Manual de Boas Práticas em Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo para Exchanges brasileiras

Coordenação

Bernardo Srur

Executivo do Mercado Bitcoin, responsável por Risco e Compliance (Prevenção à Lavagem de Dinheiro, Prevenção à Fraudes, Compliance, Segurança da Informação, Controles Internos, Riscos Corporativos e Continuidade de Negócios) e Relações Institucionais (Institucional e Governamental). Representante do Mercado Bitcoin no Conselho Fundador da ABCripto (Associação Brasileira de Criptoeconomia).

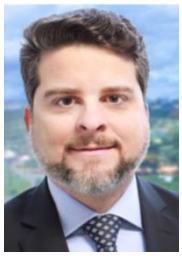
Marcelo De Callis

Legal Counsel e membro da Diretoria Jurídica, de Riscos e Compliance do Mercado Bitcoin desde o ano de 2017. Advogado, especialista em Direito Empresarial pela Pontifícia Universidade Católica de São Paulo (PUC/SP) e em Direito Digital pelo Instituto de Ensino e Pesquisa de São Paulo (Insper). Possui mais de 8 anos de experiência no âmbito da advocacia empresarial estratégica.

Rodrigo França

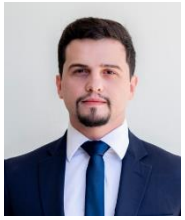
Advogado, especialista em compliance com mais de 10 anos de atuação no combate a crimes financeiros e na prevenção à lavagem de dinheiro, expert na capacitação de profissionais. Extenso conhecimento sobre legislação, políticas e procedimentos de compliance, PLD/FT, Sanções e Anticorrupção. Comprovada expertise em temas como KYC,CDD/EDD, gerenciamento de risco, investigação e análise técnica. Exercício da advocacia privada, pública e corporativa, especializada no desenvolvimento de políticas e diretrizes de compliance específicas. Compreensão da administração pública, bem como do mercado financeiro e setor bancário.

Autoria



Tiago Severo Pereira Gomes

Advogado, Secretário-Geral da Comissão de Direito Bancário da OAB-DF e professor da FGV-Rio com mais de 12 anos de experiência, que possui sólida formação e experiência nas áreas de regulação bancária, FinTechs, compliance, prevenção à lavagem de dinheiro e de financiamento ao terrorismo e casos envolvendo litígios complexos. Para o ambiente das FinTechs, entrega soluções jurídicas para negócios disruptivos nos segmentos de meios de pagamento, Microfinanças, ativos virtuais, blockchain e distributed ledger technologies (DLTs), STOs, tokens, segurança cibernética e armazenamento em nuvem. É especialista em prevenção à lavagem de dinheiro e direito administrativo sancionador no âmbito dos mercados Financeiro e de Capitais, do COAF e CADE. Assessora players desses segmentos sob os vieses consultivo, de compliance regulatório, de investigações internas e, também, em defesas administrativas nos âmbitos do BACEN, da CVM, do COAF, da BM&F e do CRSFN. Sócio do Caputo, Bastos e Serra Advogados



Aylton Gonçalves Junior

Advogado, membro da Comissão de Direito Bancário da OAB-DF, com atuação nas áreas de regulação bancária, FinTechs, compliance, prevenção à lavagem de dinheiro e ao financiamento do terrorismo, além de em casos envolvendo litígios complexos. É especialista em prevenção à lavagem de dinheiro e direito administrativo sancionador, no âmbito dos mercados Financeiro e de Capitais. Possui experiência no assessoramento de players do segmento de criptoeconomia, pelo viés consultivo, entregando soluções para virtual assets (VA) e virtual asset service providers (VASPs). Associado do Caputo, Bastos e Serra Advogados

Índice

1. Apresentação

1. A Associação Brasileira de Criptoeconomia ("ABCripto") foi fundada no ano de 2017, com o objetivo de unir *players* em criptoeconomia, para a interlocução com o poder público, bem como para executar ações em prol do desenvolvimento de tecnologia e de inovação - uma das principais características do setor[1]. Nesse objetivo fundante, insere-se este Manual de Boas Práticas em Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo para Exchanges brasileiras ("Manual").

2. Com o objetivo de possibilitar a observância pelas Exchanges brasileiras das melhores práticas domésticas e mundiais **sobre prevenção à lavagem de dinheiro e ao financiamento do terrorismo ("PLD/FT"), considerando que não existe regulação específica sobre o tema para esse setor no Brasil,** a ABCripto, em parceria com o escritório Caputo, Bastos e Serra Advogados, elaborou este Manual, **que guarda como escopo a delimitação de padrões de procedimento, para fins de observância por parte de Exchanges do regramento brasileiro sobre PLD/FT, partindo-se das diretrizes inseridas na Circular BACEN nº 3.978, de 21 de janeiro de 2020 ("Circular 3978/2020"), que hoje representa o que existe de mais moderno e eficiente na jurisdição brasileira quanto a regras de PLD/FT.**

3. A escolha da Circular 3978/2020 como parâmetro de elaboração deste Manual passa também pela recente alteração legislativa a qual determinou que o Conselho de Controle de Atividades Financeiras ("COAF") faz parte da estrutura do Banco Central do Brasil ("BACEN"). No dia 11.12.2019, o Plenário da Câmara dos Deputados aprovou a Medida Provisória nº 893, de 2019, que foi convertida na Lei nº 13.974, de 7 de janeiro de 2020, a qual, em seu artigo 2º, estabelece que *"o Coaf dispõe de autonomia técnica e operacional, atua em todo o território nacional e vincula-se administrativamente ao Banco Central do Brasil".*

4. Especificamente para este Manual, adotaremos a conceituação de Exchange prevista no artigo 5º, inciso II, da Instrução Normativa RFB nº 1.888, de 3 de março de 2019 ("IN 1888/2019"), qual seja a *"pessoa jurídica, ainda que não financeira, que oferece serviços*

[1] Como aponta o sítio eletrônico da Associação. Acessível em https://www.abcripto.com.br/. Acesso em 25 de junho de 2020.

referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios pagamento, inclusive outros criptoativos", haja vista esta definição abarcar as empresas alvo deste Manual ("Exchanges").

5. No capítulo de introdução, segundo capítulo deste Manual, proporcionamos às Exchanges *overview* acerca do contexto fático-jurídico que orientou à existência do atual cenário regulatório de PLD/FT no Brasil e no mundo, e, especificamente, da necessidade de uma autorregulação do segmento, em razão da inexistência de orientação em grau legal ou infralegal sobre os procedimentos a serem adotados por Exchanges, quanto à PLD/FT.

6. No terceiro capítulo, "Tratamento da atividade de Exchange via GAFI/FATF", explicamos, em atenção às mais recentes manifestações do GAFI/FATF, quais são as principais preocupações do órgão intergovernamental, as quais orientam a elaboração deste Manual e de seu ANEXO A.

7. No quarto capítulo, "Três passos básicos para Exchanges COAF *Compliant*", orientamos, por meio de 3 (três) passos, quais procedimentos as Exchanges devem adotar para fins de observância a deveres previstos artigos 10 e 11 da Lei nº 9.613, de 9.613, de 3 de março de 1998 ("Lei 9613/1998" ou "Lei de Lavagem"), que, embora não tenham obrigatoriedade para Exchanges, norteiam como deve ser a sua atuação no que concerne ao bom relacionamento com o COAF.

