

m) **Resolução COAF 40, de 22 de novembro de 2021** - Dispõe sobre procedimentos a serem observados, em relação a pessoas expostas politicamente, por aqueles que se sujeitam à supervisão do Conselho de Controle de Atividades Financeiras (Coaf) na forma do § 1º do art. 14 da Lei nº 9.613, de 3 de março de 1998. Após a entrada em vigor desta resolução, fica revogada a Resolução nº 29, de 7 de dezembro de 2017, do Coaf;

n) **Resolução CMN nº 4.557, de 23 de fevereiro de 2017** - Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital, estabelecendo requisitos para a implementação de uma gestão contínua e integrada de riscos pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;

o) **Resolução CMN nº 4.595, de 28 de agosto de 2017** - Estabelece diretrizes para a política de conformidade (compliance) das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, visando assegurar o efetivo gerenciamento do risco de conformidade;

p) **Resolução CMN nº 4.935, de 29 de setembro de 2021** - Dispõe sobre a contratação de correspondentes no País pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, estabelecendo critérios e procedimentos para essa contratação;

q) **Resolução BCB nº 1, de 12 de agosto de 2020** - Regulamenta o arranjo de pagamento instantâneo denominado Pix, estabelecendo as diretrizes e regras para seu funcionamento no âmbito do Sistema de Pagamentos Brasileiro;

r) **Resolução BCB nº 277, de 31 de março de 2022** - Regulamenta o mercado de câmbio, capitais brasileiros no exterior e capitais estrangeiros no País, estabelecendo normas para a realização de operações no mercado de câmbio;

s) **Avaliação Interna de Riscos (AIR);**

t) **Política de Cadastro do Banco Semear S. A.**;

4. DEFINIÇÕES, CONCEITOS E SIGLAS

a) **AIR: Avaliação Interna de Riscos** – avaliação que possui como objetivo identificar e mensurar o risco de utilização dos produtos e serviços da Instituição na prática da lavagem de dinheiro e do financiamento do terrorismo;

b) **Beneficiário Final –** pessoa natural que, em última instância, de forma direta ou indireta, possui, controla ou influencia significativamente certa entidade; ou a pessoa natural em nome da qual uma transação é conduzida ou dela se beneficie;

c) **COAF**: Conselho de Controle de Atividades Financeiras. Unidade de Inteligência Financeira Brasileira. Órgão criado pela Lei 9.613, de 1988, e reestruturado pela Lei 13.974, de 2020, que tem como finalidade: "*i) produzir e gerir informações de inteligência financeira para a prevenção e o combate à lavagem de dinheiro;*" e "*ii) promover a interlocução institucional com órgãos e entidades nacionais, estrangeiros e internacionais que tenham conexão com suas atividades*";

d) **Colaborador** – funcionário da Instituição;

e) **Combate ao Financiamento do Terrorismo** – ações que visam impedir o financiamento do terrorismo, criminalizando a coleta de fundos para este fim e bloqueando os bens financeiros dos terroristas;

f) **FT**: Financiamento do Terrorismo;

g) **GAFI:** Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo **–** entidade intergovernamental, cujas atividades visam estabelece padrões e promover a efetiva implementação de leis, regulamentos e medidas operacionais para combater a lavagem de dinheiro, o financiamento do terrorismo e outras ameaças à integridade do sistema financeiro internacional;

h) **Instituição** – Banco Semear S.A.;

i) **Instrumento** – Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa;

j) **LD**: Lavagem de Dinheiro – é o processo pelo qual um indivíduo ou organização criminosa busca, por meio de operações financeiras ou comerciais, ocultar a origem ilegal de recursos ou bens, incorporando-os à economia formal, de maneira que esses recursos tenham a aparência de origem lícita;

k) **Parceiro –** pessoa jurídica que intermedia operações comerciais para a Instituição;

l) **Pessoas Expostas Politicamente ("PEP") –** consideram-se PEP os ocupantes de cargos e funções públicas, conforme definido no art. 27, da Circular 3.978, de 2020 e Resolução COAF 40, de 2021;

m) **PLD/FTP**: Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa – procedimentos que tem por objetivo orientar os funcionários da Instituição, de forma a evitar a prática de "Lavagem de Dinheiro".

5. PRINCÍPIOS

Os princípios abaixo constituem diretrizes para o processo de PLD/FTP:

I. **Ética e Legalidade:** atuação em conformidade com a legislação e regulação vigentes, com altos padrões de ética, moralidade, retidão e conduta ilibada, de forma a manter a integridade em todas as operações;

II. **Melhoria contínua:** compromisso de aperfeiçoar continuamente os padrões de ética e conduta, a aplicação de medidas corretivas, os adequados níveis de segurança, a qualidade dos produtos ofertados e a eficiência dos serviços;

III. **Colaboração com as Autoridades Públicas:** promoção estreita e transparente da colaboração com as autoridades públicas, por meio de um sistema de controle adequado, de políticas rígidas e robustas no processo de PLD/FTP, e do fornecimento de informações às autoridades.

