

Política de Prevenção à Lavagem de Dinheiro, Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa

ÍNDICE

1. Introdução	4
2. Aplicabilidade	4
3. Papéis e Responsabilidades	4
3.1. Diretor de PLD/FTP	4
3.2. Canais de Atendimento	5
3.3. Colaboradores	5
3.4. Área de Prevenção a Crimes Financeiros (PCF)	6
3.5. Jurídico	7
3.6. Pessoas e Cultura	8
3.7. Controles Internos	8
3.8. Auditoria Interna	8
3.9. Órgãos de Governança	9
3.9.1. Comitê de Diretoria	9
3.9.2. Comitê Executivo de PLD/FTP	9
3.10. Segurança da Informação	10
4. Diretrizes	10
4.1. Gestão de Controle de Cadastro	11
4.1.1. Cadastro de Clientes	11
4.2. Processos de Análises	11
4.2.1. Avaliação Interna de Riscos (AIR)	11
4.2.2. Conheça Seu Cliente (KYC)	12
II. Fatores geográficos	14
III. Fatores reputacionais, restritivos e de integridade	15
IV. Fatores comportamentais e transacionais	15
4.2.3. Conheça seu Empregado (KYE)	16
4.2.4. Conheça seu Parceiro (KYP) e Conheça seu Fornecedor (KYS)	17
4.2.5. Conheça seu Prestador de Serviços de Ativos Virtuais (KYVASP)	18
4.2.6. Identificação do Beneficiário Final	18
4.3. Monitoramento, Seleção, Análise e Comunicação (MSAC)	19
4.3.1. Monitoramento, Seleção e Análise de Operações Suspeitas	19



4.3.2. Comunicação de Operações Suspeitas	19
4.4. Especial Atenção	20
4.4.1. Jurisdições com Deficiências em PLD/FTP (GAFI)	20
4.4.2. Cumprimento de Sanções Internacionais	20
4.4.3. Relacionamentos Vedados	20
4.5. Monitoramento de Organizações Sem Fins Lucrativos	21
4.6. Práticas Específicas para Ativos Tokenizados	21
4.6.1. Validação de Contratos Inteligentes	22
4.6.2. Análise de Transações On-Chain	22
4.6.3. Due Diligence sobre Originadores	22
4.6.4. Validação sobre Ativos Lastreados	23
5. Treinamento e Conscientização	23
6. Canal de Denúncias	24
7. Penalidades	24
8. Disposições Finais	24
9. Referências	25
10. Controle de Versões	25
Anexo I - Definições	26
Anexo II - Listas Restritivas (“Listas de Sanções”)	29

1. Introdução

Esta Política estabelece as diretrizes e responsabilidades a serem observadas pela 2TM Participações S.A. e suas empresas controladas (“Grupo 2TM”), na prevenção à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa (“PLD/FTP”).

2. Aplicabilidade

Aplica-se a todos os administradores (incluindo diretores executivos), membros do Conselho de Administração e membros dos Comitês e/ou Comissões de Assessoramento ao Conselho de Administração, sócios, Colaboradores, estagiários do Grupo 2TM (todos, em conjunto, os “Colaboradores”), bem como a todos os terceiros que se relacionem com o Grupo 2TM.

3. Papéis e Responsabilidades

Para disseminar os princípios e diretrizes expostos, atuamos nos seguintes níveis de Governança, com as respectivas atribuições:

3.1. Diretor de PLD/FTP

São atribuições do Diretor de PLD/FTP:

- Implementar e manter a Política de PLD/FTP compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da instituição, de forma a assegurar o efetivo gerenciamento dos riscos de LD/FTP apontados;
- Difundir a cultura de PLD/FTP entre os colaboradores e prestadores de serviços, conforme aplicável, 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 e a conformidade legal e regulatória;

- Coordenar ações disciplinares com colaboradores e prestadores de serviços que venham a descumprir os procedimentos de PLD/FTP;
- Coordenar o Comitê Executivo de PLD/FTP, bem como pautas de PLD/FTP no Comitê de Diretoria da MB Pay;
- Avaliar regularmente o programa de PLD/FTP, de modo a garantir sua eficiência e efetividade, assim como incorporar novos fatores de risco, quando aplicável.

O diretor de PLD/FTP desempenha suas funções com independência e autonomia, não estando sujeito a conflitos de interesse ou outras restrições ao pleno cumprimento dos seus deveres.

3.2. Canais de Atendimento

As áreas de Canais de Atendimento tem como responsabilidades:

- Suportar o cumprimento das diligências de identificar e qualificação de clientes, pessoas física e jurídica, conforme diretrizes desta Política, da Política de Cadastro e do Manual de KYC;
- Comunicar comportamentos suspeitos de clientes para a área de Prevenção a Crimes Financeiros.

3.3. Colaboradores

Os colaboradores têm como responsabilidades:

- Informar a área de PCF sobre as novas contratações com parceiros de negócios e fornecedores para que sejam realizadas as análises de integridade (KYP e KYS); e
- Comunicar à área de PCF quaisquer irregularidades ou suspeitas de ato ilícito que tomarem conhecimento, e utilizar o Canal de Denúncias caso haja envolvimento de colaboradores ou pessoas relacionadas ao MB.

