MRB INTERMEDIAÇÃO E NEGÓCIOS DIGITAIS	**Política de Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/CFT)**	Código:	POL-RC-001
		Nº Versão:	1.0

Categoria:	Riscos e Compliance	
Classificação:	Última publicação:	Próxima revisão:
Pública	02/04/2024	30/03/2025

SUMARIO

1. TERMOS E DEFINIÇÕES

- **Alta Administração** – Sócios e executivos de alto escalão responsáveis por definir estratégias, tomar decisões cruciais e direcionar o rumo geral da organização.
- **Avaliação Interna de Riscos (AIR)** – Nos termos da Circular BCB nº 3.978/2020.
- **Background check** – Processo de verificação de informações básicas e antecedentes de uma pessoa ou entidade, geralmente focado em histórico criminal, emprego e educação, visando confirmar a veracidade das informações fornecidas. Mais simplificado e superficial que o *due diligence*, mais voltado a verificar veracidade de informações prestadas previamente.
- **BACEN ou BCB** – Banco Central do Brasil.
- **Colaboradores** – Indivíduos que trabalham para a organização, incluindo funcionários em tempo integral, meio período, temporários, contratados, terceirizados e freelancers, inclusive estagiários e jovens aprendizes.
- **Comissão de Valores Mobiliários (CVM)** – Órgão regulador do mercado de capitais no Brasil, responsável por regulamentar e fiscalizar empresas e profissionais atuantes nesse mercado, visando proteger investidores e garantir a integridade do mercado.
- **Conselho de Controle de Atividades Financeira (COAF) –** Unidade de inteligência financeira brasileira, criada pela Lei 9.613/98, responsável por combater crimes de lavagem de dinheiro, determinando políticas e diretrizes para prevenir atividades ilícitas no sistema financeiro.
- **Diretoria da Instituição** – Sócia-Administradora ou Diretor designado para representar a Alta Administração.
- **Due diligence** – Investigação abrangente e detalhada de todos os aspectos relevantes de uma pessoa, empresa ou negócio, envolvendo análise financeira, legal, regulatória e operacional, com o objetivo de identificar riscos, oportunidades e questões críticas antes de tomar decisões estratégicas ou financeiras.
- **Fraude** – Quaisquer atos ilegais ou ilegítimos caracterizados por engano malicioso, dissimulação ou violação da verdade, independentemente da aplicação de ameaça, de violência ou de força física. São perpetradas por indivíduos e/ou organizações para obtenção de dinheiro, bens ou serviços; evitar o pagamento ou perda de serviços; assegurar vantagem pessoal ou nos negócios.
- **Grupo de Ação Financeira (GAFI)** – Organismo intergovernamental que tem como objetivo desenvolver e promover políticas, nacionais e internacionais, de combate ao branqueamento de capitais e ao financiamento do terrorismo.
- **Instituição de Pagamento** – Pessoa jurídica que viabiliza serviços de compra e venda e de movimentação de recursos, no âmbito de um arranjo de pagamento, sem a possibilidade de conceder empréstimos e financiamentos a seus clientes, e que que tenham, como atividade principal ou acessória, alternativa ou cumulativamente, as opções listadas no art. 6º, inciso III, da Lei nº 12.865 de 09 de outubro de 2013. Não compõem o SFN, mas são reguladas e fiscalizadas pelo BC, conforme diretrizes estabelecidas pelo CMN.
- **Know Your Client (KYC)** – "Conheça seu Cliente" – regras e procedimentos institucionais adotados para identificar e mitigar riscos relacionados a clientes, durante seu credenciamento e em momento posterior, visando ao conhecimento de suas atividades e ao monitoramento eficaz de suas operações para prevenir que a estrutura e/ou produtos da MRB sejam utilizados como instrumentos para a prática de ilícitos.
- **Know Your Employee (KYE)** – "Conheça seu Funcionário" – regras e procedimentos institucionais para identificar e mitigar riscos relacionado a colaboradores, durante sua contratação e em momento posterior, para que a estrutura da MRB seja utilizada para prática de ilícitos e outras situações de conflitos de interesse.
- **Know Your Partners (KYP)** – "Conheça Seu Parceiro" – regras e procedimentos institucionais adotados para identificar e mitigar riscos relacionados a parceiros de negócios, avaliando e legitimando a reputação deles para evitar a associação da MRB com atividades ilegais.
- **Know Your Supplier (KYS)** – "Conheça Seu Fornecedor" – regras e procedimentos institucionais para examinar a credibilidade e práticas dos fornecedores para garantir fornecimento ético e reduzir riscos regulatórios, prevenindo que a estrutura da MRB seja envolvida em práticas ilícitas.
- **LD / FT** – Lavagem de dinheiro / Financiamento ao terrorismo.
- **MRB** – MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA, inscrita no CNPJ sob o nº 38.354.463/0001-24.

- **Office of Foreign Assets Control (OFAC)** – Agência de inteligência financeira do Departamento do Tesouro dos Estados Unidos da América que monitora e atualiza a lista de pessoas e empresas proibidas de realizar negócios com o governo norte-americano e empresas que têm negócios no território americano, com alcance extraterritorial.
- **Oportunidades de melhoria** – Áreas ou processos que podem ser aprimorados para aumentar eficiência, qualidade ou resultados.
- **Pessoa Exposta Politicamente (PEP)** – É todo agente público com exposição pública ou pessoa de seu relacionamento próximo, considerando a verificação dessa condição nos termos do art. 27, bem como da condição de representante, familiar ou estreito colaborador dessas pessoas nos termos do art. 19, ambos da Circular nº 3978/2020 do BCB.
- **PLD/CFT** – Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo.
- **Riscos e Compliance** – Área responsável por pela governança, implementação e monitoramento do programa de PLD/CFT da MRB, gestão de riscos e conformidade regulatória.
- **Sistema Financeiro Nacional (SFN)** – Rede de instituições públicas e privadas responsável por fiscalizar e fazer a regulação das operações do mercado financeiro no Brasil.
- **Sistema de Pagamentos Brasileiro (SPB)** – Sistema gerido pelo Banco Central do Brasil (BCB) para permitir a realização de operações e a transferência de recursos financeiros em território nacional, tanto em reais quanto em moeda estrangeira. É composto por dois segmentos: Infraestruturas do Mercado Financeiro (IMF) e Arranjos de Pagamento.