8. No quinto capítulo, "Contextualização do novo marco regulatório da Circular 3978/2020", esclarecemos às Exchanges quais são as principais preocupações que circundam as diretrizes brasileiras e estrangeiras quanto à PLD/FT. Essas preocupações, traduzidas em normas cogentes e não cogentes, balizam a elaboração deste Manual.

9. No sexto capítulo, "Elaboração de Política de PLD/FT para Exchanges em etapas" apontamos, em 5 (cinco) etapas, todos os procedimentos que devem orientar a elaboração de Políticas de PLD/FT de Exchanges, para que estejam em linha com as melhores práticas domésticas e internacionais em PLD/FT.

10. No sétimo capítulo, "Dever de Diligência do administrador" da Exchange, demonstramos, pelo lado do consequencialismo, quais seriam as possíveis imputações ao administrador de

Exchange, caso não sejam observados os deveres apontados neste Manual e em seu ANEXO A.

11. Por fim, apresentamos o ANEXO A deste Manual, denominado "Norma de Autorregulação de Exchanges Para Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo", que tem por objetivos a delimitação de deveres específicos a Exchanges, pelo viés de autorregulamentação, no âmbito de PLD/FT.

2. Introdução

12. Entre os anos de 2010 e 2017, 1 (um) Bitcoin deixou de representar o valor de US$ 0,39 (trinta e nove centavos), para representar US$ 20.000 (vinte mil dólares)[2]. Nesse contexto, de robusta valorização das "criptomoedas"[3] e da descoberta de seu potencial disruptivo como investimento, reserva de valor ou meio de pagamento, surgiram as primeiras Exchanges ao redor do mundo[4][5]. No Brasil, a criação das Exchanges teve início em 2011, com a fundação do sítio eletrônico do Mercado Bitcoin.

13. A possibilidade de investimento e de uso como meio de pagamento, podendo trazer alternativa à moeda fiduciária, fez dos criptoativos, em específico do Bitcoin, tema de interesse para a da sociedade civil e para autoridades públicas, ao redor do mundo. Para se ter nossa da dimensão da criptoeconomia, o total do valor de mercado capitalizado pelas "criptomoedas" de maior relevo excedeu o equivalente a 330 bilhões de euros, no início de 2018, conforme o estudo *"Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion"*[6], elaborado pelo Parlamento

---

[2] Acessível em https://www.blockchain.com/charts/market-price. Acesso em 28 de junho de 2020.

[3] Optamos por utilizar o termo "criptomoeda" entre aspas, em atenção à divergência sobre a correção técnica do termo, e também com o intuito de distinção aos demais criptoativos.

[4] *"Hi everyone. I'm in the process of building an exchange. I have big plans for it, but I still have a lot of work to do. It will be a real market where people will be able to buy and sell Bitcoins with each other. In the coming weeks I should have a website with a basic framework set up. Please bear with me".* Esta mensagem, datada de 15 de janeiro de 2010, postada no fórum Bitcointalk, foi possivelmente a primeira manifestação registrada da primeira exchange de que se tem notícia: a Bitcoinmarket. Acessível em https://bitcointalk.org/index.php?topic=20.0. Acesso em 25 de junho de 2020.

[5] *"I am trying to create a market where Bitcoins are treated as a commodity. People will be able to trade Bitcoins for dollars and speculate on the value. In theory, this will establish a real-time exchange rate so we will all have a clue what the current value of a Bitcoin is, compared to a dollar".* Acessível em https://bitcointalk.org/index.php?topic=20.0. Acesso em 25 de junho de 2020.

[6] Acessível em https://www.europarl.europa.eu/cmsdata/150761 . Acesso em 28 de junho de 2020.

Europeu, em junho de 2018. No âmbito da União Europeia, foi publicada, no Diário Oficial da União Europeia do dia 19.6.2018, a *5th Anti-Money Laundering Directive* ("5AMLD"), que determinou às Exchanges europeias o cumprimento das mesmas exigências em PLD/FT que as seguidas por instituições financeiras[7].

14. Na medida em que a tecnologia evolui, os mercados evoluem e a regulação se ajusta. No Reino Unido[89], por exemplo, o Poder Judiciário lançou consulta pública para receber contribuições acerca das definições sobre cripto ativos, redes distribuídas ("DTLs", o *Blockchain* é uma dessas redes), contratos inteligentes ("Smart Contracts"), entre outros. A consulta procurou se antecipar às demandas judiciais no que atine às imprecisões e à imprevisibilidade envolvendo o mundo digital e suas relações contratuais. Ainda no âmbito do Reino Unido, a *Financial Conduct Authority* ("FCA") anunciou, em 10.1.2020, que seria a autoridade responsável pela supervisão de Exchanges daquela região[10]. Em publicação do dia 22.6.2020, denominada "*FCA reminds cryptoasset businesses to register before the end of June"*, a autoridade financeira britânica destacou que (i) as Exchanges que começaram suas atividades antes de 10 de janeiro de 2020 devem se registar na FCA até 10 de janeiro de 2021, sob pena de interrupção do funcionamento; e (ii) as Exchanges que começaram suas atividades após 10 de janeiro de 2020 devem, desde o primeiro dia de funcionamento, estarem registradas no FCA.

15. Nos Estados Unidos da América, reguladores afirmam que podem estabelecer normas para disciplinar o uso das moedas virtuais, pois, ainda que não possuam a natureza jurídica de uma moeda na acepção da legislação em vigor, elas possuem valor econômico que cresce a cada

---

[7] Acessível em https://www.europarl.europa.eu/RegData/etudes/STUD/2020. Acesso em 06 de julho de 2020.

[8] Acessível em https://br.lexlatin.com/portal/opiniao/o-direito-brasileiro-garante-validade-juridica-de-contratos-eletronicos. Acesso em 28 de junho de 2020.

[9] Acessível em https://www.judiciary.uk/announcements/have-your-say-new-consultation-launched-on-cryptoassets/. Acesso em 28 de junho de 2020.

[10] Acessível em https://www.fca.org.uk/news/news-stories/fca-becomes-aml-and-ctf-supervisor-uk-cryptoasset-activities. Acesso em 28 de junho de 2020. Conforme a publicação, as Exchanges britânicas devem dentre outras obrigações, (i) identificar e avaliar os riscos de lavagem de dinheiro e financiamento do terrorismo aos quais seus negócios estão sujeitos; (ii) ter políticas, sistemas e controles para mitigar o risco de o negócio ser usado para fins de lavagem de dinheiro ou financiamento do terrorismo; (ii) quando apropriado ao tamanho e natureza de seus negócios, nomeie um indivíduo que seja membro do conselho ou da gerência sênior como responsável pelo compliance em PLD/FT; (iii) realizar a devida diligência do cliente ao entrar em um relacionamento comercial ou em transações ocasionais; (iv) aplique uma *due diligence* mais intrusiva, conhecida como *due diligence* aprimorada, ao lidar com clientes que possam apresentar um risco maior de lavagem de dinheiro e/ou financiamento ao terrorismo. Isso inclui clientes que atendem à definição de pessoa politicamente exposta; e (v) realizar monitoramento contínuo de todos os clientes para garantir que as transações sejam consistentes com o conhecimento da empresa e com o perfil de negócios e risco do cliente.

