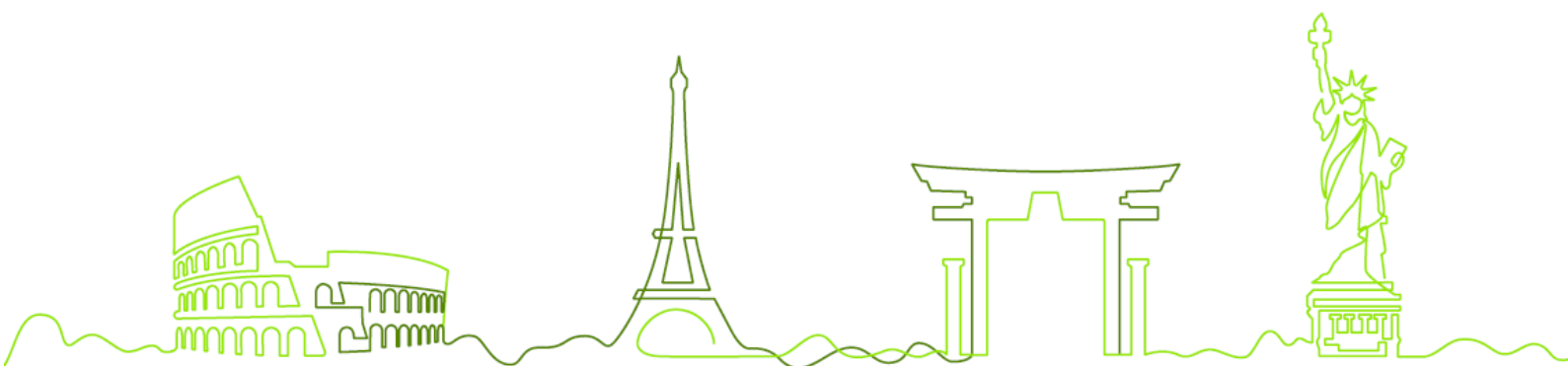




intex international
exchange bank



Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa ("PLD/FTP")

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1ª	11/2020	Compliance / “PLD/FTP”	Versão Original
2ª	11/2022	Compliance / “PLD/FTP”	Atualização
3ª	06/2023	Compliance / “PLD/FTP”	Atualização
4ª	04/2024	Compliance / Riscos / Controles Internos / “PLD/FTP”	Atualização
5ª	07/2025	Compliance / Riscos / Controles Internos / “PLD/FTP”	Atualização
6ª	06/2026	Compliance / Riscos / Controles Internos / “PLD/FTP”	Atualização

Mudanças ocorridas na atualização de 06/2026

Documento alterado para inclusão de:

- CNR, CCME, eFX e ativos digitais referenciados em moeda fiduciária no escopo de serviços do Intex Bank.
- Inclusão da Travel Rule para mercado de ativos digitais.
- Alinhamento da referida Política às novas diretrizes definidas na Avaliação Interna de Risco (AIR).

Público:

"Este documento contém informações que podem ser compartilhadas internamente ou fora da INTEx BANK BANCO DE CÂMBIO S/A, com baixo risco ou até mesmo sem risco de imagem para a instituição, sob a condição de não haver alterações em seu conteúdo original".

Sumário

1.	Apresentação	5
2.	Introdução	5
3.	Objetivo	6
4.	Público	6
5.	Regulamentação Aplicável	6
6.	Diretrizes	8
7.	Estrutura de “PLD/FTP”	9
8.	Funções e Responsabilidades	10
9.	Definições e Glossário em “PLD/FTP”	15
10.	Contexto Histórico e Jurídico da Lavagem de Dinheiro	21
10.1	O Princípio de “Conheça o seu Cliente” e as Comunicações de Operações Suspeitas	21
10.2	Conceito de “Lavagem de Dinheiro”	21
10.3	Etapas do Processo	22
10.4	Resumindo as três fases da “Lavagem de Dinheiro”	22
10.5	Métodos e Tendências	23
11.	Financiamento ao Terrorismo	24
12.	Crimes de Terrorismo	24
13.	Pessoas Expostas Politicamente	25
14.	Beneficiário Final	27
15.	Operações com Ativos Virtuais	28
15.1	Monitoramento e Rastreamento On-Chain	28
16.	Avaliação Interna de Risco - Diretrizes	29
17.	Novos Produtos e Projetos - CCME, CNR e eFX	30
18.	Produtos, Serviços e Novas Tecnologias	30
19.	Produtos e Serviços oferecidos pelo “Intex Bank”	31
20.	Procedimentos de Controles Internos	32
21.	Documentos Corporativos	33
21.1	“Conheça seu Cliente”	33
21.1.1	KYC Reforçado para Operações com Ativos Virtuais	34
21.2	“Conheça seu Funcionário”	34
21.3	“Conheça seu Fornecedor”	34
21.4	“Conheça seu Correspondente”	35
21.5	“Conheça sua Transação”	35

21.6	Cadastro de Clientes	35
21.7	Conheça seu Prestador de Serviços de Ativos Virtuais	36
22.	Teste da Base Cadastral	36
23.	Registro das Operações	36
23.1	Rastreamento On-Chain de Operações com Ativos Virtuais	37
24.	Monitoramento	37
24.1.	Monitoramento de Operações com Jurisdições de Risco	39
24.2.	Monitoramento de Ativos Virtuais e Rastreamento On-Chain	39
24.3.	Segurança de Ativos Virtuais	40
25.	Análise de Operações Suspeitas	40
26.	Comunicação de Operações Suspeitas	41
26.1.	Comunicação de Operações Suspeitas com Ativos Virtuais	42
27.	Dossiês das Operações Suspeitas e Atípicas	42
28.	Procedimentos de Arquivamento e Registro das Operações Suspeitas e Atípicas	42
29.	Declaração Negativa - SISCOAF	43
30.	Formalização do Monitoramento, Seleção e Análise de Operações e Situações Suspeitas	43
31.	Bloqueio de Ativos	43
32.	Treinamentos	44
32.1.	Treinamento Específico em Ativos Virtuais	44
32.2.	Programa de Treinamentos	45
32.3.	Acompanhamento e Manutenção de Registro dos Treinamentos	45
33.	Ciência dos Colaboradores	45
34.	Avaliação de Efetividade da Política de “PLD/FTP”	46
34.1.	Avaliação de Efetividade para Operações com Ativos Virtuais	46
35.	Diretoria Responsável	47
36.	Manutenção dos Arquivos	47
37.	Exceções	47
38.	Considerações Finais	48
39.	Vigência	48
	Anexo I - Procedimentos Operacionais da Travel Rule	49
	Anexo II - Novos Produtos e Projetos	56

1. Apresentação

Apresentamos a “PLD/FTP”, **“Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa”** do Intex Bank Banco de Câmbio S/A, denominado neste documento simplesmente “Intex Bank”.

A presente Política visa apresentar os conceitos, orientações e diretrizes a serem seguidos pelo “

Bank” em consonância com as leis federais e reguladoras no que tange a Prevenção à Lavagem de Dinheiro, ao Financiamento ao Terrorismo e à Proliferação de Armas de Destruição em Massa – “PLD/FTP”.

Não será considerada qualquer assertiva acerca do desconhecimento desta política, bem como não serão consideradas quaisquer justificativas que resultem no seu descumprimento. Assim, diante de qualquer dúvida, esclarecimento ou aconselhamento, é necessário a imediata consulta às Áreas de Compliance e “PLD/FTP”.

Todo colaborador tem a obrigação de reportar imediatamente às Áreas de Compliance e “PLD/FTP” qualquer ato suspeito, ilícito ou que viole os preceitos aqui estabelecidos e a legislação aplicável, de que tiver conhecimento.

Esta Política deve ser seguida e respeitada, permanentemente, por todos os colaboradores do “Intex Bank” no desempenho de suas funções. Ela estará disponível para consulta, a qualquer tempo, na plataforma ClickCompliance de apoio à Governança Corporativa e no sítio eletrônico do “Intex Bank”, na internet.

2. Introdução

A presente Política identificará os conceitos de Lavagem de Dinheiro, ao Financiamento ao Terrorismo e à Proliferação de Armas de Destruição em Massa (“LD/FTP”), as etapas que configuram o delito e as características de pessoas e produtos suscetíveis ao envolvimento com estes crimes. A Política reforça ainda o compromisso de toda a estrutura organizacional do “Intex Bank” na Prevenção à Lavagem de Dinheiro, ao Financiamento ao Terrorismo e à Proliferação de Armas de Destruição em Massa.

É extremamente relevante que todos os diretores e colaboradores entendam sua responsabilidade no processo, bem como a importância de manter o “Intex Bank” na condição de instituição alinhada com os melhores princípios e boas práticas, sempre disposta a coibir qualquer atividade ilícita.

O “Intex Bank” está comprometido com o estabelecimento, a divulgação e o devido

cumprimento de políticas, normas e procedimentos para o gerenciamento do risco de ser utilizada 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, assim como não ser utilizada como veículo para a prática de crimes financeiros ou qualquer outro tipo de ilícito, de acordo com a Legislação Brasileira aplicável.

3. Objetivo

A presente política tem como objetivo informar a todos os funcionários, parceiros, correspondentes cambiais, fornecedores, colaboradores e prestadores de serviços relevantes a respeito da “PLD/FTP” e outros ilícitos os quais o “Intex Bank” adota e é aderente em toda sua atividade, mas, principalmente, nas suas operações diárias, objetivando garantir um programa formal e eficiente de Compliance e “PLD/FTP”, destinado ao cumprimento das leis e regulamentos na prevenção à “LD/FTP”.

4. Público

Esta política tem como público-alvo todos os Diretores, Colaboradores, Parceiros, Fornecedores, Prestadores de Serviços e Clientes do “Intex Bank”, bem como os Correspondentes no país para operações de câmbio que realizam atividades conforme contrato específico firmado com o “Intex Bank”.

5. Regulamentação Aplicável

- **Lei Complementar nº 105 de 10 de janeiro de 2001** - Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências;
- **Lei nº 9.613 de 3 de março de 1998**, com alterações dadas pela Lei nº 12.683/12 - 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;
- **Lei nº 12.846 de 1 de agosto de 2013** - Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;
- **Lei nº 14.286 de 29 de dezembro de 2021** - Dispõe sobre o mercado de câmbio brasileiro, o capital brasileiro no exterior, o capital estrangeiro no País e a prestação de informações ao Banco Central do Brasil;
- **Lei nº 13.260 de 16 de março de 2016** - 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; e altera as Leis nº 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013;
- **Lei nº 13.810 de 08 de março de 2019** - 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;

- **Resolução CMN nº 4.968 de 25 de novembro de 2021** - Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;
- **Resolução BCB nº 277 de 31 de dezembro de 2022** - Regulamenta a Lei nº 14.286, de 29 de dezembro de 2021, em relação ao mercado de câmbio e ao ingresso no País e à saída do País de valores em reais e em moeda estrangeira, e dá outras providências;
- **Resolução CMN nº 4.879 de 23 de dezembro de 2020** - Dispõe sobre a atividade de auditoria interna nas instituições autorizadas a funcionar pelo Banco Central do Brasil;
- **Resolução CMN nº 4.595 de 28 de agosto de 2017** - Dispõe sobre a política de conformidade das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;
- **Resolução BCB nº 131 de 20 de agosto de 2021** - Consolida as normas sobre o rito do processo administrativo sancionador, a aplicação de penalidades, o termo de compromisso, as medidas acautelatórias, a multa cominatória e o acordo administrativo em processo de supervisão, previstos na Lei nº 13.506, de 13 de novembro de 2017, e os parâmetros para a aplicação das penalidades administrativas previstas na Lei nº 9.613, de 3 de março de 1998;
- **Resolução BCB nº 44 de 24 de novembro de 2020** - 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;
- **Circular nº 3.978 de 23 de janeiro de 2020** - Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, 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 4001 de 29 de janeiro de 2020** - Divulga a relação de operações e situações que possam configurar indícios da prática dos crimes de lavagem de dinheiro ou ocultação de bens, direitos e valores, nos termos da Lei nº 9.613, de 3 de março de 1998, bem como de financiamento ao terrorismo, conforme previsto na Lei nº 13.260, de 16 de março de 2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf).
- **Lei nº 14.478, de 21 de dezembro de 2022** - Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.
- **Resolução BCB nº 520, de 10 de novembro de 2025** - Disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais e a prestação de serviços de ativos virtuais por outras instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução BCB nº 519, de 10 de novembro de 2025** - Disciplina os processos de autorização relacionados ao funcionamento das sociedades prestadoras de serviços de ativos virtuais e atualiza os processos aplicáveis às sociedades corretoras de câmbio e às corretoras e distribuidoras de títulos e valores mobiliários;
- **Resolução BCB nº 521, de 10 de novembro de 2025** - Altera as Resoluções BCB nº 277, 278 e 279, de 31 de dezembro de 2022, para disciplinar as atividades e operações com ativos virtuais no mercado de câmbio, submetendo ao tratamento cambial os pagamentos e as transferências internacionais realizados por meio de ativos virtuais e vedando a compra e a venda de ativos virtuais com pagamento ou recebimento em moeda estrangeira;
- **Decreto nº 11.563, de 13 de junho de 2023** - Regulamenta a Lei nº 14.478, de 21 de dezembro de 2022, e estabelece o Banco Central do Brasil como o órgão responsável por regular, autorizar e supervisionar a prestação de serviços de ativos virtuais;