3.4. Área de Prevenção a Crimes Financeiros (PCF)

A área de PCF tem como responsabilidades:

- Coordenar o programa de Prevenção à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa (“PLD/FTP”);
- Conduzir o processo de identificação, verificação, qualificação e classificação de riscos de clientes (“Conheça seu Cliente - Know your Client - KYC”)
- Conduzir o processo de verificação de fornecedores e parceiros de negócios (“Conheça seu Parceiro - Know your Partner - KYP” e “Conheça seu Fornecedor - Know your Supplier - KYS”) e Colaboradores (“Conheça seu Empregado - Know your Employee - KYE”);
- Verificação da necessidade de encerramento de conta de clientes com apontamentos cadastrais / transacionais e mediante a confirmação da idoneidade de recursos oriundos de outras instituições financeiras.
- Conduzir o processo de homologação de contrapartes que atuem como prestadores de serviço de ativos virtuais, “Conheça seu PSAV - Know your VASP - KYVASP”;
- Conduzir o processo de monitoramento transacional de clientes (“Conheça sua Transação - Know your Transaction - KYT”) mediante o tratamento de alertas de suspeição oriundos de soluções tecnológicas providas por terceiros ou desenvolvidas internamente para o monitoramento cadastral e transacional dos clientes;
- Adotar as providências cabíveis para os casos suspeitos de ilicitude;
- Assegurar a conformidade com a legislação, normas e regulamentos que disciplinam o tema PLD/FTP;
- Convocar o Comitê de PLD/FTP para deliberar sobre temas relevantes relacionados aos processos da área e casos suspeitos;

- Definir e monitorar indicadores relacionados aos riscos de LD-FTP e à eficácia dos processos de PLD-FTP descritos na Política;
- Buscar o aprimoramento contínuo dos alertas e mecanismos de detecção de situações suspeitas, visando sua eficácia e a redução de falsos-positivos;
- Assegurar o bom funcionamento de soluções tecnológicas providas por terceiros ou desenvolvidas internamente para o monitoramento cadastral e transacional dos clientes, compreendendo a integração dos dados requeridos, a sua correta parametrização (listas restritivas, classificação de riscos, parâmetros de alertas, etc.) e revisão ou atualização periódica;
- Comunicar ao Conselho de Controle de Atividades Financeiras (COAF) os casos considerados suspeitos em deliberação pelo Comitê de PLD/FTP;
- Desenvolver e promover programas de treinamento e de conscientização sobre PLD/FTP para todos os Colaboradores e Terceiros;
- Avaliar riscos de PLD/FTP oriundos de novas tecnologias, produtos e serviços;
- Avaliar e gerir os riscos de PLD/FTP conforme diretrizes da Política de Risco Operacional e Controles Internos;
- Elaborar a Avaliação Interna de Riscos (AIR) e a revisar a cada dois anos, ou mediante alterações significativas no perfil de riscos PLD/FTP;
- Estabelecer a Abordagem Baseada em Riscos do Programa de PLD-FTP, bem como estabelecer e acompanhar os indicadores de efetividade, sensíveis às exposições à risco mapeadas na AIR; e
- Armazenar todos os documentos relacionados aos processos de PLD/FTP pelo prazo mínimo de 10 anos.

3.5. Jurídico

O Jurídico é responsável por apoiar a área de PCF na interpretação de regulamentações, que contempla os normativos estabelecidos pelos órgãos reguladores aplicáveis e por suportar o processo de contratação de terceiros (KYP / KYS) considerando o emprego de

cláusulas-padrão e mitigações de riscos apontados pela área de Prevenção a Crimes Financeiros.

3.6. Pessoas e Cultura

A área de Pessoas e Cultura é responsável por iniciar o processo de KYE relacionado às novas contratações e solicitar avaliação dos candidatos à área de PCF, observando que contratações somente podem ser realizadas após a conclusão das diligências de KYE.

3.7. Controles Internos

A área de Controles Internos é responsável por promover o ambiente de controles pertinentes aos processos de PLD/FTP. Entre suas atribuições, considera-se:

- Auxiliar na identificação e monitorar os riscos operacionais e os controles internos e, quando aplicável, acompanhar os planos de ação para a adequação do ambiente de controles internos, inclusive aqueles oriundos de apontamentos realizados por auditorias internas e externas;
- Realizar os reportes de controles internos aos órgãos de governança competentes abrangendo, dentre outros pontos, o acompanhamento dos planos de ação;
- Realização da avaliação anual de efetividade da Política e dos controles internos de PLD/FTP relativos às empresas do grupo sujeitas à regulação pelo Banco Central; e
- Manter à disposição das autoridades regulatórias, em observância à regulações específicas das unidades de negócio, os relatórios referentes às atividades de Controles Internos relacionados a PLD/FTP.

3.8. Auditoria Interna

São responsabilidades da Auditoria Interna:

- Assegurar a inclusão em seu Plano Anual de Auditoria Interna (PAAI) e cumprir com os trabalhos de auditoria em observância aos requerimentos regulatórios do Banco Central;

- Auditar os processos e controles internos de forma independente e periódica, visando o cumprimento da Política e de requisitos legais e regulatórios aplicáveis;
- Acordar junto aos responsáveis sobre ações de correção para deficiências identificadas e apresentação dos resultados gerais aos órgãos de governança competentes; e
- Manter à disposição das autoridades regulatórias, em observância a regulações específicas das unidades de negócio, os relatórios referentes às atividades da Auditoria Interna relacionados a PLD/FTP.

