

TÍTULO: PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PLD-FTP)

ÍNDICE

1. OBJETIVO	2
2. APROVAÇÃO E VIGÊNCIA.....	3
3. ABRANGÊNCIA.....	4
4. BASE NORMATIVA.....	5
5. DEFINIÇÕES (GLOSSÁRIO).....	8
6. DECLARAÇÃO DO BMG SOBRE PLD-FTP E PRINCÍPIOS GERAIS.....	13
7. ABORDAGEM BASEADA NO RISCO (ABR), AVALIAÇÃO INTERNA DE RISCO (AIR) E AVALIAÇÃO DE EFETIVIDADE (AE).....	15
8. PROGRAMA DE PLD-FTP DO BANCO BMG	17
9. RESPONSABILIDADES	21
10. PROMOÇÃO DA CULTURA ORGANIZACIONAL, ACULTURAMENTO E TREINAMENTOS	29

1. OBJETIVO

Esta Política tem como objetivo definir o conjunto de princípios, diretrizes e responsabilidades que norteiam as atividades de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD-FTP) do Grupo Financeiro Bmg e do *Bmg Bank (Cayman) Limited* (doravante “Bmg”), considerando-se a natureza e a complexidade da Instituição e de suas operações, transações, produtos e serviços, canais de distribuição, tecnologias, atividades e clientes, assegurando que:

- O Bmg esteja em conformidade com as leis e regulamentos vigentes relacionados às atribuições da área de PLD-FTP, reduzindo os riscos de exposição negativa de imagem e/ou de aplicações de multas e demais sanções por parte dos órgãos reguladores;
- Todas as áreas e colaboradores compreendam claramente o papel, objetivo, funções e responsabilidades de PLD-FTP do Bmg;
- Todas as áreas e colaboradores do Bmg compreendam seus deveres e responsabilidades no entendimento e cumprimento das suas responsabilidades de PLD-FTP;
- Estejam formalizados todos os elementos necessários para a efetiva governança e garantia da qualidade dos procedimentos de PLD-FTP; e
- Todas as ações necessárias sejam devidamente implementadas e monitoradas, de forma a mitigar o risco de utilização da instituição para os crimes de lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

2. APROVAÇÃO E VIGÊNCIA

A presente Política foi aprovada pelo Conselho de Administração (CONAD) do Bmg e, a partir da aprovação, tem vigência de 1 (um) ano.

3. ABRANGÊNCIA

Esta Política abrange todas as áreas e colaboradores do Bmg, de todos os níveis hierárquicos, e inclusive os parceiros, prestadores de serviços e demais terceiros que estejam exercendo atividades em nome e/ou para o Bmg.

4. BASE NORMATIVA

- Diretrizes e Recomendações do Grupo de Ação Financeira Internacional (GAFI), órgão intergovernamental responsável por liderar os esforços normativos e práticos globais sobre PLD-FTP;
- Lei nº. 9.613, de 3 de março de 1998, que “dispõe sobre os crimes de ‘lavagem’ ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências”;
- *Anti-Money Laundering Regulations (AMLR)* das Ilhas Cayman, de acordo com a revisão de 2023;
- Lei nº. 13.260, de 16 de março de 2016, que “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 nº. 13.810, de 8 de março de 2019, que “dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados; e revoga a Lei nº 13.170, de 16 de outubro de 2015”;
- Decreto nº. 7.722, de 20 de abril de 2012, relativo à prevenção do financiamento da proliferação de armas de destruição em massa e que obrigou as autoridades brasileiras, no âmbito de suas respectivas atribuições, ao cumprimento do disposto nas Resoluções nº. 1977 (2011), adotada pelo Conselho de Segurança das Nações Unidas em 20 de abril de 2011, e nº. 1540 (2004), adotada por aquele mesmo órgão em 28 de abril de 2004;

- Circular nº. 3.978, de 23 de janeiro de 2020, do Banco Central do Brasil (BCB), que “dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº. 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº. 13.260, de 16 de março de 2016”;
- Carta Circular nº. 4.001, de 29 de janeiro de 2020, do Banco Central do Brasil (BCB), que “divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes de “lavagem” ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento ao terrorismo, previstos na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf);
- Resolução nº. 44, de 24 de novembro de 2020, do Banco Central do Brasil (BCB), que estabelece procedimentos para a execução pelas instituições autorizadas a funcionar pelo Banco Central do Brasil das medidas determinadas pela Lei nº 13.810, de 8 de março de 2019, que dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados;
- Resolução nº. 50, de 31 de agosto de 2021, da Comissão de Valores Mobiliários (CVM), que “dispõe sobre a prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa – PLD/FTP no âmbito do mercado de valores mobiliários [...]”;
- Circular nº. 612, de 18 de agosto de 2020, da Superintendência de Seguros Privados (SUSEP), que “dispõe sobre a política, os

procedimentos e os controles internos destinados especificamente à prevenção e combate aos crimes de ‘lavagem’ ou ocultação de bens, direitos e valores, ou aos crimes que com eles possam relacionar-se, bem como à prevenção e coibição do financiamento do terrorismo”;

- Atos e Regulações da *CIMA – Cayman Islands Monetary Authority* (Autoridade Monetária das Ilhas Cayman).
- Normativo Sarb 11/2013, da Febraban, que estabelece diretrizes que consolidam as melhores práticas, nacionais e internacionais de prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo a serem observadas pelas Signatárias, em consonância com as normas e aos mecanismos de controle existentes.