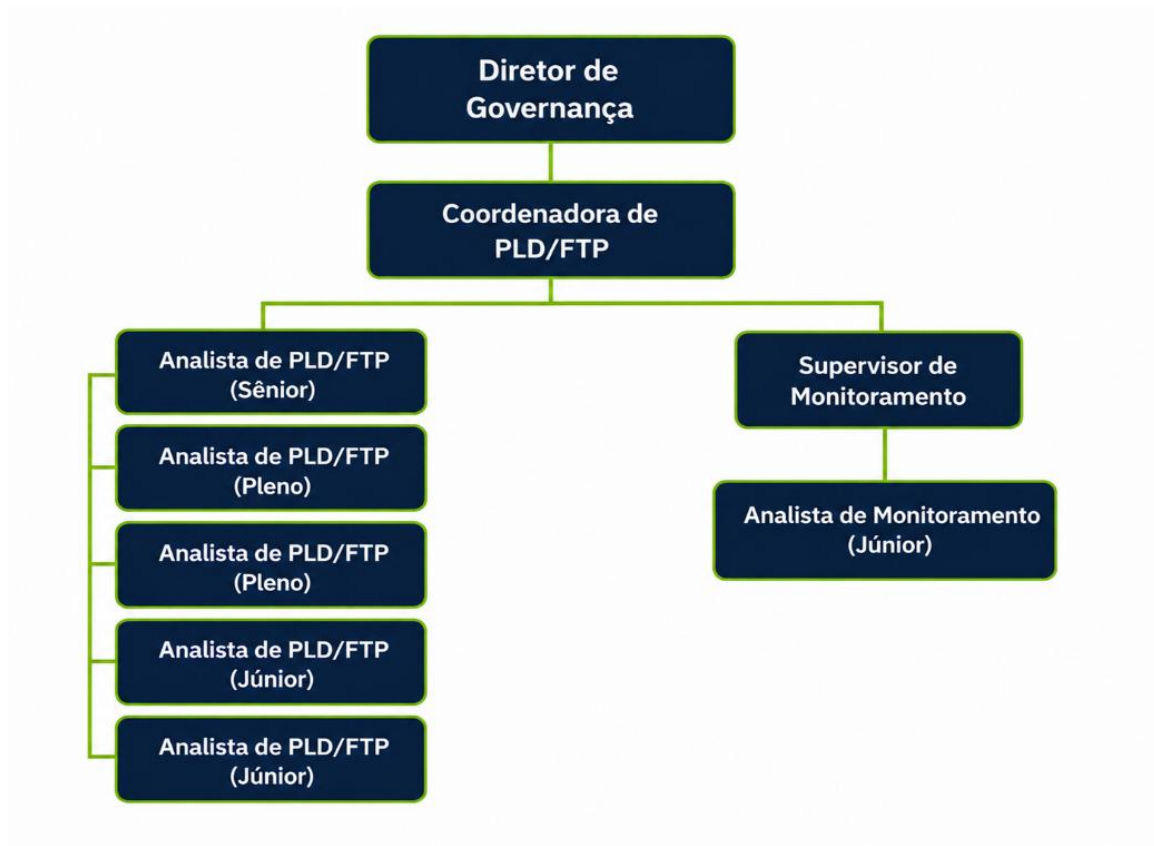
6. Diretrizes

Os Diretores e todos os demais colaboradores deverão adotar as seguintes diretrizes que regem a política de “PLD/FTP” do “Intex Bank”:

- Cumprir as leis e regulamentos aplicáveis à “PLD/FTP”, conforme estabelecido pelos órgãos reguladores locais e internacionais;
- Proteger a reputação e a imagem do “Intex Bank”;
- Cooperar, sempre que possível e sem prejuízo à legislação nacional vigente, com os órgãos reguladores nacionais e internacionais que atuem na prevenção e combate aos crimes de lavagem de dinheiro e financiamento ao terrorismo e proliferação de armas ou quaisquer outros ilícitos;
- Manter por escrito sua Política Institucional de “PLD/FTP”, bem como do combate à Corrupção e quaisquer outros ilícitos. Essa política é compatível com a “natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócios” do “Intex Bank”;
- Identificação e designação das responsabilidades e atribuições em todos os níveis hierárquicos e operacionais;
- Disseminação de princípios éticos e regras de conduta aplicáveis a todos os colaboradores no cumprimento das regras relacionadas à “PLD/FTP”;
- Implementar um Sistema de Controles Internos que contemple “suas atividades desenvolvidas, seus sistemas de informações financeiras, operacionais e gerenciais”, visando o permanente cumprimento das normas legais e regulamentares aplicáveis ao “Intex Bank”;
- Indicar o diretor responsável pela implementação e cumprimento da Lei 9.613/98 e da Circular Nº 3.978/20. O referido diretor ficará responsável pela comunicação direta com os órgãos reguladores e fiscalizadores, além da responsabilidade pela aprovação das políticas, diretrizes e procedimentos para o cumprimento da legislação aplicável na “PLD/FTP” e quaisquer outros ilícitos.
- Enfatizar a cultura de Compliance no que tange a “PLD/FTP” com treinamentos adequados contemplando ações de conscientização e de avaliação de conhecimento, inclusive a terceiros, quando aplicável;
- Análise prévia de riscos inerentes a atuação do “Intex Bank” na operacionalização de novos produtos e/ou prestação de serviços sob a ótica da “PLD/FTP”.

7. Estrutura de “PLD/FTP”

A estrutura da área de “PLD/FTP” do “Intex Bank” é composta pelos seguintes níveis hierárquicos:



8. Funções e Responsabilidades

Diretor Responsável por “PLD/FTP”

- Revisar e aprovar as regras e diretrizes do processo de “PLD/FTP”;
- Supervisionar, com o auxílio da área de Compliance, o cumprimento desta política;
- Participar do Comitê de “PLD/FTP”;
- Agir com probidade, boa fé e ética profissional, empregando, no exercício de suas funções, todo cuidado e diligência esperada dos profissionais em sua posição;
- Pelo cumprimento das normas estabelecidas na referida Circular Bacen nº 3.978/20 e Circular Bacen nº 4.001/20, em especial, pela implementação e manutenção da política de “PLD/FTP” compatível com a natureza, o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio do “Intex Bank”, de forma a assegurar o efetivo gerenciamento dos riscos de “LD/FTP”.

Demais Diretores

- Todos os Diretores têm a responsabilidade de apoiar e suportar o programa de “PLD/FTP”;

- Divulgar a importância do programa para suas respectivas áreas de atuação.

Comitê de “PLD/FTP”

- Aprovar as normas, medidas e orientações, de caráter corporativo, relacionados à “PLD/FTP”;
- Submeter à Diretoria propostas para adoção ou alterações de políticas aplicáveis ao tema;
- Acompanhar a efetividade das atividades e das ações relacionadas à “PLD/FTP”;
- Apreciar os relatórios e comunicações emitidos pelos órgãos reguladores, autorreguladores, pela auditoria interna e auditoria externa, determinando as ações e providências necessárias para atendimento das demandas;
- Ter ciência das atribuições das áreas operacionais diretamente afetadas pelas regras de “PLD/FTP”, com a designação das responsabilidades correlatas;
- Deliberar sobre a contratação de serviços profissionais especializados, investimentos em sistemas de controle e em tecnologia, em “PLD/FTP”, quando julgar necessário.
- Deliberar sobre situações com indícios de lavagem de dinheiro, financiamento do terrorismo ou outras atipicidades envolvendo clientes, partes e contrapartes, avaliando a necessidade de comunicação ao COAF, bem como a adoção de medidas relacionadas à continuidade, restrição ou encerramento do relacionamento comercial, observadas as disposições legais e regulamentares aplicáveis.

Compliance

- Assegurar que o programa de “PLD/FTP”, seja sólido, seguido e respeitado por todas as instâncias de gestão do “Intex Bank”;
- Assegurar a conformidade com a legislação, as normas, os regulamentos e as políticas que norteiam o processo de “PLD/FTP”;
- Aprovar e revisar as políticas e manuais nos padrões utilizados pelo “Intex Bank”, bem como as estratégias e requisitos;
- Criar e incentivar o fluxo adequado de informações em todo o “Intex Bank” estando sempre informada e atualizada acerca das questões relacionadas à “PLD/FTP”;

- Garantir o cumprimento desta política por meio da realização de testes de controles, com periodicidade mínima anual;
- Supervisionar os treinamentos periódicos sobre a matéria de “PLD/FTP” para os colaboradores, assegurando-se de que abordem os requisitos adequados, conforme determinado pela legislação aplicável;
- Divulgar aos colaboradores eventos e tendências no que tange à “PLD/FTP”, contemplando, inclusive, a divulgação das políticas e manuais de procedimentos ou suas alterações, quer seja por meio de e-mails e demais plataformas operacionais disponibilizadas pelo “Intex Bank” (Ex.: ClickCompliance);
- Manter em arquivo registro dos treinamentos ministrados, lista de presença, conteúdo programático, e;
- Guardar o registro e o controle dos registros das comunicações efetuadas aos órgãos reguladores e de controle da atividade.

“PLD/FTP”

- Realizar análises dos prospectivos clientes, indicados e interessados em contratar operações de câmbio. Análises estas, amparadas nos documentos e informações cadastrais completas, utilizando as ferramentas que o “Intex Bank” disponibiliza;
- Emitir parecer conclusivo com relação às análises realizadas e dar conhecimento sobre o deferimento ou indeferimento ao Assessor Comercial, à Área de Negócios e à Área de Cadastro;
- Efetuar a guarda do parecer finalizado, em arquivos eletrônicos, mantendo-os na rede interna (diretórios de rede), identificados pelo nome de cada cliente, assim como armazenando-os no sistema de controle informatizado de “PLD/FTP”;
- Analisar operações de clientes com indícios de irregularidade e/ou atipicidade e/ou suspeição, como por exemplo, diferenças substanciais entre o volume operado e a situação financeira patrimonial declarada em cadastro etc.;
- No que tange ao monitoramento das operações, a área de “PLD/FTP” apoiada, principalmente, na ferramenta tecnológica de seleção de operações (e-Guardian), por meio de relatórios diários, analisa as transações atípicas/suspeitas, encaminhando, ao Comitê de “PLD/FTP”, relatório detalhado com a pertinência de se efetuar a comunicação ao órgão regulador

(COAF), ao amparo da análise técnica e criteriosa dos fatos relacionados com as contrapartes envolvidas;

- Monitorar mídias disponíveis, a fim de verificar informações desabonadoras que atinjam os clientes do “Intex Bank”;
- Acompanhar, de forma periódica, os casos envolvendo eventuais transações com clientes incluídos nas listas de sanções do Conselho de Segurança das Nações Unidas (CSNU), deliberando sobre as medidas cabíveis, quando aplicável;
- Proceder a revisão periódica dos formulários “Conheça seu Cliente”, “Conheça seu Funcionário” e “Conheça seu Parceiro” e, certificar-se de que todos os colaboradores receberam treinamentos adequados quanto à “PLD/FTP”.