3.9. Órgãos de Governança

O comprometimento da Diretoria por meio da definição das atribuições e do correto funcionamento dos órgãos de governança é um elemento central para o cumprimento e aprimoramento contínuo desta Política. Abaixo são apresentados os papéis e as responsabilidades dos principais órgãos de governança.

Cabe destacar que o Grupo 2TM é composto por empresas sujeitas a requisitos regulatórios e à autorregulação. Desta forma, são admitidas a existência de instâncias de governança voltadas para funções de PLD/FTP específicas a estas entidades. Deve ser, contudo, respeitada a primazia desta Política e das diretrizes que estabelece.

3.9.1. Comitê de Diretoria

São responsabilidades do Comitê de Diretoria:

- Aprovar manuais e procedimentos das atividades referenciadas pela Política, bem como atualizações da Avaliação Interna de Riscos;
- Acompanhar os indicadores de performance e de riscos referentes à PLD/FTP; e
- Assegurar que o Grupo 2TM disponha de recursos e competências necessários para a realização das atividades e diretrizes da Política.

3.9.2. Comitê Executivo de PLD/FTP

São responsabilidades do Comitê Executivo de PLD/FTP:

- Sugerir alterações à Política de PLD/FTP para assegurar sua adequação aos requerimentos regulatórios e às necessidades de negócio;
- Avaliar dossiês de clientes considerados suspeitos e deliberar pela realização de reporte ao COAF; e
- Acompanhar os indicadores de performance e de riscos referentes à PLD/FTP.

3.10. Segurança da Informação

O risco de FTP (Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa) está diretamente associado a ataques cibernéticos e invasão de contas de clientes, de modo que o cumprimento das diretrizes da Política de Segurança da Informação é condição primordial para a efetividade das ações de PLD/FTP.

A área de Segurança da Informação deve atuar de forma colaborativa com a equipe de PCF em casos onde haja indícios de envolvimento de grupos ou indivíduos associados a práticas terroristas ou a países objeto de sanção, comunicando ocorrências relevantes que possam impactar as ações de monitoramento de clientes e detecção de práticas ilícitas, como ataques cibernéticos que comprometam a segurança de dados pessoais, ataques a sistemas financeiros, sistemas de monitoramento, criação de contas falsas, dentre outros.

4. Diretrizes

O Grupo 2TM preza pela ética e transparência na condução de suas atividades e acredita que a prevenção à lavagem de dinheiro e o combate ao financiamento do terrorismo e proliferação de armas de destruição em massa fazem parte de sua responsabilidade perante a sociedade. Assim, o Grupo 2TM tem o compromisso de manter um ambiente de controles robustos alinhados com a regulamentação, boas práticas e recomendações internacionais.

O devido cumprimento das diretrizes apresentadas a seguir pressupõem ampla e irrestrita colaboração entre as empresas do Grupo 2TM, no tocante ao acesso a informações cadastrais, transacionais e quais outras informações relevantes para

cumprimento integral das diligências e procedimentos detalhados a seguir. Restrições ou impeditivos no cumprimento das diretrizes devem ser submetidos ao Comitê Executivo de PLD/FTP.

4.1. Gestão de Controle de Cadastro

4.1.1. Cadastro de Clientes

A área de Prevenção a Crimes Financeiros (PCF) é responsável pela análise e registro das informações e documentos de identificação dos clientes com os quais o Grupo 2TM mantém relacionamento. Muitas dessas informações são obtidas por meio de busca automatizada em fontes de dados públicas e privadas, executadas pelo sistema de cadastro utilizado para pessoas físicas e jurídicas, visando agilizar o processo de “onboarding digital” de clientes mas sem comprometer a segurança e as informações, conforme sua classificação de sigilo.

As informações cadastrais deverão estar atualizadas de acordo com os dados apresentados pelo cliente, e revisadas periodicamente, observando o nível de risco PLD/FTP de cada cliente, conforme Abordagem Baseada em Risco do MB. As diretrizes específicas para a identificação, qualificação e classificação de risco dos clientes do Grupo 2TM são apresentadas em detalhe na Política de Cadastro e no Manual de KYC.

4.2. Processos de Análises

4.2.1. Avaliação Interna de Riscos (AIR)

A AIR é parte integrante do Programa de PLD/FTP e é elaborada pela área de PCF. Essa avaliação considera os riscos inerentes às atividades da organização e contempla os seguintes elementos:

- Segmentação de produtos, serviços, canais de distribuição, classificando-os em baixo, médio e alto risco de LD/FTP;
- Classificação de risco de clientes em baixo, médio, alto e severo risco de LD/FTP;
- Indicadores de efetividade do programa, como:

- Percentual de alertas com falso positivo;
 - Tempo médio de análise de operação suspeita;
 - Taxa de atualização cadastral em dia;
 - Número de revisões de classificação de risco.
- Tabela estatística com o número de:
 - Operações e situações atípicas detectadas;
 - Análises realizadas;
 - Comunicações efetuadas ao COAF;
 - Declaração negativa enviada, se aplicável.
 - Recomendações e cronograma de ações para mitigação de riscos identificados e não tratados.

A AIR é aprovada pela Diretoria e está disponível para órgãos reguladores sempre que solicitado.

