POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO

03/06/2021

SUMÁRIO

POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO

1. OBJETIVO

Estabelecer padrões de conduta e controles quanto à prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo, em linha com a legislação aplicável e as melhores práticas de mercado.

2. APLICAÇÃO E VIGÊNCIA

Aplica-se a todos os Colaboradores e Terceiros associados à Vixi Exchange, a partir de **03/06/2021**. A presente Política será renovada anualmente.

3. DEFINIÇÕES

- **Circular BCB 3.978**: a Circular nº 3.978, de 23 de janeiro de 2020, do Banco Central do Brasil;

- **Colaborador(es):** todos os funcionários e empregados da Vixi Exchange, bem como todos que possuam cargo, função, posição, ou relação societária, empregatícia, comercial, profissional, contratual ou de confiança com a Vixi Exchange, assim como os estagiários e trainees;

- **Diretoria**: trata-se de grupo formado pelos membros da diretoria da Vixi Exchange. A Diretoria tem por função acompanhar os projetos da Companhia e seus respectivos resultados, bem como deliberar e direcionar os referidos projetos com base no melhor interesse da Companhia;

- **Parceiro**: pessoas físicas ou jurídicas que mantêm negócios com a Vixi Exchange;

- **PLD/CFT**: prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo;

- **Política**: a presente Política de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo;

- **Terceiro(s):** fornecedores e prestadores de bens e serviços, representantes, agentes

intermediários, procuradores, consultores técnicos, despachantes, colaboradores externos e/ou quaisquer outros terceiros que atuem em nome, benefício ou interesse da Vixi Exchange.

4. CONCEITOS PRELIMINARES

4.1. LAVAGEM DE DINHEIRO (LD)

4.1.1. A Diretoria da Vixi Exchange está altamente comprometida com o programa de Compliance e demonstra seu comprometimento com o combate à lavagem de dinheiro e ao financiamento do terrorismo incorporando o assunto em seus discursos, assim como tornando o tema "compliance" pauta de suas reuniões e direcionador para tomadas de decisões.

4.1.2. A presente Política visa a coibir quaisquer práticas de lavagem de dinheiro e de financiamento do terrorismo, em qualquer das etapas abaixo descritas:

- **Colocação**: a etapa em que o criminoso introduz o dinheiro obtido ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou bens. Trata-se da remoção do dinheiro do local em que foi ilegalmente adquirido e sua inclusão, por exemplo, no mercado financeiro;

- **Ocultação**: o momento em que o criminoso realiza transações suspeitas caracterizadoras do crime de lavagem. Nesta fase, transações complexas se configuram para desassociar a fonte ilegal do dinheiro, dificultando o rastreamento da origem pelas autoridades. O objetivo é "quebrar" a cadeia de evidências ante o risco de investigações sobre a origem dos recursos;

- **Integração**: os ativos são incorporados formalmente ao sistema econômico e financeiro. A partir deste momento, o dinheiro recebe aparência lícita.

4.1.3. [Corretoras de criptoativos], como a Vixi Exchange, podem ser utilizadas inadvertidamente como intermediárias em algum processo de ocultação de recursos procedentes de atividades criminosas, sobretudo na segunda fase do processo de lavagem de dinheiro, na qual o objetivo é "quebrar" a cadeia de evidências sobre a origem do dinheiro (rastreabilidade).

4.2. FINANCIAMENTO AO TERRORISMO (FT)

4.2.1. Financiamento do terrorismo é o apoio financeiro, por qualquer meio, ao terrorismo ou àqueles que o incentivam, planejam ou cometem. Tem como objetivo fornecer fundos ou capital para atividades terroristas.

4.2.2. Essa arrecadação de fundos ou capital pode acontecer de diversas formas, tanto a partir de fontes legais (tais como contribuições associativas, doações ou lucros de atividades comerciais) ou a partir de fontes criminosas, como o tráfico de drogas, o contrabando de armas, a prostituição, bens e serviços tomados indevidamente, crime organizado, fraude, sequestro, extorsão etc.

4.2.3. A luta contra o financiamento do terrorismo está intimamente ligada ao combate à lavagem de dinheiro, já que as técnicas utilizadas para lavar o dinheiro são essencialmente as mesmas utilizadas para ocultar a origem e o destino do financiamento do terrorismo, para que, assim, as fontes continuem a enviar montantes sem a devida identificação.