ano. As observações das autoridades estão na linha de evitar que a regulação diminua as possibilidades de inovação. A intenção é aumentar a segurança jurídica e econômica dessas transações e proteger os investidores-consumidores das ofertas públicas potencialmente enganosas via *Initial Coin Offering* ("ICO")[11]. Na jurisdição estadunidense, chamam atenção iniciativas como (i) a do *Financial Crimes Enforcement Network* ("FinCEN"), Unidade de Inteligência Financeira dos Estados Unidos da América, que, em 18 de março de 2013, publicou o *Guideline "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies"*, o qual definiu a atividade de Exchange e orientou à aplicabilidade do *Bank Secrecy Act*, norma sobre PLD/FT, aplicável às instituições financeiras estadunidenses, às Exchanges[12]; e (ii) a do *New York State Department of Financial Service*, que, em 8.6.2015, estabeleceu a necessidade de que empresas que operem com criptoativos, no âmbito do Estado de Nova York, obtenham a licença denominada "*BitLicense*"[13].

16. Nesse contexto internacional de PLD/FT, insere-se o papel exercido pelo Grupo de Ação Financeira Internacional ("GAFI/FATF")[14][15]. Criado em 1989, em reunião do G-7, o GAFI/FATF é órgão intergovernamental que tem como objetivo desenvolver e promover políticas nacionais e internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo. Para o cumprimento desse objetivo, o GAFI publicou, no ano de 1990, 40

---

11 Acessível em https://www.sec.gov/files/OCIE%202019%20Priorities.pdf. Acesso em 28 de junho de 2020.

12 A versão mais atual do documento está disponível em https://www.fincen.gov/sites/default/files/2019-05. Acesso em 15 de julho de 2020.

13 Acessível em https://govt.westlaw.com/nycrr/Document/I85908c6b253711e598dbff5462aa3db3?. Acesso em 15 de julho de 2020.

14 Como indica o sítio eletrônico do órgão: "*The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas".*

15 Na lição de David Chaikin, em *Corruption and Money Laundering A Symbiotic Relationship, "The most influential body in setting AML standards from its inception to the present day has undoubtedly been the FATF. The FATF is not a formal treaty organization, but rather depends on periodic decisions to renew its existence by member states. Meeting in plenary sessions three times a year, it has only a small permanent secretariat of fifteen staff members housed within the OECD headquarters in Paris. But the FATF's lack of formal treaty status and limited personnel have not restricted its policy influence, both within and beyond its membership. The first international institution founded specifically to counter money laundering, the FATF once again grew out of a concern with the war on drugs. Following the call of the 1989 G7 heads of state summit, the organization took shape in an intensive process of meetings between government officials and regulators in late 1989 and early 1990. Aside from the G7 members, participation was soon extended to the other OECD states. The FATF has since been keen to expand to incorporate "strategically important" developing countries, including Brazil, Argentina, South Africa, India, China, as well as Russia, with a further round of expansion in progress".*

(quarenta) Recomendações[16], que funcionam como guia para que os países adotem padrões e promovam a efetiva implementação de medidas legais, regulatórias e operacionais para a consecução das melhores práticas em PLD/FT.

17. Entre os anos de 2013 e 2015, o GAFI/FATF divulgou os primeiros dois guias de Abordagem Baseada em Risco ("ABR") aplicáveis à criptoeconomia: (i) "*Guidance for a Risk-Based Approach – Prepaid Cards, Mobile Payments and Internet-Based Payment Services*"[17] e o "*Guidance for a Risk-Based Approach – Virtual Currencies*"[18]. O objetivo do GAFI/FATF foi sinalizar para o mundo globalizado a importância de se dar atenção para esse novo segmento de mercado, a criptoeconomia, e para as novas janelas de risco envolvendo a lavagem de dinheiro.

18. Em manifestação recente, denominada "*Regulation of virtual assets*"[19], o GAFI/FATF buscou criar definição de prestador de serviço de ativo virtual – categoria que abarca a atividade de Exchange - a qual inclui pessoa natural ou jurídica que realize uma ou mais atividades empresariais ou operações, para ou em nome de outra pessoa natural ou jurídica, que envolvam: (i) câmbio entre criptoativos e moedas soberanas; (ii) câmbio entre uma ou mais formas de criptoativos; (iii) transferência de criptoativos; (iv) custódia e/ou administração de criptoativos ou instrumentos que possibilitam o controle sobre criptoativos; e (v) participação em prestação de serviços financeiros relacionados à oferta de um emissor e/ou à venda de um ativo virtual.

19. Em publicação do dia 7 de julho de 2020, denominada "*FATF Report to G20 on So-called Stablecoins"*[20], o GAFI/FATF ressaltou mais uma vez preocupações com o uso de criptoativos para o cometimento de práticas de lavagem de dinheiro e de financiamento do terrorismo. Especificamente quanto às *stablecoins*, criptoativos que têm como característica a estabilidade, muitas vezes lastreados em moedas fiduciárias, o GAFI/FATF afirmou que a

---

16 Acessível em http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs. Acesso em 28 de junho de 2020.

17 Acessível em http://www.fatf-gafi.org/media/fatf/documents/recommendations/ Acesso em 28 de junho de 2020.

18 Acessível em http://www.fatf-gafi.org/media/fatf/documents/reports/. Acesso em 28 de junho.

19 Acessível em https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html. Acesso em 28 de junho de 2020.

20 Acessível em http://www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-so-called-stablecoins-june-2020.html. Acesso em 07 de julho de 2020.

difusão do uso desse tipo de criptoativos pode ser atraente para que sejam utilizados como meio de lavagem de capitais.

20. Na prática brasileira em PLD/DT, destaca-se a criação, pelo Ministério da Justiça no ano de 2003, da Estratégia Nacional de Combate à Corrupção[21] e à Lavagem de Dinheiro, a principal rede brasileira de articulação entre órgãos dos Poderes Executivo, Legislativo e Judiciário das esferas federal e estadual e, em alguns casos, municipal, bem como do Ministério Público de diferentes esferas, para a formulação de políticas públicas e soluções voltadas à PLD/FT.

21. No ano de 2016, a jurisdição brasileira, via XIII Reunião Plenária do Fórum qualificado da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro ("ENCCLA"), manifestou as suas primeiras preocupações com o tema de criptoativos, quando recomendou "*a seus participantes que tenham especial atenção para as operações que envolvam esse meio de pagamento*"[22].

22. Para o ano de 2017, na XIV Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, a ENCCLA definiu a "Ação 8", que teve como objetivos *"elaborar diagnóstico sobre a atual conjuntura da utilização de moedas virtuais e meios de pagamento eletrônico".* Como resultados da "Ação 8", obteve-se: (i) a criação de glossário com termos relacionados a moedas virtuais[23]; e (ii) o levantamento de tipologias de lavagem de dinheiro e corrupção mediante o uso de moedas virtuais e meios de pagamento eletrônico[24].

