RB Investimentos

POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA – PLD/FTP

Sumário

1. Abrangência e Aplicabilidade

Esta Política é de aplicação obrigatória e integra o Sistema de Controles Internos da RB Investimentos Gestão de Recursos Ltda. ("RBI Gestora" ou "Instituição"), sendo vinculante para todos os seus colaboradores, independentemente do nível hierárquico, além de sócios, estagiários, terceiros, prestadores de serviços, parceiros comerciais e quaisquer representantes que atuem em nome da Instituição.

Seu cumprimento é essencial para garantir a conformidade da RBI Gestora com as obrigações previstas na legislação e regulamentação aplicável, especialmente a Lei nº 9.613/98 (com alterações da Lei nº 12.683/12), a Lei nº 13.260/16, a Lei nº 13.810/19, a Resolução CVM nº 50/21, entre outras normas expedidas por autoridades nacionais e organismos internacionais voltadas à prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e à proliferação de armas de destruição em massa.

Esta Política aplica-se a todas as áreas da RBI Gestora, abrangendo desde o relacionamento inicial com clientes, fornecedores, parceiros e prestadores de serviço, até a execução de operações, prestação de serviços, desenvolvimento de produtos e contratação de colaboradores. Todos os envolvidos devem observar rigorosamente as diretrizes, procedimentos e controles nela estabelecidos.

Quaisquer dúvidas sobre a aplicação desta Política devem ser direcionadas à área de *Compliance*, responsável por sua implementação, orientação e monitoramento contínuo, bem como pela comunicação com os órgãos reguladores e autorreguladores.

A presente política encontra-se de acordo com os seguintes regulamentos:

Regulamentação	Fonte	Assunto
Lei nº 9.613/98, cfe. alterada pela Lei nº 12.683/12	Presidência da República	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.
Lei nº 13.260/16	Presidência da República	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.
Lei 13.810/19	Presidência da República	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.

Resolução CVM nº 50 de 2021	Comissão de Valores Mobiliários (CVM)	Dispõe sobre a prevenção à lavagem de dinheiro e ao financiamento do terrorismo – PLDFT no âmbito do mercado de valores mobiliários.
Resolução CVM 35/21, Resolução CVM 13/20	Comissão de Valores Mobiliários (CVM)	Estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários.

2. Definições

Colaboradores: Estagiários e funcionários de todos os níveis operacionais e gerenciais, seja nas funções de negócio, suporte e/ou de controle.

Pessoa Exposta Politicamente (PEP): Nos termos da Resolução nº 40/21 do Conselho de Controle de Atividades Financeiras ("COAF"), são clientes que ocupam, ou ocuparam nos últimos cinco anos cargos públicos ou políticos, assim elencados na norma. Estes clientes exigem atenção especial no monitoramento de suas atividades.

Cliente: Pessoa (física ou jurídica) que utiliza os produtos ou serviços da RBI Gestora.

Beneficiário Final: Pessoa natural identificada como último membro da participação societária. É também considerado beneficiário final o representante, inclusive o procurador e o preposto, que exerça o comando de fato sobre as atividades da pessoa jurídica.

Lista de Abreviatura: Uma lista de abreviaturas é fornecida ao final deste documento.

Lavagem de Dinheiro (LD): O crime de lavagem de dinheiro ocorre por meio de um conjunto de operações comerciais ou financeiras para dar aparência lícita e incorporar à economia, de modo transitório ou permanente, recursos, bens e valores de origem ilícita, disfarçando os lucros ilícitos sem comprometer os envolvidos.

Financiamento ao Terrorismo (FT): O crime de financiamento ao terrorismo se trata da reunião de ativos financeiros ou bens patrimoniais para financiar a realização de atividades terroristas, tendo, pois, fontes legais ou ilegais. Em ambos os casos, é necessária a prevenção e no combate de tais condutas, desempenhando papel fundamental na adoção de procedimentos relativos à prevenção, identificação e reporte de ocorrências suspeitas – de acordo com a legislação e regulação aplicáveis.

Proliferação de Armas de Destruição em Massa (P): Proliferação de armas de destruição em massa significa a exposição e/ou envolvimento com a disseminação de armas capazes de causar um número elevado de

mortos numa única utilização, podendo ser nucleares, materiais físseis, armas de químicas, biológicas, radioativas. O uso de tais armas é considerado como crime de guerra.

3. Governança de PLD/FTP

3.1. Diretoria Colegiada

A alta administração é o mais alto nível hierárquico da RBI Gestora, possuindo compromisso efetivo com o programa de PLD/FTP e com objetivo de garantir que o programa se estenda a todas as demais áreas.

A alta administração ou Diretoria Colegiada é composta pelos diretores estatutários da RBI, conforme descrito no contrato social vigente. A Diretoria é responsável por estabelecer as diretrizes estratégicas de PLD/FTP, assegurando que as normas internas e externas sejam observadas em todas as unidades de negócio e áreas de suporte. Além disso, a Diretoria Colegiada monitora periodicamente as atividades de conformidade, analisando relatórios e dando orientações para aprimorar o programa de PLD/FTP da RBI Gestora.

3.2. Diretor Responsável

A Diretoria também designou o Diretor responsável pelo cumprimento das normas de PLD/FTP e representante junto aos órgãos reguladores. O Diretor também é o responsável por assegurar que o programa de PLD/FTP receba suporte adequado para sua efetiva implementação, manutenção e monitoramento. Na RBI Gestora, o Diretor lidera a equipe de *Compliance*, fornecendo orientação e suporte às áreas da empresa para garantir o cumprimento das normas e regulamentações de PLD/FTP, reportando as situações mais críticas sobre o tema ao Comitê de *Compliance*.

Também são responsabilidades do Diretor responsável pelo programa de PLD/FTP:

- Difundir a cultura de PLD/FTP entre os colaboradores e prestadores de serviços, inclusive por meio da adoção de programas periódicos de capacitação.
- Implementar e acompanhar o cumprimento da política, regras, procedimentos e controles de PLD/FTP, assim como de suas respectivas atualizações, de modo a assegurar o efetivo gerenciamento dos riscos relacionados.
- Coordenar ações disciplinares com colaboradores e prestadores de serviços que venham a descumprir os procedimentos de PLD/FTP.
- Coordenar a atuação da área responsável por PLD/FTP, conforme critério de cada instituição, com o comitê de PLD/FTP.
- Avaliar, ao menos anualmente, o programa de PLD/FTP, de modo a garantir sua eficiência e efetividade, assim como incorporar novos fatores de risco, quando aplicável.