2. INTRODUÇÃO

À luz do crescente panorama de ameaças financeiras, que inclui não apenas fraudes e mecanismos de lavagem de dinheiro tradicionais, mas também a preocupação com o financiamento de atividades terroristas, a implementação desta *Política de Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/CFT)* é crucial para Instituições de Pagamento do país, obedientes às diretrizes do Banco Central do Brasil (BCB) e às demais exigências regulatórias que impõem padrões rigorosos de segurança e monitoramento.

Ao investir em tecnologias e procedimentos adequados para efetivar o cumprimento da lei, a *MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA* ("MRB"), busca não apenas reduzir os riscos associados ao tema, mas também promover uma cultura organizacional de integridade e transparência em suas atividades. Isso reforça a confiança dos clientes na instituição de pagamento, demonstrando seu compromisso com a segurança dos dados e transações financeiras, além de fortalecer a reputação e a credibilidade da empresa no mercado.

Como fim maior, a implementação da presente Política protege os interesses da instituição, mas também contribui para a segurança, integridade e a estabilidade do Sistema de Pagamentos Brasileiro (SPB).

3. OBJETIVO

Por meio desta Política, a MRB objetiva:

- Estabelecer diretrizes para prevenção, identificação e tratamento de atividades relacionadas a fraudes e lavagem de dinheiro, incluindo o combate ao financiamento de terrorismo, considerando os perfis de risco da MRB; de seus clientes; das operações, transações, produtos e serviços; e dos funcionários, parceiros e prestadores de serviços terceirizados.
- Definir as obrigações e responsabilidades de cada área da empresa neste tema;
- Assegurar a adequação, o fortalecimento e o funcionamento do sistema de controles internos.

4. ABRANGÊNCIA

Esta Política aplica-se a todos da MRB, incluindo gestores, investidores, colaboradores, estagiários, prestadores de serviço, consultores e demais pessoas físicas ou jurídicas que utilizam ou suportam os negócios da Instituição de Pagamento.

5. REFERÊNCIAS NORMATIVAS

- **Recomendações do Grupo de Ação Financeira – GAFI**
- **Lei nº 9.613, de 3 de março de 1998** – 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 12.865 de 09 de outubro de 2013** – Dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).
- **Lei nº 13.260, de 16 de março de 2016** – Regulamenta o inciso XLIII do art. 5º da CF, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.
- **Circular n° 3.978 de 23/1/2020** – 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 9.613/1998, e de financiamento do terrorismo, previsto na Lei nº 13.260/ 2016.
- **Carta Circular n° 4.001 de 29/1/2020** – Divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de "lavagem" ou ocultação de bens, direitos e valores, e de Financiamento do Terrorismo, passíveis de comunicação ao COAF.
- **Resolução Coaf nº 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).
- **Resolução BCB nº 80/2021** – Disciplina a constituição e o funcionamento das instituições de pagamento, estabelece os parâmetros para ingressar com pedidos de autorização de funcionamento por parte dessas instituições e dispõe sobre a prestação de serviços de pagamento por outras instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução Conjunta n° 6 de 23/5/2023** – Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução BCB n° 343 de 4/10/2023** – Dispõe sobre as medidas necessárias à execução do compartilhamento de dados e informações sobre indícios de fraudes de que trata a Resolução Conjunta nº 6, de 23 de maio de 2023.
- **Lei 14.790/23 de 29 de dezembro de 2023** – Permite que empresas privadas operem apostas esportivas online e em estabelecimentos físicos, como casas de apostas e cassinos.

As leis e normas são citadas de forma exemplificativa, e não esgotam toda a legislação aplicável às atividades da MRB.

5.1. Aplicabilidade

A MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA é Instituição de Pagamento, fundada em 2020, que tem, como objeto social: *"Atividade de execução ou facilitação de pagamento relacionada a determinado*

serviço de pagamento, inclusive transferência originada de ou destinada a conta digital de pagamento, serviços na área de meios eletrônicos de pagamento, atividades auxiliares de serviços financeiros, atividades de intermediação e agenciamento de serviços e negócios, exceto imobiliários, serviços prestados em plataformas de pagamento online, carteiras digitais para realização de pagamentos por meio de dispositivos eletrônicos, soluções eletrônicas comerciais na transmissão, processamento e liquidação financeira com cartões de crédito e débito, serviços de processamento e liquidação de transações com cartões de crédito e débito, intermediação na obtenção de empréstimos."

Deste modo, a MRB realizará a alteração desta Política, quando necessário para:

- Cumprimento à integralidade dos procedimentos de monitoramento e seleção previstos na Circular n° 3.978/2020; e
- Caso venha a solicitar autorização de funcionamento ao Banco Central para a modalidade de "Instituição de Pagamento", nos termos da Lei nº 12.865 de 09 de outubro de 2013 e da Resolução BCB nº 80/2021. Neste momento, também, a MRB providenciará o necessário para o cumprimento da Resolução Conjunta n° 6 de 23/5/2023 e da Resolução BCB n° 343 de 4/10/2023, relacionadas ao compartilhamento de dados e informações sobre indícios de fraudes.