5. DEFINIÇÕES (GLOSSÁRIO)

ABR – Abordagem Baseada em Risco: É fruto da recomendação nº. 1 do GAFI, onde está estabelecido que, com base nessa avaliação, os países devem aplicar uma abordagem baseada em risco para garantir que as medidas de PLD-FTP sejam proporcionais aos riscos identificados. A metodologia da ABR também é exigida pelos reguladores brasileiros (a exemplo do § 3º do art. 10 da Circular nº. 3.978/2020 do BCB), os quais demandam que as instituições adotem controles de gerenciamento e de mitigação reforçados para as situações de maior risco e tenham controles simplificados para as situações de menor risco.

AMLCO – Anti-money Laundering Compliance Officer: Termo em inglês que se aplicaria ao Diretor de Conformidade de PLD-FTP na Instituição.

AIR – Avaliação Interna de Riscos: As instituições devem realizar Avaliação Interna de Risco com o objetivo de identificar e mensurar o risco de utilização de seus produtos e serviços na prática de lavagem de dinheiro, financiamento do terrorismo e da proliferação de armas de destruição em massa, considerando, no mínimo, os perfis de risco dos clientes; da instituição, incluindo o modelo de negócio e a área geográfica de atuação; das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e das 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 instituição.

BCB – Banco Central do Brasil: Órgão normatizador e supervisor, inclusive de PLD-FTP, das instituições financeiras. Como regulador, emite normativos e instruções aos entes do Sistema Financeiro Nacional cujo funcionamento é autorizado pelo órgão. Como supervisor, verifica o grau de aderência às normas em seus entes supervisionados, bem como seu efetivo cumprimento.

CIMA – Cayman Islands Monetary Authority: Autoridade Monetária das Ilhas Cayman.

COAF – Conselho de Controle de Atividades Financeiras: Unidade de Inteligência Financeira do Brasil, cuja missão é produzir Inteligência Financeira e promover a proteção dos setores econômicos contra a lavagem de dinheiro, o financiamento ao terrorismo e o financiamento da proliferação de armas de destruição em massa. Dentre suas funções está a de receber as comunicações de operações suspeitas e em espécie oriundas dos diversos setores econômicos.

CONAD: Conselho de Administração do Bmg.

CVM – Comissão de Valores Mobiliários: Órgão cujo objetivo é fiscalizar, normatizar, disciplinar e desenvolver o mercado de valores mobiliários no Brasil, inclusive no que diz respeito a PLD-FTP.

DDC – Devida Diligência sobre o Cliente: Decorre da Recomendação nº. 10 do GAFI, caracterizando-se por um conjunto de ações que visam a completa identificação e validação do cliente, seu perfil de negócios e sua capacidade financeira.

DMLRO – Deputy Money Laundering Reporting Officer: Termo em inglês que se aplicaria ao Adjunto do Responsável por PLD-FTP na instituição.

FRA – Financial Reporting Authority: Unidade de Inteligência Financeira das Ilhas Cayman.

FEBRABAN – Federação Brasileira dos Bancos: Principal entidade representativa dos bancos brasileiros.

GAFI – Grupo de Ação Financeira Internacional: Organização intergovernamental cujo propósito é desenvolver e promover políticas nacionais e internacionais de prevenção e combate à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa. Para cumprir seus objetivos, o GAFI edita as chamadas Recomendações, que devem ser cumpridas pelos diversos países, sob pena de sua inclusão na lista pública de países com deficiências em PLD-FTP, o que pode acarretar a perda de investimentos e sancionamentos às jurisdições não cooperantes.

KYC – Know your Customer: Termo em inglês que significa “Conheça seu Cliente”.

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

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

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

LD-FTP – Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa: No Brasil, o crime da lavagem de dinheiro (“LD”) foi tipificado pela Lei nº. 9.613/1998 e, posteriormente, com a publicação da Lei 12.683/12, foi ampliada a abrangência da legislação penal que configurou o crime como sendo a dissimulação e ocultação da origem de recursos provenientes de qualquer infração penal. Desse modo, a LD é o processo pelo qual o criminoso busca transformar recursos ganhos por meio de atividades ilegais em ativos com uma origem aparentemente lícita. O financiamento ao terrorismo (“FT”), por sua vez, consiste no processo

de armazenamento, recebimento ou fornecimento de recursos a serem utilizados, no todo ou em parte, em atividades terroristas ou outras atividades de indivíduos e organizações terroristas. Tais recursos podem ser oriundos das atividades de outras organizações criminosas envolvidas com o tráfico de drogas, pessoas, armas e munições e com o contrabando, entretanto, em alguns casos, os terroristas utilizam recursos obtidos de forma legal. O financiamento da proliferação de armas de destruição em massa (“P”) caracteriza-se como a utilização de fundos ou serviços financeiros para a fabricação, aquisição, posse, desenvolvimento, exportação, transbordo, corretagem, transporte, transferência, armazenamento ou uso de armas nucleares, químicas ou biológicas e seus meios de entrega e materiais relacionados (incluindo tecnologias e bens de dupla utilização utilizados para fins não legítimos).

MLRO – Money Laundering Reporting Officer: Termo em inglês que se aplicaria ao Responsável por PLD-FTP na instituição.