4. Papéis e Responsabilidades

Na RBI Gestora, são definidos papéis e responsabilidades das áreas envolvidas no processo de PLD/FTP, conforme apresentado abaixo:

Comercial: Realizar análise prévia e periódica dos clientes e parceiros comerciais, identificando em primeira instancia, situações ou solicitações atípicas que possam configurar indícios de ilícitos e/ou lavagem de dinheiro, financiamento do terrorismo ou proliferação de armas de destruição em massa.

Compliance: Compõe as atividades da área de *Compliance*:

- Difundir a cultura de PLD/FTP para a RBI Gestora.
- Aplicar, manter e atualizar a política, regras, procedimentos e controles internos pertinentes a PLD/FTP.
- Monitorar o cumprimento e a eficácia do programa de PLD/FTP.
- Analisar as informações coletadas pelas demais áreas da RBI Gestora e monitorar as operações dos clientes, reportando-as, caso necessário, ao comitê de PLD/FTP, a Diretoria Colegiada e/ou as autoridades competentes, caso aplicável.
- Desenvolver e aprimorar ferramentas e sistemas de monitoramento de operações ou situações atípicas.
- Elaborar programas periódicos de treinamento, capacitação e conscientização dos colaboradores e prestadores de serviços, conforme aplicável.
- Interagir com os órgãos reguladores e autorreguladores sobre o tema de LD/FTP.

Jurídico: Realizar a revisão de documentos atendendo as exigências legais e regulatórias relacionado ao processo de PLD/FTP.

Operações: Realizar o controle de monitoramento das operações com objetivo de identificar situações atípicas relacionadas a liquidação de operações.

Recursos Humanos: Apoiar na disseminação de informação, no momento do embarque do funcionário e/ou contrapartes, enviando as políticas e procedimentos ao conhecimento de todos.

Riscos: Possui a função de monitorar os riscos operacionais e, em caso de suspeita de ilícito ou atividade não usual, comunicar a área de *Compliance* para diligência avançada.

Tecnologia da Informação: Fornecer e manter a disponibilidade de ambiente de sistema e infraestrutura tecnológica para que as análises de PLD/FTP sejam devidamente conduzidas.

5. Normas de conduta de PLD/FTP

5.1. Observações Preliminares

A RBI Gestora está sujeita às normas de conduta destinadas a impedir a lavagem de dinheiro e o financiamento do terrorismo, estabelecidas na Lei nº 9.613/1998 e alterações introduzidas pela Lei nº 12.683/2012 e pela Resolução CVM nº 50/21, emitida pela Comissão de Valores Mobiliários.

Os procedimentos e controles internos adotados pela RBI Gestora serão compatíveis com o porte e o volume de operações da instituição, com o objetivo de prevenir a sua utilização nos crimes previstos na Lei nº 9.613/98.

O Processo de "*Know Your Client*", instituído na política interna "Conheça seu cliente – KYC", é o conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de parceiros comerciais, visando prevenir a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas. Para aqueles que representarem maior risco, devem ser adotados procedimentos complementares e diligências aprofundadas de avaliação e alçadas específicas de aprovação, de acordo com a criticidade dos apontamentos ou exceções.

No Processo de "*Know Your Employee*", instituído na política interna "Conheça seu colaborador – KYE", se trata de um conjunto de regras e procedimentos que devem ser adotados para identificação e aceitação de estagiários, colaboradores, sócios, diretores, fornecedores e prestadores de serviços, prevenindo a contratação de pessoas e, ou, empresas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

As referidas políticas internas exigem que a RBI Gestora realize diversas tarefas de *Due Diligence* para obter uma visão geral de seus parceiros contratuais, o que possibilita avaliar os riscos de lavagem de dinheiro e financiamento do terrorismo decorrentes de relacionamentos com clientes e suas operações, a fim de definir e implementar medidas preventivas com base nos riscos.

A RBI Gestora conduz *Due Diligencies* de relacionamentos nas seguintes circunstâncias, por exemplo:

- Celebrar relações comerciais e, ocasionalmente, relações comerciais existentes (durante a atualização dos dados, em casos de dúvida ou suspeita, monitoramento).
- Em hipótese de circunstâncias que indiquem lavagem de dinheiro ou financiamento do terrorismo.
- Em hipótese de dúvidas com relação às informações sobre a identidade do parceiro contratual ou beneficiário final.

A RBI Gestora confirmará e atualizará o cadastro, identificando os beneficiários finais das operações, sempre que possível, e indicando se eles são ou não PEPs, além de mais informações necessárias. Periodicamente, serão realizados testes para confirmar a adequação das informações cadastrais.

A compatibilidade entre a movimentação de recursos, atividade econômica e capacidade financeira do relacionamento será monitorada por meio de sistema automatizado que fará uma varredura dos registros dos serviços financeiros prestados e operações realizadas contra parâmetros mínimos pré-estabelecidos que são capazes de deflagrar alertas para o caso de atividades suspeitas ou fora dos parâmetros estabelecidos.

As comunicações formais das ocorrências suspeitas serão realizadas até o dia útil seguinte àquele em que tiverem sido finalizadas as investigações e a decisão tomada pelo colegiado do Comitê de PLD/FTP e não será dada ciência aos clientes envolvidos.

Os clientes PEPs serão identificados por meio de listagens apropriadas e estarão sujeitos a um monitoramento reforçado, nos termos do item 7 abaixo, e contínuo. Tais listagens também identificam os parentes e as pessoas de relacionamento próximo, o que possibilita que todos os nomes sejam destacados para o monitoramento contínuo não só em relação as listas, mas também com relação à mídia negativa.

Os clientes na condição de Organizações Sem Fins Lucrativos (ONGs e outras organizações da sociedade civil) serão avaliados pela área de *Compliance*, que deverá considerar aspectos relacionados às fontes e natureza dos recursos do Cliente (doações pulverizadas ou não, campanhas junto a grupos sociais ou profissionais, provimento por benfeitor etc.), quais as atividades desenvolvidas (assistência e socorro a comunidades carentes, bolsas de estudo, patrocínio desportivo etc.) quanto a licitude e razoabilidade.

