POLÍTICA PREVENÇÃO
LAVAGEM DINHEIRO
FINANCIAMENTO AO TERRORISMO
E DESTRUIÇÃO EM MASSA
PLD/FTP

Versão: 2026.1
Data Aprovação: 18/03/2026
Aprovação: DIRETORIA

1. OBJETIVO

O presente documento, denominado política, tem por finalidade orientar o comportamento esperado na relação estabelecida entre a COLUNA DTVM e seus clientes, funcionários, prestadores de serviço, órgãos reguladores e a sociedade em geral no que tange a prevenção a lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa e apresentar a metodologia adotada na identificação de clientes, manutenção de registros, monitoramento de atividades e comunicações suspeitas para cumprimento das legislações em vigor que regulam as Instituições Financeiras autorizadas a funcionar pelo Banco Central do Brasil.

REGULAMENTAÇÃO APLICÁVEL

I	Circular BCB n° 3.978/2020
II	Carta Circular BCB nº 4.001/2020
III	Resolução BCB nº 44/2020
IV	Lei nº 9.613/1998
V	Lei n° 12.683/2012
VI	Lei nº 12.846/2013
VII	Lei nº 13.260/2016
VIII	Lei nº 13.810/2019
IX	IN RFB nº 1037/2010
X	Resolução BCB nº 277/2022
XI	Resolução ANM nº 129/2023

2. PRINCIPIOS E DIRETRIZES

A COLUNA DTVM se compromete a atuar com valores éticos de honestidade, integridade, transparência e responsabilidade nas suas atividades e relacionamentos, e em conformidade com a legislação e regulamentação vigentes.

As diretrizes que sintetizam os compromissos assumidos pela instituição são:

- Instituir e propagar em todas as áreas da instituição as principais normas e procedimentos referentes à prevenção e combate à lavagem de dinheiro, corrupção e financiamento do terrorismo e proliferação de armas de destruição em massa, com a disseminação de seu teor a todos os funcionários, colaboradores, parceiros e prestadores de serviços;

- Estabelecer e disseminar ações direcionadas à detecção de operações e situações suspeitas, a análise destas e a sua comunicação aos órgãos competentes;

- Disseminação de princípios éticos e regras de conduta aplicáveis a todos os colaboradores no cumprimento das regras relacionadas à PLD/FTP;

- Enfatizar a cultura de Compliance no que tange a Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa com treinamentos adequados contemplando ações de conscientização e de avaliação de conhecimento, inclusive a terceiros, quando aplicável;

- Monitorar possíveis desvios na implementação das diretrizes definidas pela instituição;

- Preservar sigilo relativamente às propostas, operações e situações analisadas e/ou comunicadas ao Conselho de Controle de Atividades Financeiras – COAF, entre outros órgãos competentes.

3. DIVULGAÇÃO DA POLÍTICA

Elaborada de modo a garantir a divulgação, conscientização e comprometimento por todos os funcionários, colaboradores, parceiros, prestadores, quanto ao compromisso da COLUNA DTVM, ao fiel cumprimento à regulamentação vigente, viabilizando pleno conhecimento e acessibilidade de suas políticas, incorporadas às suas diretrizes, valores e conduta ética e moral.

A COLUNA DTVM, divulga amplamente sua Política de Prevenção a Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa, tornando acessível através do site https://www.colunadtvm.com.br/, na seção “Políticas Internas”, ainda e-mail e treinamentos.

4. CONCEITO

Lavagem de Dinheiro

É o processo pelo qual recursos originados de atividades ilegais são transformados em ativos de origem aparentemente legal. Essa prática geralmente envolve múltiplas transações, usadas para ocultar a origem dos recursos financeiros e permitir que eles sejam utilizados de forma a aparentar ter origem lícita.

Os valores obtidos por meio das atividades ilícitas e criminosas (tráfico de drogas, corrupção, armas, terrorismo, entre outros) sejam dissimulados ou escondidos, aparecendo como resultado de operações comerciais legais e que possam ser absorvidas pelo sistema financeiro, naturalmente.

O processo de lavagem é composto por três fases:

- ✓ **Colocação** – ingresso no sistema financeiro de recursos provenientes de atividade ilícitas, por meio de depósitos, compra de instrumentos financeiros ou compra de bens.
  Nesta fase, é comum a utilização de instituições financeiras para a introdução de recursos obtidos ilicitamente;

- ✓ **Ocultação** - caracteriza-se pela tentativa do criminoso em dificultar o rastreamento contábil dos recursos ilícitos, ocultando a origem e realizando múltiplas transações em diversas instituições, tanto no Brasil quanto em outros países;

- ✓ **Integração** - nesta última etapa, o infrator começa a incorporar os ativos ilegais ao sistema econômico. Concluída esta fase, os recursos aproximam-se da “legitimidade”.

Financiamento ao Terrorismo

Consiste no processo de distribuição dissimulada de recursos a serem utilizados em atividades terroristas.

Os recursos são oriundos, geralmente, das atividades de outras organizações criminosas envolvidas com o tráfico de drogas, armas e munições e com o contrabando, ou ainda derivados de atividades ilícitas.