5. RESPONSABILIDADES

5.1. É de reponsabilidade da Diretoria Executiva promover e disseminar a Política para a estrutura organizacional, clientes, Parceiros, sócios e prestadores de serviços da Vixi Exchange, assim como as boas práticas para monitoramento e identificação preventiva de eventuais ilícitos.

5.2. A Diretoria Executiva deverá adotar mecanismos de comunicação, informação e conscientização da importância da PLD/CFT dentro da organização, inclusive provendo a estrutura organizacional e todas as ferramentas tecnológicas para as diligências que decorrem desta Política.

5.3. Caberá à Diretoria Executiva instituir o Comitê de Compliance, composto por profissionais das áreas operacionais, legal e Compliance.

5.4. O Comitê de Compliance é responsável por monitorar as atividades destacadas na presente Política e nos procedimentos relacionados, assim como executar as diligências necessárias para monitoramento e identificação de riscos relacionados à PLD/CFT.

5.5. A área de Compliance é responsável pelo monitoramento das atividades operacionais e financeiras da Vixi Exchange. Para eventuais desvios e constatações, a área de Compliance deverá comunicar oportunamente o Comitê de Compliance, que dará as devidas tratativas.

5.6. Constatado desvios e/ou tentativas de práticas de lavagem de dinheiro e de estruturas de financiamento do terrorismo, será de responsabilidade da Diretoria Executiva, com o apoio da área de Compliance, comunicar, imediatamente, as autoridades competentes.

5.7. Todos os Colaboradores da Vixi Exchange são responsáveis por monitorar suas atividades de risco por meio dos instrumentos mitigatórios. Em casos de constatação de desvio e/ou tentativa de ações de lavagem de dinheiro e formação de estruturas de terrorismo, o Colaborador deverá comunicar imediatamente sua liderança e área de Compliance, que iniciará suas diligências.

6. CULTURA ORGANIZACIONAL

6.1. A Diretoria da Vixi Exchange está altamente comprometida com seu programa de compliance. A Diretoria demonstra seu comprometimento com PLD/CFT incorporando o assunto em seus discursos, bem como tornando o tema “compliance” pauta de suas reuniões.

6.2. Treinamentos de compliance que abordem temas como PLD/CFT, ética, prevenção à corrupção, prevenção à fraude, segurança da informação, dentre outros, serão ministrados, no mínimo, anualmente aos Colaboradores. Aos Terceiros, os treinamentos serão ministrados conforme demanda.

6.3. Os treinamentos acima mencionados servem para a promoção de cultura organizacional ética e de PLD/CFT da Vixi Exchange.

6.4. Todas as ações para engajamento do time Vixi Exchange são respaldadas pelo cumprimento do Código de Ética, a qual é submetido para conhecimento de todos os Colaboradores, Terceiros, líderes e Diretoria Executiva.

7. DIRETRIZES E CONTROLES-CHAVE

7.1. Com o objetivo de garantir que a Vixi Exchange não seja utilizada para práticas de lavagem de dinheiro e de financiamento do terrorismo, os Colaboradores deverão aplicar todos os

esforços possíveis para determinar a verdadeira identidade de todos os clientes/parceiros que solicitam os produtos e/ou serviços da Vixi Exchange.

7.2. Estão terminantemente proibidas as transações comerciais com terceiros que deixem de apresentar comprovação de identidade ou qualquer outro documento e/ou informações relevantes requeridas pela empresa para seu cadastramento.

7.3. A Vixi Exchange conduz seus negócios em conformidade com os mais elevados padrões éticos, observando todas as leis e regulamentos aplicáveis às suas atividades e as melhores práticas de mercado, especialmente no que tange à PLD/CFT. Para tanto, os seguintes aspectos sempre são observados e executados:

- Matriz de responsabilidades dos integrantes de cada nível hierárquico;

- Avaliação interna dos riscos de ocorrência da prática dos crimes supracitados no que tange a clientes, Colaboradores e Terceiros;

- Definição dos critérios e atividades para seleção, treinamento e avaliação periódica dos Colaboradores, em linha com as diretrizes estabelecidas na presente Política;

- Avaliação interna dos riscos de ocorrência da prática dos crimes supracitados no que tange os próprios produtos e serviços oferecidos pela Vixi Exchange;

- Práticas para análise das operações e identificação de operações suspeitas;