5.2. Abordagem Baseada em Risco

Para suportar a RBI Gestora na identificação, classificação, qualificação e monitoramento dos riscos relacionados a Lavagem de Dinheiro, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, foi criada a metodologia ABR – Abordagem baseada em risco (Anexo I), contendo a definição dos critérios para a classificação dos riscos de:

I. Clientes.
II. Fornecedores e prestadores de serviço.
III. Funcionários.
IV. Operações, transações, produtos, serviços, canais de distribuição e ambientes de negociação e registro.
V. Jurisdição.
VI. Cadeia de relacionamento.
VII. Instituição, incluindo o modelo de negócio e a área geográfica de atuação.

5.3. Avaliação Interna de Risco e Indicadores de Efetividade

Com objetivo de assegurar a aderência e eficácia das métricas e procedimentos estabelecidos na Política de PLD/FTP, a RBI Gestora, possui controles internos implementados para, no limite de suas atribuições,

identificar, analisar e mitigar os riscos de lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa inerentes às atividades desempenhadas no mercado de valores mobiliários.

O resultado da avaliação dos controles internos do ano civil é consolidado no Relatório da Avaliação Interna de Risco ("RAIR"), que deve ser emitido até o último dia útil do mês de março do ano subsequente e ser previamente encaminhado para a diretoria colegiada.

O RAIR detalha o resultado dos testes realizados durante o ano para cara um dos aspectos testados e, em caso de inconsistências ou erros operacionais, são definidos e alinhados junto a diretoria colegiada os planos de ação para endereçar os aspectos de melhoria. Esses planos corretivos devem ser consistentes ter data de implementação factível e, sendo o processo de implementação monitorado pela área de Controles Internos.

Para verificação da efetividade em relação ao nível de aderência a Política de PLD/FTP, a RBI Gestora possui indicadores de efetividade que são utilizados. Abaixo seguem apresentadas as métricas definidas e resultados esperados para indicador:

Ref.#	Métrica Definida	Resultado Esperado
1	Atualização da Política de PLD/FTP e documentos internos.	Atualização da Política de PLD/FTP e documentos relacionados dentro do prazo definido em cada documento.
2	Avaliação dos controles internos para atendimento as regulamentações vigentes.	100% dos riscos regulatórios endereçados pelos controles internos implementados.
3	Avaliação/diligência de contrapartes (KYC, KYP, KYE).	. 100% realizado no momento da contratação, aceitação de cliente ou contratação de funcionário. . Mínimo de 80% das atualizações de diligências realizadas no prazo, conforme risco atribuído na última avaliação/atualização.
4	Avaliação das operações e situações atípicas.	100% dos alertas avaliados no prazo máximo de 45 dias.
5	Comunicação de situações atípicas com indícios de ilícitos ou irregularidades.	100% das comunicações realizadas no prazo máximo de 24 horas.
6	Implementação de planos de ação definidos para os apontamentos realizados de criticidade baixa e média.	Redução de, no mínimo, 40% dos apontamentos realizados, quando não houver replanejamento.

7	Implementação de planos de ação definidos para os apontamentos realizados de criticidade alta.	Redução de, no mínimo, 70% dos apontamentos realizados, quando não houver replanejamento.

6. Due Diligence

A RBI Gestora deve realizar as tarefas de *Due Diligence* nos parceiros comerciais, que compreende as seguintes tarefas:

- Identificação.
- Obtenção de informações sobre a finalidade e natureza da relação comercial.
- Identificação do beneficiário final e verificação baseada em risco.
- Esclarecimento das estruturas de controle e propriedade.
- Monitoramento contínuo da relação comercial e atualização de dados.
- Esclarecimento da origem de fundos e ativos.
- Obrigação de rescindir/negar o ingresso em uma relação/operação comercial, no caso de descumprimento contínuo das exigências de *Due Diligence* de Cliente.
- Registro e armazenamento de todas as informações.

A RBI Gestora deve receber a documentação necessária completa para abrir e manter a conta antes do início da relação comercial. Tal documentação necessariamente deverá permitir a identificação do beneficiário final.

Potenciais Clientes são pesquisados em notícias negativas, avaliados em listas de sanções e restritivas nacionais ou internacionais, e classificados como PEP ou não.

Além da avaliação de risco reputacional, os Clientes e suas respectivas atividades comerciais são analisados para fins da Resolução CMN nº 4.945/2021, publicada pelo Banco Central do Brasil, atendendo à exigência de análise, quando cabível, de possíveis impactos socioambientais causados pelo relacionamento comercial em potencial.

Caso seja necessário um limite superior ao estipulado acima ou fora do escopo definido neste documento e no documento de “Regras de Operações Alavancadas”, deverá ser realizada a solicitação da aprovação do Diretor Comercial.

Para investidores institucionais, qualquer operação que exceda o limite operacional estabelecido deverá ter a aprovação prévia do Diretor Comercial.

6.1. Beneficiários Finais

A RBI Gestora deve perguntar se o parceiro contratual atua em nome de um beneficiário final e deve diligenciar, com base nos melhores esforços, para identificar o indivíduo final por trás de qualquer entidade legal, parceria ou outra estrutura. Caso se mostre impraticável, impossível ou comercialmente inatingível, a RBI Gestora deverá submeter a situação à avaliação do Diretor responsável por PLD/FTP, quanto a iniciar ou manter relacionamento comercial com tal cliente ou parceiro. Caso seja autorizado, deve-se adotar monitoramento reforçado e análise mais criteriosa ao considerar eventual comunicação ao COAF.

6.2. Monitoramento contínuo da relação comercial e atualização dos dados

A RBI Gestora deve monitorar a relação comercial, inclusive as operações realizadas durante a relação, continuamente, visando identificar quaisquer discrepâncias entre as informações disponíveis sobre o Cliente, o beneficiário final, quando aplicável, sua atividade de negócio e o perfil do Cliente e, caso necessário, as informações disponíveis sobre a fonte dos ativos/recursos.

Esse procedimento geralmente é feito como parte do processo de monitoramento. O gerente de relacionamento também deve monitorar a conduta comercial dos clientes.

6.3. Atualização de documentos, dados e informações do cliente, renovações com base em risco, incluindo categoria de risco

Como parte do monitoramento contínuo da relação comercial, a RBI Gestora deve garantir que os documentos, dados e informações disponíveis a respeito da relação comercial sejam atualizados anualmente.