A aderência a estes princípios fornece uma base sólida à Instituição, permintindo-a exercer análise eficiente e eficaz com respeito aos seus clientes, parceiros, prestadores de serviços terceirizados e colaboradores, de forma a promover a conformidade legal, a integridade nas operações financeiras e a prevenção de atos ilícitos, mitigando riscos e protegendo tanto a Instituição quanto todos aqueles com quem mantém relacionamento.

6. DIRETRIZES

Esta Política estabelece as diretrizes para:

I. a definição de papéis e responsabilidades, quanto à adequação e ao cumprimento das obrigações ora estabelecidas;

II. a definição de procedimentos e controles integrados, voltados à avaliação e à análise, prévia e complementar, de forma a identificar, monitorar e impedir atividades de natureza criminosa em produtos e serviços disponibilizados pela Instituição, assim como àqueles voltados à seleção e contratação de funcionários, prestadores de serviços terceirizados, parceiros de negócio e clientes, adotando, para tanto, uma abordagem baseada em risco;

III. a elaboração da avaliação interna de riscos e da avaliação de efetividade;

IV. a verificação do cumprimento das obrigações, dos procedimentos e dos controles internos estabelecidos nesta Política, assim como a identificação e a correçã das deficiências apontadas;

V. a promoção da cultura organizacional de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa para todos aqueles que possuem relacionamento com o Banco Semear S.A.;

VI. a capacitação de funcionários e funcionários de correspondentes bancários que prestem

atendimento em nome do Banco Semear S.A..

Tendo como base os princípios elencados no item 5, a Instituição seguirá as seguintes diretrizes no processo de PLD/FTP:

a) Desenvolver a atividade financeira com rigoroso atendimento à legislação, às normas e às regulamentações vigentes.

b) Promover adequada estrutura de governança com normas de atuação, sistemas de controle, sistemas de comunicação e atribuição de papéis e responsabilidades.

c) Assegurar estrutura e mecanismos de acompanhamento à implementação e adequação dos procedimentos e controles de PLD/FTP para cumprimento das diretrizes que constam nesta Política.

d) Promover a Avaliação Interna de Risco (AIR), conforme modelo estipulado por meio da Circular 3.978, de 2020, e fornecer as informações necessárias à elaboração da Avaliação de Efetividade.

e) Aplicar medidas reforçadas nos casos identificados de risco elevado.

f) Aplicar procedimento de aceitação de relacionamento, tendo por base a abordagem baseada em risco, bem como a recusa, no caso de não cumprimento das obrigações de identificação e diligência.

g) Instituir obrigação de abstenção da realização de operações que evidenciem fundada suspeita de constituir-se em prática de crime de LD/ FTP.

h) Monitorar operações e providenciar a comunicação ao COAF de práticas suspeitas de LD/FTP, sempre que identificadas situações que reflitam suspeita, nos termos da Carta-Circular 4.001, de 2020.

i) Adotar procedimentos prévios no desenvolvimento de produtos e serviços, para inibir sua utilização para as práticas de LD/ FTP, incluindo a utilização de novas tecnologias.

j) Aplicar medidas de diligência reforçada às operações que envolvam produtos classificados como de alto risco LD/ FTP.

k) Assegurar efetivo processo de seleção, contratação e capacitação de colaboradores, parceiros e prestadores de serviços terceirizados no que se refere a PLD/FTP.

l) Garantir a guarda dos documentos gerados no processo e mantê-los arquivados pelos prazos exigidos e à disposição dos reguladores.

m) Cooperação com atividades de investigação e/ou fiscalização de órgãos, entidades e agentes públicos.

n) Assegurar adequado processo de avaliação de situações a serem comunicadas aos órgãos reguladores e garantir o processo de comunicação das situações obrigatórias.

o) Instituir obrigação de sigilo face aos clientes e a terceiros envolvidos em processo de comunicação legal ou que se encontrem em investigação.

p) Promover a cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, inclusive por meio de treinamentos com certificação anual aos colaboradores.

7. PAPÉIS E RESPONSABILIDADES

Todos os colaboradores do Banco Semear S.A., independentemente do nível hierárquico, devem cumprir rigorosamente as diretrizes estabelecidas nesta Política, garantindo a conformidade com as normas internas e regulatórias. O descumprimento dessas diretrizes poderá ser caracterizado como falta grave, sujeitando o infrator às sanções cabíveis.

Além disso, a seguir são detalhados os papéis e responsabilidades dos diversos órgãos de governança corporativa do Banco Semear S.A., assegurando o cumprimento das obrigações previstas na Circular 3.978, de 2020, bem como a efetividade das medidas de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa (PLD/FTP).