4.2.2. Conheça Seu Cliente (KYC)

O Grupo 2TM definiu o processo de KYC adequado às características e especificações dos negócios por ele administrados, objetivando prevenir que o cliente e/ou usuário utilize qualquer empresa do Grupo para atividades ilegais ou impróprias.

O processo de KYC tem por objetivo permitir que o Grupo 2TM identifique e qualifique seus clientes e atribua uma classificação inicial de risco no momento do cadastro, por meio de mecanismos automatizados de classificação parametrizados em ferramenta especializada de monitoramento cadastral, complementados por análises de background check e consultas automatizadas a bureaus de identidade e outras bases de dados relevantes para avaliação do risco de PLD/FTP.

De forma complementar ao processo cadastral e durante todo o período de relacionamento comercial, a identificação de situações que possam implicar na incompatibilidade de renda ou patrimônio deste cliente ensejam a realização de ações adicionais para conhecimento das propriedades e especificidades do contexto financeiro do cliente, para que fique clara a origem e o destino dos ativos financeiros movimentados, para aferir a compatibilidade entre a operação e o perfil da outra parte



do negócio e para atualizar a classificação do risco do cliente frente aos demais produtos e serviços ofertados.

Em se tratando de clientes PEP, os processos a serem observados para o estabelecimento de relação de negócios e acompanhamento das movimentações financeiras da pessoa, bem como seus relacionados (representante, familiares e outras pessoas de relacionamento próximo), são estruturados de forma a possibilitar a sua identificação, bem como a origem dos fundos envolvidos nas transações e a aprovação do cadastro por profissional em nível hierárquico superior ao responsável pela análise.

Em caso de clientes Pessoa Jurídica, é realizada também a avaliação KYC dos beneficiários finais com participação igual ou superior a 25% no capital da empresa. O processo de KYC compreende, além da identificação e qualificação dos beneficiários finais, a análise da estrutura societária, da atividade econômica, do ramo de atuação, do tempo de constituição da empresa, da compatibilidade entre o perfil do negócio e os produtos contratados e de outros fatores relevantes para avaliação de risco de PLD/FTP.

Classificação do Risco do Cliente

A classificação do risco do cliente é realizada de forma automatizada por meio do sistema de monitoramento cadastral e transacional utilizado pelo Grupo 2TM, contemplando duas etapas complementares e integradas.

A primeira etapa ocorre durante o processo de cadastro e aceitação do cliente (KYC), considerando as informações cadastrais, documentos apresentados, consultas automatizadas a bases de dados e bureaux especializados, bem como outras avaliações de background check realizadas no onboarding. Os fatores de risco identificados nessa etapa podem ser incorporados, a depender da sensibilidade, à metodologia de classificação e utilizados para compor a classificação inicial de risco do cliente no sistema de monitoramento.

A segunda etapa ocorre de forma contínua ao longo de todo o relacionamento comercial, por meio do monitoramento cadastral, reputacional, comportamental e transacional. Novos eventos, alertas ou alterações relevantes identificados durante o relacionamento são automaticamente incorporados à metodologia de classificação de risco, permitindo



a atualização dinâmica do perfil de risco do cliente e a adoção das medidas de diligência e monitoramento compatíveis com a sua classificação.

Na qualificação e atualização do nível de risco do cliente, podem ser considerados, entre outros, os seguintes fatores:

I. Fatores cadastrais

Pessoa Física

- condição de PEP;
- representantes e procuradores;
- ocupação;
- renda;
- não residente.

Pessoa Jurídica

- atividade econômica (CNAE);
- ramo de atuação;
- natureza do negócio;
- estrutura societária;
- beneficiários finais;
- tempo de constituição;
- compatibilidade entre o perfil do negócio, o porte da empresa, os produtos contratados e a movimentação financeira esperada.
- atuação em segmentos de maior exposição ao risco de LD/FTP.

Nos casos de clientes Pessoa Jurídica, a classificação de risco também considera aspectos relacionados à estrutura societária, atividade econômica desenvolvida, ramo de atuação, tempo de constituição da empresa, beneficiários finais, localização das operações e demais informações que possam indicar maior exposição aos riscos de LD/FTP.

II. Fatores geográficos

- país de residência, domicílio, constituição ou atuação do cliente;

INTERNA RESTRITA

- relacionamento comercial ou realização de operações envolvendo países, territórios ou jurisdições classificados pelo GAFI como de alto risco ou sujeitos a monitoramento reforçado;
- relacionamento comercial ou realização de operações envolvendo países, territórios ou jurisdições sujeitos a sanções, embargos ou outras medidas restritivas impostas por organismos nacionais ou internacionais.

III. Fatores reputacionais, restritivos e de integridade

- presença em listas restritivas nacionais ou internacionais;
- existência de mídia negativa relevante;
- processos administrativos ou judiciais relacionados a crimes financeiros, corrupção, fraude ou outras atividades ilícitas.

IV. Fatores comportamentais e transacionais

- utilização de terceiros para realização de operações;
- movimentações consideradas atípicas em relação ao perfil esperado do cliente;
- recorrência de alertas gerados pelos mecanismos de monitoramento;
- operações envolvendo contrapartes ou jurisdições classificadas como de maior risco;
- outras situações identificadas pelos sistemas de monitoramento e análise que indiquem potencial exposição a riscos de LD/FTP.

A classificação de risco é revisada periodicamente ou sempre que forem identificadas alterações relevantes no perfil cadastral, comportamental ou transacional do cliente.