Cadastro

- Validar e armazenar informações e documentos que compõem o dossiê cadastral, assegurando-se, inclusive, da tempestiva atualização sempre que a validade dos documentos se expire ou quando da ocorrência de alteração que alcance a relevância dos dados cadastrais e da atividade operacional observada como fatores determinantes do VDO – Valor Disponível para Operar (“limite operacional”) do Cliente;
- Habilitar, aprovando o Cadastro de Clientes somente após o preenchimento de todos os dados e apresentação do dossiê cadastral com ênfase nos requisitos obrigatórios;
- Comunicar à área de “PLD/FTP” quando identificada a relutância no fornecimento de informações requeridas ou quaisquer informações atípicas que forem verificadas na Ficha Cadastral do cliente, como indícios de fraude em documentos;
- Fornecer a documentação cadastral dos clientes sempre que solicitado pela área de “PLD/FTP”;
- Assegurar que os dossiês cadastrais correspondam quantitativa e qualitativamente aos perfis dos clientes que, em razão da atividade em câmbio (valor unitário ou somatória de valores em determinado período) estejam sempre em conformidade com a “Política de Cadastro” e “Conheça Seu Cliente”;
- Identificar os clientes classificados como PEP – Pessoas Expostas Politicamente, clientes em listas restritivas, clientes que residem em região de fronteira ou possuem nacionalidade em país considerado sensível para fins de

“PLD/FTP”, ou que apresentam enquadramento em profissão ou atividade de risco, que seguem procedimento particular para os quais a efetivação do processo cadastral ocorra apenas após autorização explícita do supervisor geral da área.

Gestores, Colaboradores, Assessores e demais áreas

- Reportar imediatamente à “PLD/FTP” quando constatado quaisquer indícios de “LD/FTP” ou burla do sistema financeiro, como propostas realizadas ou alteração sem motivação aparente do “modus operandi” (comportamento) dos clientes;
- Utilizar o canal corporativo, e-mail: pld@intexbank.com.br para qualquer comunicação ou informação a ser reportada relativamente aos clientes, parceiros e suas propostas de operações de câmbio;
- Zelar pelo cumprimento desta Política e reportar imediatamente ao Compliance qualquer irregularidade no processo, utilizando-se o canal corporativo, e-mail: compliance@intexbank.com.br.

Correspondentes Cambiais

- Responsáveis pela prospecção, abertura e manutenção do relacionamento com os clientes, bem como pela avaliação da legitimidade e adequação das operações a serem realizadas junto ao “Intex Bank”, identificando preventivamente potenciais riscos relacionados à “LD/FTP”;
- Cumprir as diretrizes do processo de "Conheça seu Cliente" (KYC), adotando as melhores práticas na prospecção de clientes, na análise de propostas e na condução de operações, bem como comunicar prontamente à área de “PLD/FTP” quaisquer indícios de operações ou situações atípicas e/ou suspeitas.
- Manter controles para garantir que todos os funcionários sob sua responsabilidade (“correspondentes”), sejam treinados anualmente em relação ao tema “PLD/FTP”;
- Reportar imediatamente à área de “PLD/FTP” quando constatado qualquer indício de “LD/FTP” ou burla do sistema financeiro, tais como, propostas atípicas e sem motivação aparente do “modus operandi” (comportamento) dos clientes.

Auditoria Interna

- Revisar e avaliar a eficácia, suficiência e aplicação dos controles da Política de “PLD/FTP”;
- Determinar a extensão do cumprimento das normas, dos planos e procedimentos visando assegurar a aplicação desta política;
- Determinar a extensão dos controles sobre a “PLD/FTP” e da sua proteção contra todo tipo de perda;
- Determinar o grau de confiança das informações, dados e evidências quanto à “PLD/FTP” nos processos do “Intex Bank”;
- Avaliar a qualidade alcançada na execução de tarefas determinadas para o cumprimento das respectivas responsabilidades no âmbito da “PLD/FTP”;
- Realizar testes para verificar a assertividade e integridade do sistema de monitoramento de operações e clientes.
- A auditoria interna deve realizar auditorias periódicas de operações com stablecoins, incluindo: a) Verificação de conformidade com procedimentos de KYC; b) Verificação de conformidade com procedimentos de monitoramento; c) Verificação de segurança de custódia; d) Verificação de rastreamento on-chain; e) Verificação de reporte de operações suspeitas.

Tecnologia da Informação (“TI”)

- Responsável por garantir o adequado e necessário desempenho dos sistemas operacionais, contratados pelo “Intex Bank” e disponibilizados aos funcionários e colaboradores, quer seja no tocante à estabilidade, à eficiência e à continuidade ininterrupta das atividades às quais se destinam;
- Incumbência de tratar ou demandar tratamento das eventuais falhas e buscar a melhoria contínua, quer seja, no âmbito da segurança da informação, controle de acessos, preservação e conservação do parque tecnológico e da base de dados cadastrais e operacionais, tudo em conformidade com as normas vigentes e, em especial, a Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709 de 14 de agosto de 2018).

9. Definições e Glossário em “PLD/FTP”

COAF – Conselho de Controle de Atividades Financeiras: responsável por receber, analisar e retransmitir aos órgãos competentes as comunicações de operações suspeitas/atípicas ou em espécie recebidas de todos os setores

obrigados por lei a prevenir o crime de lavagem de dinheiro e financiamento do terrorismo e proliferação de armas;

Recomendação nº 6: Além de aplicar as medidas de vigilância normais, as instituições financeiras devem:

- a) Dispor de sistemas de gestão de riscos adequados a determinar se um cliente é ou não uma pessoa exposta politicamente (PEP);
- b) Obter autorização da Direção para estabelecer ou manter relações de negócios com tais clientes;
- c) Tomar medidas razoáveis para determinar a origem de patrimônio e de fundos;
- d) Assegurar a vigilância, de forma reforçada e contínua, da relação de negócio.

CSNU – Conselho de Segurança das Nações Unidas: tem como responsabilidade primária a manutenção da paz e da segurança internacionais, além de capacidade jurídica para autorizar o uso da força e fazer cumprir suas decisões em caso de qualquer ameaça à paz, ruptura da paz ou ato de agressão. Por meio de suas sanções impostas por resoluções do CSNU, conforme Lei nº 13.810/19, determina 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.

Branqueamento de dinheiro: ver “lavagem de dinheiro”.

Comunicação de operação suspeita: é a comunicação, destinada à unidade de inteligência financeira (UIF) de um país, com a finalidade de informar a prática de ato possivelmente destinado à lavagem de bens. Com base nessa comunicação, a UIF buscará reunir informações que confirmem ou afastem a suspeita. No primeiro caso, levará esses dados ao conhecimento do Ministério Público, para as medidas apropriadas, de natureza criminal.

Crime antecedente: A lavagem de bens sempre ocorre para ocultar o ganho obtido com um crime anterior, o qual é chamado de crime (ou delito) antecedente, subjacente, precedente ou prévio. Em alguns países, como é o caso do Brasil, a lei indica expressamente quais crimes podem ser considerados antecedentes da lavagem. Por isso, sem a comprovação do crime antecedente não é possível iniciar um processo criminal pela prática de lavagem. No Brasil, os crimes antecedentes estão relacionados no art. 1.º da Lei n.º 9.613, de 3 de março de 1998.

Dólar-Cabo: o Sistema “Dólar-Cabo” (“Euro-Cabo”) é uma expressão brasileira

de um sistema antigo e mundial, alternativo e paralelo ao sistema bancário ou financeiro “tradicional”, de remessa de valores, através de um sistema de compensações, o qual tem por base a confiança. Pode-se citar três espécies de operações típicas complementares encontradas, com frequência, em investigações criminais:

- » **Na primeira**, um cliente entrega, em espécie ou por transferência bancária, reais a um “doleiro” no Brasil, o qual disponibiliza moeda estrangeira equivalente, em taxa pré-ajustada, em favor do seu cliente, no exterior, em reais ou por transferência bancária;
- » **Na segunda**, o cliente recebe do “doleiro”, no Brasil, em reais, recursos em moeda estrangeira que mantinha no exterior e que disponibilizou, fora do Brasil, ao “doleiro”;
- » **Na terceira**, o “doleiro” aproveita a existência simultânea de clientes nas duas posições anteriores e determina a troca de recursos entre esses clientes, no Brasil e no exterior, atuando como um “banco de compensações” (*clearing*), isto é, movimentando recursos sem que nada passe por contas de sua titularidade. Isso se torna mais complexo quando mais de um “doleiro” entra em ação emprestando entre si recursos, ou harmonizando clientes em posições opostas, numa mesma operação. Ao operar nesse sistema, é comum que o “doleiro” mantenha conta no exterior em nome de uma empresa “*off-shore*” por ele controlada. Sistemas semelhantes existem por todo o mundo, como o “*hawala*” na Índia, Paquistão e Irã, ou ainda o sistema “*chop*”, “*chit*” ou “*flying money*”, os quais, quando não são legítimos ou reconhecidos pelos países nos quais são operados, são categorizados como “*underground banking*”.

O dólar-cabo ou euro-cabo é um sistema muito procurado no Brasil para lavagem de ativos, uma vez que não existe um controle ou informação às Autoridades Públicas sobre as operações. A atuação de “doleiros” no sistema de dólar-cabo caracteriza vários crimes contra o Sistema Financeiro Nacional e pode caracterizar “lavagem de dinheiro”.

FATF-GAFI: é um organismo internacional, criado em 1989 pelo chamado G-7 (os países com as sete maiores economias do planeta), com sede em Paris, o qual tem como finalidade o desenvolvimento e a promoção de políticas nacionais e internacionais para combater a lavagem de bens e o financiamento do terrorismo. Um dos mais importantes trabalhos do GAFI foi a edição de 40 (e depois mais nove) recomendações destinadas à prevenção e à repressão da lavagem de bens. Essas recomendações serviram como base para que muitos países, inclusive o Brasil,

aprovassem leis destinadas a reprimir a lavagem de bens.

Lavagem de Dinheiro: é o ato ou conjunto de atos que tem como finalidade ocultar ou dissimular a natureza, a origem, a localização, a disposição, a movimentação ou a propriedade de bens de qualquer natureza, obtidos com a prática de atividade ilegal. No caso do Brasil, apenas a prática de crimes formalmente previstos em lei pode ser fonte dos bens passíveis de lavagem. Esses crimes são chamados de crimes antecedentes. A “lavagem de dinheiro” é também chamada de lavagem de ativos, de capitais ou de valores. Em Portugal, usam-se as expressões “branqueamento de dinheiro”, “de ativos”, “de valores” ou “de capitais”.

Paraísos Fiscais: Paraísos fiscais são locais que oferecem às pessoas jurídicas constituídas em seus territórios uma tributação reduzida e segurança na realização de negócios, desde que esses últimos não ocorram dentro de suas fronteiras e as empresas pertençam a não-residentes. Podem ser países, territórios afiliados, principados, ilhas sem qualquer autonomia ou apenas regiões. Suas principais características são:

- a) alto padrão em sigilo financeiro e comercial;
- b) ausência/precariedade de controles internos;
- c) flexibilidade da legislação societária;
- d) ampla oferta de assessoria jurídico-contábil;
- e) presença de filiais das principais instituições financeiras do mundo;
- f) baixíssimo dever de Compliance das instituições financeiras;
- g) incentivos fiscais diversos;
- h) estabilidade política; e
- i) existência de ampla infraestrutura de comunicação e hotelaria.

Sujeito ativo: Chama-se sujeito ativo ao autor de um crime, isto é, à pessoa que pratica a ação ou omissão prevista na lei como crime. No caso do crime de lavagem, a lei brasileira não exige condição jurídica específica para que alguém possa praticar atos de ocultação de bens obtidos com o crime antecedente. Por consequência, qualquer pessoa, no Brasil, é potencialmente um sujeito ativo da lavagem de bens.

Sujeitos obrigados: Sujeitos obrigados são pessoas físicas ou jurídicas legalmente obrigadas, pela lei, a informar ao órgão de inteligência financeira de um país a prática de atos suspeitos de caracterizar lavagem de bens. No Brasil, as pessoas obrigadas a fazer essa comunicação estão indicadas no art. 9.º da Lei n.º 9.613, de 03 de março de 1998.

Unidade de inteligência financeira (UIF): é o órgão criado por lei, com a finalidade de receber comunicações de operações suspeitas e analisá-las, a fim de identificar possíveis atos de lavagem de bens. A UIF também pode coletar informações, por iniciativa própria, a fim de detectar tais atos. No Brasil, a UIF é o Conselho de Controle de Atividades Financeiras (COAF), criado pela Lei n.º 9.613, de 03 de março de 1998.

Doleiros: são pessoas físicas ou jurídicas (em especial Casas de Câmbio e Turismo) que operam no mercado cambial paralelo ou negro (*underground banking*) com recursos pertencentes a brasileiros, no Brasil e/ou no exterior.