7.1. CONSELHO DE ADMINISTRAÇÃO (CAD)

a) Analisar e aprovar o presente instrumento;
b) Apreciar relatórios das auditorias e determinar ao Diretor de PLD/FTP a adoção de ações, providências e medidas necessárias para eventuais correções de irregularidades apontadas;
c) Ter conhecimento das diretrizes da AIR e acompanhar e aprovar melhorias para os casos que estejam em desacordo;
d) Prover os meios necessários para o entendimento do arcabouço legal de PLD/FTP; e
e) Aprovar e acompanhar melhorias dos pontos das Auditorias Interna, Externa e do Banco Central do Brasil.

7.2. DIRETOR RESPONSÁVEL POR PLD/FTP

a) Assegurar o cumprimento desta Política promovendo meios e ferramentas necessários;
b) Posicionar regularmente o Conselho de Administração sobre as atividades do Departamento de Compliance e PLD/FTP e fazer as recomendações apropriadas;
c) Garantir à área gestora de PLD/FTP agir de forma independente e com acesso irrestrito às informações e a todas as instâncias da Administração, em assuntos relativos à PLD/FTP;
d) Aprovar e assegurar o cumprimento da AIR;
e) Prover os meios necessários para o entendimento do arcabouço legal de PLD/FTP;
f) Encaminhar aos diretores e aprovar o “Manual de Conheça seu Cliente (KYC)”;
g) Adotar medidas para que todos os novos produtos e serviços a serem disponibilizados pelo Banco atendam aos procedimentos de prevenção e combate à lavagem de dinheiro.

7.4. DIRETOR RESPONSÁVEL POR CONTROLES INTERNOS

a) Instruir a elaboração e aprovar a Avaliação de Efetividade;

b) Instruir acompanhamento do Plano de Ação para cumprimento de eventual apontamento na Avaliação de Efetividade, se houver;

c) Aprovar, em conjunto com os demais Diretores, o "Manual de Conheça seu Cliente (KYC)";

7.5. DEPARTAMENTO DE PLD/FTP

a) Criar procedimentos que possibilitem o monitoramento e a identificação de situações consideradas atípicas, realizadas pelos clientes e colaboradores da Instituição;

b) Avaliar as movimentações financeiras dos clientes em todas as modalidades de negócio da Instituição, comunicando ao COAF qualquer indício de lavagem de dinheiro;

c) Emitir relatório de análise de cliente, colaborador, parceiro, correspondente bancário e prestador de serviços terceirizados, oferecendo parecer consistente e posição sobre aceitação ou recusa ao início e/ou manutenção de relacionamento com a Instituição;

d) Adotar os princípios de "Conheça seu Cliente", com foco em PLD/FTP, e abordagem baseada em risco;

e) Adotar de princípios de "Conheça seu Colaborador", com foco em PLD/FTP, e abordagem baseada em risco;

f) Adotar de princípios "Conheça seu Prestador de Serviço e Parceiro", com foco em PLD/FTP, e abordagem baseada em risco;

g) Estabelecer avaliação prévia na ótica de PLD/FTP de novos produtos e serviços;

h) Fomentar a cultura de PLD/FTP por meio de treinamentos específicos e certificação de colaboradores;

i) Fazer cumprir as normas e procedimentos dos instrumentos do programa de PLD/FTP;

j) Propor alterações na AIR;

k) Manter registro e controle das análises efetuadas e de toda a documentação suporte; e

l) Atualizar as informações contidas nesta Política, revisando o documento.

7.6. DEPARTAMENTO DE CADASTRO

a) Atender às exigências dos órgãos reguladores, exigindo completa documentação para início e/ou manutenção do relacionamento com o cliente;

b) Informar ao Departamento de PLD/FTP qualquer indício de irregularidade ou recusa no fornecimento de informações obrigatórias para cadastro;

c) Atender a toda e qualquer solicitação do Departamento de PLD/FTP, inclusive registrar em cadastro

eventuais marcações específicas indicadas para clientes, tais como PEP, "Especial Atenção", dentre outras; e

d) Informar ao Departamento de PLD/FTP sobre situações atípicas, relacionadas aos clientes e aos gerentes responsáveis.

7.7. GERENTE RESPONSÁVEL PELA CONTA PJ E INTERNET BANKING (IB)

a) Elaborar o relatório de visita, quando solicitado e/ou quando for realizar visita *in loco* a clientes e correspondentes bancários;

b) Requerer esclarecimentos, e, eventualmente, justificar as movimentações atípicas, conforme solicitação do Departamento de PLD/FTP;

c) Realizar os procedimentos de segurança necessários à proposição de relacionamento, indicado ao Departamento de PLD/FTP qualquer suspeita ou inconsistência nas informações prestadas e documentos apresentados; e

d) Comunicar ao Departamento de PLD/FTP sobre atitudes suspeitas, situações atípicas, recusas injustificadas no fornecimento de documentos e/ou informações ou propostas de operações incompatíveis, relacionadas aos seus clientes.