23. Como objetivo para o ano de 2018, a ENCCLA, na XV Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, estabeleceu a "Ação 8", então com o escopo de *"aprofundar os estudos sobre a utilização de moedas virtuais para fins de*

---

21 Quando da criação do grupo, o escopo da atuação era tão somente de PLD. No de 2006, entendeu-se pela necessidade de que se acrescentasse expressamente o termo "corrupção" às atividades do grupo, reforçando a abrangência de seu trabalho.

22 *"Considerando a identificação, no âmbito internacional, do crescente uso de moedas virtuais, como o Bitcoin, em esquemas de lavagem de dinheiro, a ENCCLA recomenda a seus participantes que tenham especial atenção para as operações que envolvam esse meio de pagamento".* Acessível em http://enccla.camara.leg.br/acoes/acoes-de-2016. Acesso em 25 de junho.

23 Acessível em http://enccla.camara.leg.br/acoes/arquivos/resultados-enccla-2017/moedas-virtuais-glossario. Acesso em 26 de junho.

24 Acessível em http://enccla.camara.leg.br/acoes/arquivos/resultados-enccla-2017/moedas-virtuais-tipologias. Acesso em 26 de junho.

lavagem de dinheiro e eventualmente apresentar propostas para regulamentação e/ou adequações legislativas". Como resultados da "Ação 8" de 2018, obteve-se: (i) minuta de proposta de alteração da Lei 9613/1998, com foco no segmento de ativos virtuais; (ii) a adoção de expedientes para iniciar a elaboração de uma coletânea de jurisprudência sobre o tema de criptoativos; e (iii) a proposta de nova Ação para a ENCCLA 2019, com foco no âmbito penal.

24. Para o ano de 2019, a ENCCLA, por meio da XVI Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, definiu novo texto para a "Ação 8", dessa vez prevendo a meta de "*aprofundar os estudos sobre a utilização de ativos virtuais para fins de lavagem de dinheiro e financiamento do terrorismo, apresentando (i) levantamento de boas práticas relacionadas com a investigação do delito em diversas esferas; (ii) eventual proposta de adequação normativa em matéria investigativa e de persecução penal"*. Os resultados de 2019 foram: (i) elaboração do produto "Roteiro de Boas Práticas de Investigação Relacionada a Criptoativos"; (ii) solicitação/consulta ao IBGE/CONCLA sobre a possibilidade de criação de classe ou subclasse de CNAE para as corretoras ou exchanges de criptoativos; e (iii) elaboração de modelo de comunicação/notificação de transação suspeita por corretoras ou exchanges.

25. Para 2020, a ENCCLA, via XVII Reunião Plenária da Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro, definiu novo texto para a "Ação 8", a fim de *"elaborar diagnóstico sobre as possibilidades de uso de tecnologias como blockchain no setor público".*

26. Como se observa da descrição das "Ações" do ENCCLA, apesar do louvável esforço em se envidar esforços para compreensão do tema de criptoativos, temos que não houve avanços significativos na disciplina, principalmente no que concerne à criação de regramento quanto à PLD/FT, o que se busca fazer neste documento, por iniciativa do setor, aqui representado pela ABCripto.

27. Vale destacar que, entre 16 a 18 de outubro de 2019, o Plenário do GAFI/FATF reuniu-se em Paris, França, e publicizou suas novas definições interpretativas à Recomendação nº 15[25], envolvendo a criptoeconomia[26]. **E, em 2020, o Brasil será avaliado se está ou não em conformidade com as Recomendações.**

28. Do lado do Poder Legislativo, observa-se também cenário de incerteza. Atualmente 4 (quatro) Projetos de Lei ("Pls" ou, quando no singular, "Pl") tramitam no Congresso Nacional com tema de criptoativos: (i) o PL 2303/2015[27], que tramita na Câmara dos Deputados e *"dispõe sobre a inclusão das moedas virtuais e programas de milhagem aéreas na definição de arranjos de pagamento sob a supervisão do Banco Central";* (ii) o PL 2060/2019[28], que tramita na Câmara dos Deputados *e "dispõe sobre o regime jurídico dos criptoativos";* (iii) o PL 3949/2019[29], que tramita no Senado Federal e *"dispõe sobre transações com moedas virtuais e estabelece condições para o funcionamento das exchanges de criptoativos"*; e (iv) o PL 3825/2019[30], que tramita no Senado Federal e *"propõe a regulamentação do mercado de criptoativos no país, mediante a definição de conceitos; diretrizes; sistema de licenciamento de Exchanges; supervisão e fiscalização pelo Banco Central e CVM; medidas de combate à lavagem de dinheiro e outras práticas ilícitas; e penalidades aplicadas à gestão fraudulenta ou temerária de Exchanges de criptoativos"*. Estes dois últimos PLs têm como característica em comum a propositura de que se insira a atividade das Exchanges dentre as que compõe o rol das atividades abarcadas pela Lei de Lavagem.

29. Ainda em caráter introdutório, entendemos importante destacar uma das mais recentes vitórias do setor de Exchanges: a criação de um número de Classificação Nacional de Atividades Econômicas ("CNAE") junto ao Instituto Brasileiro de Geografia e Estatística

---

[25] Acessível em https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF. Acesso em 28 de junho de 2020.

[26] Acessível em http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2019.html. Acesso em 28 de junho de 2020.

[27] Acessível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra. Acesso em 28 de junho de 2020.

[28] Acessível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1728497. Acesso em 28 de junho de 2020.

[29] Acessível em https://legis.senado.leg.br/sdleggetter/documento?dm=7976961&ts. Acesso em 28 de junho de 2020.

[30] Acessível em https://legis.senado.leg.br/sdleggetter/documento?dm=7973487&ts. Acesso em 28 de junho de 2020.

("IBGE"), para atividade de Exchange[31]. Temos este como um dos mais profícuos resultados da caminhada trilhada pela ABCripto ao longo dos últimos anos.

30. A partir deste cenário, entendemos que o segmento das Exchanges necessite deste documento de autorregulação, para que se estabeleça um ambiente de segurança à sociedade civil e às autoridades públicas, no que concerne ao cometimento de condutas de lavagem de dinheiro e de financiamento ao terrorismo via criptoeconomia, a fim de que esse mercado se consolide em definitivo na prática do brasileiro.

3. Tratamento da atividade de Exchange via GAFI/FATF

31. Em 15 de outubro de 2018, o GAFI/FATF realizou atualização de seu glossário, para incluir as definições dos termos *virtual assets* ("VAs") e *virtual asset service provider* ("VASP" ou "VASPs", quando no plural). O órgão intergovernamental definiu VAs como *"uma representação digital de valor que pode ser negociada digitalmente ou transferidos e podem ser usados para fins de pagamento ou investimento"*, e VASPs como *"qualquer pessoa natural ou jurídica, que não seja coberta em outras Recomendações e, como negócio, conduza uma ou mais das seguintes atividades ou operações por ou em nome de outra pessoa natural ou jurídica: (i) câmbio entre ativos virtuais e moedas fiduciárias; (ii) câmbio entre uma ou mais formas de ativos virtuais; (iii) transferência de ativos virtuais; (iv) guarda e/ou administração de ativos ou instrumentos virtuais, permitindo controle sobre ativos virtuais; e (v) participação e prestação de serviços financeiros relacionados ao emissor de um oferta e/ou venda de um ativo virtual".* **Portanto, a atividade de Exchange está abarcada no conceito de VASP.**

32. Na mesma data, o GAFI/FATF alterou a redação de sua Recomendação nº 15, para determinar que *"para gerenciar e mitigar os riscos emergentes dos ativos virtuais, os países devem garantir que prestadores de serviços de ativos virtuais são regulados para fins de PLD/FT, e licenciados ou registrados e sujeitos a sistemas eficazes para monitorar e garantir a conformidade com os medidas relevantes previstas nas Recomendações do GAFI/FATF".*

[31] Acessível em https://cnae.ibge.gov.br/?option=com_cnae&view=atividades&Itemid=6160. Acesso em 28 de junho de 2020.