Destacam-se três formas principais de atuação:

- a) câmbio manual;
- b) Dólar-Cabo ou Euro-Cabo (ver verbete neste glossário);
- c) gestão de “caixa 2” e de contas (categorias contábeis) em nome de clientes, o que é uma nova forma de atuação que tem sido cada vez mais constatada.

Tem sido detectada a participação de “doleiros” nos mais variados casos de “lavagem de dinheiro” no país, tais como: COPEL ADIFEA (peculato), MALUF (corrupção), ZAPATA (tráfico), LINCE (corrupção) etc.

A atuação dos “doleiros” pode ser vista como um movimento crescente de terceirização da lavagem de ativos e da manipulação de recursos oriundos de “caixa 2”.

Off-Shores: empresas *off-shore* (“fora da costa”) são empresas situadas em paraísos fiscais e que funcionam inclusive ou (como regra) exclusivamente em outro país. São também denominadas “*shell companies*” em razão de, como “concha”, esconderem os seus reais titulares, ou ainda “*shelf companies*” porque podem ser facilmente adquiridas como se fossem pinçadas de uma “prateleira”. Dentre os atrativos para sua conformação em um paraíso fiscal (vide verbete neste glossário) estão a baixa ou nenhuma tributação, a infraestrutura satisfatória no tocante a telecomunicações e estabilidade política, e o sigilo bancário quase ou totalmente impenetrável.

Embora possa assumir uso lícito, é utilizada para inúmeras finalidades ilícitas que muitas vezes estarão num contexto de lavagem de ativos:

- a) Esconder a identidade dos reais proprietários;
- b) É uma evolução do uso de “laranjas” e “fantasmas” em contratos sociais, na medida em que escondem os verdadeiros donos;

- c) Proteção patrimonial – contratos sociais e sucessões imobiliárias;
- d) Internação de recursos a título de integralização de capital (investimento) em empresas nacionais;
- e) Manutenção de recursos no exterior sem a devida declaração às autoridades competentes;
- f) Intermediar operações de comércio exterior em conjugação com crimes de falsidade.

e-Guardian: Software de monitoramento de “PLD/FTP” utilizado pelo “Intex Bank”.

Ativo virtual: representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, nos termos do art. 3º da Lei nº 14.478/2022, não incluídas a moeda nacional e as moedas estrangeiras.

Ativo virtual referenciado em moeda fiduciária (stablecoin): ativo virtual cujo valor é referenciado em moeda fiduciária, conforme o glossário do art. 2º da Resolução BCB nº 520/2025. USDC, EURC e USDT enquadram-se nesta categoria.

Prestadora de Serviços de Ativos Virtuais (PSAV/SPSAV): pessoa jurídica que executa, em nome de terceiros, serviços de ativos virtuais nas modalidades de intermediação, custódia e/ou corretagem, conforme a Resolução BCB nº 520/2025.

On-chain: registrado e verificável diretamente na rede blockchain em que o ativo virtual é transacionado.

Blockchain: tecnologia de registro distribuído que armazena transações em blocos encadeados e protegidos por criptografia, garantindo a integridade, rastreabilidade e imutabilidade das informações, sem a necessidade de uma autoridade central.

Travel Rule: regra que exige o compartilhamento de informações sobre remetente e beneficiário entre prestadoras de serviços de ativos virtuais nas transferências de ativos virtuais, em linha com a Recomendação 16 do GAFI.

Carteira autocustodiada (não custodial): carteira de ativos virtuais cujas chaves privadas são controladas diretamente pelo próprio titular, sem intermediação de prestador de serviço de custódia.

Carteiras fria, morna e quente: classificação das carteiras de custódia de ativos virtuais de acordo com o grau de conexão com a internet e a exposição a riscos. As carteiras frias (*cold wallets*) permanecem desconectadas da internet; as mornas

(*warm wallets*) possuem conexão intermitente e controlada; e as quentes (*hot wallets*) permanecem conectadas para a realização de operações correntes.

10. Contexto Histórico e Jurídico da Lavagem de Dinheiro

Com a internacionalização do crime organizado, especialmente do tráfico de drogas, em meados da década de 1980 e recentemente a questão do terrorismo internacional, foi percebida a necessidade de mudar a forma de combater a criminalidade: não bastava prender os criminosos, já que, em uma estrutura organizada, eles eram rapidamente substituídos por outros na cadeia de comando da organização. Era necessário estrangular as fontes de recursos dessas organizações. Surge o combate à “lavagem de dinheiro”. Uma vez que as autoridades não tinham como identificar esses recursos, foi necessário engajar as instituições financeiras nesse esforço. Posteriormente, diversos outros setores e profissionais, denominadas entidades ou setores obrigados, foram sendo incluídos como parceiros do Estado nesta luta.

10.1 O Princípio de “Conheça o seu Cliente” e as Comunicações de Operações Suspeitas

A terminologia adotada no Brasil é muito similar àquela utilizada em outros países, onde se fala de “blanqueo de capitales”, “money laundering”, “blanchiment d’argent”, “geldwashing” e “riciclaggio di denaro sporco”. A lei brasileira, entretanto, não menciona exatamente as palavras “dinheiro” ou “capital”, optando por referir à lavagem de bens, direitos ou valores o que confere maior abrangência ao conceito de lavagem.

10.2 Conceito de “Lavagem de Dinheiro”

Ainda que existam algumas diferenças conceituais sobre o tema “lavagem de dinheiro” entre os órgãos disciplinadores e supervisores, o que há de comum nas diversas interpretações é que se trata de processo utilizado por criminosos visando disfarçar ou ocultar, em operações aparentemente legítimas, recursos obtidos ilegalmente.

Na lei brasileira está definida a “lavagem de dinheiro” como a ocultação ou a dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, dos crimes que relaciona tráfico de drogas, terrorismo e seu financiamento, de

contrabando ou tráfico de armas, munições ou material destinado à sua produção, extorsão mediante sequestro, crimes contra a Administração Pública, contra o Sistema Financeiro Nacional, crimes praticados por organização criminosa, ou praticados por particular contra a administração pública estrangeira.

10.3 Etapas do Processo

As três fases do processo de lavagem de capitais são consideradas como sendo:

(i) Colocação - Corresponde às ações dos criminosos que visam afastar de si os valores ilicitamente obtidos, geralmente aplicando-os em estabelecimentos que lidam com grande volume de dinheiro (restaurantes, hotéis, bares, bingos, dentre outros), ou mesmo instituições financeiras (bancos, casas de câmbio, corretoras de ações, dentre outras);

(ii) Ocultação - Pode ser entendido pela lavagem propriamente dita. Consiste em dificultar o rastreamento contábil dos recursos ilícitos, buscando quebrar a cadeia de evidências a vista da possibilidade da realização de investigações sobre a origem do dinheiro. Os criminosos buscam movimentá-lo de forma eletrônica, transferindo os ativos para contas anônimas – preferencialmente, em países amparados por lei de sigilo bancário – ou realizando depósitos em contas "fantasmas".

(iii) Integração - Quando os ativos ilícitos já se encontram com sua origem criminosa encoberta, são transformados em valores aparentemente lícitos. Essa transformação ocorre por meio da criação, aquisição ou investimento dos valores em empresas lícitas de modo que os negócios dessas empresas apresentem resultados legítimos.

10.4 Resumindo as três fases da “Lavagem de Dinheiro”

A essência do processo, portanto, é separar o dinheiro de sua fonte ou origem (o delito antecedente);

Movimentá-lo tantas vezes quanto possível, criando camadas de operações (através de interpostas pessoas, físicas e/ou jurídicas) que o distanciem cada vez mais da origem e tornem imensamente difícil recompor as pistas de auditoria;

Para, ao final, reinvesti-lo em uma atividade inserida na economia legal, de forma que pareça ser inteiramente legítimo.

10.5 Métodos e Tendências

As formas de “lavar dinheiro” são múltiplas e extremamente variadas.

Os métodos utilizados e as técnicas empregadas mudam de acordo com a eficiência das medidas de prevenção (descoberto um ‘esquema’, os agentes da lavagem buscam outras brechas nas leis e na fiscalização para atingir seus objetivos).

A “lavagem de dinheiro” utiliza com frequência, instrumentos que são, em si, lícitos. Não é ilegal, por exemplo, abrir contas bancárias, fazer apólices de seguro, constituir sociedades comerciais, ou aplicar no mercado financeiro nacional ou internacional. Estas operações tanto poderão ser lícitas ou ilícitas, dependendo da finalidade para a qual foram praticadas, e da origem dos valores nelas envolvidos.

Quando forem praticadas com o objetivo de ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores que tenham sido obtidos com a prática de crimes, qualquer destes atos poderá caracterizar “lavagem de dinheiro”.

De uma forma geral, contudo, as tipologias refletem as formas mais frequentes através das quais ocorre a “lavagem de dinheiro”, em escala regional e internacional.

Indicam-se, a seguir, as principais tipologias de lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa (“LD/FTP”) às quais a instituição está potencialmente exposta e que são consideradas na Avaliação Interna de Riscos (AIR), entre as quais se destacam:

- Utilização de empresas de fachada ou empresas de passagem;
- Fracionamento de operações (*smurfing*);
- Uso de interpostas pessoas (laranjas);
- Movimentação financeira incompatível com a capacidade econômica;

- Transferências internacionais sem justificativa econômica;
- Utilização de ativos virtuais para ocultação da origem de recursos;
- Uso de *mixers*, *tumblers*, *bridges*, protocolos DeFi e carteiras não custodiadas;
- Conversão sucessiva entre diferentes ativos virtuais (*chain hopping*);
- Operações envolvendo jurisdições de alto risco ou sancionadas;
- Financiamento do terrorismo por meio de pequenas remessas pulverizadas;
- Financiamento da proliferação por operações envolvendo bens de uso dual ou países sujeitos a sanções internacionais.

11. Financiamento ao Terrorismo

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, o “Intex Bank” está preparado para identificar e reportar operações e situações atípicas e/ou suspeitas que possam ter relação com os crimes de terrorismo e o seu financiamento.

12. Crimes de Terrorismo

O “Intex Bank” adotará o processo de pesquisa para identificação de clientes, colaboradores, parceiros e prestadores de serviços, que possam estar associados à prática de Crimes de Terrorismo. Caso haja qualquer suspeita, a área de “PLD/FTP” deverá ser imediatamente informada para que faça as análises necessárias, tendo esta 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 consumir 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.

13. Pessoas Expostas Politicamente

A pessoa natural que ocupa algum dos cargos descritos abaixo é definida como Pessoa Exposta Politicamente – PEP, esta condição perdura por 5 (cinco) anos contados da data em que deixou o referido cargo.

- I. Detentores de mandatos eletivos dos poderes executivo e legislativo da União;
- II. Ocupantes de cargo, no poder executivo da União, de:
 - a) Ministro de Estado ou equiparado;
 - b) Natureza especial ou equivalente;
 - c) Presidente, vice-presidente e diretor, ou equivalentes, de entidades da

administração pública indireta;

d) Grupo direção e assessoramento superior – DAS, nível 6, ou equivalente.

- III. Membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores, dos Tribunais Regionais Federais, dos Tribunais Regionais do Trabalho, dos Tribunais Regionais Eleitorais, do Conselho Superior da Justiça do Trabalho e do Conselho da Justiça Federal;
- IV. Membros do Conselho Nacional do Ministério Público, o Procurador Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, os Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal;
- V. Membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;
- VI. Presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;
- VII. Governadores e os Secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os presidentes de Tribunais de Justiça, Tribunais Militares, Tribunais de Contas ou equivalentes dos Estados e do Distrito Federal; e
- VIII. Prefeitos, os Vereadores, os Secretários Municipais, os presidentes, ou equivalentes, de entidades da administração pública indireta municipal e os Presidentes de Tribunais de Contas ou equivalentes dos Municípios.
- IX. Também são consideradas pessoas expostas politicamente aquelas que, no exterior, sejam:
 - a) Chefes de estado ou de governo;
 - b) Políticos de escalões superiores;
 - c) Ocupantes de cargos governamentais de escalões superiores;

- d) Oficiais gerais e membros de escalões superiores do poder judiciário;
 - e) Executivos de escalões superiores de empresas públicas;
 - f) Dirigentes de partidos políticos;
 - g) Dirigentes de escalões superiores de entidades de direito internacional público ou privado.
- X. Também será considerado PEP a pessoa natural que seja familiar ou estreito colaborador, conforme especificado abaixo, de pessoa natural que ocupa algum cargo descrito acima.
- XI. Familiar: parentes, na linha direta ou colateral, até o segundo grau, cônjuge, companheiro, companheira, enteado e enteada; e
- XII. Estreito colaborador:
- Pessoa natural conhecida por ter qualquer tipo de estreita relação com pessoa exposta politicamente:
- 1) Ter participação conjunta em pessoa jurídica de direito privado;
 - 2) Figurar como mandatária, ainda que por instrumento particular da pessoa mencionada acima; ou
 - 3) Ter participação conjunta em arranjos sem personalidade jurídica.