- Confirmação de informações cadastrais e identificação de beneficiários finais;

- Procedimentos para a identificação de Pessoa Exposta Politicamente – PEP, bem como a diferenciação em sua análise, em conformidade com o artigo 19 da Circular BCB 3.978, a título de melhores práticas;

- Instruções para o início de relacionamento com instituições financeiras, representantes ou correspondentes no exterior, especialmente em países, territórios e dependências que não adotam procedimentos de registro e controle similares aos definidos nesta Política;

- Instruções de comunicação aos órgãos competentes quanto às informações requeridas nas regulamentações vigentes, em especial quanto a suspeitas relacionadas à lavagem de dinheiro e ao financiamento de atividades terroristas; e

- Pontos de atenção no cadastramento dos clientes e parceiros de negócios, detalhado de forma completa no ato do cadastro e aprovação de propostas.

7.4. Todos os procedimentos de PLD/CFT serão tratados de forma mais minuciosa em documento apartado formalizado.

8. PROCEDIMENTOS PARA CONHECER COLABORADORES (KYE)

8.1. Os controles de prevenção funcionam adequadamente apenas se todos os Colaboradores estiverem conscientes de sua importância e de como devem ser operacionalizados. Para tanto, é fundamental que todos conheçam as normas externas, normas internas e controles em operação relativos à PLD/CFT.

8.2. Os procedimentos "conheça-seu-funcionário" (*Know Your Employee – KYE*) são rotinas de trabalho, incluindo as respectivas ferramentas necessárias para sua execução, que visam propiciar à instituição um adequado conhecimento sobre seus Colaboradores, principalmente no que tange aos seguintes aspectos:

- Foco na identificação de fraudes e conivência com a prática de crimes;

- Alteração inusitada nos padrões de vida e comportamento;

- Atenção especial com Colaboradores envolvidos em processos mais vulneráveis; e

- Modificação inusitada do resultado operacional do Colaborador.

8.3. Para toda e qualquer contratação deverá ser seguido procedimento de análise e coleta de documentação pela área de RH. Para áreas/processos de maior vulnerabilidade, deverão ser efetuadas análises mais detalhadas do profissional, nos termos do Procedimento de Conheça seu Funcionário. As análises, bem como seus resultados, são de responsabilidade da área de Compliance e deverão ser mantidas sob confidencialidade.

9. PROCEDIMENTOS PARA CONHECER PRODUTOS E SERVIÇOS (KYPS)

9.1. Todos os produtos e serviços ofertados pela Vixi Exchange serão analisados segundo seu risco de utilização para lavagem de dinheiro e financiamento do terrorismo.

9.2. O risco do produto ou serviço será analisado conjuntamente com o risco do cliente e/ou parceiro que utilizá-lo.

9.3. O Procedimento de KYPS compreenderá a avaliação e a análise prévia de novos e produtos e serviços, bem como a utilização de novas tecnologias, tendo em vista o risco de lavagem de dinheiro e de financiamento do terrorismo. No âmbito dessa análise, a área de Compliance avaliará se a presente Política está adequada e suficiente para a oferta do novo produto ou serviço e/ou utilização da nova tecnologia pretendida.

10. PROCEDIMENTOS PARA CONHECER CLIENTES (KYC) E PARCEIROS DE NEGÓCIOS (KYP)

10.1. A Vixi Exchange estabelece como seus principais procedimentos de PLD/CFT o Procedimento de *Know Your Customer – KYC* (conheça seu cliente) e o *Know Your Partner – KYP* (conheça seu parceiro de negócios).

10.2. Por meio dos procedimentos específicos, a Vixi Exchange busca não só conhecer a verdadeira identidade de seus clientes e prospects, mas também traçar o perfil de risco de cada um, estabelecendo relacionamento mais próximo, de forma a entender as suas reais expectativas e necessidades para atendimento de demandas.

10.3. Este conceito de relacionamento permite identificar os reais propósitos dos clientes/parceiros para prevenir a atuação daqueles que procuram a empresa com objetivos inidôneos.