Para suportar a classificação e o monitoramento contínuo dos riscos de LD/FTP, o Grupo utiliza ferramentas tecnológicas especializadas, capazes de consolidar alertas cadastrais, comportamentais e transacionais, permitindo a atualização dinâmica do perfil de risco do cliente durante todo o relacionamento comercial.

Os clientes são classificados em categorias de risco Baixo, Médio, Alto e Severo, conforme critérios definidos através do Manual de KYC e Manual MSAC e devem observar os resultados da Avaliação Interna de Riscos (AIR). A classificação atribuída é utilizada

para definir a abordagem baseada em risco quanto à intensidade das medidas de monitoramento, diligência, atualização cadastral, monitoramento reforçado, escalonamento para análise especializada, eventual encerramento do relacionamento ou deliberação em instâncias de governança, conforme aplicável.

A classificação de risco atribuída ao cliente poderá ser elevada ou reduzida ao longo do relacionamento comercial em razão da identificação de novos fatores de risco, alterações cadastrais, eventos reputacionais, comportamentos transacionais ou outros elementos relevantes obtidos por meio do sistema de monitoramento cadastral e transacional, de consultas automatizadas a bases de dados e plataformas externas, bem como de análises realizadas pela área de PCF, quando aplicável.

4.2.3. Conheça seu Empregado (KYE)

Visando a proteger o Grupo 2TM de práticas de atos ilícitos, no momento da contratação dos Empregados, é adotado um conjunto de procedimentos de análise como parte do processo de seleção e monitoramento dos empregados efetivos.

Quando solicitado pela área de Pessoas e Cultura, a área de PCF realiza análises de background check para identificar possíveis ressalvas nos aspectos de integridade e idoneidade dos participantes de processos seletivos. Para todos os casos, é atribuída uma nota de risco, a partir de um dossiê gerado com informações sobre listas restritivas, mídias negativas, processos sancionadores e em tribunais, bureaus de crédito, situação de cadastro na Receita Federal e relacionamento com PEP.

Periodicamente, é realizada reavaliação do background check conforme frequência definida de acordo com o nível de risco de cada colaborador.

Adicionalmente às avaliações feitas pela área de PCF, o monitoramento de comportamentos atípicos é de responsabilidade do conjunto dos colaboradores do MB, notadamente dos gestores, conforme diretrizes dispostas em treinamentos de segurança da informação e de PLD/FTP. Assim, no monitoramento, devem ser observados:

- Alteração inusitada nos padrões de vida e de consumo sem causa aparente;
- Piora comportamental no ambiente de trabalho, como falta de cooperação, isolamento e resistência às atividades de supervisão;

- Falta de aderência às regras definidas pela empresa no que tange a segurança da informação, como acessos indevidos a informações sensíveis ou solicitações de acesso sem motivo;
- Descoberta de relações, anteriores ou não, do colaborador com concorrentes não declaradas anteriormente;
- Realização de qualquer negócio de modo diverso aos procedimentos formais do Grupo 2TM, conforme definido no Código de Ética e Conduta; e
- Fornecimento de informações, remuneradas ou não, a cliente em prejuízo do programa de PLD/FTP, ou de auxílio para estruturar ou fracionar operações, burlar limites regulamentares, operacionais entre outros.

Em qualquer situação dessa natureza, a ocorrência deve ser comunicada via Canal de Denúncias.

Os procedimentos e diretrizes de Conheça seu Empregado (KYE) são endereçados na Política de Contratação de Colaboradores.

4.2.4. Conheça seu Parceiro (KYP) e Conheça seu Fornecedor (KYS)

O Grupo 2TM adota processos para identificação, classificação de riscos LD/FTP e aceitação de parceiros e fornecedores, com a finalidade de prevenir a realização de negócios com parceiros inidôneos ou suspeitos de envolvimento em atividades ilícitas.

Para terceiros analisados e classificados com maior grau de risco, segundo a Abordagem Baseada em Riscos, serão adotados procedimentos aprofundados de diligências para avaliação e eventual encaminhamento para alçadas superiores de aprovação da relação de negócios.

As diretrizes de Conheça seu Parceiro / Fornecedor (KYP / KYS) são endereçadas na Política de Contratação de Terceiros e os procedimentos são detalhados no Manual de KYP/KYS.

4.2.5. Conheça seu Prestador de Serviços de Ativos Virtuais (KYVASP)

O Grupo 2TM adota o procedimento de Conheça seu Prestador de Serviços de Ativos Virtuais (PSAV) ou “Know Your Virtual Asset Service Provider (VASP) - KYVASP” para assegurar a integridade e conformidade às exigências aplicáveis às operações com ativos virtuais, quando aplicável.

A prática do KYVASP é conduzida em estrita observância às disposições da Resolução BCB nº 520 e nº 521, utilizando uma abordagem baseada em risco que considera fatores como a jurisdição do PSAV, existência de efetiva regulação prudencial e aspectos reputacionais.

As diretrizes detalhadas, os fluxos de identificação e os procedimentos operacionais para a condução das análises e monitoramento estão descritos e formalizados no Manual KYVASP.