Pessoa natural que tem o controle de pessoas jurídicas ou de arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de pessoa exposta politicamente.

14. Beneficiário Final

Pessoa natural ou pessoas naturais que, em conjunto, possuam, controlem ou influenciem significativamente, direta ou indiretamente, o qual se beneficie de uma transação que esteja sendo conduzida. Também é considerado beneficiário o representante, inclusive o procurador e o preposto, que exerça o comando de fato sobre as atividades da pessoa jurídica.

Para fins de identificação do beneficiário final, o “Intex Bank” considera todas as pessoas naturais que compõem o quadro societário e detenham participação direta

ou indireta na sociedade, observando o nível de risco atribuído ao cliente, nos termos das diretrizes estabelecidas no Manual de Conheça Seu Cliente (KYC) da instituição, respeitado o percentual mínimo de 25% (vinte e cinco por cento) previsto na legislação vigente.

No caso de pessoas jurídicas constituídas sob a forma de companhia aberta ou entidade sem fins lucrativos e as cooperativas, para identificação do beneficiário final, as informações coletadas devem abranger as informações das pessoas naturais autorizadas a representá-las, bem como seus controladores, administradores e diretores, se houver.

15. Operações com Ativos Virtuais

As operações com ativos virtuais referenciados em moeda fiduciária (*stablecoins*) realizadas pelo “Intex Bank” incluem intermediação de USDC, EURC e USDT. O “Intex Bank” atua exclusivamente como intermediário, não realizando custódia de ativos virtuais.

15.1 Monitoramento e Rastreamento On-Chain

Para operações com ativos virtuais, o “Intex Bank” implementa procedimentos de monitoramento e rastreamento *on-chain*, abrangendo:

- Rastreamento e monitoramento de transações em blockchain;
- Identificação e verificação de endereços de origem e destino;
- Análise de padrões e comportamentos transacionais na blockchain;
- Detecção de operações anômalas, suspeitas ou incompatíveis com o perfil do cliente;
- Integração com ferramentas especializadas de análise e inteligência blockchain;
- Comunicação e compartilhamento de informações relevantes com custodiantes e demais prestadores de serviços de ativos virtuais, quando identificadas transações suspeitas, observadas as disposições legais e regulatórias aplicáveis.

Os procedimentos para cumprimento da Travel Rule estão disciplinados no **Anexo I** desta Política, o qual estabelece o escopo de aplicação, as informações a serem compartilhadas, os procedimentos operacionais, os controles internos e as responsabilidades das áreas envolvidas, em conformidade com a legislação e a regulamentação vigentes.

16. Avaliação Interna de Risco - Diretrizes

A avaliação interna de risco visa identificar, analisar, mensurar e monitorar o risco de utilização de seus produtos e serviços na prática de lavagem de dinheiro e do financiamento do terrorismo e proliferação de armas, ou seja, o risco de “LD/FTP” que o “Intex Bank” está exposto.

A principal fonte de Risco de “LD/FTP” está concentrada nas operações de câmbio realizadas com clientes, em sua posição própria, no segmento primário, classificadas como comerciais e financeiras.

A classificação de Risco de “LD/FTP” parte da classificação de finalidade das operações conforme os anexos III, IV e V da Resolução BCB no 277/22.

O score de risco por código de finalidade representa o grau de atratividade de determinada finalidade para a lavagem de dinheiro/financiamento do terrorismo.

Para avaliação do Risco de “LD/FTP” do Produto/finalidade são considerados vários fatores tais como:

- Tipologias de Risco de “LD/FTP” presumíveis para o produto;
- Modelo de Negócios da Corretora, considerando os canais de distribuição do produto;
- Faixa de valores;
- Forma de Realização;
- País origem ou destino;
- Área Geográfica de Atuação;
- Atendimento presencial ou por meio de novas tecnologias; e
- Perfil da clientela.

A Avaliação Interna de Risco está formalizada em documento específico, devidamente aprovada pela Diretoria.

Ativos virtuais como vetor de risco: a avaliação interna de risco contempla, adicionalmente às operações de câmbio tradicionais, os riscos próprios das operações com ativos virtuais — entre os quais a pseudonímia das transações, a liquidação transfronteiriça quase instantânea e irreversível, a exposição a carteiras auto custodiadas, a serviços de anonimização (*mixers*) e a jurisdições de maior risco —, com tipologias e fatores de risco específicos, conforme detalhado na Avaliação Interna de Risco aprovada pela Diretoria.

17. Novos Produtos e Projetos - CCME, CNR e eFX

O “Intex Bank” avalia, com previsão de início em meados do segundo semestre de 2026, a operação de novos produtos no âmbito do mercado de câmbio: a Conta em Moeda Estrangeira no País (“CCME”), a Conta de Não Residente em reais (“CNR”) e o Serviço de Transferência ou Pagamento Internacional, ou câmbio eletrônico (“eFX”).

Tais produtos decorrem integralmente do mandato regulatório do “Intex Bank” como banco de câmbio autorizado a operar no mercado de câmbio, não constituindo nova autorização perante o Banco Central do Brasil.

Além disso, em razão da substancial similaridade desses produtos com as operações de câmbio já realizadas pelo “Intex Bank”, os controles, as ferramentas e os procedimentos de “PLD/FTP” aplicáveis são os mesmos já previstos nesta Política, sem prejuízo dos reforços específicos descritos no Anexo II.

O detalhamento do mandato regulatório permissivo, das tipologias de risco e dos controles e ferramentas de “PLD/FTP” aplicáveis a cada produto consta do Anexo II – Novos Produtos e Projetos: Mandato Regulatório e Controles de “PLD/FTP”, parte integrante desta Política. A operacionalização de cada produto observará a avaliação prévia de que trata esta Seção 17 e a aprovação pela Diretoria, sendo o respectivo produto incluído no rol da Seção 18 quando do início efetivo de sua operação.

18. Produtos, Serviços e Novas Tecnologias

O “Intex Bank” adotará procedimentos para avaliação de novos produtos, serviços e

novas tecnologias considerando a suscetibilidade à lavagem de dinheiro e financiamento do terrorismo e proliferação de armas. Todos os novos produtos, serviços e novas tecnologias deverão ser formalizados e aprovados pela Diretoria do “Intex Bank”.

São pontos pertinentes às particularidades de novos produtos ou serviços:

- Se está em consonância com a legislação vigentes e “PLD/FTP”;
- Compatibilidade com os objetivos da empresa;
- Identificação do público-alvo;
- Quais os benefícios;
- Se há região de abrangência ou se a abrangência é geral;
- Se a utilização e benefícios estão claros; e
- Se a rentabilidade esperada está de acordo com o custo envolvido na implementação.

As avaliações realizadas para os novos produtos, serviços e novas tecnologias, seguem as diretrizes sob ótica de “lavagem de dinheiro” estão de acordo com a Avaliação Interna de Risco e com requisitos contidos nesta política.

19. Produtos e Serviços oferecidos pelo “Intex Bank”

- Transferências internacionais;
- Câmbio Comercial;
- Câmbio e Turismo;
- Câmbio Financeiro;
- Money Transfer VIP;
- Assessoria especializada em câmbio;
- Consultoria técnica em serviços declaratórios;
- Câmbio internacional pré-pago multimoedas, inclusive em criptoativos;

- Cartão Corporativo;
- Serviços de Ativos Virtuais:
 - Intermediação de Ativos Virtuais: Facilitar a negociação de *stablecoins* (USDC, EURC, USDT) entre clientes;
 - Conversão de Ativos Virtuais: Converter *stablecoins* para moeda fiduciária e vice-versa;
 - Operações Cambiais com Ativos Virtuais: Realizar operações de câmbio envolvendo *stablecoins* e moedas fiduciárias.

Todos os serviços de ativos virtuais estão sujeitos aos mesmos procedimentos de “PLD/FTP” aplicáveis a operações de câmbio tradicional, com reforço adicional de controles conforme estabelecido pela Resolução BCB nº 520/2025.

20. Procedimentos de Controles Internos

Os clientes do “Intex Bank” são pessoas físicas e jurídicas que utilizam serviços e/ou operações cambiais. Todos os clientes são analisados sob ótica de “PLD/FTP”, por analistas treinados e especializados, apoiados no sistema de monitoramento e-Guardian (Advice – Compliance Solutions).

A utilização de ferramenta tecnológica específica para seleção, detecção e análise de operações e situações atípicas ou suspeitas, contribui para os procedimentos de controles internos e, a presente política, coaduna e complementa outros mecanismos de controle aplicáveis na “PLD/FTP” os quais, são adotados pelo “Intex Bank” e, devem ser aplicados em seu conjunto, de maneira organizada e metódica, para produzirem um resultado efetivo:

- Conheça seu Cliente (*Know Your Client - KYC*);
- Conheça seu Funcionário (*Know Your Employee - KYE*);
- Conheça seu Fornecedor (*Know Your Supplier - KYS*);
- Conheça seu Correspondente (*Know Your Partner - KYP*);
- Conheça sua Transação (*Know Your Transaction – KYT*);

- Cadastro de Clientes; Avaliação de Produtos;
- Procedimentos de Monitoramento, Seleção, Análise e Comunicação (“MSAC”);
- Dossiê das Operações Analisadas;
- Manual de Diagnósticos de Casos Atípicos e Suspeitos e Comunicação ao COAF;
- Treinamento.

21. Documentos Corporativos

21.1 “Conheça seu Cliente”

O procedimento denominado “Conheça seu Cliente”, é uma recomendação do Comitê de Basiléia, para que as instituições financeiras estabeleçam um conjunto de regras e procedimentos bem definidos com o objetivo de conhecer seu cliente, buscando identificar a origem e constituição do seu patrimônio e dos respectivos recursos financeiros. Conhecer o próprio cliente é uma medida de extrema importância no processo de prevenção à “lavagem de dinheiro”.

Conhecida internacionalmente como KYC (“*Know Your Customer*”), busca classificar e identificar os diferentes perfis de clientes, tanto para evitar que eles efetuem operações que possam acarretar riscos ao “Intex Bank” quanto para que o atendimento seja realizado da forma mais pontual possível, personalizada, atendendo às expectativas e necessidades.

Os procedimentos para obtenção dos detalhamentos requeridos são realizados na forma de uma “due dilligence” sobre o cliente (“DDC”) e quando necessário, devido à complexidade da análise, “due dilligence reforçada” (“EDD – Enhanced Due Dilligence”, a fim de dar maior segurança às informações apresentadas na Ficha Cadastral, cujo documento deverá estar preenchido em todos os campos obrigatórios, tanto na pessoa física como jurídica, e, para esta última, as informações cadastrais devem abranger as pessoas naturais autorizadas a representá-la, bem como a cadeia de participação societária, até alcançar a pessoa natural caracterizada como beneficiário final, conforme estabelece a legislação.

21.1.1 KYC Reforçado para Operações com Ativos Virtuais

Para clientes que realizam operações com *stablecoins*, o “Intex Bank” deve:

- a) Verificação Reforçada de Identidade: Utilizar múltiplas fontes para verificar identidade;
- b) Análise de Origem de Recursos: Investigar origem de recursos utilizados em operações com *stablecoins*;
- c) Análise de Destino de Recursos: Investigar destino de recursos obtidos da conversão de *stablecoins*;
- d) Verificação de Beneficiários Finais: Identificar e verificar todos os beneficiários finais;
- e) Análise de Padrão de Operação: Analisar padrão de operações com *stablecoins*;
- f) Atualização Periódica: Atualizar informações de KYC periodicamente (mínimo 18 meses).

21.2 “Conheça seu Funcionário”

Conhecida como “KYE” (*Know Your Employee*) ou Conheça Seu Empregado, consiste na aplicação de procedimentos que visam proporcionar um adequado conhecimento dos colaboradores do “Intex Bank”.