MSAC: Monitoramento, Seleção, Análise e Comunicação de Operações com Índícios de Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

OFAC – Office of Foreign Assets Control: O Escritório de Controle de Ativos Estrangeiros do Departamento do Tesouro dos Estados Unidos da América (EUA) administra e aplica sanções econômicas e comerciais com base na política externa dos EUA e metas de segurança nacional contra países e regimes estrangeiros designados como terroristas, narcotraficantes internacionais e envolvidos em atividades relacionadas à proliferação de armas de destruição em massa e outras ameaças à segurança nacional, política externa ou economia dos Estados Unidos. O OFAC atua sob os poderes de emergência nacionais presidenciais, bem como com a autoridade concedida por legislação específica, para impor controles às transações e congelar ativos sob jurisdição dos EUA.

ONU – Organização das Nações Unidas: É uma organização intergovernamental criada para manter a paz e a segurança internacionais; desenvolver relações amistosas entre as nações; realizar a cooperação internacional para resolver os problemas mundiais de caráter econômico, social, cultural e humanitário, promovendo o respeito aos direitos humanos e às liberdades fundamentais; e para ser um centro destinado a harmonizar a ação dos povos para a consecução desses objetivos comuns.

PEP – Pessoas Expostas Politicamente: De modo geral, considera-se PEP pessoas que desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, no Brasil ou em países, territórios e dependências estrangeiros, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

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

SAR – Suspicious Activity Report: Termo em inglês para o Relatório de Atividades Suspeitas.

SFN: Sistema Financeiro Nacional.

SUSEP – Superintendência de Seguros Privados: Órgão responsável pelo controle e fiscalização, inclusive de PLD-FTP, dos mercados de seguros, previdência privada aberta, capitalização e resseguros no Brasil.

UE – União Europeia: Bloco econômico e político formado por países europeus.

6. DECLARAÇÃO DO BMG SOBRE PLD-FTP E PRINCÍPIOS GERAIS

As práticas de LD-FTP, como forma de abastecimento ao crime organizado e às organizações terroristas, têm levado países de todo o mundo a adotarem medidas de combate a tais crimes. E as instituições que compõem os sistemas financeiros desses países, por meio de seus Bancos Centrais e demais organismos, têm estabelecido ações direcionadas à prevenção desses ilícitos.

Dentre estas ações, destacam-se aquelas que visam o aprofundamento do conhecimento dos clientes dessas instituições a fim de facilitar a identificação de recursos que possam ter sua origem e/ou o seu destino em atividades criminosas.

Outras ações visam à consolidação e o compartilhamento das informações relativas a indícios de LD-FTP, com o objetivo de tornar sem efeito uma das principais características desses crimes: a diversificação de operações e instituições utilizadas.

Em linha com os esforços empreendidos por organismos nacionais e internacionais, o Bmg entende que a melhor forma de contribuir para a prevenção a esses crimes é estabelecer políticas, normas e procedimentos validados pelo Diretor responsável por PLD-FTP e aprovados pelo Fórum Executivo de Aceitação de Clientes e PLD-FTP que impeçam que seus produtos e serviços sejam utilizados para tais atividades e, ao mesmo tempo, visem à identificação, análise e comunicação às autoridades competentes de quaisquer operações que possam representar indícios de LD-FTP.

Desta forma, a Administração do Bmg estabelece e torna obrigatório o cumprimento de todas as diretrizes voltadas a PLD-FTP, com base nos seguintes Princípios Gerais:

- Aderência e conformidade com as normas internacionais e legislações e regulações nacionais, e atualização constante em referência às melhores práticas;
- Qualidade cadastral de clientes, parceiros, prestadores de serviços e demais terceiros que se relacionem com o Bmg;
- Adequação do conhecimento de clientes (*KYC*), colaboradores (*KYE*), parceiros e prestadores de serviços terceirizados (*KYPI/KYS*);
- Efetivo monitoramento, seleção e análise de operações consideradas atípicas e suspeitas;
- Realização de comunicações ao COAF com qualidade e tempestividade, preservando o sigilo das comunicações; e
- Governança para manutenção e evolução da maturidade e qualidade do programa de PLD-FTP.

7. ABORDAGEM BASEADA NO RISCO (ABR), AVALIAÇÃO INTERNA DE RISCO (AIR) E AVALIAÇÃO DE EFETIVIDADE (AE)

De acordo com o GAFI, a Abordagem Baseada no Risco (ABR) aplicada à PLD-FTP demanda que os países, as autoridades competentes e as instituições financeiras identifiquem, avaliem e entendam os riscos de LD-FTP aos quais estão expostas, e tomem medidas proporcionais de PLD-FTP a fim de mitigá-los de maneira efetiva. Deste modo, a compreensão do risco e avaliação dos seus impactos serão a base de aplicação das medidas de PLD-FTP, as quais deverão ser reforçadas para as situações de maior risco e poderão ser simplificadas para as situações de menor risco.

O GAFI também dispõe que, para o setor bancário, a ABR se aplicará à forma como a instituição deverá alocar seus recursos destinados à conformidade, organizar seus controles e estruturas internas e implementar políticas e procedimentos para impedir, detectar e mitigar o risco de situações de LD-FTP, inclusive a nível de conglomerado.