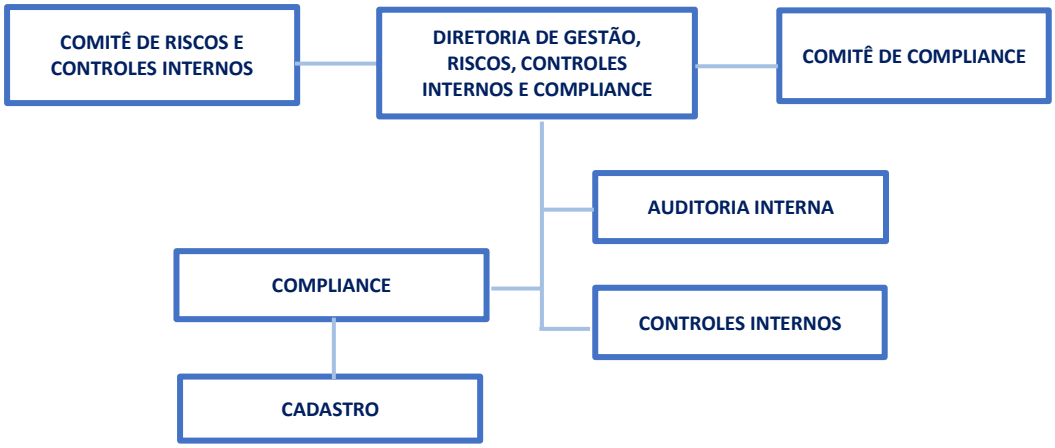
Os métodos utilizados pelos terroristas para dissimular o vínculo entre eles e as fontes de financiamento são semelhantes aos utilizados na prática de crime de lavagem de dinheiro. Entretanto, os terroristas utilizam recursos obtidos de forma legal, visando reduzir o risco de serem descobertos antes do ato terrorista.

5. ESTRUTURA DE PREVENÇÃO

A estrutura responsável pela Prevenção à Lavagem de Dinheiro, Combate, Financiamento do Terrorismo e Proliferação de Armas de destruição em massa, está centralizada na Gerência de Compliance, subordinada à Diretoria de Gestão, Riscos e Controles, ligada diretamente à mais Alta Governança da Instituição.

A estrutura é compatível com o perfil de risco da instituição, suas operações, produtos e serviços, bem como seus clientes, funcionários, parceiros e prestadores de serviços terceirizados.

Organograma PLD/FTP:



6. RESPONSABILIDADES E ATRIBUIÇÕES

Todos os colaboradores dentro de suas atividades têm funções e responsabilidades relacionadas ao Programa de PLD/FTP.

6.1. *Diretoria de Gestão, Riscos, Controles Internos e Compliance*

Representa a COLUNA DTVM perante o Banco Central do Brasil como Diretor responsável pelo cumprimento das obrigações previstas na Circular BCB 3.978/20.

Dentre as principais responsabilidades, destacam-se:

- ✓ Divulgar e operacionalizar a implantação da Política de PLD/FTP;
- ✓ Providenciar a revisão e atualização anual, bem como propor os aprimoramentos na Política e nos respectivos manuais da instituição;
- ✓ Aprovar e acompanhar a implementação de novos mecanismos de controles internos, revisão dos processos de identificação e análise de perfil de clientes, colaboradores e terceiros;
- ✓ Aprovar a Política de PLD/FTP;
- ✓ Decisão pela Comunicação ao COAF de operações, situações ou propostas que apresentem indícios de crimes de lavagem de dinheiro e/ou financiamento ao terrorismo;

- ✓ Efetuar a comunicação ao COAF de operações, situações ou propostas que apresentem indícios de crimes de lavagem de dinheiro e/ou financiamento ao terrorismo após a tomada de decisão pela comunicação.

6.2. Comitê de Compliance

Dentre as principais responsabilidades, destacam-se:

- ✓ Revisar esta Política e demais diretrizes relacionadas a Compliance, bem como suas posteriores alterações;
- ✓ Deliberar acerca de assuntos relacionados à revisão de políticas, formulários e demais mecanismos de controles internos, bem como tratamento de exceções;
- ✓ Deliberar sobre os programas de treinamento em PLD/FTP;
- ✓ Atuar na disseminação interna da cultura de PLD/FTP, capacitar suas equipes a agir em situações suspeitas e reportar operações, conforme os meios internos estabelecidos.
- ✓ Aprovar o relacionamento com parceiros “Correspondentes Cambiais “ e Postos de Compra de Ouro.
- ✓ Análise prévia de novos produtos e serviços, bem como novas tecnologias.

As reuniões do Comitê ocorrerão com periodicidade máxima de 90 dias ou sempre que houver situações que demandem deliberação imediata.

As deliberações serão formalmente registradas em “Ata de Reunião”, contendo as decisões tomadas, responsáveis designados e eventuais prazos para implementação das ações deliberadas.

Nota: Será permitido o registro em documento único, denominado “Ata de Reunião”, quando os Comitês de Compliance e de Riscos e Controles Internos se reunirem em conjunto, desde que sejam devidamente registradas as matérias tratadas e as respectivas deliberações

6.3. *Comitê de Riscos e Controles Internos*

Dentre as principais responsabilidades, destacam-se:

- ✓ Definir Políticas de Gerenciamento de Riscos;
- ✓ Supervisionar a gestão dos riscos, perfil e apetite ao risco;
- ✓ Deliberar em conjunto com Diretor PRSAC, a gestão e o gerenciamento do risco social, ambiental e climático, associado as atividades da COLUNA DTVM, em especial a atividade de aquisição de ouro primário;
- ✓ Identificar e avaliar os riscos operacionais, financeiros e reputacionais no relacionamento com clientes inseridos em listas restritivas, embargos ambientais e exposição em mídia negativa.

As reuniões do Comitê ocorrerão com periodicidade máxima de 90 dias ou sempre que houver situações que demandem deliberação imediata.

As deliberações serão formalmente registradas em “Ata de Reunião”, contendo as decisões tomadas, responsáveis designados e eventuais prazos para implementação das ações deliberadas.

Nota: Será permitido o registro em documento único, denominado “Ata de Reunião”, quando os Comitês de Compliance e de Riscos e Controles Internos se reunirem em conjunto, desde que sejam devidamente registradas as matérias tratadas e as respectivas deliberações.