33. Em junho de 2019, o órgão intergovernamental publicou a Nota Interpretativa da Recomendação nº 15, a qual estabelece que os países, inclusive o Brasil, devem:

a) identificar, avaliar e entender os riscos de lavagem de dinheiro e financiamento do terrorismo envolvendo as atividades de VASPs;
b) aplicar uma abordagem baseada no risco no tratamento das atividades de VASP, a fim de garantir que a adoção de medidas em PLD/FT sejam proporcionais aos riscos identificados;
c) exigir das VASPs que identifiquem, avaliem e tomem medidas efetivas para mitigar o risco de lavagem de dinheiro e financiamento do terrorismo;
d) exigir que as VASPs sejam licenciadas ou registradas na jurisdição em que forem criadas;
e) tomar medidas para identificar pessoas naturais ou jurídicas que realizem atividades de VASP sem a licença necessária ou registro necessário, com aplicação de sanções apropriadas;
f) garantir que as VASPs estejam sujeitas à regulamentação, à supervisão e ao monitoramento da PLD/FT;
g) garantir que as VASPs estejam implementem efetivamente as Recomendações do GAFI/FATF, para mitigar os riscos de lavagem de dinheiro e financiamento ao terrorismo;
h) garantir que as VASPs estejam sujeitas a sistemas eficazes para monitorar e garantir conformidade com os requisitos nacionais de PLD/FT; e
i) garantir que haja uma gama de medidas efetivas, sejam criminais, civis ou administrativas, disponíveis para lidar com VASPs que não cumprirem com os requisitos de PLD/FT.

34. Essa Nota Explicativa ainda esclareceu a aplicabilidade às VASPs da Recomendação nº 10 do GAFI/FAT, que trata sobre deveres em *Customer Due Diligence*, os quais descreveremos no tópico seguinte deste Manual; e da Recomendação nº 16 do GAFI/FATF, que estabelece a necessidade de conhecimento e manutenção de informações sobre beneficiários e destinatários da operação envolvendo criptoativos. Especificamente quanto a este último ponto, é importante a medida adotada pelo *Joint Working Group on interVASP Messaging Standards*, grupo composto por mais de 130 (cento e trinta) especialistas técnicos, que produziu documento com o objetivo de padronizar a transmissão de informações entre

VASPs, a fim de possibilitar, de modo mais acurado, a identificação de beneficiários e destinatários finais ("IVMS101")[32]. Neste ponto, vale também destacar o software *Sygna Bridge*, que auxilia na observância da Recomendação nº 16 do GAFI/FATF pelas VASPs[33].

35. Ainda em junho de 2019, especificamente no dia 21, o GAFI/FATF publicou o "*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers"*[34]. Neste guia, o órgão intergovernamental endereçou que as VASPs devem considerar os seguintes elementos, para fins de avaliar o risco de suas atividades: (i) os riscos potencialmente mais altos associados a VASPs que trablham com a conversão de moeda fiduciária em criptoativo; (ii) os riscos associados aos modelos de negócios VASP centralizados e descentralizados; (iii) os tipos específocos de relacionamentos com produtos e serviços, que possam ser limitantes da correta adoção de políticas de *Customer Due Diligence* e *Know Your Client*; (iv) o modelo de negócio específico de cada VASP e se esse modelo de negócios introduz ou exacerba riscos específicos; (v) se as operações da VASP occorem somente em meio virtual ou se também em meio físco (v) a possibilidade de exposição a anonimizadores de *Internet Protocol*; (vi) os riscos potenciais em operações envovlendo VASPs oriundas de múltiplas jurisdições; (vii) a natureza e o escopo da conta, produto ou serviço da atividade de VASP.

36. Em documento publicado no dia 7.7.2020, denominado "*12 Month Review of Revised FATF Standards - Virtual Assets and Virtual Assets Service Providers*"[35], o GAFI/FATF, após analisar o segmento de criptoeconomia entre os meses de junho de 2019 e junho de 2020, concluiu que, de maneira geral, os setores público e privado avançaram na implementação das Recomendações do GAFI/FATF. Destacou-se que 35 (trinta e cinco) das 54 (cinquenta e quatro) jurisdições declarantes informaram a implementação das Recomendações. Por meio desse documento, O GAFI/FATF se comprometeu a: (i) continuar seu monitoramento aprimorado de ativos virtuais e VASPs, além de realizar uma segunda revisão do segmento até junho de 2021; (ii) publicar orientações atualizadas sobre ativos virtuais e VASPs; (iii) continuar promovendo o entendimento dos riscos de PLD/FT envolvidos nas transações que

---

[32] Acessível em https://intervasp.org/wp-content/uploads/2020/05/IVMS101-interVASP-data-model-standard-issue-1-FINAL.pdf. Acesso em 06 de julho de 2020.

[33] Fazemos referência ao documento *Sygna Bridge Report – FATF Recommendation 16 Technical Solution Virtual Asset Transactions*. O texto aborda quais são os desafios enfrentados pelas VASPs e como o sistema desenvolvido pela empresa poderia auxiliar nisso. Acessível em https://www.sygna.io/bridge/. Acesso em 06 de julho de 2020.

[34] Acessível em https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf. Acesso em 30 de junho de 2020.

[35] Acessível em https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf. Acesso em 10 de julho de 2020.

utilizam ativos virtuais, publicando indicadores de *red flags* e estudos de caso relevantes até outubro de 2020; (iv) continuar e aprimorar seu envolvimento com o setor privado, incluindo VASPs, provedores de tecnologia, especialistas técnicos e acadêmicos; e (v) continuar seu programa de trabalho para melhorar a cooperação internacional entre os supervisores de VASPs.

4. Três passos básicos para Exchanges COAF *Compliant*

37. Os artigos 10 e 11, da Lei de Lavagem, tratam de deveres das pessoas naturais e jurídicas que estão obrigadas a atenderem as determinações da norma, listadas em seu artigo 9º ("Pessoas Obrigadas" ou "Pessoa Obrigada", quando no singular").

38. Apesar de as Exchanges não integrarem o rol de Pessoas Obrigadas da Lei de Lavagem, entendemos que a observância desses dispositivos legais tenha importância, sob o ponto de vista da consecução de um mercado seguro e confiável, no que atine à PLD/FT. Vale mencionar que recente estudo, publicado em 15.6.2020, denominado "*Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report*"[36], que analisou a relação entre lavagem de dinheiro e o segmento de criptoeconomia, especificamente entre os meses de janeiro e maio de 2020, concluiu que maior parte das VASPs analisadas ainda não possuíam níveis adequados de procedimentos para conhecer os seu clientes.