Isto considerado, enquanto a ABR se apresenta como a metodologia de identificação, avaliação e compreensão de riscos de LD-FTP para a correta alocação de controles, a Avaliação Interna de Risco (AIR) é o instrumento pelo qual a instituição irá identificar e mensurar o risco concreto de utilização de seus produtos e serviços na prática de LD-FTP, e o avaliará quanto à sua probabilidade de ocorrência e à magnitude dos impactos financeiro, jurídico, reputacional e socioambiental, definindo-se, sequencialmente, as medidas mitigatórias proporcionais e apropriadas.

A AIR considerará, no mínimo: os perfis de risco dos clientes; da instituição, incluindo o modelo de negócio e a área geográfica de atuação; das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a

utilização de novas tecnologias; e das atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados.

A documentação e formalização da AIR, atualizada a cada 2 (dois) anos e/ou quando ocorrerem alterações significativas nos perfis de risco, constitui-se como o principal roteiro para a aplicação da ABR na prática de PLD-FTP da instituição.

A Avaliação de Efetividade (AE), por sua vez, é um relatório elaborado anualmente pela instituição que avalia a efetividade da sua política, dos seus procedimentos e dos seus controles internos de PLD-FTP, e que detalhará a metodologia, os testes aplicados e os resultados da avaliação, contemplando, no mínimo: os procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais; os procedimentos de monitoramento, seleção, análise e comunicação ao COAF, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas; a governança da Política de PLD-FTP; as medidas de desenvolvimento da cultura organizacional voltadas à PLD-FTP; os programas de capacitação periódica de pessoal; os procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados; e as ações de regularização.

Desta forma, a AE divulgará o resultado da efetividade da ABR na instituição com base nos dados e informações disponíveis na AIR.

8. PROGRAMA DE PLD-FTP DO BANCO BMG

O Programa de PLD-FTP do Bmg é aderente às normas internacionais e legislações e regulações nacionais dos países nos quais atua, de modo que prevê uma série de procedimentos para a efetiva consecução das atividades de prevenção aos crimes de LD-FTP.

Conheça Seu Cliente (*Know Your Customer*): Trata-se de um conjunto de regras fundamentais para o conhecimento dos riscos de LD-FTP aos quais a instituição está exposta e para a proteção da utilização dos produtos e serviços da instituição para a prática de ilícitos. Por esta razão, o BMG possui documento próprio e específico (Manual de Conheça seu Cliente – *KYC*) que dispõe sobre: A base normativa dos procedimentos de Conheça Seu Cliente; Regras de cadastramento de clientes; Etapas do processo de Conheça Seu Cliente; Responsabilidade pelo Processo de Atualização Cadastral e Prazos; Clientes de Especial Atenção e Clientes Impedidos e Restritos; Identificação de Beneficiário Final; Pessoas Expostas Politicamente (PEPs) e as questões relativas ao Início ou Manutenção de Relacionamento com PEPs; Programa de Sanções; Encerramento de Relações; Arquivamento de Informações; e Governança, entre outros assuntos relevantes.

Conheça seu Colaborador (*Know Your Employee*): Trata-se de um conjunto de regras destinadas a cumprir com o dever de cautela da instituição relativo à prevenção de possíveis desvios (operacionais e estratégicos, voluntários ou não) e cooptações de colaboradores que possam operacionalizar ou facilitar situações de LD-FTP. Por esta razão, o Bmg possui documento próprio e específico (Manual de Conheça Seu Colaborador – *KYE*) que dispõe sobre: A base normativa dos procedimentos de Conheça Seu Colaborador; Responsabilidade da área de recursos humanos; Procedimentos de Recrutamento, Seleção e Contratação; Atualização de Dados Cadastrais; Procedimentos de PLD-FTP; Classificação de Risco de Colaboradores; Papéis

e Responsabilidades das áreas; Contratações Diferenciadas; Divulgações de Políticas; Atualização dos Cadastros dos Funcionários; Acompanhamento da Situação Socioeconômica; Monitoramento de Transações; Programa de Capacitação; Encerramento do Vínculo Empregatício; Arquivamento de Informações; Canal de Denúncias e; Governança, entre outros assuntos relevantes.

Conheça Seu Fornecedor, Parceiro e Prestador de Serviço Terceirizado (*Know Your Partner e Know Your Supplier*): Considerando o volume, extensão e complexidade das atividades necessárias para o funcionamento da instituição, é comum o estabelecimento de parcerias e contratação de prestadores de serviços a fim de terceirizar algumas demandas. Deste modo, é importante identificar e compreender quais são as atividades que representam maior risco de alteração, anulação e/ou burla de controles de PLD-FTP. Por esta razão, o Bmg possui documento próprio e específico (Manual de Conheça Seu Fornecedor, Parceiro e Prestador de Serviço – *KYPI/KYS*) que dispõe sobre: A base normativa dos procedimentos de Conheça Seu Fornecedor, Parceiro e Prestador de Serviço; Responsabilidade da Área de Compras; Atualização Cadastral; Procedimentos de PLD-FTP; Classificação de Risco; Adesão dos Fornecedores, Parceiros e Prestadores às Políticas do Bmg; Monitoramento; Beneficiários Finas; Impedimento e Restrições; Encerramento da Relação de Negócio; Arquivamento de Informações; Canal de Denúncias e; Governança, entre outros assuntos relevantes.