6.4. Compliance

A COLUNA DTVM, através de sua área de Compliance, possui uma estrutura independente e específica de PLD/FTP com o objetivo de prevenir, detectar e analisar transações e situações suspeitas.

Principais funções e atribuições do Gestor da área quanto ao tema de PLD/FTP:

- ✓ Responsável por gerir e controlar os procedimentos desta Política;
- ✓ Supervisão ao cumprimento das normas referentes ao Programa de PLD/FTP;
- ✓ Divulgação das Políticas Internas;
- ✓ Análise de clientes classificados como de maior risco, antes do início de relacionamento;
- ✓ Monitoramento ocorrências sobre operações atípicas ou suspeitas e decisão pelo arquivamento ou encaminhamento para análise;
- ✓ Sanitização periódica da base de clientes em listas restritivas e PEP;
- ✓ Elaborar respostas para as demandas dos órgãos reguladores;
- ✓ Efetuar a comunicação ao COAF de operações, situações ou propostas que apresentem indícios de crimes de lavagem de dinheiro e/ou financiamento ao terrorismo após a decisão do Diretor de PLD/FTP.

6.5. Controles Internos

- ✓ Responsável por garantir a segregação das atividades atribuídas aos integrantes das instituições, de forma a ser evitado o conflito de interesses, bem como meios de minimizar e monitorar adequadamente áreas identificadas como de potencial conflito;

- ✓ A existência de canais de comunicação que assegurem aos funcionários o acesso às confiáveis, tempestivas e compreensíveis informações;
- ✓ A revisão e atualização periódica dos pontos de Controles Internos com o objetivo de incorporar a eles novos riscos ou riscos anteriormente não abordados relativos a PLD/FTP.

6.6. Auditoria Interna

Dentre as principais responsabilidades, destacam-se:

- ✓ Avaliar a eficiência quanto a implementação desta Política;
- ✓ Avaliar a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança e a confiabilidade do processo de coleta;

- ✓ Recomendar melhorias em função das conclusões dos exames realizados;
- ✓ Executar o Plano de Auditoria Interna.

6.7. Cadastro

Responsável pelo cumprimento dos preceitos contidos na Política PLD/FTP e Política de Cadastro.

Principais funções e atribuições da área quanto ao tema de PLD/FTP:

- ✓ Identificação e comprovação dos dados do cliente;
- ✓ Identificação da cadeia societária, representantes e beneficiários finais;
- ✓ Identificação de pessoa PEP ou relacionada;
- ✓ Pesquisas sobre as atividades profissionais e localização do endereço,
- ✓ Consulta a base de listas restritivas e mídias
- ✓ Atualização cadastral da base de cliente ativos, conforme prazos definidos na "Abordagem Baseado no Risco".
- ✓ Comunicar ao Compliance sobre atitudes suspeitas, propostas de operações incompatíveis com o cliente/segmento de negócio ou qualquer outro procedimento que saia do curso normal e que cause estranheza;
- ✓ Sinalizar a área de Compliance quaisquer dúvidas ou suspeições quanto às informações prestadas no cadastro de clientes.

6.8. Demais Colaboradores

- ✓ Conhecer, entender e aplicar as diretrizes de PLD/FTP em suas as áreas de atuação;
- ✓ Reportar ao Compliance qualquer atividade ou transação que seja incomum ou suspeita.

7. PREVENÇÃO E MONITORAMENTO

O Programa de Prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa, engloba processos que sustentam uma atuação preventiva.

São eles:

7.1. Conheça seu Cliente (Know Your Customer - KYC)

O processo de conheça seu cliente (KYC) tem como objetivo principal coletar informações e montar o "perfil" dos clientes, bem como monitorar as operações efetuadas por estes, visando identificar e mitigar as situações atípicas ou com indícios de envolvimento com os crimes de "lavagem de dinheiro" ou "financiamento ao terrorismo".

É de fundamental importância que todo o processo de conhecimento do cliente seja finalizado antes da realização de qualquer tipo de operação. O processo de conhecimento deve ser mantido durante todo o relacionamento com a COLUNA DTVM , através de testes, atualização de informações, dentre outros.

7.2. Pessoas Obrigadas

Define-se por "Pessoas Obrigadas" aquelas para as quais existe determinação legal para adoção de procedimentos de prevenção e combate ao crime de lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa de acordo com a Lei nº 9.613/1998 e Resolução ANM nº 129/2023.

Como parte do processo de Due Diligence da "Pessoa Obrigada", deverão ser evidenciados através de Políticas/Manuais a implementação dos procedimentos e mecanismos de prevenção PLD/FTP, identificação e validação de clientes, registros e monitoramento das transações e a

comunicação de situações atípicas ou suspeitas ao COAF que possam configurar indícios de crimes, previstos na Carta Circular 4.001/2020.

- Política de Prevenção a Lavagem de Dinheiro, Financiamento do Terrorismo e Proliferação de Armas de destruição
- Política de Cadastro de Clientes KYC;
- Questionário Due Diligence.

Devido à complexidade e importância do processo de KYC, os procedimentos e diretrizes estão contemplados na "**Política Conheça seu Cliente - KYC**."

7.3. Conheça seu Funcionário (Know Your Employee - KYE)

O processo de conheça seu funcionário (KYE) estabelece critérios de contratação e monitoramento do comportamento e conduta dos funcionários e colaboradores.