39. Nesse contexto, os "passos" descritos neste tópico, dizem respeito à (i) identificação de clientes e manutenção de registros; e (ii) comunicação de operações financeiras ao COAF.

4.1 Passo nº 1: Cadastro

40. As Exchanges devem requerer ao COAF a realização de cadastro ao Sistema de Controle de Atividades Financeiras ("SISCOAF"), via https://siscoaf.fazenda.gov.br, ainda que não figurem como uma das Pessoas Obrigadas previstas no artigo 9º, como se tem observado da interlocução entre o segmento e o órgão de supervisão nos últimos anos. A norma que

[36] Acessível em https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/. Acesso em 06 de julho de 2020.

disciplina este cadastro – e que pode servir de parâmetro às Exchanges - é a Carta-Circular COAF nº 1, de 1º de dezembro de 2014[37] ("Carta-Circular 1/COAF").

41. Ao realizar o cadastro, a Exchange passa a ter acesso a um canal de relacionamento exclusivo com o COAF, que lhe permite atualizar seus dados, efetuar comunicações, receber informações de interesse, verificar a conformidade com as normas pertinentes, consultar lista de pessoas politicamente expostas, entre outras funcionalidades.

4.2 Passo nº 2: Adoção de políticas de *KYC, KYE, KYP* e *KYT*

42. As Exchanges devem cadastrar e identificar adequadamente: seus clientes; seus empregados; e seus parceiros comerciais. Durante um prazo de 5 (cinco) anos o COAF poderá entrar em contato e solicitar informações armazenadas, esta deverá atender o pedido do órgão obedecendo, é claro, o sigilo das informações prestadas.

43. O processo de cadastro deve ter início pela obtenção e análise de dados de pessoas físicas e jurídicas. É necessário que a Exchange mantenha rotinas definidas para o cadastro inicial, renovações periódicas, e manutenção de registros.

44. A política de *Know Your Client (*"KYC" ou "Conheça Seu Cliente") deve ter como norte, em linhas gerais, o conhecimento sobre características e especificidades do negócio do cliente, de maneira que seja possível: conhecer a origem e o destino dos ativos financeiros movimentados (beneficiário final), aferir a compatibilidade entre a operação e o perfil da contraparte e de classificar o risco do cliente vis-à-vis produtos ofertados.

45. Uma metodologia eficaz para o adequado conhecimento do cliente é a *background check* (verificação de antecedentes), bastante utilizada em jurisdições estrangeiras. Em geral, as empresas se valem de duas formas de *background check:* a simplificada, em que se verifica situação cadastral na Receita Federal, antecedentes criminais, protestos, e situação econômico-financeira; e a detalhada, que se vale desses elementos somados à análise de: enquadramento como Pessoa Politicamente Exposta[38]; expulsões da Administração Federal;

---

[37] Acessível em http://www.fazenda.gov.br/orgaos/coaf/legislacao-e-normas/normas-coaf/carta-circular-no-1-de-1o-de-dezembro-de-2014. Acesso em 28 de junho de 2020.

[38] Nos termos da Resolução COAF nº 29, de 7 de dezembro de 2017

inscrição em lista de inabilitados em instituições financeiras; inscrição em lista de sanções a financiamento ao terrorismo (ONU, EU, UK, etc.); inscrição na lista *Specially Designated Nationals and Blocked Person (*"SDN") *do Office of Foreign Assets Control* ("OFAC"); situação eleitoral; cadastro em programa de benefícios governamentais; participação em sociedades empresariais; e outros que adéquem à realidade fática do negócio.

46. A OFAC, parte da estrutura do *U.S Department of Treasury*, administra e aplica sanções econômicas e comerciais, baseadas na política externa dos Estados Unidos da América e em objetivos de segurança nacional, contra países e regimes estrangeiros visados, terroristas, traficantes internacionais de narcóticos, envolvidos em atividades relacionadas à proliferação de armas de destruição em massa e outras possíveis ameaças. Como parte de seus esforços de fiscalização, a OFAC publica uma lista de indivíduos e empresas pertencentes ou controladas ou atuando em nome ou em nome de países-alvo. A OFAC também divulga lista de indivíduos, grupos e entidades, como terroristas e narcotraficantes designados por programas que não são específicos de cada país. Coletivamente, esses indivíduos e empresas são chamados de *Specially Designated Nationals and Blocked Person*[39].

47. É necessário ainda que a Exchange observe as determinações da Recomendação nº 10, do GAFI/FATF, que trata sobre *Customer Due Diligence* ("CDD"), e estabelece a necessidade de: (i) identificar o cliente e verificar sua identidade por meio de documentos, informações ou dados confiáveis e de fontes independentes; (ii) identificar o beneficiário e adotar medidas razoáveis para verificar a identidade de tal beneficiário, de forma que a Exchange obtenha conhecimento satisfatório sobre quem é o beneficiário; (iii) compreender e, quando apropriado, obter informações a respeito do propósito e da natureza pretendidos da relação de negócios; (iv) conduzir diligência contínua quanto à relação de negócios e uma análise minuciosa das transações conduzidas durante a relação para garantir que tais transações sejam consistentes com o conhecimento da instituição sobre o cliente, seus negócios e perfil de risco, incluindo, quando necessário, a origem dos recursos.

48. No contexto de KYC, é também importante que as Exchanges se atentem à possibilidade de uso de *synthetic identities*[40]. Este termo é utilizado para um tipo de fraude em que o agente

---

[39] Acessível em https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx. Acesso em 28 de junho de 2020.

[40] Acessível em https://www.experian.com/assets/decision-analytics/white-papers/synthetic-id-white-paper.pdf. Acesso em 06 de julho de 2020.

se vale de informações reais combinadas com informações falsas para a criação de uma identidade nova. A defesa contra a fraude usando identidade sintética não pode ser feita tentando identificar o indivíduo pelos dados de identidade em si, haja vista algumas das informações serem reais. É necessário um segundo fator de autenticação.

49. Ainda quanto ao conhecimento das suas relações comerciais, as Exchanges devem ter atenção quanto a novas ameaças criadas a partir da pandemia da COVID-19. Como indicou o Presidente do GAFI/FATF, em Comunicado do dia 1.4.2020, *"os criminosos estão se aproveitando da pandemia de Covid-19 para aplicar fraudes financeiras e golpes de exploração, incluindo oferta fraudulenta de oportunidades de investimento e envolvimento em esquemas de phishing baseados no medo do vírus. Crimes cibernéticos fraudulentos ou maliciosos, captação de fundos para ONG fictícias e vários golpes de cunho médico contra vítimas inocentes provavelmente aumentarão, com criminosos tentando lucrar com a pandemia por meio da exploração de pessoas em suas necessidades urgentes de cuidados básicos e da boa vontade do público em geral, além da disseminação de informações falsas sobre a Covid-19. Autoridades nacionais e organismos internacionais estão alertando os cidadãos e setores econômicos sobre esses golpes, que incluem impostores e golpes com produtos e investimentos, bem como tráfico de informações privilegiadas relativas à Covid-19. Como os criminosos, os terroristas podem também explorar essas possibilidades para angariar fundos"*[41]

50. A política de *Know Your Employee* ("KYE" ou "Conheça seu Funcionário"*)* ocorre desde a contratação dos colaboradores. A Exchange precisa adotar procedimentos que a assegurem de que seus funcionários têm aderência completa a seus padrões de ética e de conduta, e de que reconhecerá possível envolvimento de seus colaboradores em atividades ilícitas, como a lavagem de dinheiro e o financiamento do terrorismo.