4.2.6. Identificação do Beneficiário Final

O Grupo 2TM adota critérios específicos para identificação do beneficiário final, considerando:

- Participação direta ou indireta igual ou superior a 25% do capital social ou patrimônio líquido;
- Pessoa natural com influência significativa ou controle efetivo;
- Estruturas como trusts e veículos assemelhados, devendo ser identificados o instituidor (settlor), administrador (trustee), beneficiários e outros envolvidos relevantes;
- Exceções previstas em norma (companhias abertas no Brasil, instituições reguladas pelo Banco Central do Brasil, fundos não exclusivos, etc.);
- Registro e documentação comprobatória arquivada por prazo mínimo de 10 anos.

4.3. Monitoramento, Seleção, Análise e Comunicação (MSAC)

Os procedimentos utilizados para MSAC permitem a detecção e prevenção de crimes financeiros e melhor condução das atividades de KYC, sendo imprescindíveis para o gerenciamento de riscos.

4.3.1. Monitoramento, Seleção e Análise de Operações Suspeitas

O Grupo 2TM realiza o monitoramento de todas as operações realizadas pelos clientes nas plataformas do MB, por meio de regras parametrizadas que possibilitam identificar situações atípicas passíveis de encerramento da relação comercial e eventual comunicação ao COAF.

Na hipótese de suspeita de que qualquer operação desvia do seu objetivo ou que o conjunto de operações se constitui ou está relacionado a indícios de lavagem de dinheiro ou ao financiamento de terrorismo, a área de PCF será acionada para análise do risco LD/FTP do cliente e adotará as providências cabíveis, podendo inclusive, levar o caso ao Comitê de PLD/FTP.

4.3.2. Comunicação de Operações Suspeitas

Na identificação de transações suspeitas (propostas ou efetivadas) com indícios de lavagem de dinheiro ou financiamento do terrorismo, o Grupo 2TM comunicará o COAF, levando em consideração o prazo, a forma, bem como as condições previstas na legislação vigente. Isso implica o MB abster-se de fornecer aos respectivos clientes informações sobre eventuais comunicações efetuadas.

A documentação e as informações que amparam a tomada de decisão de efetuar ou não as comunicações serão formalizadas pela área de PCF, sendo repassadas em Comitê para deliberação sobre a comunicação ou não de cada caso. As análises e relatórios realizados no âmbito da investigação de operações suspeitas são estritamente confidenciais, devendo estar acessíveis aos colaboradores envolvidos na investigação e aos membros do Comitê Executivo de PLD/FTP.

Em caso de não ocorrência de transações passíveis de comunicação ao COAF, a área de PCF realizará a “Declaração Negativa” na periodicidade e forma definidas.

4.4. Especial Atenção

4.4.1. Jurisdições com Deficiências em PLD/FTP (GAFI)

O Grupo 2TM deve acompanhar continuamente as divulgações realizadas pelo GAFI sobre as atualizações das jurisdições não cooperantes ou que possuem controles deficientes no combate à lavagem de dinheiro e ao financiamento do terrorismo e a proliferação de armas de destruição em massa, com o intuito de adequar os seus controles internos.

4.4.2. Cumprimento de Sanções Internacionais

O Grupo cumpre de forma imediata e sem aviso prévio as medidas de indisponibilidade de ativos impostas por resoluções do Conselho de Segurança das Nações Unidas (CSNU), conforme previsto na Lei nº 13.810/2019. As áreas responsáveis devem:

- Monitorar diariamente as listas de sanções do CSNU;
- Adotar controles internos para bloqueio automático de ativos ou transações vinculadas a pessoas físicas, jurídicas ou entidades sancionadas;
- Comunicar imediatamente às autoridades competentes os bloqueios realizados ou eventuais falhas justificadas;
- Levantar imediatamente a indisponibilidade em caso de exclusão da lista.

4.4.3. Relacionamentos Vedados

O Grupo 2TM, engajado nos processos de PLD/FTP, veda alguns tipos de relacionamentos com colaboradores, clientes, parceiros e fornecedores nas seguintes condições:

- Localizados em países sujeitos a sanções e embargos impostos por organismos internacionais (ex: ONU, OFAC, UE), assim como pessoas físicas ou jurídicas que constem em listas de sanções internacionais, independentemente do local de sua constituição ou localização (ex: SDN List - "Specially Designated Nationals" ou "SDNs.", listas oficiais da ONU, União Européia);
- Relacionados a atividades terroristas, nos termos dos atos normativos vigentes;

- Residentes, domiciliados ou sediados em países, territórios e jurisdições consideradas não cooperantes pelo GAFI;
- Envolvidos com atividades proibidas por lei ou de natureza delitiva, especialmente as relacionadas ao narcotráfico ou crime organizado;
- Relacionados a atividades de comercialização de armas de fogo, munições, explosivos ou materiais equivalentes;
- Que realizam transações de criptoativos com carteiras identificadas como pertencentes a pessoas ou jurisdições sancionadas, mediante a sua identificação por meio de alertas de ferramenta de monitoramento transacional on-chain (alertas diretos);
- Relacionados a pornografia, prostituição, serviços de acompanhante ou relacionados; e
- Empresas e/ou bancos de fachadas, constituídos em local sem presença física e/ou que não se encontre integrado a nenhum grupo econômico regulamentado.

4.5. Monitoramento de Organizações Sem Fins Lucrativos

O Grupo realiza diligência reforçada para organizações sem fins lucrativos, com atenção especial à estrutura, fontes de recursos e finalidade social. Tais categorias são avaliadas com base na AIR e nos critérios da abordagem baseada em risco.