Quanto às medidas a serem adotadas, cumpre-nos destacar:

- ✓ Ciência e adesão de todos os funcionários às regras e diretrizes;
- ✓ Implementação de política contendo critérios e procedimentos rigorosos para a seleção e avaliação de funcionários;
- ✓ Acompanhamento e monitoramento do comportamento e conduta dos funcionários;
- ✓ Treinamento e aperfeiçoamento aos funcionários sobre a ética e prevenção aos ilícitos originados da lavagem de dinheiro, financiamento ao terrorismo, corrupção e fraudes em geral;

As regras e diretrizes adotadas, norteando suas atividades e o controle na utilização da estrutura e os riscos relacionados aos funcionários e colaboradores estão contemplados na "**Política Conheça Seu Funcionário".**

7.4. Conheça Seu Parceiro (Know Your Partner - KYP)

Estabelece critérios para a contratação, aceitação e manutenção de parceiros de negócios, de acordo com o perfil e o propósito de relacionamento, visando a prevenção aos riscos relacionados à lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa.

Principais medidas do processo de conheça seu parceiro:

- ✓ Análise e monitoramento do perfil dos parceiros;
- ✓ Pesquisa sobre o histórico econômico-financeiro e reputacional;
- ✓ Atualização do cadastro;
- ✓ Processos de CDD (*Customer Due Diligence*);
- ✓ Monitoramento das contratações, relacionamentos e rescisões contratuais;

As regras e diretrizes voltadas ao conhecimento dos parceiros, bem como à avaliação dos riscos a eles relacionados, encontram-se descritas na "***Política Conheça seu Parceiro – KYP"*****,** elaborada de forma individualizada, em conformidade com a natureza da relação de negócios estabelecida com o "**Correspondente Cambial, o Posto de Compra de Ouro e a Instituição Financeira."**

7.5. Conheça Seu Prestador (Know Your Supplier – KYS)

Estabelece regras, procedimentos e controles para identificação e aceitação de fornecedores e prestadores de serviços, prevenindo a contratação de empresas inidôneas ou suspeitas de envolvimento em atividades ilícitas.

Principais medidas do processo de conheça seu prestador:

- ✓ Realizar *screening* do prestador previamente à contratação;
- ✓ Monitoramento das contratações, serviços prestados, relacionamentos e rescisões contratuais com o prestador;
- ✓ Processos de *Due Diligence.*

As regras e diretrizes adotadas para conhecer seus fornecedores estão descritos na "**Política Conheça seu Prestador de Serviços - KYS".**

8. BENEFICIÁRIO FINAL

Considera-se beneficiário final a pessoa física que direta ou indiretamente detém o controle ou influência significativamente a entidade.

É também considerado beneficiário final, o representante, o procurador e o preposto que exerça o comando de fato sobre as atividades da pessoa jurídica.

Caracteriza-se como beneficiário final:

- A pessoa que detenha, direta ou indiretamente, o percentual mínimo de participação societária definido na categoria de risco aplicável ao cliente pessoa jurídica, conforme estabelecido no contrato social ou em documento equivalente;
- O representante, inclusive procurador ou preposto, que exerça efetivamente o comando das atividades da pessoa jurídica;
- A pessoa que detenha poder decisório e responda pela condução da estrutura empresarial;
- Os controladores, administradores, diretores ou presidentes da entidade.

Os procedimentos de análise da qualificação do cliente pessoa jurídica deve incluir a análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como "beneficiário final".

O processo consiste em analisar a estrutura societária, efetuando a identificação dos sócios até chegar ao nível da(s) pessoa(s) natural(is), obtendo minimamente o nome ou razão social, número de inscrição CPF ou CNPJ e percentual de participação no capital social.

No caso de controle societário ser detido por outra pessoa jurídica, efetuar a abertura até chegar às pessoas naturais.

A identificação do beneficiário final, será realizada conforme a referência de participação societária, definida na classificação de categoria de risco do cliente PESSOA JURÍDICA.

CLASSIFICAÇÃO	PARTICIPAÇÃO %
BAIXO	25%
MÉDIO	20%
ALTO	10%

8.1. PROCEDIMENTOS DE IDENTIFICAÇAO E QUALIFICAÇÃO

O processo de identificação e qualificação do beneficiário final abrange a coleta de informações e documentos, aplicável a todas as categorias de risco.

- ✓ Nome completo;
- ✓ Nacionalidade;
- ✓ Número inscrição cadastro de pessoas físicas (CPF);
- ✓ Autodeclaração, quanto à sua condição de PEP ou pessoa relacionada (representante, familiar ou estreito colaborador).
- ✓ Data e local de nascimento;
- ✓ Documento de identificação;
- ✓ Comprovante de endereço;
- ✓ Comprovante de rendimentos;
- ✓ Ficha Cadastral;
- ✓ Beneficiário final residente no exterior, que esteja desobrigado de inscrição no CPF, admite-se a utilização de documento de viagem na forma da Lei, devendo ser coletados, no mínimo, o país emissor, o número e o tipo do documento.

9. PESSOAS POLITICAMENTE EXPOSTA

São consideradas pessoas politicamente expostas (PEP) aquelas pessoas que desempenham ou tenham desempenhado, nos últimos 5 anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiras, bem como com seus familiares na linha reta ou colateral até o segundo grau, cônjuge, companheiro (a), enteado (a), estreitos colaboradores.

A qualificação é realizada na entrada do cliente na COLUNA DTVM e no decorrer do relacionamento, através da ferramenta de PLD/FTP.

A sanitização da base cadastral dos clientes ativos será realizada semestralmente.

10. PESSOAS EM MONITORAMENTO ESPECIAL (PME)

A área de Cadastro deve dispensar atenção especial em relação aos clientes identificados como alto risco, exercendo processo de diligência reforçada, sendo estes classificados:

- Pessoas Politicamente Expostas;
- Partes relacionadas à diretores e acionistas até o segundo grau;
- Pessoas comunicadas ao COAF.

11. FINANCIAMENTO E CRIMES DE TERRORISMO

Financiamento é o ato de prover ou destinar fundos a serem utilizados para o financiamento e manutenção de grupos terroristas e de extrema violência.