51. A Exchange deve, também, adotar procedimentos regulares para a identificação e aceitação de seus parceiros comerciais. A política de *Know Your Partner (*"KYP" ou "Conheça Seu Parceiro") tem de ser suficiente para prevenir operações com contrapartes inidôneas ou que

[41] Acessível em https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf. Acesso em 07 de julho de 2020.

não sigam adequados padrões de PLD/FT. Neste ponto, a Exchange pode se valer do conceito de questionário elaborado pelo *Wolfsberg Group*[42][43], por exemplo.

52. Por final, é importante destacar a necessidade de adoção pelas Exchanges da política de Know Your Transaction ("KYT" ou "Conheça Sua Transação"). Essa preocupação, vale mencionar, esta linha com o que prevê a Recomendação nº 20 do GAFI/FATF, a qual indica que *"se uma instituição financeira suspeitar ou tiver motivos razoáveis para suspeitar que os fundos sejam produtos de atividade criminosa ou estejam relacionados ao financiamento do terrorismo, ela deveria estar obrigada, por lei, a comunicar prontamente suas suspeitas à unidade de inteligência financeira (UIF)"*[44].

53. O objetivo da política de KYT é de que a Exchange identifique de maneira adequada transações possivelmente arriscadas, sob o ponto de vista da prática de condutas de lavagem de dinheiro, de financiamento do terrorismo, e de outras práticas fraudulentas.

54. Na prática de mercado financeiro, por exemplo, o que se tem visto é a elaboração de base de dados com parâmetros tais quais padrões de transação, códigos de transação, países de origem, nomes de clientes e bancos de origem, para fins de identificar possíveis transações suspeitas[45]. Para isso, o mercado internacional cada vez mais se vale do uso de tecnologias de Inteligência Artificial[46][47].

---

[42] Como indicado no sítio eletrônico da associação mundial de bancos: *"The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies".*

[43] Acessível em https://www.wolfsbergprinciples.com/sites/default/files/wb/pdfs. Acesso em 28 de junho de 2020.

[44] Em tradução livre de *"if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU)".*

[45] Como exemplo prático da adoção de política de KYT, vale mencionar parceria entre o Mercado Bitcoin e a empresa Chainalysis *"A exchange adotou, em parceira com a Chainalysis, um sistema que mostra os valores que foram usados para lavagem de dinheiro."*. Acessível em https://criptonizando.com/2020/05/22/mercado-bitcoin-divulga-programa-de-seguranca-contra-lavagem-de-dinheiro/. Acesso em 15 de julho de 2020.

[46] Com o uso de Inteligência Artificial, empresas criam espécies de bancos de dados "inteligentes", que, por si só, em um processo conhecido com *Machine Learning*, conseguem melhorar o seus resultados, em entregar com cada vez mais precisão análises quanto a transações arriscadas sob o ponto de vista da lavagem de dinheiro e do financiamento do terrorismo.

[47] O uso de Inteligência Artificial para fins de PLD/FT foi abordado no *"FATF Private Sector Consultative Forum"*, realizado pelo GAFI/FATF, em 6 e 7 de maio de 2019. Especificamente sobre este tema, registrou-se que "*the session discussed the use of technology, its benefits and risks in order to support innovation in financial services while addressing the regulatory and supervisory opportunities posed by emerging technologies. Participants exchanged views on how public authorities and private sector firms could make greater use of technology to manage financial crime risk,*

55. Ainda quanto à política de KYT, é importante destacar que a elaboração deve ter por base a análise de risco do produto e do serviço envolvido nas transações da Exchange. Para isso, a Exchange deve ter por base as determinações da Resolução CMN nº 4.557, de 23 de fevereiro de 2017. Além disso, a matriz de risco da política de KYT precisa estar inserida na Política de PLD/FT da Exchange, e, portanto, ser revista a cada 2 (dois) anos, pelos responsáveis por sua execução e monitoramento e pelo Conselho de Administração ou similar, partindo-se dos termos da Resolução CMN nº 4.595, de 28 de agosto de 2017.

4.3 Passo nº 3: Comunicação de ocorrência ou inocorrência de operações suspeitas

56. No âmbito da prevenção à lavagem de dinheiro, o objetivo de existir de uma Unidade de Inteligência Financeira ("UIF") é o de monitorar, de acompanhar e de registrar atividades suspeitas de lavagem de dinheiro para, posteriormente, municiar e dividir as informações agrupadas[48] com órgãos competentes para a investigação e a persecução criminais no combate à criminalidade, que, no Brasil, está mais relacionada aos atos de corrupção. Como indicamos em nossa Introdução, atualmente a UIF brasileira, o COAF, integra a estrutura do BACEN.

57. Para fins deste monitoramento, em linhas gerais, há 3 (três) previsões normativas no que toca o reporte-notificação-comunicação ao COAF, a depender do setor: (i) "comunicações de operações em espécie" ("COE", ou "COEs" quando utilizada no plural); (ii) "comunicações de operações suspeitas" ("COS", ou "COSs" no plural); e/ou (iii) "comunicação de não ocorrência", também conhecida como "Declaração Negativa" ou "Declaração de Inocorrência", que aqui chamaremos de "DI", ou "DIs" no plural.

58. De forma geral, as DIs devem ser realizadas até o dia 31 de janeiro, quando não tiveram sido realizadas notificações a título de COE ou COS ano anterior. E uma COE se diferencia de uma COS principalmente por conta do parâmetro "probabilidade-imediatismo" da ocorrência de ilícitos de branqueamento de capitais como crime "meio" para atos de corrupção, terrorismos etc.

how technology facilitated customer due diligence, sanctions screening and transaction monitoring, and how government authorities harnessed new technologies to increase efficiency and effectiveness in detecting ML/TF.

[48] Regram os "Relatórios de Inteligência Financeira, "RIFs"

59. O adequado cumprimento destes três passos relaciona-se com a observância de padrões de controles internos, os quais devem ser compatíveis com o porte da empresa e com o volume das operações, como prevê o inciso III, do artigo 10º, da Lei de Lavagem.

60. O *Committee of Sponsoring Organizations of the Treadway Commission* ("COSO"), entidade estadunidense sem fins lucrativos que emite recomendações mundialmente praticadas para fins de controles internos, publicou, no ano de 1992, o documento "*Internal Control – Integrated Framework"*[49], em que definiu controle interno com o um processo conduzido pelo conselho de administração, pela administração e pelo corpo de empregos de uma empresa, com a finalidade de possibilitar uma garantia razoável quanto à realização de objetivos correspondestes a três categorias: a eficácia/eficiência das operações **(categoria "operações")**; a confiabilidade das demonstrações financeiras **(categoria "relatórios financeiros")**; e a conformidade com leis e regulamentos cabíveis **(categoria "compliance")**.