7.8. SUPORTE COMERCIAL

a) Atender a toda e qualquer solicitação do Departamento de PLD/FTP referente a PLD;

b) Comunicar ao Departamento de PLD/FTP sobre atitudes suspeitas, situações atípicas, negativas injustificadas ao fornecimento de informações e/ou documentos ou propostas de operações incompatíveis, relacionadas aos clientes.

7.9. DEPARTAMENTO DE CAPITAL HUMANO

a) Adotar controles aderentes ao processo "Conheça seu Colaborador", seja durante a fase de contratação, seja durante a vigência de seu contrato de trabalho no Banco Semear S. A.; e

b) Auxiliar o Departamento de PLD/FTP no monitoramento do cliente, em especial com relação à situação econômico-financeira dos colaboradores.

7.10. DEPARTAMENTO DE CONTROLES INTERNOS

a) Implementar os controles relacionados aos processos e atividades da área de PLD/FTP;

b) Elaborar, anualmente, a Avaliação de Efetividade, e solicitar, se necessário, Plano de Ação para correção de eventual apontamento, acompanhando sua implementação.

7.11. AUDITORIA INTERNA

a) Revisar e avaliar a eficiência quanto à implementação e os controles da Política e Norma de PLD/FTP.

7.12. COLABORADORES

a) Realizar, anualmente, treinamento para certificação em PLD/FTP;
b) Comunicar ao Departamento de PLD/FTP toda e qualquer proposta, situação ou operação considerada atípica ou suspeita; e
c) Comunicar, através do Canal de Denúncia, atitudes suspeitas envolvendo administradores, colaboradores e/ou parceiros da Instituição.

8. ESTRUTURA ORGANIZACIONAL

O Departamento responsável pelo programa de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo da Instituição responde diretamente ao Diretor de Compliance/ PLD/FTP do Banco Semear S.A., estando segregado das áreas de negócios e da Auditoria Interna do Banco Semear S.A..

9. DETALHAMENTO

9.1. INTRODUÇÃO

O Banco Semear reconhece a importância da prevenção à lavagem de dinheiro e ao financiamento do terrorismo como parte fundamental de suas responsabilidades como entidade regulada.

A Instituição está comprometida com o adequado processo de combate e prevenção à LD/FTP, praticando- o ao exercer com diligência o procedimento de “Conheça seu Cliente, “Conheça seu Colaborador”, “Conheça seu Parceiro/ Correspondente Bancário” e “Conheça seu Fornecedor”, de forma a manter a integridade do sistema financeiro, cooperando com as autoridades competentes e protegendo sua reputação e a dos seus clientes. A instituição também promove uma cultura de conformidade e sensibilização entre seus funcionários.

9.2. CADASTRO DE CLIENTES

O cadastro de clientes é essencial na prevenção à lavagem de dinheiro e ao financiamento do terrorismo, tornando indispensável o cumprimento da regulamentação vigente, bem como das regras internas da Instituição formalizadas na Política de Cadastro e demais instrumentos internos aplicáveis.

9.3. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

A Instituição obtêm dos clientes, e por meio de busca sistêmica em bancos de dados, informações que permitam caracterizá-los, ou não, como pessoa exposta politicamente, nos termos estabelecidos em

regulamento – em especial na Circular nº 3.978, de 2020. As operações ou propostas de operações que possuam estes (PEP) como parte envolvida serão marcadas como "Especial Atenção" e serão monitoradas com maior cuidado e constância.

São consideradas PEPs aquelas pessoas que ocupam funções públicas relevantes nos diversos poderes e esferas governamentais.

No âmbito dos procedimentos de Conheça Seu Cliente (KYC), também é realizada a verificação da condição de representante, familiar ou estreito colaborador de PEPs. Para esse fim, são considerados:

✓ Familiares diretos, incluindo cônjuge, companheiro(a), enteado(a), parentes em linha reta ou colateral até o segundo grau;

✓ Estreitos colaboradores, ou seja, pessoas que possuam vínculo próximo com a PEP e que, em função desse relacionamento, possam representar um risco adicional à instituição.

Para clientes enquadrados nessas categorias, são aplicados procedimentos e controles internos específicos, compatíveis com o nível de risco associado, sendo esse fator considerado na classificação do cliente dentro das categorias de risco da instituição.

Além disso, em situações em que o risco percebido seja elevado, o interesse institucional no início ou manutenção do relacionamento será submetido a avaliação superior, sendo a decisão tomada por um gestor com nível hierárquico superior ao do responsável pela autorização inicial, conforme diretrizes estabelecidas nos manuais específicos.