6. DISPOSIÇÕES GERAIS

- A Alta Administração da MRB assume o compromisso com a efetividade e a melhoria contínua da política, dos procedimentos e dos controles internos relacionados com a PLD/CFT, adotando, por de sua área de *Riscos e Compliance*, normas internas, padrões, procedimentos, treinamentos, comunicação corporativa e medidas preventivas, corretivas e punitivas, a fim tornar a instituição, em todas as áreas, aderente a esta Política.
- Deverão ser implementados processos que possibilitem monitorar a efetividade e realizar o aprimoramento desta Política e dos meios de prevenção aos riscos de fraude.
- Esta política deve ser compreendida em conjunto com outras políticas institucionais pertinentes, e seu conteúdo não substitui nem prevalece sobre qualquer instrumento legal.
- É obrigatória a realização prévia, pela área de *Riscos e Compliance*, de análise de potenciais riscos de PLD/CFT para novos produtos e serviços, bem como da utilização de novas tecnologias, por parte da MRB. Também devem ser atendidos parâmetros e melhores práticas de Segurança da Informação estabelecidos pela área responsável.

7. CONCEITOS

7.1. Lavagem de Dinheiro

A *lavagem de dinheiro*, também conhecida como *branqueamento de capitais*, é uma prática criminosa que tem por objetivo ocultar a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de atos ilícitos ou crimes antecedentes. Por meio desse processo, os bens ou recursos obtidos de forma ilegal são inseridos na economia formal, aparentando serem legais, dificultando assim a identificação e punição dos responsáveis.

A Lavagem de Dinheiro é tipificada como crime na Lei nº 9.613/1998 e é punida com prisão de 3 (três) a 10 (dez) anos, multa e outras sanções.

São três as fases que caracterizam a Lavagem de Dinheiro:

- COLOCAÇÃO – tem por objetivo inserir os bens ou recursos ilícitos na economia formal, ou seja, em empresas ou negócios lícitos. Esta fase consiste na introdução do bem ou recurso ilícito no sistema financeiro, dificultando a identificação de sua procedência.
- OCULTAÇÃO – adoção de medidas que visam a dificultar o rastreamento dos bens ou recursos ilícitos. Nesta fase há a tentativa de camuflar as evidências e a conexão entre o bem e o crime praticado. Podem ser realizadas diversas movimentações financeiras de modo a acrescentar complexidade e dificultar um futuro rastreamento.
- INTEGRAÇÃO – depois de ocultados e "lavados", em diferentes operações financeiras, os bens ou recursos retornam aos agentes por meio da simulação de negócios aparentemente lícitos.

Não é necessário que se configurem todas as três fases do delito, pois cada fase, isoladamente, já é considerada como Lavagem de Dinheiro.

7.2. Financiamento do Terrorismo

Tal financiamento está relacionado com a distribuição dissimulada de bens ou recursos a serem utilizados em atos e/ou por organizações terroristas, assim como o financiamento da proliferação de armas de destruição em massa. Os métodos utilizados geralmente são semelhantes àqueles empregados na Lavagem de Dinheiro.

A Lei nº 13.260/2016 dispõe sobre o crime de financiamento, no seu art. 6º, prevendo pena de reclusão de 15 (quinze) a 30 (trinta) anos para quem *"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 Antiterrorismo.

No parágrafo único do mesmo dispositivo legal, afirma que *"incorre na mesma pena 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"*.

8. PAPEIS E RESPONSABILIDADES

A atribuição clara de papeis e responsabilidades na PLD/CFT é crucial para garantir uma implementação efetiva da Política, pois ajuda a garantir que todas as partes envolvidas compreendam suas funções específicas e contribuam para a conformidade regulatória e a mitigação de riscos, viabilizando a adequada prestação de contas. Deste modo, abaixo estão de forma objetiva as atribuições das áreas de negócio da MRB:

8.1. Alta Administração

- Assegurar a adesão institucional às boas práticas PLD/CFT, ao cumprimento das leis e normas vigentes relacionadas.
- Aprovar a elaboração, revisão e alterações da presente Política, para posterior publicação.
- Designar e indicar formalmente, ao Banco Central do Brasil, Diretor responsável pelo cumprimento das obrigações de gestão da PLD/CFT da MRB, nos termos da Circular BCB nº 3.978/2020.

8.2. Riscos e Compliance

- Fomentar uma cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, envolvendo administradores, clientes, colaboradores, fornecedores e parceiros de negócio.
- Assegurar a conformidade das áreas de negócio e de todos os procedimentos internos da MRB.
- Criar e gerenciar os mecanismos de controle voltados à prevenção à LD/FT.
- Criar e coordenar a comunicação e treinamento dos Administradores e Colaboradores
- Assegurar o cumprimento dos mecanismos de atuação do Canal de Denúncia
- Monitorar as ocorrências sobre Transações atípicas ou suspeitas identificadas pelas ferramentas tecnológicas da MRB ou que sejam comunicadas pelos Colaboradores
- Enquadramento e monitoramento de PEP, quando houver necessidade
- Análise de clientes, fornecedores e demais partes interessadas envolvidos em listas sancionadoras
- Comunicação com o COAF e com o Bacen, além de atendimento de auditorias e demais órgãos de fiscalização e autoridades competentes.
- Realizar uma Gestão de Riscos corporativa efetiva.
- Promover comunicação efetiva da Política, nos canais institucionais e por meio de treinamentos.
- Verificar eventual atualização, revogação e a edição de novas normas.
- Analisar potenciais riscos de PLD/CFT para novos produtos e serviços, bem como da utilização de novas tecnologias, por parte da MRB.
- Realizar a revisão periódica da Política.
- Analisar casos omissos ou exceções ao estabelecido nesta Política (via Diretoria, conforme item 20).
- Gestão de ferramentas e estabelecimento de processos relacionados à *background check* e *due diligence*.