Conhecer seu Empregado baseia-se num conjunto de regras, procedimentos e controles que devem ser adotados para seleção e acompanhamento da situação econômico-financeira e idoneidade, visando a evitar vínculo com pessoas envolvidas em atos ilícitos.

21.3 “Conheça seu Fornecedor”

Conhecida como “KYS” (*Know Your Supplier*) ou Conheça seu Fornecedor, consiste na aplicação de procedimentos destinados a proporcionar o adequado conhecimento dos fornecedores os quais o “Intex Bank” mantenha relacionamento.

O Conheça seu Fornecedor baseia-se em um conjunto de regras, procedimentos e controles que devem ser adotados para a identificação, qualificação, aceitação e monitoramento de fornecedores, visando prevenir a contratação de empresas

inidôneas ou com indícios de envolvimento em atividades ilícitas, bem como mitigar os riscos de lavagem de dinheiro, financiamento do terrorismo e demais riscos legais, regulatórios, operacionais e reputacionais aos quais o “Intex Bank” possa estar exposto.

21.4 “Conheça seu Correspondente”

Conhecida como “KYP” (*Know Your Partner*), conhecer o seu Correspondente, baseia-se num conjunto de regras, procedimentos e controles que devem ser adotados para identificação e aceitação de correspondentes parceiros comerciais, visando prevenir a realização de negócios com contrapartes inidôneas ou suspeitas de envolvimento em atividades ilícitas, bem como assegurar que eles possuam procedimentos adequados de “PLD/FTP”.

O correspondente atua por conta e sob as diretrizes da instituição contratante, que assume inteira responsabilidade pelo atendimento prestado aos clientes e usuários por meio do contratado, à qual cabe garantir a integridade, a confiabilidade, a segurança e o sigilo das transações realizadas por meio do contratado, bem como o cumprimento da legislação e da regulamentação relativa a essas transações.

21.5 “Conheça sua Transação”

Conhecida como “KYT” (*Know Your Transaction*) ou Conheça sua Transação, consiste na aplicação de procedimentos destinados a proporcionar o adequado conhecimento das transações realizadas pelos clientes do “Intex Bank”.

O Conheça sua Transação baseia-se em um conjunto de regras, procedimentos e controles destinados ao monitoramento contínuo das transações, com o objetivo de identificar operações atípicas, incompatíveis com o perfil do cliente ou com indícios de lavagem de dinheiro, financiamento do terrorismo ou outros ilícitos, possibilitando a adoção tempestiva das medidas de diligência, investigação e comunicação às autoridades competentes, quando aplicável.

21.6 Cadastro de Clientes

O cadastro deverá ser atualizado de acordo com a classificação de risco atribuída ao cliente, em observância às diretrizes previstas no Manual “Conheça Seu Cliente” (KYC). As informações cadastrais exigidas observarão o tipo e a identificação do

cliente, conforme estabelecido na Política de Cadastro e no referido Manual.

21.7 Conheça seu Prestador de Serviços de Ativos Virtuais

Para os prestadores de serviços de ativos virtuais, o “Intex Bank” deve verificar a conformidade do prestador com a regulamentação aplicável aos ativos virtuais, a implementação de procedimentos de “PLD/FTP” e a existência de controles de segurança adequados. Adicionalmente, deve manter a documentação comprobatória da conformidade do prestador e realizar auditorias periódicas, de acordo com o risco e a relevância dos serviços prestados.

22. Teste da Base Cadastral

O “Intex Bank” realizará, no mínimo, anualmente, testes de consistência e qualidade de sua base cadastral, com o objetivo de verificar a adequação, completude e atualização das informações cadastrais de seus clientes.

Os testes abrangerão os cadastros de clientes pessoas físicas e pessoas jurídicas, mediante a seleção de uma amostra representativa e compatível com o universo de cadastros ativos da Instituição.

As inconsistências eventualmente identificadas deverão ser registradas, analisadas e tratadas por meio da definição e implementação de plano de ação, contemplando as medidas necessárias para a correção das falhas, a regularização dos cadastros afetados e o aprimoramento dos processos e controles internos, de forma a prevenir a recorrência das inconsistências verificadas.

23. Registro das Operações

O “Intex Bank” realiza o registro das operações no sistema Change, da Exchange Informática, contemplando:

- Tipo da operação;
- Valor;
- Data de realização;
- Cliente pessoa física - nome e número CPF;
- Cliente pessoa jurídica – razão social, número CNPJ, nome e número CPF do

beneficiário da operação;

- Cliente não residente pessoa física – Nome, país de origem e número do passaporte;
- Cliente não residente pessoa jurídica – Razão social, número de identificação ou de registro da empresa no país de origem;
- Tipo de ambiente e canal utilizado.

23.1 Rastreamento On-Chain de Operações com Ativos Virtuais

Para operações com stablecoins, o “Intex Bank” deve observar:

- a) Registro de Endereços: Registrar endereços de blockchain de clientes e contrapartes;
- b) Rastreamento de Transações: Rastrear transações em blockchain para verificar origem e destino;
- c) Análise de Padrões: Analisar padrões de transações para identificar atividades suspeitas;
- d) Documentação: Manter documentação de rastreamento por período mínimo de 10 anos;
- e) Integração com Monitoramento: Integrar dados de rastreamento on-chain com sistema de monitoramento de operações suspeitas.

24. Monitoramento

O acompanhamento e detecção das operações, que não envolvem o segmento de ativos virtuais, que fogem do padrão é definido e parametrizado no sistema e-Guardian. Embora o parâmetro mais comum seja a comparação entre “limites pré-estabelecidos “versus” movimentações”, o sistema permite diversos outros tipos de verificação, não somente aquelas que se referem à movimentação financeira do cliente, tratando variações significativas etc., como as inconsistências cadastrais.

Separados os casos para análise, a área de “PLD/FTP”, conforme a gravidade, reporta ao Comitê de “PLD/FTP” para que delibere sobre a comunicação (ou não) às autoridades competentes se confirmada a atipicidade ou suspeição da operação.

Principais critérios utilizados pelo monitoramento:

- Operações com valores superior e/ou incompatíveis com a capacidade financeira e patrimônio do cliente;
- Quantidade de operações no período;
- Os preceitos contidos na carta circular nº 4.001 de 29/01/2020 que divulga a 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 03/03/1998, e de financiamento ao terrorismo, previstos na Lei nº 13.260 de 16/03/2016, passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (COAF);
- Operações que denotam alteração no comportamento habitual do cliente.

Outros critérios utilizados:

- Análise do cadastro; estrutura das operações; movimentação em espécie; limites utilizados;
- Operações de maior complexidade no câmbio; carteira bloqueada, cancelada ou inativa;
- Operações realizadas oriundas de algum local de alto risco; movimentação com a utilização de procuradores;
- Clientes sensíveis, mudança de CEP duas vezes no mês; denúncias registradas no sistema interno;
- Análise da frequência das movimentações atípicas ou suspeitas;
- Reincidência de ocorrências;
- Informação do operador sobre o cliente.

Outras formas de monitoramento:

- Por meio dos atendentes (quando lojas) e pelos operadores nas Mesas de Negociação (matriz), treinados e familiarizados com o perfil dos clientes com atividade frequente ou recorrente;
- Pela área financeira mediante acompanhamento e análise do fluxo financeiro

inerente (ou não) às operações contratadas;

- Por meio da análise dos relatórios de operações extraídos dos sistemas operacionais em uso.

24.1. Monitoramento de Operações com Jurisdições de Risco

O “Intex Bank” deve monitorar operações com jurisdições que:

- a) Não aplicam ou aplicam insuficientemente as recomendações do GAFI;
- b) Têm sede em países com tributação favorecida ou regimes fiscais privilegiados;
- c) Têm prática contumaz de crimes de lavagem de dinheiro ou financiamento do terrorismo;
- d) Estão em lista de sanções internacionais.

Operações com estas jurisdições devem receber análise reforçada e, quando apropriado, ser reportadas ao COAF.

24.2. Monitoramento de Ativos Virtuais e Rastreamento On-Chain

Para operações com ativos virtuais, o “Intex Bank” implementa procedimentos de monitoramento e rastreamento on-chain, abrangendo:

- Rastreamento e monitoramento de transações em blockchain;
- Identificação e verificação de endereços de origem e destino;
- Análise de padrões e comportamentos transacionais na blockchain;
- Detecção de operações anômalas, suspeitas ou incompatíveis com o perfil do cliente;
- Integração com ferramentas especializadas de análise e inteligência blockchain;
- Comunicação e compartilhamento de informações relevantes com custodiantes e demais prestadores de serviços de ativos virtuais, quando identificadas transações suspeitas, observadas as disposições legais e regulatórias aplicáveis.

24.3. Segurança de Ativos Virtuais

O “Intex Bank”, por mais que não realize custódia, observa os seguintes procedimentos de segurança para operações com ativos virtuais:

- Utilização de multi-assinatura (*multi-sig*) para transações críticas;
- Implementação de *Multi-Party Computation* (MPC) para proteção de chaves;
- Segregação de carteiras (fria, morna, quente) conforme Resolução BCB 520; e
- Auditorias periódicas de segurança

Compatibilização do modelo operacional: considerando que o “Intex Bank” declara atuar exclusivamente como intermediário, sem custódia própria de ativos virtuais, os controles de proteção de chaves (multi-sig e MPC) e de segregação de carteiras (fria, morna e quente) recaem sobre o custodiante terceiro contratado, cabendo ao “Intex Bank” a supervisão e a verificação periódica de sua adequação. A nomenclatura de carteiras observa o glossário do art. 2º da Resolução BCB nº 520/2025. Caso o modelo de negócio venha a contemplar custódia direta, o enquadramento perante a Resolução BCB nº 520/2025 (modalidade custodiante) e os respectivos requisitos de segregação patrimonial deverão ser revistos, observada a vedação de exercício de custódia direta pela modalidade intermediária.

25. Análise de Operações Suspeitas

O “Intex Bank” realiza o monitoramento contínuo de seus clientes com o apoio de ferramenta tecnológica especialmente desenvolvida e contratada para essa finalidade. Ao identificar ocorrência atípica ou com indícios de lavagem de dinheiro e financiamento do terrorismo (“LD/FTP”), a situação é submetida ao Analista de “PLD/FTP” para análise tempestiva, com base nas informações disponíveis e em conformidade com os parâmetros estabelecidos no Manual de Diagnóstico de Casos Atípicos e Suspeitos e de Comunicação ao COAF e/ou MSAC.

Conforme estabelecido na regulamentação vigente, a detecção de situações merecedoras de análise da parte dos analistas de “PLD/FTP” deve ocorrer num prazo de até 45 (quarenta e cinco) dias da sua ocorrência ou apresentação da proposta pela operação atípica, e após a detecção da situação, a área de “PLD/FTP” deve concluir

as devidas análises em até 45 (quarenta e cinco) dias. Após conclusão, deve-se formalizar um dossiê consistente e detalhado para encaminhamento ao comitê de “PLD/FTP”, a alçada competente, dentro do prazo de 45 (quarenta e cinco) incorridos após a seleção do caso, e em havendo consenso quanto à decisão de comunicação ao COAF, deverá ocorrer num prazo máximo de 24 horas.

Operações suspeitas com ativos virtuais: incluem, mas não se limitam, às seguintes situações:

- a) Conversão de stablecoins para moeda fiduciária sem justificativa econômica aparente;
- b) Transferências internacionais de stablecoins para jurisdições de risco;
- c) Operações com stablecoins para contas de terceiros não relacionados;
- d) Conversão de stablecoins seguida de remessa de recursos ao exterior;
- e) Operações com stablecoins com documentação incompleta ou inconsistente;
- f) Operações com stablecoins envolvendo pessoas sancionadas;
- g) Estruturação de operações com stablecoins (smurfing);
- h) Operações com stablecoins com padrão atípico ou inconsistente com perfil do cliente;
- i) Operações com stablecoins para jurisdições com tributação favorecida ou regimes fiscais privilegiados;
- j) Operações com stablecoins envolvendo pessoas expostas politicamente (PEP).

26. Comunicação de Operações Suspeitas

O “Intex Bank” está regularmente cadastrada no Siscoaf e suas informações são mantidas atualizadas conforme prevê a Instrução Normativa COAF nº 5, de 30/09/2020.

A comunicação ao COAF, quando da identificação de operação ou proposta de

operação atípica, suspeita ou com indícios de “LD/FTP”, conforme norma vigente e já detalhado nesta política logo acima, é realizada até o dia útil seguinte ao da conclusão da análise e deliberação favorável à comunicação.