O Banco Semear segue, para classificação de PEP, o conceito e orientação dos artigos 19 e 27, da Resolução 3.978, de 2020, como principal norte na identificação da condição de PEP do cliente e/ou proposto cliente.

9.4. ANÁLISE DE MOVIMENTAÇÕES FINANCEIRAS

Visando o cumprimento do que é disposto na legislação de PLD/FTP, a Instituição executa o monitoramento das movimentações financeiras realizadas pelos clientes. As análises possuem como objetivo a identificação de movimentações que possam se caracterizar, em tese, como lavagem de dinheiro ou financiamento ao terrorismo, conforme situações descritas na Carta Circular 4.001/20.

Os procedimentos adotados para monitoramento das movimentações financeiras dos clientes seguem os princípios e diretrizes traçados neste Instrumento e estão descritos no Manual Conheça seu Cliente.

9.5. COMUNICAÇÕES AO COAF

Após análise das movimentações atípicas/suspeitas, o Departamento de PLD/FTP deverá emitir parecer para a decisão do Diretor de PLD/FTP sobre a comunicação ou não das operações (efetivamente realizadas ou propostas). As comunicações devem ser encaminhadas ao COAF no prazo de 24h (vinte e

quatro horas) úteis contadas da decisão colegiada do Comitê, conforme exemplificado em Manual Conheça seu Cliente e Instrução de Trabalho de Comunicações ao COAF.

9.6. ENCERRAMENTO DE RELACIONAMENTO

Havendo a recorrência de casos com indícios de lavagem de dinheiro e/ou financiamento ao terrorismo por parte do cliente, o Departamento responsável pelo programa de PLD/FTP da Instituição submeterá parecer ao Comitê de Aceitação e Manutenção de Relacionamento, para que seja decidido sobre o início e/ou a manutenção (ou não) do relacionamento. Caso a decisão seja pelo encerramento do relacionamento, o Departamento encaminhará à área de cadastro, para que proceda conforme normativo em vigor.

A recorrência de casos com indícios de lavagem de dinheiro e/ou financiamento ao terrorismo não é condição necessária ao encerramento de relacionamento, uma vez que, se constatada a adequação da medida para o caso em específico, esta poderá ser tomada, ainda que a movimentação suspeita tenha ocorrido/ tenha sido identificada apenas uma vez.

9.7. ARQUIVO

O Departamento de PLD/FTP é o responsável pela guarda e o arquivamento de toda a documentação suporte relativa às análises efetuadas, devendo mantê-las em arquivo digital, em diretório próprio, pelo prazo minímo de 05 (cinco) anos, para acesso do Banco Central.

9.8. TERRORISMO E SEU FINANCIAMENTO

O Banco Semear S. A., enquanto atuante no mercado de câmbio, adota uma abordagem baseada em riscos, para a prevenção do terrorismo e seu financiamento, que tem por base a investigação das operações, bem como seu acompanhamento, conforme definido em Manual Conheça seu Cliente.

9.9. CONHEÇA SEU CLIENTE

Conhecer o cliente envolve um conjunto de regras e procedimentos bem definidos, adotadas pela Instituição com o objetivo de orientar todas as áreas do Banco Semear a “Conhecer Seu Cliente” (KYC), de forma a minimizar o risco de entrada de recursos provenientes de atividades ilícitas.

Cabe ao Departamento de PLD/FTP analisar, de forma robusta, precisa e completa, os dados, características e classificação de seus clientes e pretensos clientes, para identificar, em especial, a origem e o destino dos recursos financeiros destes, evitando, em consequência, ilegalidades e/ou irregularidades.

São adotados procedimentos para a identificação e validação da identidade do cliente, abrangendo a

obtenção, verificação e validação da autenticidade das informações cadastrais. Esse processo inclui a confrontação dos dados fornecidos com listas disponíveis em bancos de dados públicos e/ou privados, sempre que necessário e de acordo com a categoria de risco atribuída ao cliente.

Nesta fase, são coletados, no mínimo, as seguintes informações:

Pessoa Física: Nome completo e CPF;

Pessoa Jurídica: Razão social e número de registro no CNPJ.

Para clientes classificados com maior nível de risco, são exigidos dados e informações adicionais que reforcem o processo de identificação e cadastramento, garantindo maior segurança na avaliação do perfil.

A validação do CPF e do CNPJ é realizada por meio de consulta ao site da Receita Federal do Brasil (RFB), sendo vedado o início de relacionamento com clientes que apresentem status de inabilitação, incluindo cadastros suspensos, cancelados ou nulos.

Para pessoas naturais ou jurídicas residentes no exterior, que estejam dispensadas da inscrição no CPF ou CNPJ, conforme diretrizes da RFB, serão aceitos outros documentos de identificação, desde que em conformidade com a regulamentação aplicável.