Como os métodos utilizados pelos terroristas para dissimular o vínculo entre eles e as suas fontes de financiamento são semelhantes aos utilizados na prática do crime de lavagem de dinheiro, a COLUNA DTVM está preparada para identificar e reportar operações e situações atípicas e/ou suspeitas que possam ter relação com os crimes de terrorismo e o seu financiamento.

Adotará o processo de pesquisa em lista sanções CNSU para identificação de clientes, contrapartes, colaboradores, parceiros e prestadores de serviços, que possam estar associados à prática de Crimes de Terrorismo.

Caso haja qualquer suspeita, o Compliance deverá ser imediatamente realizar as análises necessárias, tendo este a autonomia de recusar a operação, contrato ou negócio, caso identificada a associação.

A Lei 13.260/16 define como terrorismo a prática por um ou mais indivíduos dos atos abaixo descritos, 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.

São atos de terrorismo:

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

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

- Atentar contra a vida ou a integridade física de pessoa;

- Promover, constituir, integrar ou prestar auxílio, pessoalmente ou por interposta pessoa, a organização terrorista;

- Realizar atos preparatórios de terrorismo com o propósito inequívoco de consumar tal delito;

- Oferecer ou receber, obter, guardar, manter 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.

12. TESTES DE CADASTRO

Anualmente a COLUNA DTVM, realizará testes de conformidade com o objetivo de assegurar a adequação dos dados cadastrais dos clientes.

Serão utilizadas bases públicas, ferramentas privadas, e o banco de dados do sistema operacional contemplando a base de clientes ativos.

São considerados clientes "**Ativos**" aqueles que mantiveram a contratação de operações nos últimos **12 meses.**

Os testes serão realizados pela área de Compliance e eventuais irregularidades e deficiências serão informadas a área de Cadastro, responsável por estabelecer um plano de ação para mitigá-las.

13. AVALIAÇÃO INTERNA DE RISCOS

A Avaliação Interna de Risco tem como objetivo identificar e estimar o risco de utilização dos produtos e serviços oferecidos pela COLUNA DTVM para a prática de lavagem de dinheiro e financiamento ao terrorismo, em documento próprio "Avaliação Interna de Risco".

Deve considerar o perfil de risco da própria instituição, assim como dos seus Clientes, Produtos, Serviços, Parceiros, Colaboradores e Prestadores de Serviços Terceirizados.

Os riscos identificados na Avaliação Interna de Riscos (AIR), especialmente aqueles classificados como de maior exposição, são utilizados como base para definição das regras e parâmetros de monitoramento adotados pela instituição.

14. ABORDAGEM BASEADA NO RISCO

A Abordagem Baseada no Risco, objetiva identificar, avaliar e entender os riscos de lavagem de dinheiro e financiamento ao terrorismo aos quais a COLUNA DTVM está exposta, a fim de estabelecer e implementar medidas de PLD/FTP proporcionais a esses riscos, mitigando de forma eficaz e efetiva.

A adoção do ABR tem como objetivo, fundamentar a diferenciação do tratamento dispensado a Clientes, Produtos, Colaboradores, Parceiros e Prestadores de Serviços Terceirizados.

Será considerado para a identificação e avaliação do risco:

- Tipos de clientes, atividade e ocupação;
- Segmento, modelo de negócio e área geográfica de atuação da COLUNA DTVM;
- As operações, transações, produtos e serviços realizados;
- Atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados;
- Natureza da operação;
- Lista Pessoa Exposta Politicamente – PEP;
- Listas Restritivas e Sanções.

Uma vez identificado o risco, será avaliado:

- Probabilidade de ocorrência;
- Magnitude dos impactos financeiro, jurídico, reputacional e socioambiental para diante de eventuais riscos de utilização de prodtos e serviços para a prática de LD/FTP.

O grau de risco de LD/FTP será classificado em categorias: **BAIXO, MÉDIO E ALTO.**

A Avaliação Interna de Risco será formalizada em documento específico, devidamente aprovada pelo Diretor responsável por PLD/FTP e encaminhada para ciência da Diretoria.

Essa avaliação deverá ser revisada a cada **02 anos**, bem como diante da ocorrência de eventuais alterações significativas nos perfis de risco mencionados anteriormente, ou ainda, em caso de alteração na legislação vigente.

15. AVALIAÇÃO DE PRODUTOS, SERVIÇOS E NOVAS TECNOLOGIAS

A COLUNA DTVM adotará procedimentos específicos para avaliação de novos produtos, serviços e novas tecnologias, considerando a suscetibilidade à lavagem de dinheiro e financiamento do terrorismo.

Todos os novos produtos, serviços e novas tecnologias, serão formalizados e aprovados pela Diretoria da COLUNA DTVM.

A avaliação para aprovação de novos produtos ou serviços, deve observar minimamente:

- ✓ Se está em consonância com a legislação vigentes a PLD/FTP;
- ✓ A compatibilidade com os objetivos da COLUNA DTVM;
- ✓ Se há região de abrangência ou se a abrangência é geral.

a) Produtos e Serviços Oferecidos

A COLUNA DTVM opera na compra e venda de moedas estrangeiras, remessas financeiras, operações comerciais e negociação de ouro.

- Moeda Estrangeira;
- Remessas Financeiras;
- Operações Comerciais;
- Ouro primário e secundário.

16. AVALIAÇÃO DA EFETIVIDADE

Anualmente, a COLUNA DTVM elaborará a avaliação da efetividade de sua Política de PLD/FTP e Controles Internos, por meio de Relatório Avaliativo de Efetividade, abrangendo a adoção de metodologia de análise quantitativo-qualitativa para identificar possíveis deficiências em seus processos e procedimentos referentes ao combate ao financiamento ao terrorismo e lavagem de dinheiro.

Neste relatório também serão delimitados os testes aplicados e a qualificação dos avaliadores.