A comunicação deve estar fundamentada e em conformidade com o dossiê de evidências e análise que culminou com a decisão favorável à comunicação.

26.1. Comunicação de Operações Suspeitas com Ativos Virtuais

Para operações suspeitas envolvendo ativos virtuais, o “Intex Bank” deve:

- a) Reporte Imediato: Comunicar ao COAF, no prazo regulamentar;
- b) Informações Detalhadas: Incluir detalhes da operação, cliente, beneficiário, endereços de blockchain e valores;
- c) Justificativa Técnica: Fornecer justificativa técnica da suspeição (padrão atípico, origem suspeita, destino suspeito, etc.);
- d) Rastreamento On-Chain: Incluir análise de rastreamento on-chain da transação;
- e) Sigilo: Manter sigilo sobre comunicação ao COAF, não informando cliente sobre o reporte.

27. Dossiês das Operações Suspeitas e Atípicas

O dossiê das operações suspeitas e atípicas é mantido sob a custódia e responsabilidade da área de “PLD/FTP”. Os arquivos são armazenados na rede interna do “Intex Bank”, com acesso restrito às alçadas autorizadas. As atas de reuniões deliberativas e demais evidências (documentos e papéis de trabalho, portanto “físicas”) que compõem o dossiê de comunicação são mantidas em arquivo próprio e de acesso restrito. A via digitalizada do dossiê de comunicação é armazenada no sistema e-Guardian.

28. Procedimentos de Arquivamento e Registro das Operações Suspeitas e Atípicas

O produto das pesquisas e análises que não resultam em comunicação ao COAF é, igualmente, arquivado na rede interna do “Intex Bank”, protegido e com acesso

restrito. Os dossiês são identificados pelo nome do cliente e preserva as informações e decisões do diretor responsável ou Comitê de “PLD/FTP”. Todos os demais casos que tenham sido selecionados via sistema e-Guardian, considerados regulares e típicos após concluída a análise, dispõem de pertinente parecer e permanecem arquivados no próprio sistema “e-Guardian”.

29. Declaração Negativa - SISCOAF

Caso o “Intex Bank” não identifique, em determinado ano civil, fato motivador para registrar comunicação ao COAF, de operações atípicas, suspeitas ou passíveis de comunicação, procederá o registro da declaração de inexistência de situações sujeitas à comunicação, no Siscoaf em até dez (10) dias úteis após o encerramento do ano civil.

30. Formalização do Monitoramento, Seleção e Análise de Operações e Situações Suspeitas

O Procedimento de Monitoramento, Seleção e Análise de Operações Suspeitas está formalizado em documento específico, aprovado pela Diretoria e mantido atualizado, contendo os critérios utilizados para a definição das informações necessárias e dos procedimentos de verificação e validação, em linha com a Avaliação Interna de Risco.

31. Bloqueio de Ativos

O “Intex Bank” 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 naturezas, 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. O monitoramento é realizado pela área de “PLD/FTP” a qual também é responsável pelo bloqueio dos ativos.

Distinção entre obrigação legal e diligência prudencial: o dever legal de indisponibilidade decorre exclusivamente das resoluções sancionatórias do Conselho de Segurança das Nações Unidas e das designações nacionais e judiciais, nos termos da Lei nº 13.810/2019 e da Resolução BCB nº 44/2020. O rastreamento de operações contra listas estrangeiras (por exemplo, OFAC e União Europeia), embora

adotado pelo “Intex Bank” como medida prudencial, em razão do nexo das stablecoins com o dólar e o euro e dos relacionamentos com correspondentes, não constitui, por si só, fundamento legal autônomo de indisponibilidade de ativos no Brasil, devendo eventual recusa ou bloqueio observar base normativa adequada e os direitos do titular, inclusive sob a ótica da Lei nº 13.709/2018 (LGPD).

32. Treinamentos

O “Intex Bank” irá treinar periodicamente e de maneira adequada seus funcionários, colaboradores, correspondentes cambiais, prestadores de serviços e parceiros, mantendo-os capacitados e atualizados sobre o tema “PLD/FTP”. Os treinamentos poderão ser presenciais ou por plataformas digitais sendo mantidos em arquivo o histórico de testes/avaliações individuais aplicados (quando requerido), bem como o conteúdo dos treinamentos e eventuais certificados de participação, para consultas dos órgãos reguladores / fiscalizadores ou auditores. É incumbência da área de Compliance, zelar pelo programa de treinamento cuidando para que seja eficaz, incorporando eventos atuais e/ou alterações nas leis e regulamentos sobre a matéria “PLD/FTP”. O treinamento abrangerá casos reais ilustrativos dos esquemas de “LD” nos quais clientes e instituições financeiras são envolvidos e, também, situações adaptadas às atividades desempenhadas pelos participantes, orientando-os e instruindo-os quanto à detecção, o tratamento e solução das ocorrências.

32.1. Treinamento Específico em Ativos Virtuais

O “Intex Bank” deve oferecer treinamento específico sobre operações com stablecoins, incluindo:

- a) Características e riscos de stablecoins;
- b) Procedimentos de custódia segura;
- c) Monitoramento on-chain;
- d) Identificação de operações suspeitas com stablecoins;
- e) Procedimentos de bloqueio de ativos virtuais.

32.2. Programa de Treinamentos

O Programa de Treinamento na “PLD/FTP” utiliza-se dos seguintes recursos:

- Treinamento presencial ou pelo método EAD, assim como, treinamento específico para os novos colaboradores;
- Apresentação elaborada em Power Point, destacando diversos pontos e enfatizando a legislação vigente;
- Utilização dos vídeos educativos disponibilizados pelo COAF, Banco Central do Brasil e demais autoridades que disciplinam o Mercado Financeiro de Câmbio;
- Disponibilização, para consultas, de obras literárias versando sobre casos observados e registrados por autores especializados, contendo exemplos oriundos dos diversos segmentos do mercado financeiro, inclusive do mercado de câmbio;
- Disponibilização de notícias, via e-mail e comunicados internos, sobre o tema “LD/FTP” e assuntos de interesse inerentes ao negócio;
- Outros – Treinamentos em vídeo, teleconferências, palestras, reuniões ou workshops.

32.3. Acompanhamento e Manutenção de Registro dos Treinamentos

O registro de todos os colaboradores que receberam treinamento na “PLD/FTP” será mantido em arquivo como evidência concreta de que o “Intex Bank” está em conformidade e atende à exigência regulatória e, igualmente, para assegurar que todos os colaboradores tenham sido submetidos e atenderam ao requisito de treinamento obrigatório.

33. Ciência dos Colaboradores

Os colaboradores (staff, em geral) declaram ter ciência de que o “Intex Bank” faz o monitoramento das atividades por eles desempenhadas com o intuito de identificar casos suspeitos ou em não-conformidade com o Programa de “PLD/FTP”, quer seja por meio da presente Política e, também, demais documentos e normas aplicáveis.

34. Avaliação de Efetividade da Política de “PLD/FTP”

O “Intex Bank” avaliará a efetividade da política, dos procedimentos e dos controles internos de “PLD/FTP” e será documentado em relatório específico com data-base de 31 de dezembro, encaminhando-o ao Comitê Diretivo, para ciência, até 31 de março do ano seguinte.

A avaliação deverá contemplar:

- Procedimento Conheça seu Cliente (“KYC”), incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
- Procedimento de monitoramento, seleção, análise e comunicação ao COAF (“MSAC”;
- Ações de disseminação de informações voltadas à “PLD/FTP”;
- Programa de treinamento de colaboradores e correspondentes cambiais;
- Procedimentos conheça seu Colaborador e Prestadores de Serviços (“KYE”); conheça seu Parceiro (“KYP”), conheça seu fornecedor (“KYS”) e, cumprimento desta Política;
- Acompanhamento dos apontamentos da Auditoria Interna e da supervisão do Banco Central do Brasil.

34.1. Avaliação de Efetividade para Operações com Ativos Virtuais

A avaliação de efetividade deve incluir testes específicos para operações com stablecoins:

- a) Testes de Bloqueio: Verificar se sistema bloqueia operações com pessoas sancionadas;
- b) Testes de Monitoramento: Verificar se sistema identifica operações suspeitas com stablecoins;
- c) Testes de Rastreamento: Verificar se sistema consegue rastrear transações on-chain;
- d) Testes de Reporte: Verificar se sistema consegue gerar relatórios de operações

suspeitas com stablecoins.

35. Diretoria Responsável

A Diretoria de Governança é responsável pela emissão e atualização desta Política, assim como por orientar as áreas do “Intex Bank” quanto aos requisitos necessários para a implementação de mecanismos e controles necessários ao cumprimento da Lei nº 9.613/98, da Circular Bacen nº 3.978/20, e demais regulamentações relativas à “PLD/FTP”.

36. Manutenção dos Arquivos

O “Intex Bank” manterá armazenados e conservados todos os arquivos e informações pertinentes ao cumprimento desta Política, por período mínimo de 10 (dez) anos, contados da data do fim do relacionamento conforme legislação vigente, com ênfase nos documentos: conheça seu Cliente; conheça seu Fornecedor; conheça seu Empregado; conheça seu Parceiro e conheça seu Prestador de Serviços, Registro de Operações, dossiês de análises e comunicação, kit cadastral completo e documentos inerentes ao cadastro.

O “Intex Bank” manterá armazenados e conservados, igualmente, todos os arquivos e informações pertinentes ao cumprimento desta Política, por período mínimo de 05 (cinco) anos, conforme legislação vigente, com ênfase aos documentos de: versões da política de “PLD/FTP”; Ata de reuniões de Diretoria; versões da Avaliação Interna de Risco, contratos com outros bancos correspondentes, relatórios de efetividade, dados e mecanismos de acompanhamento de controles e planos de ação de acompanhamentos e todas as versões, políticas, manuais de procedimentos internos, manual de seleção, análise e comunicação etc.

37. Exceções

As situações não contempladas, não previstas ou que estejam em desacordo com esta política, deverão ser submetidas às áreas de Compliance e “PLD/FTP” para análise (das circunstâncias e fundamentos) e, subsequente encaminhamento ao Comitê Diretivo, para deliberação conjunta quanto ao acolhimento ou não das exceções.

38. Considerações Finais

A adesão a esta Política é obrigatória para todos os colaboradores do “Intex Bank”. O seu inteiro teor permanecerá publicado e disponível para consulta, a qualquer tempo, no ClickCompliance.

Cada funcionário declara ciência e conhecimento desta Política, mediante registro do “ACEITE”, quer seja quando de sua publicação no ClickCompliance (ferramenta tecnológica especialmente desenvolvida e utilizada para apoiar a governança corporativa), quer seja quando do início da relação de trabalho estabelecida com o “Intex Bank”. O referido termo de “ACEITE”, permanecerá armazenado no ClickCompliance, devendo um novo ser assinado eletronicamente sempre que esta for atualizada ou uma nova versão seja publicada.

39. Vigência

Esta política entra em vigor na data de sua publicação, sendo revisada no prazo de 12 (doze) meses, ou a qualquer momento, conforme a necessidade.

A aprovação formal desta política e posteriores atualizações devem ser realizada por todos os Diretores do “Intex Bank”.

São Paulo, 30 de junho de 2026.

O presente documento foi aprovado pelo Comitê Diretivo conforme Ata de Reunião realizada em 30/06/2026.

Anexo I - Procedimentos Operacionais da Travel Rule

1. Definição e Objetivo

A Travel Rule (Regra de Viagem) estabelece requisitos para a coleta, o registro e a transferência de informações relativas às operações com ativos virtuais entre prestadores de serviços de ativos virtuais (VASPs), no âmbito nacional e internacional, com o objetivo de fortalecer os controles de prevenção à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (“PLD/FTP”).

2. Informações a serem Transferidas

Em conformidade com o art. 44 da Resolução BCB nº 520/2025, as informações referentes às operações com ativos virtuais deverão ser coletadas, registradas e compartilhadas com os prestadores de serviços de ativos virtuais (VASPs) envolvidos, conforme aplicável, contemplando, no mínimo:

- Identificação do originador (cliente ou usuário remetente);
- Identificação do beneficiário (destinatário);
- Identificação do ativo virtual objeto da transferência;
- Montante transacionado; e
- Finalidade da transação.