As informações e dados cadastrais dos clientes são periodicamente atualizados, conforme a classificação de risco, assegurando a aderência aos procedimentos estabelecidos no manual específico.

9.10. QUALIFICAÇÃO

São adotados procedimentos para a qualificação dos clientes, baseados na coleta, verificação e validação de informações, de acordo com o perfil de risco e a natureza da relação de negócios a ser estabelecida.

A coleta de informações tem como objetivo identificar o local de residência, no caso de pessoa natural, e o local da sede ou filial, no caso de pessoa jurídica. Além disso, o processo de qualificação permite avaliar a capacidade financeira do cliente, considerando renda para pessoas naturais e faturamento para pessoas jurídicas.

A verificação e validação dos dados coletados — incluindo documentos exigidos e informações complementares — serão realizadas de acordo com a classificação de risco do cliente e a natureza do relacionamento entre a Instituição e o cliente, conforme previsto no manual específico aplicável.

Nas situações de maior risco percebido, especialmente para pessoas jurídicas, a verificação e validação das informações poderão incluir visitas presenciais ou reuniões específicas com o cliente, além da implementação de níveis diferenciados de controle.

A qualificação do cliente será reavaliada continuamente, conforme a evolução da relação de negócios e do perfil de risco, garantindo que as informações coletadas permaneçam atualizadas.

O início da relação de negócios está condicionado à conclusão dos procedimentos de identificação e qualificação do cliente. Excepcionalmente, nos casos aprovados pela Gerência de PLD/FTP, poderá ser concedido um prazo máximo de 30 (trinta) dias para a finalização do processo, desde que sejam asseguradas as medidas de monitoramento, seleção e análise de operações suspeitas.

O processo de qualificação do cliente inclui a avaliação de aspectos comportamentais e reputacionais, por meio de consultas a bases de dados públicas e privadas, abrangendo:

✓ Listas restritivas globais e domésticas;

✓ Mídias negativas;

✓ Sanções internacionais;

✓ Riscos socioambientais;

✓ Histórico de processos judiciais;

✓ Outras fontes relevantes para a mitigação de riscos.

9.11. CONHEÇA SEU COLABORADOR

Os colaboradores e pretensos colaboradores da Instituição deverão passar pelo processo de análise de relacionamento, orientado pela perspectiva da ética e da transparência, conforme descrito em Manual específico, levando em conta a função desempenhada e o risco que este apresenta ao Banco Semear S.A.. O Departamento de Capital Humano é o responsável por recrutar e selecionar colaboradores para ocupação dos diversos cargos da Instituição, cabendo-lhes, ainda, solicitar a análise do pretenso colaborador à área de PLD/FTP, para aferição do risco envolvido na contratação, antes de seguir com a informação de eventual aprovação em processo seletivo.

9.12. CONHEÇA SEUS PARCEIROS/PRESTADOR DE SERVIÇO

O Banco Semear S. A. adota procedimentos para a identificação e análise de aceitação e manutenção de relacionamento com parceiros comerciais, fornecedores e correspondentes bancários, visando prevenir a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas. As regras de aceitação estão descritas nos manuais específicos de “KYP e KYS”.

9.13. BENEFICIÁRIO FINAL

Nos procedimentos de qualificação de clientes pessoa jurídica, a cadeia de participação societária é analisada até a identificação da pessoa natural caracterizada como beneficiário final, nos termos da legislação e regulamentação vigentes. Para essa pessoa, serão aplicados, no mínimo, os procedimentos de qualificação compatíveis com a categoria de risco do cliente pessoa jurídica no qual detenha participação societária.

Além disso, são considerados beneficiários finais os representantes legais, procuradores e prepostos que exerçam efetivamente o comando sobre as atividades da empresa.

O Manual Específico KYC Integrado estabelece, de forma documentada e justificada, um valor mínimo de participação societária para a identificação do beneficiário final, definido com base na avaliação de risco. Esse limite não pode ser superior a 20% (vinte e cinco por cento), considerando tanto a participação direta quanto a indireta na estrutura societária.

Para clientes com configurações societárias especiais, conforme listado no §3º do artigo 24 da Circular BCB nº 3.978/2020, não é realizada a análise da cadeia de participação societária. No entanto, são coletadas informações detalhadas sobre as pessoas naturais autorizadas a representá-las, bem como seus controladores, administradores, gestores e diretores, conforme aplicável a cada caso.

9.14. DIRETRIZES AVALIAÇÃO INTERNA DE RISCO DE LD/FTP (''AIR'')

A Avaliação Interna de Risco (“AIR”) tem como base a abordagem baseada em Risco (“ABR”) a ser aplicada pelo Banco para mensuração do risco LD/FTP, sendo o princípio geral conhecer os riscos aos quais o Banco está exposto e, para os riscos mais elevados, ministrar medidas de diligências reforçadas para mitigar e administrar os riscos.