8.3. Tecnologia da Informação / Segurança da Informação

- Estabelecer parâmetros e melhores práticas de Segurança da Informação para produtos, serviços e operações da MRB.
- Garantir que sejam obedecidas integralmente as determinações de restrições de acesso a sistemas, aprovações de processos eletrônicos, alterações de parametrizações de regras em sistemas e outras, que estejam formalizada, implementando Gestão de Acessos baseada em funções, Política de Segurança da Informação e demais normativos e procedimentos internos necessários.
- Testar os controles relacionados à segurança cibernética para prevenção a fraudes;
- Atuar com diligência na proteção e sigilo dos dados e para manutenção das ferramentas tecnológicas e infraestrutura da MRB.
- Acompanhar e gerir a segurança de todas as aplicações, sistemas, comunicação com fornecedores e estruturas de tecnologia da MRB a fim de mitigar qualquer risco de manipulação, cyber ataque ou exploração de vulnerabilidades sistêmicas;
- Monitorar o tráfego de informações da marca a fim de mitigar possíveis vulnerabilidades ou pontos de exploração encontrados e gerar alertas de possíveis dados comprometidos à área de Riscos e Compliance, reportando à mesma área qualquer risco cibernético que impacte o negócio sem plano de mitigação adequado.
- Garantir que sejam implementados múltiplos fatores de autenticação e demais práticas que sirvam para assegurar o controle de acessos os ativos e informações da empresa.
- Gestão de fornecedores de Tecnologia da Informação e Segurança.

8.4. Comercial / Marketing

- Observar os processos de KYC e KYP para Clientes e Parceiros de Negócio.
- Observar o processo de KYP com relação aos Fornecedores, por meio dos processos de cadastro e verificação das informações fornecidas, conforme aplicável.
- Observar o processo de KYE com relação aos Colaboradores nas funções de ações e campanhas de vendas, prospecção, publicidade e concessão de brindes, premiações, conforme aplicável.

8.5. Financeiro / Controladoria

- Manter o bom desempenho das atividades da MRB, criando metodologias e sistemas que desenvolvam controles gerenciais, atuando em conjunto com a área de Riscos e Compliance para a otimização de processos e mitigação de riscos e indícios de crimes de LD/FT.
- Estabelecer os procedimentos referente às funções de tesouraria, controle das contas a pagar e a receber, gestão de recursos de terceiros, contabilidade, planejamento, gestão dos impostos e o controle de riscos de possíveis indícios de fraudes.

8.6. Operações

- Observar os processos de KYC, KYS e KYP para Clientes, Fornecedores e Parceiros de Negócio, no que diz respeito aos processos operacionais, logísticos, de credenciamento, abertura de contas e habilitação de Clientes.

8.7. Compras

- Observar o processo de KYS com relação aos Fornecedores, por meio de cadastro e verificação das informações fornecidas após a solicitação de propostas, cotações ou outros trâmites de contratação aplicáveis.

8.8. Recursos Humanos

- Estabelecer critérios e processos de KYE para a seleção e contratação de Colaboradores que possuam perfil condizente com esta Política, e em observância do grau de responsabilidade dos indivíduos de acordo com as funções e responsabilidades que lhe forem atribuídas.

9. AVALIAÇÃO INTERNA DE RISCOS (AIR)

- A Avaliação Interna de Risco define as metodologias, os parâmetros, as técnicas e as ferramentas necessárias para identificar e mensurar o risco de utilização dos produtos e serviços da MRB, na prática da LD/FT. Para tanto, segue-se a recomendação da Circular BCB nº 3.978/2020, considerando, no mínimo, os seguintes **perfis de risco**:
  - *Clientes;*
  - *Instituição, incluindo o modelo de negócio e a área geográfica de atuação;*
  - *Operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias;*
  - *Atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados.*
- O risco identificado deve ser avaliado quanto à sua probabilidade de ocorrência e à magnitude dos impactos financeiro, jurídico, reputacional e socioambiental para a MRB.
- Ficam definidas 04 (quatro) **categorias de risco**: Risco Muito Alto / Risco Alto / Risco Médio / Risco Baixo.

  - Essas categorias possibilitam a adoção de controles de gerenciamento e de mitigação reforçados para as situações de maior risco e a adoção de controles simplificados nas situações de menor risco.
  - A pontuação final representa os mesmos percentuais indicados na matriz de riscos (tabela de probabilidade versus impacto) incluída na AIR.
- Devem ser utilizadas como subsídio à avaliação interna de risco, quando disponíveis, avaliações realizadas por entidades públicas do País relativas ao risco de lavagem de dinheiro e de financiamento do terrorismo.
- A avaliação interna de risco deve ser:
  - Documentada e aprovada pelo Diretor responsável, perante o Banco Central do Brasil, pelo cumprimento das obrigações de gestão da PLD/CFT da MRB.
  - Encaminhada para ciência à diretoria da instituição; e
  - Revisada a cada 02 (dois), bem como quando ocorrerem alterações significativas nos perfis de risco utilizados.