Além da atualização anual predefinida, todo evento que resultar na modificação de dados de Clientes (como alterações nos principais dados ou em informações relevantes dos Clientes, ajustes/alterações dos parâmetros de risco e listas de riscos, informações negativas importantes) deve ser utilizado para atualizar os dados do Cliente, bem como a categoria de risco (se adequado).

As revisões e renovações cadastrais serão revisadas periodicamente, no que diz respeito à integração, dependendo da classificação de risco do Cliente, de acordo com uma abordagem baseada no risco, usando metodologia apropriadas para o propósito, conforme “Metodologia ABR”. Por exemplo, os Clientes classificados como de alto risco serão revisados anualmente cada 12 meses, risco moderado a cada 36 meses e risco baixo a cada 60 meses. Esses períodos serão executados a partir da data de conclusão do processo de aceitação do Cliente no sistema interno da empresa.

Será feito reporte para o COAF, sempre que os valores, métodos e instrumento usados, ou a ausência de uma base econômica ou legal para as operações, indicarem a possível ocorrência de crimes previstos na Lei nº 9.613/1998, além de outros casos estabelecidos nas leis aplicáveis.

Uma vez detectada eventual ocorrência, caberá ao *Compliance* analisar o cadastro, as operações e transações do cliente, bem como solicitar diversas providências tais como – a atualização cadastral e o pedido de esclarecimento ao assessor do relacionamento. Somente após decorrido todos os prazos para regularização de eventual situação em não conformidade ou se, após todas as análises, o indício de ocorrência de crimes de PLD se confirmar, ou se situações de atenção eventualmente verificadas, quando houver informação completa que possibilite tal avaliação, deverá ser reportado o relatório sobre o caso aos membros do Comitê de PLD, que deliberará pela comunicação ou não ao COAF e/ou aos órgãos reguladores e autorreguladores do mercado de capitais.

Em caso de deliberação positiva, a área de *Compliance* será responsável por proceder a comunicação ao COAF a respeito de operações suspeitas até o dia útil seguinte à deliberação do Comitê de PLD/FTP. Já o prazo de análise e tomada da decisão em até 45 dias. Todos os dossiês com a análise dos respectivos casos suspeitos, independentemente de terem, ou não, sido comunicados ao COAF, deverão ser mantidos arquivados à disposição das autoridades, por até cinco anos.

Não se limitam, mas são hipóteses possíveis de comunicação ao COAF até o dia seguinte da ocorrência:

1. Operações com utilização de recursos em espécie de valor individual superior a R$ 2.000,00 (dois mil reais) com a respectiva identificação do portador dos recursos.
2. Solicitação ou operação, envolvendo recebimento em espécie ou transferência de fundos contra pagamento em espécie, de valor igual ou superior a R$ 50.000,00 (cinquenta mil reais) ou o equivalente em moeda estrangeira deverão ser reportadas e autorizadas previamente pelo Diretor de PLD/FTP.
3. Operações com utilização de recursos em espécie cujo valor individual seja igual ou superior a R$ 50.000,00 (cinquenta mil reais).
4. Operações de valores próximos dos limites determinados pelo marco regulatório com características de fracionamento para burlar as disposições normativas.

Na hipótese de não ocorrência de comunicações ao COAF, durante o exercício social compreendido entre o dia 01 de janeiro à 31 de dezembro do ano anterior, a RBI Gestora deverá encaminhar ao COAF, a declaração de não ocorrência de transações passíveis de comunicação (“Declaração de Não Ocorrência”), pela área de *Compliance*, por meio do Sistema de Controle de Atividades Financeiras (“SisCoaf”), em até o dia 31 de janeiro do ano civil subsequente, para o segmento CVM.

6.4. Efetividade do dossiê de validação de dados de clientes

A RBI Gestora realiza, semestralmente, testes em seu sistema responsável pela geração dos dossiês dos clientes, com o objetivo de garantir a integridade, consistência e conformidade dos dados cadastrados

obtidos por meio dos *bureaus* consultados pelo sistema. Esses testes são essenciais para assegurar que as operações realizadas e as informações geradas pelo sistema estejam em linha com as exigências regulatórias e os critérios internos de KYC.

O processo de teste do sistema de geração de dossiês abrange as seguintes etapas:

- **Validação da coleta e tratamento de dados cadastrais:** Verificação da precisão e conformidade das informações obtidas pelo dossiê com os dados presentes no documento de identidade fornecido pelo cliente. Esse teste assegura que as informações capturadas e processadas pelo sistema correspondem fielmente aos dados fornecidos, garantindo a confiança de que o sistema está gerando dossiês com informações corretas e confiáveis.
- **Verificação da conformidade com os critérios de identificação de PEPs:** O sistema é testado para garantir que realiza a identificação adequada de PEPs.
- **Análise de mídia negativa:** O sistema é testado para garantir que realiza a varredura adequada de fontes de mídia negativa, identificando possíveis notícias ou informações públicas que possam comprometer a reputação do cliente. Essa análise visa detectar potenciais riscos à imagem e integridade do cliente, permitindo uma avaliação mais criteriosa antes da aprovação ou manutenção da relação comercial.

Os testes são realizados pelo Departamento de Controles Internos, que analisa eventuais falhas ou inconsistências identificadas e adota as medidas corretivas necessárias. Esses testes garantem que o sistema esteja operando de forma eficiente e em total conformidade com os padrões internos e regulatórios, assegurando que as informações geradas possam ser usadas de forma confiável no processo de aceitação ou manutenção de clientes.

6.5. Cálculo dos limites externos às relações comerciais existentes

6.5.1. Smurfing (divisão de operações)

O "*Smurfing*", ou seja, a divisão artificial de operações realizadas com objetivo de burlar as exigências de identificação, é proibida. Caso seja detectado um *smurfing* ou uma tentativa de *smurfing*, uma denúncia de atividade suspeita deve ser apresentada a área de *Compliance*. As exigências de *Due Diligence* também são aplicáveis fora das relações comerciais existentes, caso a RBI Gestora realize várias operações que atinjam ou excedam o respectivo limite, e caso seja visível que cada operação, individualmente, está conectada com as outras. Nesse caso, deve-se pressupor que uma única operação financeira foi dividida artificialmente, caracterizando o *smurfing*.

Normalmente pressupõe-se a divisão artificial (*smurfing*) caso certa quantidade de operações em um período definido seja visível devido à sua similaridade em termos de conclusão, objetivo ou liquidação da operação. Portanto, deve-se pressupor que, de fato, é apenas uma (única) operação.