A avaliação tem como foco principal prevenir que o Banco, no desempenho de suas atividades, possibilite a utilização de seus produtos e serviços para a prática dos crimes de lavagem de dinheiro, ou ocultação de bens, direitos, valores e de financiamento ao terrorismo; permitindo a avaliação de suas vulnerabilidades, riscos e controles existentes, de modo a orientar objetivamente os esforços a serem envidados no combate à LD/FTP.

Neste cenário, é necessário avaliar e documentar a complexidade dos riscos, a probabilidade e os impactos financeiros, jurídicos, reputacionais e socioambientais.

A avaliação deverá ser devidamente aprovada pela Diretoria de PLD/FTP e encaminhada ao conselho de Administração e Comitê de Risco para ciência. A “AIR” será revisada bienalmente ou anterior a esse prazo em caso de necessidade .

10. LIMITE OPERACIONAL – OPERAÇÕES DE CÂMBIO

A definição dos limites operacionais das operações de natureza cambial, é realizada com base na avaliação da capacidade financeira do cliente e na análise das operações propostas, com ênfase na origem primária

dos recursos. Esse processo assegura a compatibilidade e proporcionalidade ao nível de risco envolvido, considerando:

✓ Pessoa Física: renda declarada e outras fontes de comprovação de capacidade financeira;

✓ Pessoa Jurídica: faturamento declarado e outras formas que comprovem a capacidade financeira.

A aplicação desses critérios tem como objetivo garantir que as operações estejam alinhadas ao perfil econômico-financeiro do cliente, minimizando riscos e assegurando a aderência às diretrizes regulatórias, de conformidade e PLD/FTP.

11. ENTREVISTA DE *DUE DILIGENCE*

O início de relacionamento com clientes pessoa jurídica que apresentam maior nível de risco, especialmente aqueles de natureza cambial, poderá ser condicionado à realização de uma visita presencial ou reunião *online*, tendo como objetivo verificar a compatibilidade do perfil de negócios do cliente com o volume, a natureza e as características das operações pretendidas, considerando também o propósito do relacionamento.

Os manuais e políticas específicas de KYC estabelecem os critérios e condições para a realização dessas visitas/reuniões, levando em conta, de forma cruzada e integrada, os seguintes fatores:

✓ O nível de risco calculado;

✓ O início de relacionamento com empresa desconhecida e não tradicional;

✓ A localização e a distância das instalações;

✓ O volume de negócios pretendidos e realizados.

No âmbito cambial, é dedicada atenção especial às operações que, por sua natureza, apresentam risco elevado para a instituição, conforme matriz AIR, tais como:

✓ e-FX (câmbio eletrônico);

✓ CNR para movimentação de terceiros.

Para cada visita realizada, um relatório ou formulário específico deve ser preenchido, contendo tanto informações de interesse comercial quanto elementos que possam subsidiar a análise de PLD/FTP pelo serviço de cadastro. As informações mínimas a serem registradas incluem:

✓ Descrição objetiva da estrutura, do ambiente e da qualidade das instalações;

✓ Quantidade de empregados, máquinas e equipamentos;

✓ Descrição da movimentação de pessoas, mercadorias e veículos no dia da visita;

✓ Outras percepções relevantes identificadas pelo visitante;

✓ Histórico da empresa.

Essa abordagem visa garantir um processo de *due diligence* robusto, assegurando conformidade regulatória e mitigação de riscos no início e manutenção do relacionamento com clientes de maior complexidade.

12. NOVOS PRODUTOS E SERVIÇOS

Na criação de novos produtos ou serviços, o Departamento de PLD/FTP deve ser acionado para que sejam feitas análises e apontamentos em relação à PLD/FTP, bem como os eventuais riscos apresentados.

13. CULTURA ORGANIZACIONAL DE PLD/FTP

O Departamento de PLD/FTP, com o suporte das áreas de Comunicação Interna, CH e Marketing da Instituição, propagará a cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo aos seus colaboradores, prestadores de serviços e parceiros, bem como treinará, no mínimo a cada 12 (doze) meses, os colaboradores da Instituição. Ainda, periodicamente, serão divulgados comunicados institucionais com fulcro na disseminação da cultura organizacional da PLD/FTP.

14. DIRETRIZES AVALIAÇÃO DE EFETIVIDADE

A avaliação de efetividade representa a relação a ser observada entre a implementação e os resultados gerados pelo programa de PLD/FTP. Assim, devem ser avaliados os impactos e o grau de proximidade aos objetivos alcançados.