10. AVALIAÇÃO DE EFETIVIDADE

- A Avaliação de Efetividade deve ser capaz de verificar o cumprimento desta Política, dos procedimentos e dos controles internos relacionados à PLD/CFT, bem como a identificação e a correção das deficiências verificadas e oportunidades de melhoria.
- A **Avaliação de Efetividade** deve ser documentada em **relatório específico**, que deve:
  - Ser elaborado anualmente, com data-base de 31 de dezembro; e
  - Ser encaminhado, para ciência, até 31 de março do ano seguinte à Diretoria da instituição.
  - Conter informações que descrevam:
    a) a metodologia adotada na avaliação de efetividade;
    b) os testes aplicados;
    c) a qualificação dos avaliadores; e
    d) as deficiências identificadas;
  - Conter, no mínimo, a avaliação:
    a) dos procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
    b) dos procedimentos de monitoramento, seleção, análise e comunicação ao Coaf, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas;
    c) da governança da política de prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
    d) das medidas de desenvolvimento da cultura organizacional voltadas à prevenção da lavagem de dinheiro e ao financiamento do terrorismo;
    e) dos programas de capacitação periódica de pessoal;
    f) dos procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados; e
    g) das ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do Banco Central do Brasil.
- Deverá ser elaborado um **Plano de Ação** destinado a solucionar as deficiências identificadas na Avaliação de Efetividade e apontadas no relatório.

- O acompanhamento da implementação do Plano de Ação deve ser documentado por meio de Relatório de Acompanhamento.
- O Plano de Ação e o respectivo Relatório de Acompanhamento devem ser encaminhados para ciência e avaliação da Diretoria da instituição, até 30 de junho do ano seguinte ao da data-base do relatório da Avaliação de Efetividade.

11. DUE DILIGENCE

- Os dados informados nos procedimentos de KYC, KYS e KYP serão confirmados por meio do envio de documentos e/ou mediante consulta em bancos de dados públicos ou privados, tais como bureaux de análises de crédito e risco, além de base de dados interna ou que seja compartilhada por outras empresas.
- São verificados processos junto aos tribunais, mídias desabonadoras e listas restritivas, a fim de apurar possível envolvimento do terceiro/proponente em atos ilícitos. O monitoramento de terceiros ocorre de forma contínua, onde são verificados processos judiciais, situação do CNPJ junto à Receita Federal entre outros.
- Haverá o armazenamento das informações obtidas nos procedimentos de KYC, KYS e KYP, as quais devem ser compatíveis com o perfil de risco definido pela área de Riscos e Compliance, de acordo com a natureza do negócio e o risco ao qual a MRB será exposta.
- O *due diligence* ocorrerá de forma sistematizada e periódica.
- As informações cadastrais serão arquivadas pelo período mínimo de 5 (cinco) anos, contados a partir do primeiro dia do ano seguinte após o término do relacionamento com o Cliente, Fornecedor ou Parceiro Comercial.
    - Após esse período, o descarte de informações deverá observar a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13709/2018), no que couber, e a legislação específica aplicável às atividades de negócio da MRB.
- A atualização dos dados inerentes a Clientes, Fornecedores e Parceiros deve ocorrer de forma sistematizada e periódica.
    - Porém, a cada 12 meses deverão ser executados testes para a validação das informações cadastrais e de registro, de modo que inconsistências eventualmente encontradas deverão ser sanadas tempestivamente, para regularização.

12. CONHECIMENTO DE CLIENTES (KYC)

12.1. Know Your Client (KYC)

- A MRB implementará *Política de Know Your Client (KYC)*, que conterá disposições e regramentos específicos destinados à adoção de diligência prévia e periódica que assegure sua identificação, qualificação e classificação para conhecimento de seus Clientes, prevenindo a ocorrência de LD/FT.
    - São adotados procedimentos que permitem identificar e validar a identidade e a idoneidade do cliente, incluindo a obtenção, a verificação e a validação da autenticidade de informações de sua identificação, mediante confrontação dessas informações com as listas disponíveis em bancos de dados de caráter público e/ou privado (conforme disposto no item 11 da presente Política), quando necessário, e de acordo com a categoria de risco do cliente.
    - A qualquer momento, inclusive após o cadastro, poderá ser solicitado o envio de informações complementares, declarações e documentos para validação das informações.

    - São adotados procedimentos que permitem qualificar os clientes da MRB por meio da coleta, da verificação e da validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócios a serem realizados.
- Só serão considerados potenciais clientes da MRB aqueles que cujas atividades sejam lícitas, integralmente em conformidade com a lei, e com a documentação atualizada, válida e vigente perante os órgãos e autoridades competentes e cabíveis.
- O cadastro dos Clientes será realizado de forma individualizada e padronizada, contendo todos os dados pessoais e informações exigidas pela legislação vigente.
- Haverá classificação específica para Clientes considerados como PEP.
- Para fins de *Combate ao Financiamento do Terrorismo*, não haverá a aprovação do cadastro de potenciais Clientes incluídos na lista da OFAC.
- A classificação de riscos será revista sempre que houver alterações no perfil de risco do cliente e na natureza da relação de negócio.

12.2. Pessoas Expostas Politicamente (PEP)

- A MRB implementará procedimentos que permitam qualificar seus Clientes como Pessoa Exposta Politicamente (PEP), sem exceção, assim considerada aquela que detém relevantes funções públicas no âmbito dos diversos poderes, conforme relação prevista na Circular BCB nº 3.978/2020.
- Os procedimentos de qualificação inclui a consulta às listas públicas e privadas disponíveis ou por meio de autodeclaração que constará do cadastro de cada um deles.
- A decisão de iniciar ou manter o relacionamento de Cliente classificado como PEP é baseada na percepção de risco, feita por gestores de hierarquia superior ao responsável pela atividade de aprovação do cadastro. A decisão, se positiva, deverá ser submetida à área de Riscos e Compliance, a quem caberá, com exclusividade, aprovar ou declinar o prosseguimento.
- Caso haja a aprovação, as áreas respectivas deverão reportar à área de Riscos e Compliance todas as transações realizadas pelos Clientes PEP.