10.4. Todos os Colaboradores devem conhecer os principais conceitos do mercado e indicações dos organismos reguladores e autorreguladores relacionados à identificação, prevenção e combate à lavagem de dinheiro e ao financiamento do terrorismo. Abaixo recomendações de extrema relevância:

- Identificar o cliente/parceiro via documentos, dados e informações de origem fidedigna e independente;

- Identificar o beneficiário efetivo e tomar medidas para verificar a sua real identidade;

- Manter vigilância contínua sobre a relação de negócios e examinar atentamente as operações realizadas no decurso dessa relação, verificando se são condizentes com o conhecimento que a instituição possui do cliente/parceiro, seus negócios, perfil de risco e origem de fundos, caso aplicável;

- Examinar com particular atenção todas as operações complexas, com montantes significativos e todos os tipos não habituais de operações sem causa econômica ou lícita aparente; e
- Comunicar à área de Compliance todo e qualquer indício de informações falsas, operações divergentes à situação financeira, operações divergentes do perfil ou qualquer situação atípica que gere suspeita de irregularidade.

11. PESSOAS EXPOSTAS POLITICAMENTE – PEP

11.1. Consideram-se PEPs, no Brasil:

- Detentores de mandatos eletivos dos Poderes Executivo e Legislativo da União;

- 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; e (d) Grupo Direção e Assessoramento Superiores (DAS), nível 6, ou equivalente;

- 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;

- 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;

- Membros do Tribunal de Contas da União, o Procurador-Geral e os Subprocuradores-Gerais do Ministério Público junto ao Tribunal de Contas da União;

- Presidentes e os tesoureiros nacionais, ou equivalentes, de partidos políticos;

- Governadores e 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

- 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.

11.2. Consideram-se também PEPs, no exterior:

- Chefes de estado ou de governo;

- Políticos de escalões superiores;

- Ocupantes de cargos governamentais de escalões superiores;

- Oficiais-generais e membros de escalões superiores do Poder Judiciário;

- Executivos de escalões superiores de empresas públicas; e

- Dirigentes de partidos políticos.

11.3. São também consideradas PEPs os dirigentes de escalões superiores de entidades de direito internacional público ou privado.

11.4. A condição de PEP deve ser aplicada pelos 5 (cinco) anos seguintes à data em que a pessoa deixou de se enquadrar nos cargos supracitados.

11.5. Considera-se familiar de PEP: os parentes, na linha reta ou colateral, até o segundo grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada.

11.6. Considera-se estreito colaborador de PEP: (a) a pessoa natural conhecida por ter qualquer tipo de estreita relação com PEP, inclusive por (i) ter participação conjunta em pessoa jurídica de direito privado; (ii) figurar como mandatária, ainda que por instrumento particular da pessoa mencionada no item (i); (iii) ter participação conjunta em arranjos sem personalidade jurídica; e (b) pessoa natural que tem o controle de pessoas jurídicas ou de arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de PEP.

11.7. As operações ou propostas de operações que possuam PEP, seu representante, familiar ou estreito colaborador como parte envolvida serão sempre consideradas como merecedoras de especial atenção, nos termos da presente Política.

11.8. Toda documentação cadastral de clientes enquadrados como PEP, familiar ou estreito colaborador de PEP deve ser encaminhada à área de Compliance, sendo que, nesses casos, a realização do *Third-Party Due Diligence* (TDD), detalhada no item 13 desta Política, é obrigatória.

11.9. Ao efetuar operações para PEPs, familiares ou estreitos colaboradores de PEPs, ou em seus nomes, os Colaboradores deverão estar atentos a qualquer indício, mesmo que potencial, de lavagem de dinheiro ou de financiamento de atividades terroristas, conforme exemplos abaixo:

- Solicitação de associar alguma forma de sigilo com uma transação, como, por exemplo, registrar a transação em nome de outra pessoa ou de uma empresa cujo favorecido não tenha sua identidade revelada;

- Direcionamento de transações por meio de várias jurisdições e/ou instituições financeiras, sem propósito evidente, exceto o de ocultar a natureza, fonte, detenção ou controle dos fundos;

- Rápido aumento ou redução dos recursos ou valor dos ativos na conta de uma PEP, familiar ou estreito colaborador de PEP, que não seja atribuível a flutuações no valor de mercado dos instrumentos de investimento detidos na conta;

- Uso frequente ou excessivo de transferências de fundos ou transferências eletrônicas para a conta de uma PEP, familiar ou estreito colaborador de PEP ou originando-se dela;

- Depósitos ou retiradas de alto valor que não sejam condizentes e proporcionais ao tipo de conta e patrimônio legítimo ou atividades do cliente;

- Existência de um modelo segundo o qual, depois que um depósito ou transferência eletrônica é recebido pela conta, os fundos são rapidamente transferidos no mesmo valor para outra instituição financeira, especialmente se a transferência for efetuada para uma conta em instituição financeira *offshore* ou em "jurisdição sigilosa"; e

- Consulta pela PEP a respeito de exceções aos requisitos de manutenção de registros ou apresentação de relatório ou outras normas que exigem a comunicação de transações suspeitas.