Em geral, o risco de uma única operação financeira ser dividida artificialmente para burlar as exigências de identificação, utilizadas, portanto, para fins de lavagem de dinheiro ou financiamento do terrorismo, é reduzido conforme os intervalos entre as operações individuais aumentam.

7. Pessoa Politicamente Exposta

Uma pessoa politicamente exposta ("PEP") é uma pessoa física nacional ou estrangeira que ocupa ou ocupou um "cargo público importante", um "familiar direto" dessa pessoa ou é um "colaborador conhecido" dessa pessoa (definição global).

A RBI Gestora deve aplicar processos adequados com base em risco que possibilitem a identificação se um parceiro contratual e o beneficiário final são pessoas politicamente expostas.

Em geral, devido a seu escopo considerável para exercer influência e fazer contatos comerciais, as PEPs também devem ser consideradas mais vulneráveis para tirar proveito de atividades ilegais. Portanto, elas representam aumento do potencial de risco e maior risco de reputação para a RBI Gestora.

7.1. Cargo público importante

A RBI Gestora deve dedicar especial atenção às operações ou propostas de operações envolvendo pessoa exposta politicamente, bem como com seus familiares, estreitos Colaboradores e ou pessoas jurídicas de que participem.

Com o monitoramento de PEPs, conforme recomendado pelas autoridades reguladoras, sempre que existirem operações financeiras atípicas com indicação de lavagem de dinheiro, as instituições deverão reportar o fato ao COAF, que tomará as medidas cabíveis.

A RBI Gestora realizará um monitoramento mais rigoroso de Clientes PEPs, seus familiares e relacionamento próximo, identificados como tais nas listas. Os Clientes PEP são, por definição, Clientes de alto risco. Portanto, é imprescindível identificá-los, já no início do relacionamento, na Ficha Cadastral, na qual os próprios Clientes atestam sua classificação como PEPs. Assim, de acordo com a Resolução CVM 50/21, a RBI Gestora coletará as informações que permitam classificar o Cliente como PEP e identificar a origem dos recursos envolvidos nas operações realizadas por Clientes permanentes.

Periodicamente, a RBI Gestora compara a lista de PEPs com sua base de Clientes, uma vez que a situação do Cliente pode mudar: ele/ela pode se tornar, ou deixar de ser, uma PEP.

A definição de PEP e os representantes do governo elegíveis para essa finalidade estão descritos na Resolução CVM 50/21 e alterações posteriores, incluindo a Resolução Coaf nº 40, de 22 de novembro de 2021. Os representantes do Governo que ocupem, ou tenham ocupado, cargos, colocações ou funções públicas importantes no Brasil ou em outros países, territórios e dependências, nos últimos cinco anos, bem como seus representantes, parentes e outras pessoas com quem mantenham um relacionamento próximo, são considerados PEPs.

O período de cinco anos deve ser considerado retroativamente, a partir da data de início do relacionamento comercial, ou da data na qual o Cliente passou a ser uma PEP.

Além dos detentores desses cargos, seus familiares ou pessoas com quem eles mantenham um relacionamento próximo também são PEPs.

Os exemplos de situações que caracterizam relacionamentos próximos e resultam na classificação de Clientes permanentes como PEPs incluem:

- A contratação de uma PEP como procuradora ou representante.
- Controle direto ou indireto da PEP, no caso de sociedades.
- Transferência periódica de recursos financeiros para/de uma PEP que é Cliente da instituição, não justificada por eventos econômicos, tais como a compra de bens ou a prestação de serviços.

7.2. Familiares Diretos

São considerados familiares os parentes, na linha direta, até o segundo grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada.

7.3. Beneficiários final na condição de PEP

Também deve ser verificado se o status de PEP aplica-se aos beneficiários finais.

O status da PEP é documentado no arquivo do Cliente e as medidas com base em risco são aplicadas à relação comercial.

8. Comitês e Fóruns da RBI Gestora

8.1. Comitê de PLD/FTP

O Comitê de PLD/FTP é o órgão colegiado, formado por diretores, não estatutário, que ocorre de forma extraordinária, e tem como objetivo de deliberar sobre a aprovação para criação ou extinção de relacionamento com clientes ou parceiros, comunicação de indícios de ilícitos ao COAF, tratativas ou procedimentos necessários para conformidade com demandas regulatórias, avaliação de transações suspeitas e analisar as métricas do período levantadas pela área de Prevenção à Lavagem de Dinheiro.

8.2. Fórum de Riscos e Novos Produtos

O gerenciamento de riscos da RBI Gestora compreende o conjunto de políticas, estratégias, processos e procedimentos destinados a manutenção da exposição ao risco nos níveis estabelecidos de acordo com o apetite a risco da RBI (definido no documento *Risk Appetite Statement RAS*).

O Fórum de Risco de Novos Produtos tem como objetivo deliberar e aprovar, em primeira instância, a política de Avaliação de Riscos de Novos Produtos, baseando-se em seu conteúdo para efetuar a avaliação de novos produtos disponibilizados pela RBI. Fazem parte do Fórum de Risco de Novos Produtos, de forma obrigatória e quando existir a posição, o Gestor da Área de Riscos, o Gestor da Área de Produtos e o Diretor da Área de Riscos (CRO).

Todos os fóruns deverão ocorrer com uma periodicidade mínima de um ano e deverão possuir atas de deliberações.

9. Treinamento

A área de *Compliance* anualmente proporciona aos funcionários da RBI Gestora, incluídos, mas não limitados aos funcionários, sócios, agentes autônomos, parceiros / funcionário terceirizados, treinamentos e palestras, com periodicidade anual, que abordam o tema de Lavagem de Dinheiro e Financiamento do Terrorismo e a Proliferação de Armas de Destruição em Massa.

10. Características Especiais de Certos Tipos de Operação e Segmento de Cliente

10.1. Definição de "Terrorismo"

A Lei nº 13.260, de 2016 define, de forma inequívoca, por meio de seu artigo 2º, que o terrorismo consiste na prática por um ou mais indivíduos, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública, dos seguintes atos:

i. Usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa.

ii. Sabotar o funcionamento ou apoderar-se, com violência, grave ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento.

iii. Atentar contra a vida ou a integridade física de pessoa.

Para os atos supramencionados, é definida pena de reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.