3. Cronograma de Implementação

O “Intex Bank” implementará os requisitos da Travel Rule em observância aos prazos estabelecidos pela regulamentação vigente, conforme o cronograma abaixo:

Etapa I – Mercado Nacional

- Implementação dos procedimentos para coleta, registro e compartilhamento de informações entre prestadores de serviços de ativos virtuais (VASPs) estabelecidos no Brasil;
- Prazo: até 365 (trezentos e sessenta e cinco) dias contados da entrada em vigor

da Resolução BCB nº 520/2025;

- Status: Implementação em andamento.

Etapas II – Mercado Internacional

- Implementação dos procedimentos para coleta, registro e compartilhamento de informações em operações com ativos virtuais envolvendo prestadores de serviços de ativos virtuais (VASPs) estabelecidos no exterior, com os quais o “Intex Bank” mantenha relacionamento comercial;
- Prazo: até 365 (trezentos e sessenta e cinco) dias contados do término da Etapa I;
- Status: Planejamento em andamento.

Obrigatoriedade Integral (a partir de 2 de fevereiro de 2028)

- Cumprimento obrigatório de todos os requisitos da Travel Rule.
- Aplicável a todas as prestadoras de serviços de ativos virtuais autorizadas.

4. Procedimentos de Transferência de Informações

O “Intex Bank” implementa procedimentos para a transferência de informações relativas às operações com ativos virtuais, contemplando:

4.1 Identificação do Remetente e do Beneficiário:

- Coleta das informações completas do cliente ou usuário (remetente);
- Coleta das informações completas do beneficiário (destinatário);
- Verificação da identidade das partes, em conformidade com os procedimentos de Conheça Seu Cliente (KYC) reforçado.

4.2 Identificação do Ativo Virtual:

- Identificação do tipo de ativo virtual (ex.: USDC, EURC e USDT);
- Identificação do endereço da *blockchain*;

- Identificação da rede *blockchain* utilizada.

4.3 Montante e Finalidade:

- Registro preciso do montante transacionado;
- Registro da finalidade da transação;
- Análise da compatibilidade da transação com o perfil do cliente.

4.4 Transferência de Dados:

- Transferência das informações para outras prestadoras de serviços de ativos virtuais, conforme aplicável;
- Observância dos formatos e protocolos de transferência estabelecidos;
- Realização da transferência das informações em tempo real ou conforme os procedimentos internos aplicáveis;
- Manutenção e retenção de todos os registros pelo prazo mínimo de 5 (cinco) anos.

5. Autodeclarações (Período Transitório - até 2 de fevereiro de 2028)

Durante o período transitório (até 2 de fevereiro de 2028), o “Intex Bank” pode utilizar autodeclarações fornecidas por clientes e usuários:

5.1 Modelo de Autodeclaração:

- Declaração fornecida pelo cliente/usuário;
- Formato definido pelo “Intex Bank”;
- Deve identificar: cliente/usuário, beneficiário, ativo virtual, montante, finalidade;
- Informações devem ser de forma categórica (não genérica).

5.2 Processo de Coleta:

- Coleta da autodeclaração no momento da realização da operação;
- Armazenamento seguro da autodeclaração, em conformidade com os procedimentos internos de guarda e segurança da informação;

- Validação das informações declaradas em confronto com os dados cadastrais e as informações obtidas no âmbito dos procedimentos de Conheça Seu Cliente (KYC).

5.3 Documentação e Retenção:

- As autodeclarações deverão ser formalmente documentadas;
- Deverão ser mantidas à disposição do Banco Central do Brasil, sempre que solicitadas;
- Preferencialmente armazenadas em formato eletrônico, observados os requisitos de segurança e integridade da informação;
- Os registros deverão ser mantidos pelo prazo mínimo de 5 (cinco) anos, observado o disposto na regulamentação aplicável.

6. Análise Baseada em Riscos (Período Transitório - até 2 de fevereiro de 2028)

Durante o período transitório, o “Intex Bank” pode efetuar análise das operações realizadas com base nos riscos envolvidos:

6.1 Critérios de Risco:

- Montante da operação;
- Perfil de risco do cliente;
- Padrão transacional;
- Jurisdição de origem e de destino dos ativos virtuais;
- Tipo de ativo virtual envolvido na operação.

6.2 Procedimentos de Análise:

- Realização de análise de risco para cada operação, conforme abordagem baseada em risco;
- Documentação das análises realizadas e das diligências adotadas;
- Identificação e tratamento de operações classificadas como de maior risco;
- Comunicação ao COAF das operações ou situações com indícios de lavagem de dinheiro, financiamento do terrorismo ou outros ilícitos, quando aplicável.

6.3 Flexibilidade Regulatória:

- Observância das disposições transitórias previstas na regulamentação aplicável;
- Implementação gradual dos requisitos da Travel Rule, em conformidade com o cronograma regulatório;
- Comunicação tempestiva ao Banco Central do Brasil sobre eventuais dificuldades relacionadas à implementação ou ao cumprimento dos requisitos regulatórios, quando aplicável.

7. Integração com Custodiantes e Terceiros

Atualmente, o “Intex Bank” não presta serviços de custódia de ativos virtuais nem mantém relacionamento contratual com custodiantes para esse fim, atuando exclusivamente como intermediador nas operações envolvendo ativos virtuais. Não obstante, considerando a evolução regulatória e as melhores práticas de mercado, o banco optou por estabelecer diretrizes para eventual integração com custodiantes e demais Prestadores de Serviços de Ativos Virtuais (VASPs), de modo a assegurar, quando aplicável, o cumprimento dos requisitos da Travel Rule e das demais obrigações regulatórias relacionadas às transferências de ativos virtuais.

7.1 Comunicação com Custodiantes:

- Comunicação dos requisitos aplicáveis à Travel Rule;
- Solicitação de observância dos requisitos regulatórios aplicáveis;
- Monitoramento da conformidade dos custodiantes;
- Registro e documentação das comunicações realizadas.

7.2 Procedimentos de Integração:

- Integração de sistemas para o compartilhamento de informações relativas às operações com ativos virtuais;
- Definição de protocolos de comunicação com outras prestadoras de serviços de ativos virtuais;
- Realização de testes de integração e validação dos controles implementados;

- Documentação dos procedimentos operacionais adotados.

7.3 Monitoramento da Conformidade:

- Verificação periódica da conformidade dos custodiantes;
- Auditoria dos procedimentos de compartilhamento de informações;
- Comunicação ao Banco Central do Brasil sobre eventuais dificuldades relacionadas ao cumprimento da regulamentação, quando aplicável;
- Implementação de ações corretivas sempre que identificadas deficiências ou não conformidades.

7.4 Relacionamento com Entidades Internacionais:

- Identificação das entidades estrangeiras com as quais o “Intex Bank” mantenha relacionamento comercial;
- Alinhamento quanto aos requisitos aplicáveis à Travel Rule;
- Implementação de procedimentos para o compartilhamento de informações em operações internacionais com ativos virtuais;
- Observância da regulamentação aplicável às operações internacionais.

8. Reporte ao Banco Central do Brasil

O “Intex Bank” implementa procedimentos de reporte ao Banco Central do Brasil (BCB), visando assegurar a conformidade com os requisitos da Travel Rule e demais obrigações regulatórias aplicáveis.

8.1 Comunicação de Dificuldades:

- Comunicação tempestiva ao Banco Central do Brasil sobre eventuais dificuldades relacionadas ao controle e ao monitoramento das operações com ativos virtuais;
- Comunicação de dificuldades decorrentes de práticas adotadas por outras instituições autorizadas a funcionar pelo Banco Central do Brasil que possam comprometer o cumprimento das obrigações regulatórias;
- Registro e documentação das dificuldades identificadas, bem como das medidas corretivas adotadas.

8.2 Documentação:

- Manutenção de documentação completa que comprove a conformidade com os requisitos da Travel Rule;
- Disponibilização da documentação ao Banco Central do Brasil, sempre que solicitada, para fins de supervisão ou inspeção;
- Retenção da documentação e dos registros relacionados pelo prazo mínimo de 5 (cinco) anos, observado o disposto na regulamentação aplicável.

Anexo II - Novos Produtos e Projetos

1. Objetivo e alcance

Este Anexo integra a Política de “PLD/FTP” e detalha, para os novos produtos com previsão de início no segundo semestre de 2026 – CCME, CNR e eFX –, o mandato regulatório que autoriza o “Intex Bank” a operá-los e os controles e ferramentas de “PLD/FTP” aplicáveis. Por se tratar de operações do mercado de câmbio análogas às já realizadas pela instituição, os controles são, em regra, os mesmos já vigentes nesta Política, com os reforços específicos indicados em cada produto.

2. Mandato regulatório permissivo

O “Intex Bank” é banco de câmbio, instituição financeira especializada na realização de operações de câmbio nos termos do art. 1º da Resolução CMN nº 3.426, de 21 de dezembro de 2006. Como banco autorizado a operar no mercado de câmbio, está apto a realizar todas as operações desse mercado, nos termos do Título II da Resolução BCB nº 277, de 31 de dezembro de 2022. O escopo do mercado de câmbio, definido no art. 1º da Resolução BCB nº 277/2022 e na Lei nº 14.286, de 29 de dezembro de 2021, abrange os pagamentos e as transferências internacionais (inciso II), as contas em reais de titularidade de não residentes (inciso III) e as contas em moeda estrangeira mantidas no Brasil (inciso IV, com redação dada pela Resolução BCB nº 521/2025). Os três produtos enquadram-se nesse escopo, conforme o quadro a seguir:

Produto (sigla)	Base do mandato no mercado de câmbio	Norma específica / observação
Conta em Moeda Estrangeira no País (CCME)	Lei nº 14.286/2021; Res. BCB nº 277/2022, art. 1º, IV (red. Res. BCB nº 521/2025) e Título VIII; mandato de banco de câmbio (Res. CMN nº 3.426/2006, art. 1º)	Res. BCB nº 575/2026 (norma específica das contas em moeda estrangeira)
Conta de Não Residente em reais (CNR)	Lei nº 14.286/2021; Res. BCB nº 277/2022, art. 1º, III e Título VII; mandato de banco de câmbio (Res. CMN nº 3.426/2006, art. 1º)	Res. BCB nº 277/2022, arts. 67 e 68 e Anexo II (prestação de informações ao BCB)
Serviço de Transferência ou Pagamento	Lei nº 14.286/2021; Res. BCB nº 277/2022, art. 1º, II, Título V; mandato de banco de câmbio	Realizado diretamente pelo “Intex Bank” como instituição autorizada;

Internacional – câmbio eletrônico (eFX)	(Res. CMN nº 3.426/2006, art. 1º) e Resolução BCB nº 575.	
---	--	--

3. Controles e ferramentas de “PLD/FTP” aplicáveis

Por integrarem o mercado de câmbio, os três produtos estão sujeitos à mesma estrutura de controles de “PLD/FTP” adotada pelo “Intex Bank”, observando os procedimentos de governança, diligência, monitoramento e gestão de riscos aplicáveis às operações da instituição. Nas operações que envolvam ativos virtuais, aplicam-se, adicionalmente, os controles específicos previstos para esse segmento, incluindo o rastreamento on-chain e a observância da Travel Rule.

CCME – vetores de risco específicos: movimentações da conta passíveis de uso para estruturação, além da convergência com o arcabouço de ativos virtuais (Res. BCB nº 521/2025). Reforço de controle: monitoramento das movimentações e do saldo da conta em moeda estrangeira, integrado às tipologias da Avaliação Interna de Risco.

CNR – vetores de risco específicos: identificação de beneficiário final e de estruturas no exterior (offshore), movimentações por interesse de terceiros e exposição a jurisdições de maior risco. Reforço de controle: diligência reforçada de beneficiário final, monitoramento das movimentações por interesse de terceiros e prestação de informações ao Banco Central do Brasil na forma do Anexo II da Res. BCB nº 277/2022.

eFX – vetores de risco específicos: atendimento não presencial por meio de canal eletrônico – fator de risco já contemplado na Avaliação Interna de Risco –, velocidade transacional e risco de fracionamento. Reforço de controle: controles de onboarding não presencial, detecção de fracionamento (vedado pela Res. BCB nº 277/2022) e classificação de finalidade conforme os Anexos da referida Resolução.

4. Remissão

Este Anexo deve ser lido em conjunto com a Avaliação Interna de Risco, com a Seção 17 (Avaliação de Produtos, Serviços e Novas Tecnologias) e com a Seção 18 (Produtos e Serviços oferecidos pelo “Intex Bank”) desta Política. A inclusão de cada produto no rol da Seção 18 ocorrerá quando do início efetivo da respectiva operação, mantida a aplicação integral dos controles aqui previstos.