12. PESSOAS DE MÍDIA

12.1. São consideradas “Pessoas de Mídia” aquelas que estejam em voga na mídia, como artistas, esportistas, jornalistas, incluindo membros de suas ‘’famílias imediatas’’ (pais, irmãos, cônjuge, filhos e parentes por afinidade) e ‘’associados próximos’’ (pessoa ampla e publicamente conhecida por manter relacionamento extraordinariamente próximo com a Pessoa de Mídia, incluindo uma pessoa que está em condições de realizar transações financeiras, em âmbito nacional e internacional, em nome desta última) e sociedades, empresas, ou outras pessoas jurídicas que tenham sido formadas por uma Pessoa de Mídia ou em seu benefício.

12.2. Quando um Colaborador identificar a existência real ou potencial de negócios com Pessoa de Mídia, deve comunicar o fato imediatamente à área de Compliance para análise. No caso de comprovação, devem ser adotados os mesmos procedimentos para PEPs, conforme disposto acima, com exceção da autodeclaração.

13. THIRD-PARTY DUE DILIGENCE

13.1. O *Third-Party Due Diligence* é uma pesquisa mais detalhada de diversas informações relacionadas aos clientes e parceiros que demandem atenção diferenciada por nível de risco, volumes de operações, segmento de atuação, endereço residencial ou comercial, rede de relacionamentos, características de operações, comunicação por Colaboradores, órgãos reguladores ou pessoal externo, suspeitas de transações irregulares, informações na mídia ou qualquer outro motivo que justifique tal pesquisa.

13.2. Trata-se de um procedimento específico, com pesquisas criteriosas, checagem “in-loco” de endereços, inclusive sobre o país de origem e se consta em alguma lista específica de entidades na prevenção e combate à lavagem de dinheiro e ao financiamento de terrorismo (ex.: COAF, GAFI, ONU, Transparência Internacional, FBI, INTERPOL e órgãos policiais nacionais).

13.3. Toda e qualquer comunicação aos órgãos reguladores competentes deve ser efetuada exclusivamente pela área de Compliance e precedida do *Third-Party Due Diligence* do envolvido.

14. TRATAMENTO DE INDÍCIOS DE LD E FT

14.1. A área de Compliance é responsável pelas rotinas de monitoramento para identificação de indícios de lavagem de dinheiro e financiamento ao terrorismo. As rotinas visam identificar operações com reincidência de contrapartes, transferências injustificadas, operações com incompatibilidade patrimonial, entre outras.

14.2. Para o gerenciamento das ocorrências e tratamento dos indícios de lavagem de dinheiro e controle de operações com vistas a coibir práticas abusivas, a Vixi Exchange utiliza serviços de pesquisas e cruzamento de dados manuais/informatizados, em linha com boas práticas e junto a fornecedores reconhecidos no mercado. Como parte da análise, também são realizadas buscas em ferramentas que verificam o envolvimento do cliente com notícias negativas, comportamento em mídias sociais ou listas de sanções públicas.

14.3. O sistema de prevenção à lavagem de dinheiro coleta diariamente informações cadastrais, operacionais e de movimentação financeira. Casos de incompatibilidade com as regras definidas no sistema gerarão alertas, identificando quais filtros foram acionados para análise.

14.4. Uma vez gerada a ocorrência, cabe à área de Compliance analisar o cliente/parceiro e suas operações para confirmar ou não os indícios de lavagem de dinheiro e financiamento ao terrorismo.

14.5. As análises consistem em verificação da documentação cadastral, evolução da situação financeira/patrimonial, resultado das operações (principalmente transações repetitivas), alto índice de operações entre as mesmas partes, incluindo aquelas com mesmo comitente, compatibilidade entre as operações, situação financeira, ocupação profissional e idade.

14.6. São providências que podem ser tomadas: exigência de atualização cadastral, pedido de esclarecimentos, arquivamento da ocorrência ou comunicado imediato aos órgãos competentes sobre a atipicidade identificada.