4.6. Práticas Específicas para Ativos Tokenizados

No contexto de ativos digitais tokenizados, o Grupo adota medidas adicionais de PLD/FTP, considerando os riscos específicos da estrutura via blockchain. As práticas abaixo visam garantir a rastreabilidade, integridade e conformidade dos processos de tokenização:

4.6.1. Validação de Contratos Inteligentes

Antes do lançamento de qualquer ativo digital por meio de smart contracts, deve ser realizada uma due diligence técnica e de segurança para garantir que os contratos sejam auditáveis, tenham rastreabilidade integrada aos fluxos de recursos e não contenham vulnerabilidades ou funcionalidades que permitam comportamentos indesejados ou ilícitos.

4.6.2. Análise de Transações On-Chain

Devem ser utilizadas soluções de blockchain analytics para monitorar e analisar transações relacionadas aos ativos tokenizados, incluindo:

- Rastreo da origem dos recursos cripto aportados nas ofertas;
- Identificação de carteiras vinculadas a sanções internacionais, lavagem de dinheiro, golpes ou atividades ilícitas, conforme listas e alertas fornecidos por ferramentas como Chainalysis ou equivalentes;
- Integração desses alertas ao sistema de MSAC (Monitoramento, Seleção, Análise e Comunicação).

4.6.3. Due Diligence sobre Originadores

Nas operações de tokenização de recebíveis ou contratos, deve ser conduzida análise aprofundada sobre o originador dos direitos creditórios, abrangendo:

- Histórico de inadimplência;
- Ações judiciais ou sanções;
- Análise de capacidade operacional e financeira;
- Avaliação da regularidade dos documentos cedidos e mecanismos de compensação.

4.6.4. Validação sobre Ativos Lastreados

Os ativos que servem de lastro para os tokens emitidos devem ser validados, com verificação documental e financeira. Essa prática visa garantir que os direitos creditórios existam, sejam válidos, líquidos e estejam devidamente formalizados, mitigando o risco de emissão fraudulenta ou lastro inexistente.

5. Treinamento e Conscientização

O treinamento periódico sobre o Programa de PLD/FTP ocorre de acordo com a programação definida anualmente pela área de PCF e deverá abordar, sob os pontos de vista teórico e prático:

- Conceitos e exemplos sobre PLD/FTP, bem como seus riscos, tanto para o Grupo 2TM quanto para os seus colaboradores;
- As políticas e os processos do Grupo, bem como os requerimentos legais relacionados;
- Os procedimentos a serem adotados diante de transações suspeitas; e
- Divulgação dos canais de comunicação para reporte de situações suspeitas.

Não obstante, o Grupo 2TM poderá promover ações de conscientização para todos os colaboradores e terceiros, sempre que entender necessário. As ações de treinamento e conscientização, bem como os controles decorrentes, são armazenados e geridos pela área de PCF.

As operações desenvolvidas no escopo de atividades da área de PCF observam as disposições da Política de Segurança da Informação da 2TM, no que se refere à segurança da informação, gestão de acessos, segregação de funções, proteção de dados, suporte nos processos de “KYs” e cumprimento das disposições da LGPD.

6. Canal de Denúncias

Todos os Colaboradores e líderes de negócio têm a responsabilidade de ajudar a detectar, prevenir e denunciar todas as não conformidades ou suspeitas em relação a esta Política, reportando eventuais condutas suspeitas ao Canal de Denúncias, que garante a confidencialidade, segurança, imparcialidade e, caso o denunciante assim solicite, o anonimato. Telefone: 0800 800 6262

Website: www.contatoseguro.com.br/pt/2tm/

Os nossos ouvidores estão disponíveis 24 horas por dia, 7 dias por semana, 365 dias por ano. Fique tranquilo pois, em caso de anonimato, nem mesmo o Comitê de Ética e Conduta terá acesso à sua identificação.

A 2TM proíbe a retaliação contra qualquer pessoa que denuncie, participe ou colabore com qualquer investigação. Se você acredita que está sofrendo retaliações, faça uma nova denúncia em nosso canal.

7. Penalidades

O descumprimento das disposições aqui previstas sujeita os Colaboradores do Grupo 2TM às medidas disciplinares e legais cabíveis.

A negligência e a falha voluntária são também consideradas descumprimento desta Política, sendo passíveis de aplicação de medidas disciplinares.

8. Disposições Finais

Esta Política entra em vigor a partir da data de sua publicação e deve ser revisada periodicamente.

Quaisquer dúvidas, esclarecimentos ou exceções sobre a aplicação da Política deverão ser enviadas para a área de PLD/FTP.