Monitoramento, Seleção, Análise e Comunicação de Operações com Índícios de LD-FTP: É obrigação da instituição financeira o monitoramento de todas as operações que envolvem seus produtos e serviços, a seleção inteligente e análise depurada daquelas operações que apresentem alguma suspeita e/ou atipicidade relativa a LD-FTP, e a comunicação ao COAF das operações em que se confirmar a suspeita de LD-FTP ou atipicidade injustificada, e a manutenção do sigilo sobre os procedimentos realizados. Por

esta razão, o Bmg possui documento próprio e específico (Manual de Monitoramento, Seleção, Análise e Comunicação de Operações com indícios de Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa – Manual MSAC) que dispõe sobre: A base normativa dos procedimentos de MSAC; *Onboarding* de clientes; Procedimentos de *KYE* e *KYPIKYS*; Dossiês de PLD-FTP; Sistema de Monitoramento, Seleção e Análise; Monitoramento de Operações; Análise de Operações e Situações Suspeitas; ABR; Calibragem de Regras; Papéis e Responsabilidades; Comunicações ao COAF; Comunicações de Operações em Espécie; Comunicação de Não Ocorrência; *Quality Assurance* e; Governança, entre outros assuntos relevantes.

Sanções: Atento à importante questão de tais instrumentos de natureza diplomática e econômica, os quais são utilizados por instituições e países para atuar em situações, inclusive, de PLD-FTP, o BMG adota medidas capazes de detectar e obstar propostas e operações vinculadas com países, entidades e pessoas sancionadas, de modo que possui procedimentos adequados para dar cumprimento às sanções internacionais e contramedidas financeiras, tais como *screening* de Listas de Sanções; fator de risco específico integrado na Avaliação Interna de Risco (AIR) da instituição, no *KYC* e nos procedimentos de monitoramento, seleção e análise de operações; e medidas para bloqueio de ativos em conformidade com a legislação e regulação vigentes.

Novos Produtos e Serviços e Utilização de Novas Tecnologias: Todos os novos produtos e serviços do Bmg, bem como os produtos e serviços que tenham sido alterados de forma relevante, devem ser encaminhados ao Comitê de Produtos e avaliados e analisados pela área de PLD-FTP previamente à sua efetiva disponibilização ao público consumidor, a fim de se identificar os eventuais riscos de LD-FTP e estabelecer as medidas mitigatórias compatíveis. Pelo mesmo motivo, a área de PLD-FTP do BMG também deverá ser acionada para avaliação e análise de utilização de novas tecnologias nos produtos e

serviços da instituição, sobretudo quando as inovações prejudiquem o *KYC* ou a devida diligência.

Canal de Denúncias: Visando assegurar o recebimento de denúncias de indícios de ilicitude relacionados às atividades do Bmg, está disponível o Canal de Denúncias, que tem como objetivo receber, apurar e solucionar demandas, sejam estas de colaboradores, clientes, parceiros, fornecedores e demais terceiros, atentando para indícios de ilicitude de qualquer natureza e para o descumprimento de dispositivos legais, regulatórias e/ou normativos internos aplicáveis à instituição. É garantido ao denunciante os direitos ao anonimato e à não retaliação.

A instituição repudia e não tolera violações ao seu Programa de PLD-FTP, bem como práticas de corrupção, suborno, extorsão, propina, fraude, LD-FTP e quaisquer outros ilícitos.

O Bmg submete periodicamente o seu Programa de PLD-FTP à avaliação de Auditoria Independente.

9. RESPONSABILIDADES

O gerenciamento dos riscos relacionados aos eventos de LD-FTP do Bmg é parte integrante do processo de gestão dos negócios da instituição e compreende a identificação, avaliação, mensuração, mitigação e controle desses riscos.

A gestão dos riscos de LD-FTP é realizada de forma conservadora, respeitando as alçadas e os limites e critérios definidos, buscando sempre proteger a imagem do BMG, seus valores e princípios, contribuindo assim para a sustentabilidade dos negócios.

O Bmg divulga continuamente os conceitos, princípios, diretrizes e responsabilidades relacionadas a PLD-FTP, visando o acultramento de seus administradores, colaboradores, parceiros comerciais e prestadores de serviços terceirizados, e utiliza modelos, metodologias, ferramentas e sistemas em linha com o nível de complexidade dos seus negócios, produtos e serviços.

A observância e cumprimento desta Política e da legislação, regulações e demais normas de PLD-FTP é de responsabilidade de todos os colaboradores do Bmg e dos terceiros que com a Instituição se relacionem. Sem prejuízo desta premissa, cabe a determinadas áreas e funções certas responsabilidades específicas com relação ao programa de PLD-FTP do Bmg.

Conselho de Administração (CONAD): Definir as diretrizes gerais para o gerenciamento de riscos relacionados à LD-FTP do Bmg, fazendo parte de suas atribuições a aprovação da Política de PLD-FTP da instituição.

Fórum Executivo de Aceitação de Clientes e PLD-FTP: Instância deliberativa de apoio à Alta Administração e que tem o seu funcionamento regido pelas disposições do seu Regimento, atuando com estrita observância às atribuições

designadas por meio da Política de PLD-FTP, aprovada e revisada anualmente, ou sob demanda, pelo CONAD e distribuída a todos os colaboradores como orientação à conduta. O objetivo deste Fórum é: Avaliar, discutir, aprovar e decidir quanto à aceitação de clientes, parceiros e fornecedores com foco em PLD-FTP; Orientar e definir os procedimentos para PLD-FTP no Bmg, por meio do cumprimento das regulações e legislações vigentes; e Deliberar quanto às ações a serem tomadas nos casos de clientes que realizam transações/operações com indícios de LD-FTP.