O Relatório abrangerá, no mínimo, a avaliação:

- Procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
- Procedimentos de monitoramento, seleção, análise e comunicação ao COAF, incluindo a avaliação de efetividade dos parâmetros se seleção de operações e de situações suspeitas;
- Governança da Política de Prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa;
- Medidas de desenvolvimento da cultura organizacional voltadas à prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo e Proliferação de Armas de destruição em Massa;
- Programas de capacitação periódica de pessoal;
- Procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados;
- Ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do Banco Central do Brasil.

O Relatório terá como data base o dia 31 de dezembro e deverá ser encaminhado para ciência da Diretoria até 31 de março do ano seguinte ao de sua realização.

Diante de eventuais deficiências analisadas na avaliação, será elaborado Plano de Ação com intuito de solucionar tais deficiências, bem como o respectivo Relatório de Acompanhamento da Implementação do Plano de Ação, os quais devem ser encaminhados para ciência e avaliação da Diretoria até 30 de junho do ano seguinte ao da data-base do Relatório.

17. REGISTRO DE OPERAÇÕES

A COLUNA DTVM deve manter os registros de todas as operações realizadas, produtos e serviços contratados, inclusive, pagamentos, recebimentos e transferência de recursos, independentemente dos valores.

Os registros devem conter minimamente as seguintes informações sobre cada operação/produto:

CÂMBIO:

- Tipo;
- Valor;
- Data da realização;
- Nome e número do CPF e CNPJ do titular e do beneficiário da operação, no caso de pessoa residente ou sediada no país;
- Canal utilizado;
- Identificação da origem;
- Códigos de identificação das instituições envolvidas na operação;
- Números das dependências e contas envolvidas na operação;
- Número do cheque para as transferências de recursos por meio de cheque.

No caso de operações envolvendo pessoa física residente no exterior, desobrigada de inscrição no CPF, na forma definida pela Secretaria da Receita Federal, deve conter:

- Nome;
- Tipo e número do documento de viagem e respectivo país emissor;
- Organismo internacional de que seja representante para o exercício de funções específicas no País, quando for o caso.

No caso de operações envolvendo pessoa jurídica com domicílio ou sede no exterior, desobrigada de inscrição no CNPJ, na forma definida pela Secretaria da Receita Federal, deve conter:

- Nome da empresa;
- Número de identificação ou de registro da empresa no respectivo país de origem.

OURO:

- Identificação do processo minerário vinculado à área em que foi feita a extração dos minérios ou da substância mineral;

- Dados identificação do cliente:

No caso:

- ✓ Pessoa física (CPF, número do documento de identidade com foto, e órgão expedidor, endereço, endereço eletrônico e principal(is) atividade(s) desenvolvida(s).

- ✓ Pessoa jurídica (razão social ou nome fantasia, endereço, endereço eletrônico, número de registro cadastro CNPJ, data de constituição e principal(is) atividade(s) desenvolvida(s) e dados de identificação do representante (quando aplicável).

- Descrição dos bens ou mercadorias;
- Valor bruto das operações;
- Data e hora da realização das operações;
- Meios de pagamento do valor total das operações;
- Data de pagamento;
- Identificação dos boletos de compensação financeira pela exploração mineral (CFEM)

18. OPERAÇÕES EM ESPÉCIE

a) No caso de operações com utilização de recursos em espécie de valor individual superior a **R$ 2.000,00 (dois mil reais),** serão registradas as informações do **PORTADOR** dos recursos:

- Nome completo;
- Número de inscrição no CPF.

Na hipótese de recusa do cliente ou do portador dos recursos em prestar a informação, o fato será registrado e a informação utilizada nos procedimentos monitoramento, seleção e análise de operações e situações suspeitas.

As operações realizadas por Empresa de Transporte de Valores, autorizada e registrada na autoridade competente, será considerada como a "Portadora" dos recursos.

Serão coletadas as seguintes informações da portadora Empresa de Transporte de Valores:

- Número de inscrição no CNPJ;
- Firma ou denominação social.

b) No caso de operações de APORTE em espécie de valor individual igual ou superior a **R$ 50.000,00** (cinquenta mil reais), serão registradas as informações relativas ao cliente, portador e a origem dos recursos.

✓ **Proprietário dos Recursos**

Será considerado o "**Proprietário**" dos recursos, o Cliente pessoa física ou pessoa jurídica, envolvido na operação.

- Nome completo / Firma ou denominação social;
- Número de inscrição no CPF / CNPJ.

✓ **Portador dos Recursos**

- Nome completo;
- Número de inscrição no CPF.

✓ **Origem dos Recursos**

A origem dos recursos deverá ser comprovada, mediante a apresentação dos documentos abaixo, salvo a moeda estrangeira adquirida na própria COLUNA DTVM.

- e-DBV (Declaração Eletrônica de Bens do Viajante) coletar o número de registro da declaração.
- Comprovante de aquisição da moeda estrangeira adquirida em IF autorizada, coletar o código da IF.

Na hipótese de recusa do cliente ou do portador dos recursos em prestar a informação referente a origem dos recursos, o fato será registrado e utilizada essa informação nos procedimentos de monitoramento, seleção e análise de operações e situações suspeitas.

18.1. MONITORAMENTO DE OPERAÇÕES EM ESPÉCIE

A COLUNA DTVM adota procedimentos específicos para registro, monitoramento e análise das operações realizadas com utilização de recursos em espécie, em conformidade com os Artigos 33, 34 e 35 da Circular nº 3.978/2020.

Para esse fim, a instituição mantém procedimentos destinados à identificação, registro, monitoramento e análise das operações realizadas com utilização de recursos em espécie, observando, no mínimo, as seguintes informações:

- data da operação;
- valor da operação;
- natureza da operação;
- origem e destino dos recursos;
- identificação das partes envolvidas e contrapartes.