14.7. Nenhum parceiro ou cliente da Vixi Exchange deve manter negócio com qualquer pessoa, entidade, governo ou região apontados nas listas restritivas da OFAC, Conselho de Segurança da ONU ou Interpol, dentre outras.

14.8. Os Colaboradores da Vixi Exchange poderão, a qualquer tempo, entrar em contato através do canal **compliance@vixiexchange.com.br** para obter esclarecimentos relativos aos procedimentos e controles de PLD/CFT aplicáveis.

14.9. Todos os dados e informações coletados nos termos da presente Política serão mantidos pela Vixi Exchange pelo prazo de 5 (cinco) anos.

15. ANÁLISE E COMUNICAÇÃO DE OPERAÇÕES AUTOMÁTICAS E SUSPEITAS

15.1. As comunicações automáticas são aquelas que não passam por análise de juízo de valor pela Vixi Exchange e são comunicadas diretamente ao COAF. São elas:

- Operações de depósito ou aporte em espécie ou saque em espécie de valor igual ou superior a R$50.000,00 (cinquenta mil reais);

- Operações relativas a pagamentos, recebimentos e transferências de recursos, por meio de qualquer instrumento, contra pagamento em espécie, de valor igual ou superior a R$50.000,00 (cinquenta mil reais); e

- Solicitação de provisionamento de saques em espécie de valor igual ou superior a R$50.000,00 (cinquenta mil reais).

15.2. Operações e situações suspeitas referem-se a qualquer operação ou situação que apresente indícios de utilização da instituição para a prática dos crimes de lavagem de dinheiro e de financiamento do terrorismo. Consideram-se operações suspeitas:

- As operações realizadas e os produtos e serviços contratados que, considerando as partes envolvidas, os valores, as formas de realização, os instrumentos utilizados ou a falta de

fundamento econômico ou legal, possam configurar a existência de indícios de lavagem de dinheiro ou de financiamento do terrorismo, inclusive:

- As operações realizadas ou os serviços prestados que, por sua habitualidade, valor ou forma, configurem artifício que objetive burlar os procedimentos de identificação, qualificação, registro, monitoramento e seleção;

- As operações de depósito ou aporte em espécie, saque em espécie, ou pedido de provisionamento para saque que apresentem indícios de ocultação ou dissimulação da natureza, da origem, da localização, da disposição, da movimentação ou da propriedade de bens, direitos e valores;

- As operações realizadas e os produtos e serviços contratados que, considerando as partes e os valores envolvidos, apresentem incompatibilidade com a capacidade financeira do cliente, incluindo a renda, no caso de pessoa natural, ou o faturamento, no caso de pessoa jurídica, e o patrimônio;

- As operações com PEPs de nacionalidade brasileira e com representantes, familiares ou estreitos colaboradores de PEPs;

- As operações com PEPs estrangeiras;

- Os clientes e as operações em relação aos quais não seja possível identificar o beneficiário final;

- As operações oriundas ou destinadas a países ou territórios com deficiências estratégicas na implantação das recomendações do Grupo de Ação Financeira (Gafi);

As situações em que não seja possível manter atualizadas as informações cadastrais de seus clientes; e

- As operações e situações que possam indicar suspeitas de financiamento do terrorismo.

15.3 Todas as operações que passam pela plataforma da Vixi Exchange são monitoradas. As operações suspeitas, definidas em procedimento próprio, geram análise especial. As operações

suspeitas são analisadas e reportadas num dossiê que concluirá sobre a necessidade da comunicação de referida operação suspeita ao COAF.

15.4. O período para execução dos procedimentos de análise de operações suspeitas não excederá o prazo de 45 (quarenta e cinco) dias, contados a partir da data da seleção da operação ou situação.

16. PERFIL DE INVESTIMENTO E GRAU DE SUSCETIBILIDADE

16.1. Com o intuito de conhecer a verdadeira identidade, perfil e aspirações de seus clientes, a Vixi Exchange aplica categorização de risco que contempla informações de: **Perfil de Investimento** (conservador, moderado ou agressivo) e **Suscetibilidade** (alta ou baixa).