Diretoria responsável por PLD-FTP: Além da atribuição da responsabilidade exigida pelo cargo e pelas diretrizes dos normativos dos órgãos reguladores, esta Diretoria é responsável por: (i) Aprovar normativos, procedimentos, medidas e orientações que assegurem a aderência à Política e diretrizes do Bmg no que diz respeito à PLD-FTP; (ii) Submeter ao CONAD proposta para o estabelecimento ou alterações da Política de PLD-FTP, quando necessário; (iii) Avaliar, acompanhar e garantir o adequado e efetivo funcionamento da estrutura e dos resultados do gerenciamento de riscos relacionados aos crimes de LD-FTP; (iv) Participar ativamente do Fórum Executivo de Aceitação de Clientes e PLD-FTP, atuando conforme política institucional vigente, aprovada pelo CONAD; (v) Avaliar as necessidades de treinamento e capacitação adequadas para os colaboradores da área de PLD-FTP, buscando inclusive, aprovação de orçamento para este fim; e (vi) Gerir e se responsabilizar pela estrutura de governança que vise assegurar o cumprimento integral desta Política, dos procedimentos e controles internos de PLD-FTP.

PLD-FTP: Tem responsabilidade direta para que as diretrizes tratadas nesta Política sejam efetivamente implementadas e executadas, com eficiência e efetividade a fim de identificar, avaliar, mensurar e tratar riscos relacionados aos crimes de LD-FTP, além de implementar metodologias e sistemas que reflitam as melhores práticas com foco em PLD-FTP compatíveis com a natureza e a complexidade do negócio, dos produtos, serviços, atividades, processos e

sistemas do Bmg, com o objetivo de suportar o gerenciamento dos riscos de LD-FTP, arquivando-se as documentações do processo. A área também é responsável pela correção de eventuais deficiências técnicas verificadas no processo de PLD-FTP e endereçamento de correção de outras deficiências às áreas competentes.

Diretorias: Têm como principais atribuições avaliar e acompanhar a estrutura de PLD-FTP, o funcionamento e os resultados do gerenciamento de riscos relacionados a LD-FTP. Devem ainda deliberar sobre os assuntos de gerenciamento desses riscos, pertinentes à sua competência, e submeter questões ao Diretor responsável por PLD-FTP no Bmg, tendo como ações principais nesse tema: (i) Suportar a Política de PLD-FTP, bem como divulgar a sua importância nas áreas de atuação que estão sob a sua subordinação; (ii) Garantir o cumprimento desta Política, acompanhando as ações em todos os níveis, que visem à prevenção a operações com suspeitas de LD-FTP; e (iii) Estimular e participar de ações conjuntas no âmbito do Sistema Financeiro Nacional para PLD-FTP.

Diretoria de Riscos, Finanças, Relações com Investidores (RI), Produtos, Processos e Áreas de Crédito Pessoal: (i) Em sua atribuição específica de PLD-FTP, cumprir com as Responsabilidades descritas anteriormente; (ii) Atuar e fazer com que as informações dos clientes cheguem corretas ao Bmg, por meio da equipe de sua subordinação, especialmente no tocante a cadastro e procedimentos de Conheça seu Cliente (KYC); (iii) Disseminar os normativos de prevenção buscando sua observância junto aos correspondentes e outros prestadores de serviços contratados e sob sua gestão; (iv) Apoiar as ações e procedimentos com foco em PLD-FTP; (v) Atender as demandas do Fórum Executivo de Aceitação de Clientes e PLD-FTP; e (vi) No desenvolvimento de novos produtos, avaliar e submeter ao comitê responsável a prévia avaliação no tocante ao risco de LD-FTP.

Diretoria de Auditoria Interna (e área de Auditoria Interna): (i) Avaliar o processo de PLD-FTP em todos os níveis hierárquicos, emitindo parecer e recomendações para a Alta Administração e para as diretorias responsáveis, seja em trabalhos específicos sobre o tema seja dentro de trabalhos sobre produtos e procedimentos ou do plano de trabalho da área; e (ii) Apurar possível envolvimento de colaboradores em operações suspeitas de LD-FTP.

Diretoria de Assuntos Jurídicos: (i) Atentar para as exigências legais instituídas e respectivas regulações, participando da definição de normativos pelo Bmg, aplicados em PLD-FTP; (ii) Emitir parecer conclusivo, sempre que solicitado, sobre os procedimentos aplicáveis ao objetivo de PLD-FTP, com base na legislação vigente.

Superintendência de Crédito: (i) Avaliar com o devido critério a capacidade financeira dos clientes tomadores de empréstimos, submetidos à Superintendência, considerando a compatibilidade entre o ramo de atividade, ocupação, localização geográfica, dentre outros fatores; (ii) Atender com rigor à Política de PLD-FTP e às políticas e demais normativos de análise de crédito, agindo de forma ética e isenta de conflito de interesses; (iii) Prestar informação ao Fórum Executivo de Aceitação de Clientes e PLD-FTP para os casos em que sejam identificadas suspeitas e/ou indícios de tentativa de LD-FTP, independente da negativa do crédito; (iv) Realizar visitas *in loco* a clientes quando solicitado pelo Fórum de PLD-FTP, com objetivo de comprovação de compatibilidade da movimentação financeira do cliente com os seus negócios ou com a atividade econômica exercida.