Já no artigo 6º, é definido o seu financiamento, que consiste em "*receber, prover, oferecer, obter, guardar, manter em depósito, solicitar, investir, de qualquer modo, direta ou indiretamente, recursos, ativos, bens, direitos, valores ou serviços de qualquer natureza, para o planejamento, a preparação ou a execução dos crimes previstos nesta Lei"*, estabelecendo também pena de reclusão, de quinze a trinta anos.

Também é prevista a incorrência da mesma pena para quem *"oferecer ou receber, obtiver, guardar, mantiver em depósito, solicitar, investir ou de qualquer modo contribuir para a obtenção de ativo, bem ou recurso financeiro, com a finalidade de financiar, total ou parcialmente, pessoa, grupo de pessoas, associação, entidade, organização criminosa que tenha como atividade principal ou secundária, mesmo em caráter eventual, a prática dos crimes previstos nesta Lei."*.

10.2. Combate ao financiamento do terrorismo

A RBI Gestora também não deve permitir que ela seja indevidamente utilizada para financiamento do terrorismo. As relações comerciais com organizações e indivíduos que buscam ou apoiam objetivos terroristas ou extremistas representam um risco reputacional significativo para a RBI Gestora.

Combater o financiamento do terrorismo se estende a todas as formas de atividade terrorista e extremista. Expressamente, não há, tampouco é desejado, foco em religiões, nacionalidades, regiões ou classes da população específicas. Assim, a RBI Gestora monitora continuamente todas as operações e situações, no limite de suas atribuições, inclusive potenciais suspeitas de envolvimento com atos terroristas, tais como:

a. Ativos alcançados por sanções impostas pelas resoluções do CSNU de que se venha a ter conhecimento e de que trata a Lei nº 13.810, de 8 de março de 2019.
b. Ativos alcançados por requerimento de medida de indisponibilidade oriundo de autoridade central estrangeira de que se venha a ter conhecimento.
c. A realização de negócios, qualquer que seja o valor, por pessoas que tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento, conforme o disposto na Lei nº 13.260, 16 de março de 2016.
d. Valores mobiliários pertencentes ou controlados, direta ou indiretamente, por pessoas que tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento, de que se venha a ter conhecimento, conforme o disposto na Lei nº 13.260, de 2016.
e. Movimentação passível de ser associada ao financiamento do terrorismo, conforme o disposto na Lei nº 13.260, de 2016.

Cabe acrescentar que a RBI Gestora também monitora, direta e permanentemente, as determinações de indisponibilidade emanadas da CSNU, via listas disponibilizadas por terceiros, consagradas para tal utilização no mercado financeiro, bem como eventuais informações a serem observadas para o seu adequado atendimento, inclusive o eventual levantamento total ou parcial de tais determinações em relação a pessoas, entidades ou ativos, visando ao cumprimento imediato do quanto determinado, acompanhando para tanto, sem prejuízo da adoção de outras providências de monitoramento, as informações divulgadas na página do CSNU na rede mundial de computadores.

10.3. Combate à Sonegação Fiscal

Na prática, um risco específico é o auxílio e a cumplicidade em fraudes por funcionários da RBI Gestora. O auxílio e a cumplicidade referem-se à assistência deliberadamente fornecida ao fraudador em um ato ilegal. Isso pode incluir as seguintes ações hipotéticas:

- Informações fornecidas por funcionários da RBI Gestora sobre investimentos sem risco de descoberta.
- Não divulgação de relações fiduciárias.
- Fornecimento de informações incorretas às autoridades fiscais.

Orientação

O risco de abuso da RBI Gestora para fins de sonegação fiscal por meio de seus serviços e produtos precisa ser minimizado no longo prazo por meio das seguintes medidas (algumas das quais são conhecidas e foram implementadas no contexto de combate à lavagem de dinheiro):

- Aplicação rigorosa do princípio Conheça seu Cliente (KYC) principalmente determinando o beneficiário final.
- Avaliação e verificação do envolvimento do potencial cliente com temas/aspectos restritos, principalmente relacionados a atividades ilícitas/ilegais e presença em listas restritivas internacionais para fins de Prevenção e Combate à Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.
- Perguntas detalhadas e documentação da origem de ativos.
- Perguntas sobre o objetivo e a finalidade do investimento.
- A RBI Gestora não fornece consultoria individual sobre questões fiscais, e os Clientes devem ser encaminhados a consultores tributários externos.
- Notificação padrão a ser assinada pelos Clientes informando que a receita de investimentos deve ser declarada às autoridades fiscais.
- Aplicação de contratos modelo para evitar que a sonegação fiscal seja realizada por meio de contratos individuais.

11. KYC Fiscal

"KYC Fiscal" refere-se à coleta, registro e atualização de dados pessoais e fiscais, obtenção da documentação correspondente e classificação adequada dos Clientes.

Portanto, a abordagem geral de "conheça o seu Cliente" usada para analisar e documentar os atributos específicos do Cliente de forma abrangente é complementada com aspectos relacionados a impostos. O objetivo é obter uma visão completa do domicílio fiscal do Cliente, de forma que tal domicílio possa ser adequadamente informado e benefícios fiscais potenciais possam ser usados, quando aplicável, no âmbito da retenção de impostos dos EUA.

Para esse fim, os dados relacionados a impostos são coletados em todas as contas de Clientes relevantes de maneira estruturada. Com base nisso, as entidades responsáveis identificam os países relevantes do domicílio fiscal para cada Cliente e coletam os respectivos IDs fiscais, assegurando o recebimento da documentação de suporte necessária para os dados coletados.

12. FATCA

Em 23 de Setembro de 2014, o Brasil e os EUA assinaram um Modelo 1ª IGA, o qual, juntamente com o Acordo de Troca de Informações Fiscais, permite a troca recíproca e automática de informações. Isso significa que o CBBM tem de se reportar à Receita Federal do Brasil (RFB).

O documento de requisitos fiscais funcionais do Brasil descreve os requisitos regulatórios específicos do país com base no Acordo Intergovernamental do FATCA entre o Brasil e os EUA e na regulamentação nacional para sua adoção.

13. Relações Comerciais Proibidas

13.1. Bancos de Fachada

Um banco de fachada é uma instituição estabelecida em um país em que não está fisicamente presente e que não pertence a um grupo financeiro regulamentado. Portanto, não é permitido que os bancos celebrem ou continuem relações comerciais correspondentes ou outras relações com esses bancos de fachada. Essa proibição também se aplica a relações comerciais com bancos conhecidos por permitir que suas contas sejam utilizadas por um banco de fachada.