12.3. Beneficiário Final

- Nos procedimentos de qualificação do cliente pessoa jurídica, a cadeia de participação societária é analisada até a identificação da pessoa natural caracterizada como seu beneficiário final, para a qual serão aplicados, no mínimo, os procedimentos de qualificação definidos para a categoria de risco do cliente pessoa jurídica, na qual o beneficiário final detenha participação societária.
- É considerado pela MRB, também, como beneficiário final o representante, inclusive o procurador e o preposto, que exerça o comando de fato sobre as atividades do cliente pessoa jurídica.
- Nas situações que envolvam os clientes que possuem configurações societárias especiais (conforme listados no §3º do artigo 24 da Circular BCB nº 3.978/2020), não é analisada a cadeia de participação societária, mas são coletadas informações que abranjam as das pessoas naturais autorizadas a representá-las, bem como as de seus controladores, administradores ou gestores, e diretores, conforme o caso.

12.4. Limite Operacional

- A definição do limite operacional é estabelecida com base no exame da capacidade financeira do cliente (faturamento, considerando o perfil atual de clientes serem pessoas jurídicas), observadas a compatibilidade e a proporcionalidade do nível de risco.

- A documentação exigida dos clientes para fins da comprovação da capacidade financeira, terá eu tipo e forma definidos de acordo com o respectivo propósito da relação de negócio, produtos ou serviços consumidos, bem como a natureza de suas operações.

13. SELEÇÃO DE PARCEIROS E FORNECEDORES (KYP E KYS)

- Fornecedor ou Parceiro de Negócio será verificado, de acordo com sua atividade empresária, o perfil e o propósito de relacionamento, as informações sobre o terceiro com o qual será o contrato pactuado, estabelecida alguma relação de negócio ou feita concessão de patrocínio.
- A classificação de risco da empresa fornecedora/parceira ocorrerá conforme as normas internas da área de *Riscos e Compliance*, podendo ser recusada a contratação com qualquer Fornecedor ou Parceiros de Negócio, em razão dos procedimentos de KYS e KYP.
- Caso a atividade empresarial ou profissional exercida pela empresa seja classifica como sendo de alto risco, as áreas Operacional, Financeira e de Riscos e Compliance estabelecerão monitoramento reforçado sobre os valores envolvidos.
- A remuneração a ser paga pela MRB, independentemente de sua natureza, deverá ser liquidada em conta de pagamento ou conta bancária de titularidade do respectivo Fornecedor ou Parceiro de Negócio.
- Cláusulas de obrigações relacionadas à PLD/CFT deverão ser necessariamente inseridas nos contratos a serem celebrados com os Fornecedores e Parceiros de Negócio.
- Será procedido *due diligence* conforme estabelecido no item 11 desta Política.

14. SELEÇÃO E CONTRATAÇÃO DE COLABORADORES (KYE)

- A seleção e contratação de Colaboradores, inclusive terceirizados, serão realizadas com o objetivo reduzir o risco de práticas ilícitas de qualquer natureza, incluindo, a PLD/CFT, independentemente do cargo ou função, obedecendo a critérios específicos estabelecidos nos procedimentos da área de Recursos Humanos, considerando as diretrizes estabelecidas nesta Política e os riscos identificados.
- Na etapa de contratação, cabe à área de Recursos Humanos, seguindo os processos de recrutamento e seleção, realizar a análise de perfil, identificando e as características do potencial funcionário estão alinhadas com os valores da MRB e as Políticas institucionais vigentes, além de avaliar possíveis antecedentes do candidato que possam indicar risco potencial de LD/FTP.
- O procedimento de *background check* e os demais processos correlatos devem ser validados pela área de *Riscos e Compliance*, observando-se a conformidade jurídica das informações coletadas ou validadas.
- O monitoramento preventivo inclui verificações regulares, em atenção aos riscos mapeados.
    - Deve haver isonomia de tratamento nessa conduta, abrangendo todos os Colaboradores, sendo vedado o monitoramento com fins discriminatórios.
    - O Colaborador deverá ser previamente comunicado sobre este monitoramento, mediante a assinatura do Termo disposto no Anexo I desta Política ou, ainda, por menção expressa em seu contrato de trabalho.
- Os gestores das áreas da MRB são responsáveis por identificar e comunicar a área de *Riscos e Compliance*, acerca de comportamentos contrários ao estabelecido nesta Política, ou outras políticas e procedimentos adotados pela área de Recursos Humanos da MRB.