16.2. O **Perfil de Investimento** é obtido por meio de um questionário que o cliente responde de acordo com seu entendimento e realidade como investidor. O resultado desse estudo é a definição do Perfil de Investimento, que norteará, dentre outras ações, a oferta de produtos e a categorização de riscos, conforme segue:

- **Conservador**: Objetivo principal é a segurança, com a preservação do capital e baixa tolerância a riscos. O cliente conservador tem a segurança como ponto decisivo para as suas aplicações, aceitando até uma rentabilidade menor. Destina os seus recursos em títulos de Renda Fixa (Fundos de Investimentos e Tesouro Direto);

- **Moderado**: Objetivo principal é obter retorno acima dos padrões de renda fixa disponíveis no mercado com exposição minimizada dos riscos de renda variável. É o investidor que possui boa parte do patrimônio em renda fixa, mas também quer participar da rentabilidade da renda variável. A segurança tem papel importante, assim como um retorno acima da média do mercado e, normalmente, mantém posições em médio e longo prazos. Tende a participar de Fundos (Multimercados, de Ações e Imobiliários), Letras de Créditos (LCI e LCA), Clubes de Investimentos, Empréstimos de Ações (BTC) como doador, e mercado à vista de ações, inclusive com operações de *day-trades*; e

- **Agressivo**: Tem como objetivo correr maior risco visando máxima rentabilidade para os seus investimentos. Busca a boa rentabilidade ofertada pela renda variável, reservando parcela mínima do seu patrimônio para as aplicações mais seguras. O investidor agressivo procura estar sempre atualizado para aproveitar eventuais oportunidades de

investimento e com perspectiva de retorno em curto prazo. Possui como característica operar em todos os mercados administrados por bolsas de valores e aplicar em produtos que apresentam exposição à variação cambial e inflação.

16.3. O **Grau de Suscetibilidade** de cada cliente é definido com base em suas informações cadastrais, ratificadas conforme análise. Para a categorização da suscetibilidade são verificados três tipos de informações: (i) **Segmento de Atuação**, (ii) **Origem do Cliente** e (iii) **Característica Profissional**.

16.4. Identificado cliente em qualquer condição definida como de maior suscetibilidade, a documentação cadastral deverá ser encaminhada à área de Compliance antes do início de suas operações com a Vixi Exchange. A metodologia definida quanto à suscetibilidade dos clientes estabelece os seguintes critérios:

- **Segmento de Atuação**: Instituições financeiras e *factorings* (inclusive pessoas físicas com cargos de maior relevância), casas de câmbio, corretoras e distribuidoras, empresas de turismo, jogos, igreja, entretenimento, partidos políticos, transporte aéreo e seguros;
- **Origem do Cliente**: Devem ser considerados o país de origem e o endereço residencial atual. São considerados de alta suscetibilidade: paraísos fiscais, países não cooperantes, países com histórico recente de guerras, guerrilhas ou narcotráfico; e

- **Característica Profissional**: PEPs, familiares e estreitos colaboradores de PEPs, outras personalidades políticas e personalidades da mídia.

16.4.1. Para os fins da presente cláusula, serão considerados “Paraísos Fiscais” os países com tributação favorecida ou que oponham sigilo relativo à composição societária de pessoas jurídicas (listagem RFB). Por sua vez, são “Países Não-Cooperantes” aqueles países que não atuam ou não cooperam no combate às práticas de lavagem de dinheiro e de financiamento do terrorismo por terem legislação permissiva, ou mesmo pela falta de instrumentos jurídicos para fiscalização e regulamentação dos setores econômicos vulneráveis à lavagem de dinheiro e ao financiamento de atividades terroristas (listagem COAF).

17. AVALIAÇÃO DE EFETIVIDADE

17.1. A efetividade da presente Política será avaliada anualmente pela área de compliance e será consubstanciada em relatório específico.

17.2. A Vixi Exchange elaborará plano de ação destinado a solucionar eventuais deficiências da presente Política e dos procedimentos de PLD/CFT por meio da avaliação de efetividade.

17.3. O acompanhamento da implementação do plano de ação será documentado por meio de relatório de acompanhamento, a ser elaborado pela área de compliance.

17.4. Os relatórios de efetividade, os planos de ação e os relatórios de acompanhamento serão encaminhados até 30 de junho de cada ano à Diretoria da Vixi Exchange.

17.8 Os sistemas de informação da Vixi Exchange serão submetidos a testes periódicos para verificação de sua adequação às diretrizes da presente Política.

18. APROVAÇÃO

A presente Política foi aprovada pela Diretoria da Vixi Exchange.

***