13.2. Contas *Payable-through* (de repasse) / *Payable-through accounts*

As "contas *payable-through*" podem ser utilizadas por um Cliente como se fossem dele. Assim, os pagamentos ao Cliente ou a pedido do Cliente não podem ser alocados corretamente pelos envolvidos na cadeia de pagamento e, portanto, continuam anônimos. A gestão dessas contas é contrária ao princípio de verificação da identidade do Cliente nos termos da lei tributária e é proibida por lei.

13.3. Outras Relações Comerciais e Operações Proibidas / *Other Banned Commercial Relationships and Transactions*

As seguintes operações, em especial, não são permitidas com base em exigências legais e valores éticos:

- Não abrir nem manter contas para operadores de moedas virtuais. O risco de uma moeda virtual ser utilizada para fins de lavagem de dinheiro ainda é influenciado pelo fato de que há vários canais de distribuição (não regulamentados), bem como um nível elevado de descentralização.
- Anonimato e uso de pseudônimo na internet. Devido à sua natureza virtual a moeda pode ser fácil e rapidamente transferida para qualquer lugar do mundo, sem ficar imediatamente evidente quem realiza a operação ou recebe os fundos.
- Deve-se considerar também que a transparência extremamente limitada raramente possibilita que conclusões sejam tiradas com relação ao uso da moeda virtual (por exemplo, para financiar operações ilegais) e sua rastreabilidade para fins de tributação (por exemplo, sonegação fiscal por ocultação de estruturas de propriedade).
- Operações ligadas a moedas virtuais não são processadas pela RBI Gestora.
- As contas devem ser estabelecidas com o nome verdadeiro do Cliente. Contas especificadas com números, apelidos ou pseudônimos não são permitidas.
- Comércio ilegal de armas ou operações que apoiem e sustentem o comércio ilegal de armas, inclusive armas atômicas, biológicas e químicas.
- Transferências financeiras (principalmente operações não transparentes envolvendo grandes volumes/lotes, entre outras coisas, com relação a casas de câmbio/prestadores de serviços financeiros.
- “Operações estruturadas” / “operações evasivas”. Uma operação é considerada evasiva caso seja deliberadamente diferente dos processos ou estruturas típicas ou planejadas visando evitar a implementação dos regulamentos jurídicos ou condições regulatórias que do contrário seriam aplicados. Essas operações são destinadas, por exemplo, a burlar controles cambiais localmente aplicáveis, exigências de divulgação com relação às moedas ou limites individuais, por exemplo. O país para o qual pagamentos devem ser transferidos ou os produtos entregues, ou o beneficiário final/beneficiário real de uma operação, é comumente ocultado. Além disso, o fato de que normas de sanção ou (outras) normas locais são aplicáveis a essa operação, ou que as partes envolvidas na operação estão sujeitas à jurisdição do país no qual foram emitidas normas, normalmente também é ocultado.

Os exemplos possíveis de desvio incluem:

- Fornecimento deliberado de informações incorretas em documentos para uma finalidade ou uso final para desviar a atenção da pessoa responsável pela supervisão ou monitoramento.

- Uso consciente de empresas de fachada, intermediários ou transbordos para disfarçar o fato de que o destinatário dos produtos ou dinheiro está sujeito a sanções ou localizado em um país sujeito a sanções.

Deve ser dada atenção especial caso uma operação seja estruturada de forma aparentemente incomum, não possua uma finalidade comercial claramente reconhecível, ou seja, preparada de forma contrária à estrutura originalmente pretendida. Esses casos poderão indicar sonegação.

Não há necessidade de monitorar as leis locais que sejam aplicáveis apenas ao Cliente. Contudo, caso o gerente de relacionamento ou o *Compliance* estejam cientes das restrições locais relevantes e haja suspeita de sonegação, a questão deve ser analisada, avaliada e uma medida adicional deve ser determinada.

Empresas de fachada são definidas, entre outras, como:

- Empresas não operacionais (sem produção, comercialização ou serviços).
- Empresas sem funcionários.
- Empresas sem instalações próprias.
- Empresas cujo escritório está localizado em um agente, escritório de advocacia, auditor certificado, ou em outra empresa.
- Código Postal de um agente, escritório de advocacia, auditor certificado ou coletores de correspondência.
- Provedores de apostas deverão apresentar a licença das autoridades reguladoras do país no qual os negócios de apostas são operados. Esta é uma condição prévia para abrir e manter uma conta. Caso a conta seja aberta em um país que não aquele em que os negócios de apostas são operados, as atividades de apostas devem ser autorizadas nesse país.

Devido ao risco inerente, as relações comerciais com o setor de provedores de apostas *on-line* são vedadas, mesmo se eles detiverem uma licença.

- Compra/venda de cheques de viagens em troca de dinheiro.
- *Blind trusts*, cujo objetivo é ocultar a identidade do beneficiário final.

13.4. Obrigação de Manutenção de Registros

As informações obtidas para atender às exigências de due Diligence no processo de identificação e as informações coletadas sobre parceiros contratuais, beneficiários finais, relações operações de negócio e operações devem ser registradas, com o propósito do relacionamento comercial, e as informações resultantes do monitoramento contínuo do relacionamento, se necessário.

Período de manutenção é de no mínimo 5 (cinco) anos conforme Resolução CVM 50/21.

13.5. Obrigação de Encerrar Relação Comercial

Em princípio, um relacionamento deve ser rescindido, descontinuado ou não iniciado, se os requisitos de due Diligence não puderem ser cumpridos ou se o parceiro sistematicamente (de forma ampla) e contínua (não apenas por um curto período ou quando a situação puder ser solucionada rapidamente) não providencia as informações necessárias para a diligência.

14. Relação Comercial

Um relacionamento é qualquer relacionamento comercial ou profissional que envolva diretamente as atividades comerciais ou profissionais da empresa, que, quando estabelecida, deverá durar por um período especificado.

Um relacionamento comercial pode ser estabelecido:

- Com um Cliente, para a oferta de serviços financeiros bancários e outros (“relacionamento comercial com Clientes”).
- Com um fornecedor ou prestador de serviços ("relacionamento com fornecedores").
- Com o objetivo de investir os ativos (“relacionamento de investimento”).