As informações relativas às operações são coletadas e registradas nos sistemas operacionais da instituição e monitoradas por meio da ferramenta de prevenção à lavagem de dinheiro e financiamento do terrorismo **Eguardian**, integrada aos sistemas operacionais utilizados nas operações de câmbio e de negociação de ouro ativo financeiro.

A ferramenta recebe diariamente as informações cadastrais e operacionais relativas às operações realizadas, incluindo dados sobre clientes, representantes, beneficiários finais, contrapartes, valores, instrumentos utilizados e fundamentação econômica ou legal da operação.

Com base em regras, parâmetros e cenários de monitoramento previamente definidos, o sistema realiza a identificação de possíveis atipicidades, gerando alertas para análise pela área de Compliance.

Nos casos em que o cliente ou portador dos recursos se recuse a prestar informações necessárias à identificação ou à comprovação da origem dos recursos, a ocorrência deverá ser registrada nos sistemas internos da instituição e submetida aos procedimentos de monitoramento, seleção e análise de operações e situações suspeitas.

Os procedimentos de monitoramento, seleção e análise das ocorrências são disciplinados no Manual de Monitoramento, Seleção, Análise e Comunicação de Operações e Situações Suspeitas – MSAC, documento complementar a esta Política.

As informações e registros relacionados às operações em espécie deverão ser mantidos pelo prazo mínimo previsto na regulamentação aplicável.

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

O indício de operações e situações suspeitas se configura por meio de comportamentos e atipicidades, por serem realizadas de forma distinta com o perfil, atividade, capacidade financeira e econômica das partes com quem COLUNA DTVM se relaciona, além das contrapartes constantes nas operações, para a prática dos crimes de lavagem de dinheiro e financiamento ao terrorismo.

O monitoramento é realizado de forma contínua e quando identificada uma situação ou operação com indícios de lavagem de dinheiro e financiamento ao terrorismo, a área de Compliance realiza a análise tempestiva pautada nos procedimentos internos.

A análise da operação ou proposta deve compreender uma checagem minuciosa de forma que possa ser evidenciada a caracterização ou não como suspeita de lavagem e de financiamento ao terrorismo na operação.

As situações em que o cliente ou o portador dos recursos se recuse a prestar informações relativas à identificação ou à origem dos recursos serão registradas nos sistemas da COLUNA e consideradas como evento relevante para fins de monitoramento de prevenção à lavagem de dinheiro e financiamento do terrorismo, sendo submetidas aos procedimentos de monitoramento, seleção e análise estabelecidos no Manual de MSAC

Para tanto, são indispensáveis os procedimentos a seguir:

- ✓ Identificação e qualificação de clientes e envolvidos (contraparte, representante, administrador e beneficiário final);
- ✓ Análise dos valores movimentados, capacidade financeira do cliente (renda/faturamento e patrimônio), atividade econômica, origem e destino dos recursos, contrapartes, formas de realização e instrumentos utilizados, fundamentação, citação em mídia negativa, processos criminais, socioambientais, dentre outras análises julgadas necessárias.
- ✓ Preenchimento completo do dossiê de análise relatando ao máximo informações acerca da ocorrência atípica ou suspeita, fundamentando as constatações; relatar inclusive se o cliente, representante, contraparte e beneficiário final constam em listas sanções (CSNU, OFAC), listas PEP e outras listas;
- ✓ Concluir a análise, registrado em Relatório específico, com parecer final sobre a atipicidade ou suspeita.

O monitoramento das operações e situações suspeitas é realizado com base em regras e parâmetros definidos de acordo com o perfil de risco da instituição, incluindo regras específicas para identificação de situações envolvendo funcionários, parceiros e prestadores de serviços e mercado de ouro em geral.

Adicionalmente, a instituição realiza monitoramento preventivo (pré-fato), especialmente para operações envolvendo ouro, com o objetivo de identificar inconsistências antes da efetivação da operação.

20. RELATÓRIO ANÁLISE OCORRÊNCIA

Os dossiês deverão compor documentos, pareceres e Relatório de Análise, produzido pelo Gestor de Compliance.

Para cada alerta de operação ou situação suspeita, será constituído o dossiê, amparado pelo Relatório de Análise, contendo as informações mínimas detalhadas:

- ✓ Data da análise da operação ou situação atípica;
- ✓ Motivo da análise;
- ✓ Nome ou razão social da pessoa objeto de comunicação;
- ✓ Data da última atualização cadastral;
- ✓ Pessoa PEP, familiar ou estreito colaborador;
- ✓ Pessoa praticou, tenha intentado ou praticou atos terroristas ou facilitado seu cometimento;
- ✓ Pessoa que possui ou controla recursos na instituição no caso do subitem anterior;
- ✓ Data, tipo e valor da operação ou situação atípica;
- ✓ Partes e contrapartes envolvidas e país de origem/destino;
- ✓ Relato da ocorrência;
- ✓ Parecer conclusivo do Gestor de Compliance;
- ✓ Parecer conclusivo do Diretor de PLD/FT acerca da decisão de comunicação ou não ao COAF e sua respectiva data;
- ✓ Data e o número do registro da comunicação ao COAF (quando cabível);
- ✓ Pessoa responsável pela Comunicação (quando cabível).

A análise da operação ou situação suspeita deve ser realizada em até **45 dias**, contados a partir da data da seleção da operação ou situação.

O dossiê de comunicação será mantido sob a custódia e responsabilidade da área de Compliance, com armazenamento na ferramenta de PLD/FT “E-Guardian” e em ambiente de rede corporativa, assegurando sua integridade, confidencialidade e disponibilidade para fins de auditoria e supervisão, devem ser mantidos arquivados pelo prazo mínimo de **10 anos.**

Os procedimentos para o monitoramento, seleção, análise e comunicação de operações e situações suspeitas estão formalizados no documento específico **“Manual MSAC”,** parte integrante desta Política e aprovado pela Diretoria PLD/FTP.