15. PROCEDIMENTO DE REGISTRO DE OPERAÇÕES

- A MRB manterá registros de todas as operações realizadas, produtos e serviços contratados, inclusive saques, depósitos, aportes, pagamentos, recebimentos, transferências de recursos e operações no mercado de câmbio.
- Nos termos da Circular nº 3.978/2020, serão mantidos registros com as seguintes informações mínimas, sobre cada operação:
    a) do cliente;
    b) do tipo e da natureza do negócio;
    c) do valor;
    d) da forma de entrega;
    e) da data de realização;
    f) das contrapartes envolvidas;
    g) dos canais de distribuição utilizados; e
    h) da origem e da destinação dos recursos.
- No caso de operações relativas a pagamentos, recebimentos e transferências de recursos, por meio de qualquer instrumento, são incluídos nos registros as informações necessárias à identificação da origem e do destino dos recursos.
- São incluídas no registro das operações, no mínimo, as informações que permitam identificar o nome e número de inscrição no CPF ou no CNPJ do remetente, o sacado, o recebedor ou o beneficiário, bem como os códigos de identificação, no sistema de liquidação de pagamentos ou de transferência de fundos, das instituições envolvidas na operação.
- Para o monitoramento das Transações, a área de *Riscos e Compliance* deverá estipular, além dos registros acima citados, o valor das Transações e os critérios de monitoramento e seleção que permitam identificar Transações suspeitas.
- A MRB manterá registros de todas as operações realizadas pelos Clientes, os quais serão arquivados pelo período mínimo de 5 (cinco) anos, contados a partir do primeiro dia do ano seguinte ao da conclusão da operação e, no caso de informações e registros de transferência de recursos, o prazo será de 10 (dez) anos.
- Nos termos da Lei ei 14.790/2023, as MRB deverá manter, na forma e no prazo estabelecidos pela regulamentação do Ministério da Fazenda, o registro de todas as operações realizadas, incluídos as apostas realizadas, os prêmios auferidos, e os saques e depósitos nas contas transacionais.

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

- Á área de *Riscos e Compliance* deverá definir e implementar procedimentos de monitoramento e seleção que permitam identificar operações e situações que possam indicar suspeitas de lavagem de dinheiro e de financiamento do terrorismo.
    - O período para a execução dos procedimentos de monitoramento e de seleção das operações e situações suspeitas não excede o prazo de 45 (quarenta e cinco dias), contados a partir da data de ocorrência da operação ou da situação.
    - A análise feita deverá ser formalizada em **dossiê**, independentemente da comunicação ao COAF.

- Para o monitoramento das Transações deverão ser utilizadas ferramentas tecnológicas de monitoramento e com alertas automáticos de atividades atípicas.
    - Os sistemas utilizados deverão conter informações detalhadas das operações realizadas e das situações ocorridas, inclusive informações sobre a identificação e a qualificação dos envolvidos.
- Poderão ser automaticamente reprovadas e canceladas as Transações em que, de acordo com os procedimentos de monitoramento instituídos pela área de *Riscos e Compliance*, se verifique indícios de LD/FT, considerando fatores como abaixo exemplificados:
    a) Habitualidade, valor, periodicidade, forma ou histórico do Cliente com relação às Transações anteriores;
    b) Intuito de gerar ganho, sem que haja benefício econômico fundamentado;
    c) Omissão ou atraso injustificado no envio de informações e/ou documentos pelo Cliente;
    d) Oscilação significativa em relação ao volume e/ou frequência das Transações;
    e) Alteração repentina e injustificada da modalidade ou valor da Transação;
    f) Incompatibilidade com a capacidade financeira do Cliente, diante de sua capacidade financeira previamente demonstrada;
    g) Repetição contínua de Transações entre o Cliente e o mesmo beneficiário;
    h) Compensação de créditos e débitos entre o Cliente e o mesmo beneficiário;
    i) Atuação do Cliente em nome de terceiros;
    j) Dificuldade ou impossibilidade de identificação do beneficiário final;
    k) Constatação de informações errôneas, inverídicas ou desatualizadas do Cliente; e
    l) Denúncias recebidas pelo Canal de Denúncias.
- Outras situações não previstas na relação acima poderão ser avaliadas pela área de *Riscos e Compliance*.
- A MRB deverá criar procedimento dispondo hipóteses e tratamentos associados aos casos de *Monitoramento Reforçado* de Clientes ou Transações específicas, em razão do alto risco associado.
- Todos os processos e procedimentos relacionados ao cumprimento do item 16 desta Política de PLD/CFT deverão ser definidos com base na AIR e os termos da Circular BCB nº 3.978, de 2020.

17. PROCEDIMENTO DE COMUNICAÇÃO AO COAF

- A MRB comunicará ao COAF as operações ou situações suspeitas de lavagem de dinheiro e de financiamento do terrorismo
- A decisão de comunicação da operação ou situação ao COAF deve:
    a) ser fundamentada com base nas informações contidas no dossiê da análise da operação.
    b) ser registrada de forma detalhada no referido dossiê;
    c) ocorrer até o final do prazo de análise – 45 (quarenta e cinco) dias, contados a partir da data da seleção da operação ou situação suspeita.
- A comunicação deve especificar, quando for o caso, se a pessoa objeto da comunicação:
    a) É PEP ou representante, familiar ou estreito colaborador dessa pessoa;
    b) É pessoa que, reconhecidamente, praticou ou tenha intentado praticar atos terroristas ou deles participado ou facilitado o seu cometimento, caso em que também deverá ser informado se a pessoa possui ou controla, direta ou indiretamente, recursos na instituição.
- A comunicação da operação ou situação suspeita ao COAF deve ser realizada até o dia útil seguinte ao da decisão de comunicação.
    - A comunicação ser realizada sem dar ciência aos envolvidos ou a terceiros.

- As comunicações alteradas ou canceladas após o quinto dia útil seguinte ao da sua realização devem ser acompanhadas de justificativa da ocorrência.

18. COMUNICAÇÃO E TREINAMENTO

- Esta Política é aplicada e amplamente divulgada pela Alta Administração, por meio da área de *Riscos e Compliance,* a todos os colaboradores da MRB, bem como de suas filiais, subsidiárias e escritórios de representação, se houver, e aos prestadores de serviços, conforme aplicável, em linguagem clara e acessível, observando-se as funções desempenhadas e a devida sensibilidade das informações prestadas.
- Poderão ser usados canais de comunicação diversos, incluindo: *site da MRB*, e-*mail de comunicação corporativa* e *link para acesso à Política inserido nos contratos firmados com prestadores de serviços e terceiros*.
- Para fins de manutenção do nível de conscientização, de forma contínua, a MRB deverá executar ações de prevenção, por meio de campanhas de conscientização sobre o tema e treinamentos corporativos periódicos (podendo aplicar processo de avaliação interna dos participantes, quando necessário), bem como pela atualização periódica dos normativos internos relacionados;
- Deverão ser revisados, periodicamente, os normativos internos e procedimentos, referentes ao PLD/CFT.
- Dúvidas e sugestões poderão ser dirimidas pelo contato *compliance@mrbdigitais.com.br*.