Compliance e Controles Internos: (i) Realizar monitoramento regulatório e acionar a área de PLD-FTP quando da atualização ou publicação de normativos relacionados à temática para devido cumprimento; (ii) Realizar testes de conformidade, quando necessário, identificando os pontos de inconsistências e recomendando respectivos planos de ação; (iii) Realizar atendimento regulatório

nacional e internacional e intermediar o atendimento das demandas junto à área de PLD-FTP; (iv) Realizar anualmente a Avaliação de Efetividade da política, dos seus procedimentos e dos controles internos de PLD-FTP, de acordo com a determinação regulatória.

Cadastro: (i) Atuar na gestão do setor de Cadastro, orientados pelas políticas institucionais, normativos e pelos manuais internos da área; (ii) Manter padrão de qualidade e de segurança nas informações e documentação obtidos dos clientes; (iii) Trabalhar para a manutenção de informações cadastrais completas e atualizadas conforme a Norma de Conheça seu Cliente (*KYC*); e (iv) Manter relacionamento estreito com as áreas de Compliance Regulatório e PLD-FTP.

Gerências Comerciais: (i) Observar e responsabilizar-se pelo cumprimento dos procedimentos e regras definidas na Norma de Conheça seu Cliente (*KYC*); (ii) Atuar de forma ética e alinhada às políticas e normativos do BMG na relação de negócios junto a clientes; (iii) Certificar-se da veracidade das informações cadastrais de clientes na gestão do relacionamento no BMG; (iv) Dar suporte e comunicar imediatamente a área de PLD-FTP todas as situações consideradas suspeitas e atípicas e encaminhar toda a documentação necessária à análise da suspeição/atipicidade de LD-FTP; (v) Acompanhar a atuação de seus colaboradores, bem como os correspondentes sob sua gestão; e (vi) Comunicar ao cliente quando houver recusa de início/manutenção de relacionamento, deliberada no Fórum de PLD-FTP, indicando que não há interesse comercial pelo Bmg em adquiri-lo/mantê-lo, e nunca informar ao cliente que a recusa se deu por questões de PLD-FTP.

Gerência de Formalização: (i) Conferir a documentação cadastral e de formalização das operações; (ii) Agir de forma ética e isenta de conflito de interesses, especialmente em relação à área comercial e clientes, com atenção inclusive quanto a possíveis pressões relacionadas a metas e produção; e (iii)

Informar à área de PLD-FTP os eventos suspeitos e atípicos identificados no âmbito da execução das suas rotinas.

GELFC – Administrativo: (i) Monitorar os padrões e habitualidade das movimentações das contas correntes, reportando à área de PLD-FTP eventuais situações suspeitas; (ii) Atentar para movimentações financeiras que se enquadram como suspeitas e/ou atípicas em relação à LD-FTP, bem como as de comunicação obrigatória ao COAF, providenciando a comunicação imediata à área de PLD-FTP; e (iii) Identificar, conforme definido em procedimento interno, os clientes que utilizem o serviço de caixa/tesouraria, especialmente no tocante a movimentações em espécie relevantes ou de forma costumeira .

GECAC – Gerência Geral de Operações de Cartão de Crédito: Identificar e informar à área de PLD-FTP eventos suspeitos no âmbito da área sob sua responsabilidade.

Gestores das Áreas de Negócios: São responsáveis pelos relacionamentos com clientes e transações realizadas pelos clientes, de modo que devem observar com rigor esta Política e guardar estrito relacionamento com a área de PLD-FTP, sobretudo no que se refere à informação de eventuais suspeitas e/ou atipicidades referentes a LD-FTP envolvendo os clientes.

Recursos Humanos: A área de recursos humanos terá papel central na execução desta Política, estabelecendo formas para aplicação da Norma de Conheça seu Funcionário (KYE) e na capacitação e treinamentos dos colaboradores. Portanto, a área deverá promover ações que permitam: (i) Criar e desenvolver programas de treinamento, conforme determinado pela regulação vigente e por esta Política, mediante aprovação do Fórum Executivo de PLD-FTP; (ii) Disponibilizar, a todos os profissionais que ingressarem no BMG, os cursos e informações sobre PLD-FTP, que deverão ser concluídos até o final do primeiro mês da contratação; e (iii) Certificar-se de que todos os colaboradores

receberam treinamentos adequados de PLD-FTP, além de manter as devidas evidências à disposição das auditorias e reguladores.

Gestores: Os gestores do Bmg têm a responsabilidade de contribuir com os gestores de PLD-FTP para a efetiva aplicação desta Política, disseminando entre os seus subordinados as diretrizes aqui definidas e conscientizando-os da necessidade da sua plena observância.

Colaboradores: Todos os colaboradores do Bmg deverão participar ativamente do processo de PLD-FTP, incorporando nas suas rotinas e atividades diárias a cultura do efetivo respeito e cumprimento das diretrizes aqui definidas, e reportando à área de PLD-FTP eventuais situações suspeitas de LD-FTP.