9. Referências

- Lei 9.613/98
- Lei 12.683/2012
- Circular BCB nº 3.978/2020
- Resolução BCB nº 520/2025
- Resolução BCB nº 521/2025
- Resolução CVM nº 50/2021
- Guia ANBIMA de PLD/FTP
- Código de Ética e Conduta
- Política de Contratação de Terceiros
- Política de Cadastro

10. Controle de Versões

Data	Versão	Tipo de Informação	Alterações	Aprovador (es)
08/2021	1.0	Interno	Trata-se de um novo documento	Diretoria Executiva de Compliance
08/2023	2.0	Interno	Atualização do processo e de algumas definições	Comitê de Diretoria
11/2024	3.0	Interno	Alterações em papéis e responsabilidades e diretrizes. Inclusão do anexo II.	Comitê de Diretoria
05/2025	4.0	Interno	Inclusão de diretrizes sobre AIR, cumprimento de sanções, monitoramento de ONGs e práticas específicas para ativos tokenizados.	Comitê de Diretoria
08/2026	5.0	Interno	Adequação das	Comitê de Diretoria

			responsabilidades atribuídas à estrutura de Prevenção a Crimes Financeiros; ampliação dos critérios de classificação de riscos; e inclusão de diretrizes para o processo KYVASP.	
--	--	--	--	--

Anexo I - Definições

Definições Administração Pública ou Poder Público: Administração pública, nacional ou estrangeira, por meio de empresas públicas ou controladas pelo governo, sociedade de economia mista, fundações públicas, bem como empresas prestadoras de serviços contratadas ou conveniadas para execução de atividade objeto de concessão pela administração pública. Considera-se administração pública estrangeira os órgãos, entidades estatais ou representações diplomáticas de país estrangeiro, bem como pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro.

COAF: Conselho de Controle de Atividades Financeiras.

GAFI: Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo.

Lavagem de Dinheiro: ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. A lavagem de dinheiro é um processo pelo qual o criminoso transforma ganhos provenientes de atividades ilegais e da prática de crimes em ativos com uma origem aparentemente lícita.

Terrorismo: prática realizada 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.

Representante, Familiar ou Estreito Colaborador de PEP's

Considera-se:

- Familiar: os parentes, na linha reta ou colateral, até o segundo grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada; e
- Estreito colaborador: pessoa natural conhecida por ter qualquer tipo de estreita



relação com PEP, inclusive por: (i) ter participação conjunta em pessoa jurídica de direito privado; (ii) figurar como mandatária, ainda que por instrumento particular da pessoa mencionada no tópico anterior; (iii) ter participação conjunta em arranjos sem personalidade jurídica; e (iv) ter o controle de pessoas jurídicas ou de arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de PEP.

Anexo II - Listas Restritivas (“Listas de Sanções”)

As listas de sanções são emitidas por entidades nacionais e internacionais, contendo a indicação de pessoas sujeitas a sanções econômicas, comerciais ou políticas, em resposta a comportamentos / atividades ilícitas. A consulta a essas listas auxilia na mitigação da exposição de empresas a contrapartes, incluindo clientes, parceiros e funcionários, que possuam relação com atividades de lavagem de dinheiro e financiamento ao terrorismo e armas de destruição em massa.

O Grupo 2TM, no âmbito de suas funções de identificação, monitoramento e tratamento de pessoas suspeitas, realiza verificações diárias nas principais listas restritivas disponíveis, com destaque para as listas abaixo:

Internacionais

- Office of Foreign Assets Control - OFAC (Estados Unidos da América)
- Conselho de Segurança das Nações Unidas CSNU
- Lista de sanções da União Europeia
- Bureau of Industry and Security - BIS (Estados Unidos da América)
- Office of Financial Sanctions Implementation - OFSI / Cayman Islands Monetary Authority - CIMA (Reino Unido)
- Financial Crimes Enforcement Network - FINCEN Patriot Act Section 311 Sanctions List (Estados Unidos da América)
- Office of the Superintendent of Financial Institutions - OSFI Sanctions List (Canada)
- Department of Foreign Affairs and Trade - DFAT Sanctions List (Austrália)
- Federal Bureau of Investigation - FBI Fugitives List (Estados Unidos da América)
- Lista de procurados da Interpol
- State Secretariat for Economic Affairs - SECO (Suíça)

Nacionais

- Lista de Inidôneos / Suspensos (CGU)
- Listas da Comissão de Valores Mobiliários (CVM)
- Lista de Inabilitados do Bacen
- Cadastro Nacional de Condenações por Ato de Improbidade Administrativa e Inelegibilidade, Conselho Nacional de Justiça -CNJ
- Listas TCU de inidôneos / inabilitados / contas irregulares
- Lista de Processos Administrativos Sancionadores - PAS COAF
- Lista de Acordos de Leniência - Portal da Transparência
- Processos Sancionadores da BSM
- Cadastro de Expulsões da Administração Federal - CEAF
- Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas CEPIM
- Cadastro Nacional de Empresas Punidas - CNEP

Nacionais - Socioambientais

- Áreas embargadas pelo IBAMA
- Lista Suja do Trabalho Escravo, Ministério do Trabalho e Emprego - MTE
- Lista de Desmatamento Ilegal - LDI Estado do Pará
- Autos de Infração - Instituto de Proteção Ambiental do Amazonas - IPAAM
- Autos de Infração - Secretaria do Meio Ambiente e Recursos Hídricos do Governo do Piauí (SEMARH-PI)
- Autos de Infração Ambiental, Julgamentos Autos de Infração e Áreas Embargadas da Secretaria de Estado de Meio Ambiente do Mato Grosso (SEMA-MT)



- Autos de Infração da Secretaria de Estado de Meio Ambiente e Desenvolvimento Sustentável do Governo do Goiás (SEMAD-GO)
- Autos de Infração do Instituto Natureza do Tocantins - Naturatins
- Lista de Infrações Ambientais monitoradas pelo Instituto Chico Mendes - ICMBIO