19. VIOLAÇÃO E SANÇÕES

- Eventuais descumprimentos ou suspeitas de violações às disposições desta Política, deverão ser imediatamente comunicadas ao Canal de Denúncias da MRB, que irá realizar o tratamento adequado das ocorrências pelo e-mail *ouvidoria@mrbdigitais.com.br*, por meio do(a) recebimento, análise preliminar, classificação, tratamento, monitoramento, investigação, tomada de decisão, reporte das denúncias e encerramento das ocorrências.
    - A MRB receberá e atuará nas denúncias de Administradores, Colaboradores, Fornecedores, Clientes, Parceiros de Negócio ou quaisquer terceiros, sobre atividades atípicas ou suspeitas que possam se caracterizar como indícios de crimes relacionados com a Lavagem de Dinheiro e Financiamento ao Terrorismo.
    - As denúncias serão recebidas por um profissional capacitado e com autonomia necessária, sendo garantido o anonimato e sigilo das comunicações, bem como a preservação da integridade do denunciante.
- O descumprimento da legislação aplicável à PLD/CFT, além de poder causar graves prejuízos à MRB, poderá sujeitar o(a) infrator(a) a penalidades criminais, cíveis e administrativas pelas autoridades.
    - Ademais, sujeitará o(a) colaborador(a) infrator a medidas disciplinares, com base na legislação aplicável, incluindo advertência (verbal ou formal), suspensão e sanção pecuniária, podendo, ainda, culminar na demissão por justa causa do(a) infrator (a), sem prejuízo da adoção das medidas legais cabíveis.
    - Poderão ser adotadas outras penalidades que estiverem pactuadas em contrato juridicamente válido.

20. DISPOSIÇÕES FINAIS

- Os casos omissos ou exceções ao estabelecido nesta Política ou que dependam de aprovação específica, deverão ser submetidos e formalmente avaliados pelo Diretoria responsável pela gestão de *Riscos e Compliance* da MRB.
- Esta Política está acompanhada de um *Termo de Adesão a PLD/CFT* e de um *Termo de Adesão as Alterações desta PLD/CFT*.
    - Todos os colaboradores da MRB deverão ler, compreender e formalizar sua ciência e comprometimento com esta Política, por meio da assinatura dos termos disponíveis.
    - Os dados pessoais fornecidos no preenchimento do(s) Termo(s) serão devidamente armazenados pela MRB, em conformidade com a legislação aplicável.
    - Todos os contratos, durante toda a vigência contratual, celebrados com prestadores de serviços, parceiros e terceiros, deverão conter cláusula de ciência e compromisso com o cumprimento da presente Política, compartilhada conforme disposto no item 10.

21. VIGÊNCIA, REVISÃO E ALTERAÇÕES

- Esta Política entra em vigor na data da sua publicação, revogando outros dispositivos em contrário, e vigorará por tempo indeterminado.
- Será revisada e atualizada **anualmente** (ou em menor tempo, se necessário para fins de efetividade, adequação aos riscos e melhores práticas, ou conformidade legal/regulatória), pela área de *Riscos e Compliance,* e submetidas à aprovação da Alta Administração, de acordo com suas atribuições internas, com posterior publicação.

Data	Versão	Descrição	Autores
11/03/2024	1.0	Elaboração	Consultoria Externa
02/04/2024	1.0	Aprovação	Raquel Birck – Sócia-Administradora

22. ANEXOS

ANEXO I – TERMO DE ADESÃO À PLD/CFT
ANEXO II – TERMO DE ADESÃO ÀS ALTERAÇÕES DESTA PLDFT

ANEXO I – TERMO DE ADESÃO À PLD/CFT

Eu, _____ , inscrito no CPF sob o nº _____, declaro que tenho conhecimento desta *Política de Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/CFT)*, bem como das diretrizes contidas nas demais políticas relacionadas, nas normas e nos procedimentos internos da MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

Tenho conhecimento das atividades da MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA e do quanto esta pode tentar ser aproveitada para a prática de crimes de Lavagem de Dinheiro e ao Financiamento do Terrorismo, por isso, dentro das obrigações de minha função, devo, sempre que necessário, utilizar o Canal de Denúncias para denunciar qualquer tipo de atividade suspeita e/ou tratada como criminosa por esta Política e pela MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

Local: _____ Data: _____

Nome completo: _____

Assinatura: _____

ANEXO II – TERMO DE ADESÃO ÀS ALTERAÇÕES DESTA PLD/CFT

Eu, _____ , inscrito no CPF sob o nº _____, declaro que tenho conhecimento das alterações promovidas nesta *Política de Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/CFT)*, bem como das diretrizes contidas nas demais políticas, nas normas e nos procedimentos internos da MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

Tenho conhecimento das atividades da MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA e do quanto esta pode tentar ser aproveitada para a prática de crimes de Lavagem de Dinheiro e ao Financiamento do Terrorismo, por isso, dentro das obrigações de minha função, devo, sempre que necessário, utilizar o Canal de Denúncias para denunciar qualquer tipo de atividade suspeita e/ou tratada como criminosa por esta Política e pela MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA.

Local: _____ Data: _____

Nome completo: _____

Assinatura: _____