21. COMUNICAÇÃO DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

As operações e propostas que contêm indícios de ocorrência de lavagem de dinheiro ou financiamento do terrorismo serão comunicadas ao Coaf, quando aplicável, em cumprimento às determinações legais e regulamentares.

As comunicações de boa-fé não acarretam responsabilidade civil ou administrativa à Instituição, nem a seus administradores e colaboradores.

Importante ainda salientar que todos devem ter atenção especial e, caso tenham conhecimento, nunca comunicar ao cliente, colaborador ou terceiro que o mesmo ou alguma operação realizada tenha sido comunicada ou esteja sendo objeto de investigação interna por suspeita de

envolvimento com lavagem de dinheiro, financiamento ao terrorismo, corrupção ou fraudes em geral.

A decisão pela comunicação ao COAF, caberá exclusivamente ao Diretor PLD/FTP, através de parecer documentado em Relatório específico.

A comunicação ao COAF, é de responsabilidade do Gestor de Compliance ou o Diretor PLD/FTP.

A comunicação da operação ou situação suspeita ao COAF, deve ser realizada até **1 dia útil** seguinte ao da conclusão da análise, fundamentada de acordo com o dossiê de análise que deferiu pela decisão de comunicação.

Deverá atentar ao prazo máximo de **45 dias** para a execução dos procedimentos de análise das operações e situações selecionadas, contados a partir da data da seleção da operação ou situação.

O dossiê das ocorrências selecionadas para análise, devem permanecer sob guarda por **10 anos**.

Os procedimentos para a comunicação de operações e situações suspeitas, incluindo as regras, cenários e parâmetros estão formalizados no documento específico **"Manual Seleção Análise e Comunicação - MSAC**".

22. DECLARAÇÃO NEGATIVA AO COAF

Caso não tenha efetuado comunicação ao COAF sobre operações e situações suspeitas ou passíveis de comunicação, em cada ano civil, deverá prestar declaração em até 10 dias úteis após o encerramento do ano civil, por meio do SISCOAF, atestando a não ocorrência de transações passiveis de comunicação.

23. BLOQUEIO DE ATIVOS - RESOLUÇÕES DO CSNU

Com o objetivo de combater e evitar o financiamento e expansão do terrorismo no mundo o Conselho Nacional das Nações Unidas (CSNU) constituiu o cumprimento de sanções impostas por resoluções, incluída a indisponibilidade de ativos de pessoas naturais, pessoas jurídicas e entidades e designação de investigados ou acusados de terrorismo, seu financiamento ou atos a ele correlacionados.

A COLUNA DTVM cumprirá imediatamente e sem aviso prévio aos sancionados, as medidas estabelecidas nas resoluções sancionatórias do Conselho de Segurança das Nações Unidas ou as designações de seus comitês de sanções que determinem a indisponibilidade de ativos, de quaisquer valores, de titularidade, direta ou indireta, de pessoas naturais, de pessoas jurídicas ou de entidades, nos termos da Lei nº 13.810/19, sem prejuízo do dever de cumprir determinações judiciais de indisponibilidade também previstas na referida lei.

Os procedimentos para o cumprimento das sanções impostas estão formalizados no documento no documento específico **"Manual Seleção Análise e Comunicação - MSAC**".

24. CAPACITAÇÃO E TREINAMENTO

Com o intuito de disseminar a cultura organizacional de PLD/FTP, a COLUNA DTVM investe em Treinamentos de PLD/FTP, dissemina princípios éticos e regras de condutas aplicáveis a todos os colaboradores no cumprimento das regras relacionadas à PLD/FTP e enfatiza a cultura de Compliance.

Anualmente será ministrado o Treinamento de forma presencial ou "on-line" a todos os funcionários, colaboradores e parceiros da COLUNA DTVM , por empresa especializada.

O conteúdo deve aprofundar o conhecimento, ressaltando a responsabilidade legal e regulamentar de identificar, prevenir, tratar e comunicar situações de risco ou indícios de PLD/FTP, além de destacar as Políticas de PLD/FTP, Abordagem Baseada em Risco de PLD/FTP e Conheça Seu Cliente.

Para os recém-admitidos será aplicado o Treinamento sobre Prevenção a Lavagem de Dinheiro, Combate ao Financiamento ao Terrorismo e Proliferação de Armas de Destruição em Massa, em até 120 dias da data da contratação.

Ainda, deverão ser ministrados Treinamentos adicionais aprofundados sobre tema PLD/FTP, a cada 2 anos, para os funcionários das áreas sensíveis (Compliance e Cadastro), a fim de assegurar que todos, tenham os conhecimentos e habilidades necessárias para cumprir suas responsabilidades.

A documentação comprobatória dos Treinamentos, deve permanecer sob guarda por 10 anos (Circular nº 3.978/2020), destacamos:

- Cópia do conteúdo do Treinamento em meio eletrônico;
- Certificado Institucional com os nomes e notas de aproveitamento;
- Questionário de Avaliação do Conhecimento.

25. CONSIDERAÇÕES FINAIS

A Alta Administração da COLUNA DTVM, reafirma seu compromisso com a implementação de padrões de conduta que reduzam os riscos de lavagem de dinheiro e financiamento ao terrorismo, fortalecendo seu ambiente de controles internos para assegurar a conformidade às exigências legais e de órgãos de supervisão, proporcionando a sustentabilidade da Instituição.

A referida Política será revisada a cada **01 ano**, bem como diante da ocorrência de eventuais alterações significativas, ou ainda, em caso de alteração na legislação vigente.