Para o processo de avaliação serão aplicados os seguintes testes:

a. Funcionalidade, performance, *stress*, robustez, segurança, bem como amostragem, abrangendo as formalizações, base do processo de gestão de PLD/FTP. Aqui serão avaliados os seguintes sistemas:
    - Sistema de cadastro
    - Sistema de renda fixa
    - Sistema de conta corrente
    - Sistema de câmbio
    - Sistema de empréstimos e financiamentos
    - Sistema de contas a pagar
    - Sistemas de apoio, análise e monitoramento

b. Avaliação de KPI´S de performance praticada para mensuração da efetividade;

c. Avaliação da qualidade das informações gerencias disponibilizadas;

d. Aplicação das medidas de diligências

e. Medidas de aculturamento e programa de treinamento e capacitação.

Como ponto importante à avaliação da efetividade do processo de gestão de PLD/FTP, devem ser considerados os apontamentos das deficiências relatadas no processo de inspeção pelos órgãos reguladores e pelas auditorias interna e externa. Estes relatos devem compor pauta específica do Comitê de Riscos, e implicarão na elaboração ações de priorização e acompanhamento permanente pela área de PLD/FTP (planos de ação). Deve ser gerado relatório gerencial de acompanhamento a ser aprovado pelas Diretorias de PLD/FTP e de Controles Internos.

15. GESTÃO DE CONSEQUÊNCIAS

A organização reconhece a importância de implementar medidas adequadas para gerenciar as consequências relacionadas a eventuais violações à presente Política. Para isso, estabelece uma estrutura de responsabilidade clara e transparente para a gestão de consequências.

16. TIPOS DE CONSEQUÊNCIAS

A organização estabelece uma lista de consequências que podem ser aplicadas em casos de violações da política de PLD/FTP. Essas consequências devem ser proporcionais à gravidade da violação e em conformidade com as leis e regulamentos aplicáveis. Alguns exemplos de consequências podem incluir:

a) Advertência verbal ou escrita;

b) Suspensão temporária de funções ou acesso a determinados recursos;

c) Redução de benefícios, como bônus ou incentivos;

d) Transferência para outra área ou departamento;

e) Demissão ou rescisão do contrato de trabalho;

f) Denúncia às autoridades competentes, quando apropriado.

17. PROCESSO DE GESTÃO DE CONSEQUÊNCIAS

A gestão de consequências é conduzida por meio de um processo estruturado, que inclui as seguintes etapas:

g) Identificação da violação: as violações à presente Política são identificadas por meio de mecanismos de monitoramento interno, denúncias e/ou investigações internas.

h) Avaliação da gravidade: a gravidade da violação é avaliada considerando-se fatores como o impacto potencial na reputação da organização, a quantidade de recursos envolvidos, a intencionalidade do ato e outros critérios relevantes.

i) Determinação das consequências: com base na avaliação da gravidade, é determinada a consequência apropriada, a ser aplicada em cada caso. Essa decisão deve ser tomada por uma

autoridade competente dentro da organização, garantindo a imparcialidade e a consistência.

j) Comunicação da consequência: a consequência é comunicada de forma clara e objetiva ao indivíduo envolvido na violação. Devem ser fornecidos os motivos da decisão e quaisquer direitos de recurso disponíveis.

k) Acompanhamento e revisão: as consequências aplicadas são acompanhadas e revisadas periodicamente para garantir que sejam eficazes na prevenção de futuras violações. Caso necessário, ajustes podem ser feitos para fortalecer o programa de PLD/FTP.

18. CONFIDENCIALIDADE E PROTEÇÃO DOS ENVOLVIDOS

A organização assegura a confidencialidade e a proteção dos envolvidos no processo de gestão de consequências, garantindo que as informações relacionadas às violações sejam tratadas com sigilo e que não haja retaliação contra aqueles que relatam ou participam das investigações.

Inclusive, o Banco Semear mantém ativo o Canal de Denúncias, em funcionamento no formato “24 x 7” (vinte e quatro por sete) – ou seja, a qualquer hora do dia ou da noite, todos os dias da semana, inclusive feriados; gerido por fornecedor/terceiro, como forma de assegurar o sigilo do denunciante, se assim este preferir.

19. REGISTRO E DOCUMENTAÇÃO

Todos os passos do processo de gestão de consequências devem ser registrados e documentados adequadamente. Isso inclui a identificação da violação, a avaliação da gravidade, a determinação das consequências, a comunicação da consequência e qualquer acompanhamento ou revisão subsequente.

20. ACESSO

Este documento poderá ser acessado por todos os colaboradores, prestadores de serviços e parceiros do Banco Semear S.A..

21. HISTÓRICO DAS VERSÕES

Esta política entra em vigor na data de sua publicação. Este documento será revisado anualmente após a data de publicação ou anterior a esse prazo em caso de necessidade, e, ainda, será remetida ao Conselho de Administração, para aprovação.