Gerência de Treinamento Comercial: (i) Promover a cultura organizacional de PLD-FTP, contemplando os parceiros e os seus respectivos colaboradores, capacitando-os a prospectarem e prestarem atendimento aos clientes, cientes das diretrizes do BMG sobre esse tema; e (ii) Aplicarem treinamento sobre o tema PLD-FTP aos colaboradores dos parceiros comerciais, controlando e documentando a participação desse público e disponibilizando esses controles aos auditores e reguladores, sempre que solicitado.

Correspondentes e demais Parceiros e Prestadores de Serviços Terceirizados: (i) Responsabilizarem-se pelos procedimentos de PLD-FTP; (ii) Responsabilizarem-se pela veracidade das informações cadastrais dos clientes na gestão do relacionamento com o Bmg; (iii) Atuarem de forma ética e alinhada às Políticas e normativos do Bmg na relação de negócios junto aos clientes; (iv) Manterem atualizados os seus dados junto ao BMG, devendo informar imediatamente, qualquer alteração nesse sentido; (v) Observarem todas as regras destinadas ao controle de qualidade, conforme previsto em contrato; (vi) Promoverem e incentivarem a participação dos seus colaboradores nas capacitações e treinamentos sobre o tema PLD-FTP promovidos pelo Bmg; e

(vii) Reportar à área de PLD-FTP do Bmg quaisquer suspeitas relativas aos crimes de LD-FTP.

10. PROMOÇÃO DA CULTURA ORGANIZACIONAL, ACULTURAMENTO E TREINAMENTOS

O Bmg tem a certeza de que a compreensão de todos acerca da importância do tema é essencial para a eficácia dos procedimentos de PLD-FTP. Isto considerado, além de ser uma importante área da Instituição, o programa de PLD-FTP faz parte da cultura do Bmg e está positivamente enraizada em todos os seus relacionamentos, decisões e negócios. E, como detalhado nesta Política, todos os colaboradores e terceiros que se relacionem com o Bmg possuem deveres e responsabilidades de PLD-FTP.

Entende-se que o adequado aculturação de PLD-FTP auxilia na mitigação do risco de utilização do Bmg por criminosos que se ocupam da prática de LD-FTP e estão dispostos a pagar quantias significativas e empreender esforços para perpetuar seus ilícitos, seja tentando corromper os colaboradores e terceiros e/ou visando conhecer e atingir fragilidades de controles como forma de facilitar suas atividades.

Desta forma, com o intuito de disseminar a cultura de PLD-FTP e promover tal aculturação na instituição, o Bmg investe em treinamentos e capacitações adequadas aos seus colaboradores, nos termos da legislação e da regulação vigente. O conteúdo desses treinamentos também contempla as leis, regulamentos e políticas de sanções das Ilhas Cayman.

A área de PLD-FTP possui capacitação robusta sobre o tema, mantendo-se atualizada tanto no aspecto teórico, quanto nas questões operacionais, de forma a bem desempenhar suas funções, mas também a atuar como multiplicadores de conhecimento para as demais áreas da instituição.

As áreas da instituição que se relacionem com atividades de alto risco de LD-FTP possuem capacitação especializada sobre o tema de PLD-FTP, voltada para identificar e obstar propostas ou outros comportamentos que visem viabilizar a consecução de ilícitos relacionados com LD-FTP.

Os demais colaboradores da instituição recebem capacitação sobre o tema PLD-FTP que proporcione o entendimento sobre a relevância da matéria, o reconhecimento de suas responsabilidades, bem como as consequências de eventuais falhas ou omissões, individuais ou coletivas, no processo de PLD-FTP.

O conteúdo dos treinamentos contempla, no mínimo, aspectos relacionados à importância da prevenção à LD-FTP, os riscos que esse tipo de ilícito agrega para as instituições, seus dirigentes e funcionários, bem como o prejuízo que causa à sociedade. O conteúdo dos treinamentos para as áreas de negócios inclui os aspectos relacionados à LD-FTP envolvendo suas atividades específicas. O conteúdo dos treinamentos para os parceiros, prestadores e demais terceiros também incluem as principais tipologias potencialmente incidentes nas atividades em que atuam.

É incentivada a participação em congressos ou eventos assemelhados dos quais participem especialistas e/ou reguladores.

São incentivadas as participações em eventuais treinamentos e capacitações de PLD-FTP realizados por colaboradores do Bmg e que não sejam os ministrados pela própria instituição, desde que o conteúdo seja compatível com as exigências desta Política e validado pela área responsável.

Também são exigidos treinamentos e capacitações dos colaboradores dos nossos parceiros comerciais (exemplos: correspondentes no país, lojas próprias e lojas franquizadas) e prestadores de serviços terceirizados.

Os treinamentos relacionados ao tema de PLD-FTP são aplicados a todos os colaboradores do Bmg, com compatibilidade com o risco da atividade na qual atuam.

Igualmente, é exigida capacitação compatível com o risco de LD-FTP do processo com os quais estejam envolvidos para os colaboradores dos nossos parceiros comerciais e prestadores de serviços terceirizados.

Colaboradores da área de PLD-FTP passam por capacitação, no máximo, a cada 12 meses.

Colaboradores envolvidos em atividades de alto risco de LD-FTP passam por capacitação, no máximo, a cada 24 meses.

Os demais colaboradores passam por capacitação em PLD-FTP a cada 36 meses, no máximo.

Os eventos de capacitação são documentados e objeto de verificação por ocasião da Avaliação de Efetividade (AE) da Instituição.