As exigências de due Diligence devem ser atendidas não apenas quando uma relação é estabelecida, mas também ao prorrogar relações existentes (por exemplo, usando novos produtos ou serviços).

15. Casos Suspeitos

15.1. Definição de “Casos Suspeitos”

Em geral, “casos suspeitos” envolvem circunstâncias que indicam que uma operação está sendo ou deve ser usada para fins de lavagem de dinheiro ou financiamento do terrorismo. O termo “circunstâncias” refere-se, no mais amplo sentido, a quaisquer irregularidades que surjam no processamento de operações ou desvios da conduta comercial comum do Cliente; isso também inclui a não divulgação do beneficiário final diferenciado.

Um comunicado de alerta de funcionário deve ser apresentado ao *Compliance* nos casos a seguir:

- Caso haja circunstâncias que indiquem que uma operação envolvendo ou não dinheiro está sendo, seria ou foi utilizada para lavagem de dinheiro ou financiamento do terrorismo. Quaisquer tentativas feitas por um (não) Cliente também devem ser denunciadas. Um comunicado de alerta de funcionário também deve ser preparado caso surja uma suspeita de lavagem de dinheiro ou financiamento do terrorismo posteriormente. As circunstâncias que indicam a suspeita devem ser apresentadas.

- Caso haja tentativa de realização de uma operação suspeita ou início de uma relação comercial suspeita. Isso abrange, em especial, o cenário em que um possível Cliente solicita que a RBI Gestora realize uma operação ou inicie uma relação comercial com ele e, então, sem motivo reconhecível ou plausível e, acima de tudo, dentro da estrutura de atendimento das exigências de due Diligence, desista da operação ou relação. A exigência de emissão de um comunicado de alerta de funcionário também se aplica a estes casos se houver circunstâncias que indiquem que os ativos relacionados à operação ou relação comercial proposta são objeto de um crime, de acordo com as disposições aplicáveis do direito criminal ou que os ativos estão vinculados ao financiamento de terrorismo.
- Caso haja circunstâncias que indiquem que o parceiro contratual não cumpriu sua obrigação de divulgação com relação à identidade de um beneficiário final diferenciado (ou seja, caso o parceiro contratual não esclareça a RBI Gestora que atua em nome de um terceiro).
- Caso haja quaisquer circunstâncias que pareçam suspeitas ou incomuns com relação a lavagem de dinheiro ou financiamento do terrorismo.
- Caso haja conhecimento de que o Cliente, parceiro contratual, beneficiário final, representante autorizado e/ou representante legal planeja denunciar voluntariamente sonegação fiscal. Esta disposição também se aplica mesmo em caso de conhecimento de uma denúncia voluntária bem-sucedida. Boatos são suficientes para justificar os motivos razoáveis relevantes de suspeita.

15.2. Indícios de um caso suspeito

A existência de circunstâncias que poderão indicar suspeita de lavagem de dinheiro ou financiamento do terrorismo pode, por exemplo, ter como base:

- Irregularidades na pessoa e/ou em sua conduta.
- Um terceiro (representante autorizado, acompanhante etc.).
- Explicações com relação à operação solicitada.
- A maneira como a operação é processada.
- O tipo e valor da operação, a fonte dos ativos ou as informações sobre destinatário de uma operação.
- O fato de que o histórico ou a finalidade econômica não podem ser estabelecidas.

Não é permitido informar às pessoas envolvidas na transação que a transação proposta pode estar sujeita a um preenchimento de SAR (relatório de atividades suspeitas) nem sobre as consequências de uma investigação preliminar.

16. Funções e Responsabilidades no Programa PLD/FTP

A RBI Gestora deve implementar e aplicar diretrizes e medidas para limitar e evitar riscos de *compliance*. Para seguir essa obrigação no que diz respeito à prevenção de lavagem de dinheiro a RBI Gestora desenvolveu e implementou um programa de PLD/FTP específico. Os riscos são monitorados e geridos pela gestão de *compliance* em três níveis (“três linhas de defesa”). As áreas de negócios têm a responsabilidade

básica de identificar e gerenciar riscos e de cumprir as regulamentações que regem suas operações comerciais. Isto é conseguido por meio de mecanismos de controle baseados no processo. O departamento de *Compliance* é responsável pela implementação das diretrizes legais e pelo monitoramento e gerenciamento dos riscos de conformidade.

Localmente as atividades de identificação, prevenção e monitoramento de operações suspeitas são realizadas pelo Local *Compliance* Officer que se vale de sistema automatizado de varredura de listas restritivas (ONU, GAFI, OFAC, EU e/ou Paraíso Fiscal) e também é capaz de gerar alertas de desvios de padrões de comportamento pré-estabelecidos.

A área de Controles internos realiza testes anuais de verificação das informações cadastrais, nos termos da Resolução CVM 50/21.

17. Penalidades e Sanções

O eventual descumprimento das determinações informadas neste documento, está sujeito a sanções que vão desde penalidades administrativas, criminais e até multas de grande vulto, além de medidas disciplinares tomadas pela RBI Gestora, variando conforme apuração dos indícios na investigação do fato constatado, que pode apresentar atos deliberados, negligência ou falha voluntária ou involuntária.

Além disso, o descumprimento das normas prejudica a reputação e o posicionamento de mercado da RBI Gestora. Dessa forma, todos os membros da RBI devem assegurar a conformidade com as normas aplicáveis, apresentadas na seção “1. Abrangência e Aplicabilidade”.

18. Vigência

Esta Política entra em vigor na data de sua publicação e será revisada anualmente ou sempre que houver alguma alteração na diretriz por ela estabelecida ou alterações nos requerimentos regulatórios ou de autorregulação que regem o tema.

19. Registro de alterações

Versão	Item	Descrição resumida da Alteração	Motivo	Data
01	-	Criação da Política de PLD/FTP	Criação	05/12/2024
02	-	Revisão anual	Revisão anual	01/12/2025

20. Aprovadores

Alçada Responsável	Nome	Assinatura
Diretor	Glauber da Cunha Santos	As aprovações foram realizadas através de Ata

Diretora	Marília Pimentel Garcia	As aprovações foram realizadas através de Ata
Diretor	Rafael Sabadell Carvalho	As aprovações foram realizadas através de Ata

21. Dúvidas

Área	Contato
Compliance/Controles Internos	Marília Pimentel Garcia
Compliance	Luis Paiva
Controles Internos	Renan Ribeiro