61. É importante ressaltar que, em 2015, via publicação do Relatório Anual de Atividades de Auditoria Interna[50], o BACEN indicou que se vale de COSO para fins de aplicação da Resolução nº 2.554/1998 ("Resolução CMN 2554/98"), que possui caráter normativo principiológico no que toca a aplicabilidade de diretrizes envolvendo "controles internos".

5. Contextualização do atual regramento brasileiro de PLD/FT

62. PLD/FT como política pública genérica, abstrata, em tese, realiza-se, materializa-se quando da análise particular, individual, do caso a caso de cada operação. A norma é real quando produz efeitos concretos a partir sempre da combinação entre Lei de Lavagem e uma norma infralegal, seja ela editada por órgão que regule mercado, como o BACEN, ou o próprio COAF para mercados não regulados, como, por exemplo, o segmento de fomento mercantil via Resolução COAF nº. 21, de 20 de dezembro 2012.

63. *In natura*, a combinação normativa entre a Lei de Lavagem e uma norma infralegal para fins de PLD/FT é apenas uma intenção, que passa a existir no ordenamento jurídico de cada país

[49] Acessível em https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf. Acesso em 28 de junho de 2020.

[50] Acessível em https://www.bcb.gov.br/Pre/audit/raint/Raint-2015-Banco-Central-do-Brasil.pdf. Acesso em 28 de junho de 2020.

em função do propósito de prevenir demais crimes, como atos de corrupção ou de terrorismos (i) identificando atividades suspeitas (sentido de suspeição) (ii) monitorando essas atividades e pessoas e (iii) "congelando" ou "confiscando" bens e ativos que possam vir a ser utilizados para finalidades criminosas com dimensões e proporções maiores.

64. Por conta disso, o GAFI/FATF[51] emite as suas Recomendações, para que os países tenham um catálogo de experiências e discussões consensuais, que no Brasil, são materializadas pelos encontros da ENCCLA.

65. No mesmo ano de criação da ENCCLA, 2003, um *grupo* formado pelas instituições financeiras mais importantes do mundo deu início às atividades do *Wolfsberg Group, grupo que tem por o*bjetivo compartilhar e disseminar as melhores práticas de PLD/FT no setor financeiro global. Em seu primeiro *paper*, "*Statement on the Suppression of the Financing of Terrorism[52]",* o documento reconheceu que, na época, não existiam critérios suficientes para determinar como as instituições financeiras deveriam operar, acompanhar e monitorar seus clientes, tampouco para determinar como deveriam ser realizadas as comunicações às autoridades.

66. Três anos depois, foi publicado o relatório anual do GAFI/FATF, cujo documento continha a seção "*Expanding the Fight Against Money Laundering & Terrorist Financing[53]"*. Esse título reportou que não existiam, ainda em 2005, critérios suficientes para determinar padrões de prevenção e combate à lavagem de dinheiro a serem adotados pelas instituições financeiras. A publicação trouxe ainda, como consequência, a realização de uma reunião com aproximadamente 80 (oitenta) delegações, na qual foi reconhecida a necessidade de estabelecer "normas-padrão" para políticas de *due diligence* e de abordagens baseadas no risco.

67. Era claro, portanto, que as instituições financeiras exerciam um papel fundamental na prevenção e combate à lavagem de dinheiro, especialmente relacionadas ao financiamento do tráfico de drogas e de atividades terroristas e de guerrilha. Mas não estava claro qual seria

---

51 Acessível em https://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Brazil%20full.pdf. Acesso em 28 de junho de 2020.

52 Acessível em https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs. Acesso em 28 de junho de 2020.

53 Acessível em http://www.fatf-gafi.org/media/fatf/documents/reports/2005%202006%20ENG.pdf. Acesso em 28 de junho de 2020.

este papel do ponto de vista de garantir a efetividade da política de PLD/FT como Política Pública.

68. Paralelamente a isso, em janeiro de 2003, Troy A. Paredes, que foi Secretário da *US Securities and Exchange Commission* ("SEC") entre 2008 e 2013, o equivalente à Comissão de Valores Mobiliários no Brasil, e é Professor de Direito da Universidade de Washington, publicou artigo "*Blinded by the Light: Information Overload and its Consequences for Securities Regulation*[54]*"*.

69. No texto, Paredes pontua, de forma muito interessante, que muitas vezes a premissa de que "quanto mais informação melhor" não necessariamente é verdadeira no contexto de "*mandatory disclosure"*, COEs.

70. Segundo Troy A. Paredes, é mais importante uma informação de boa qualidade do que informações em grande quantidade. Uma "boa informação" é peça chave para um regime de PLD/FT eficaz contanto que essa seja precisa, completa, verdadeira, útil e organizada.

71. Nesse mesmo sentido, Felipe Cabezon, da *University of the Southern California*, publicou, em dezembro de 2018, trabalho intitulado *"The Effect of Mandatory Information Disclosure on Financial Constraints"*[55]. O pesquisador afirma que, em um cenário de reportes não obrigatórios, o mercado tende a analisar quais informações são relevantes, desde que incentivado para tanto. De outro lado, se há obrigatoriedade de reporte, é possível que haja redução na qualidade das informações, em razão da falta de filtragem daquilo que realmente pode ter relevo[56].

72. É justamente em face deste cenário que foi criada a Circular 3978/2020, norma na qual nos baseamos para fins de **estabelecimento de parâmetro metodológico para criação de Políticas de PLD/FT em Exchanges.** Pelo viés normativo, baseamo-nos no texto da

---

54 Acessível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=413180. Acesso em 28 de junho de 2020.

55 Acessível em https://pdfs.semanticscholar.org/c13d. Acesso em 28 de junho de 2020.

56 Nas palavras do pesquisador: *"when disclosure is voluntary, there should exist a market solution to adverse selection problems because highly profitable firms might have incentives to disclose. Several theoretical models suggest that firms use voluntary disclosure signal their type. If the authority forces disclosure it eliminates this mechanism, and thus it might increase adverse selection problem. As suggested by recent works (e.g., Goldstein and Yang (2018)), more information may not be better if it reduces the informativeness of the currently available information. By shutting down the signaling mechanism, a mandatory provision of public Information may decrease -and not increase- the overall quality of information available to investors".*

Recomendação nº 16[57], do GAFI/FAT**, que está devidamente explorada no anexo deste Manual** (ANEXO A – Norma de Autorregulação de Exchanges Para Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo).

6. Elaboração de Política de PLD/FT para Exchanges em etapas

73. O BACEN alterou por completo seu quadro normativo para fins de PLD/FT, via Circular 3978/2020, diante da avaliação *peer review* pelo GAFI/FATF em relação ao Brasil[58].

74. Como destacou, com precisão habitual, o Procurador do BACEN Marcel Mascarenhas, ainda quando das discussões que culminaram na elaboração da Circular BACEN 3978/2020, o ideário deste novo *framework* regulatório *"é produzir um conjunto de normas de natureza mais principiológica e menos roteirizada, e, assim, trabalhar com uma abordagem de análise de risco como norteadora da política de prevenção à lavagem de dinheiro e ao financiamento ao terrorismo. Com isso, o Brasil estaria mais alinhado às orientações internacionais de boas práticas na área, emanadas principalmente pelo Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento ao Terrorismo"*[59].

75. A Circular BACEN 3978/2020 *"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"*[60]. **Entendemos que, caso a Exchange siga as etapas aqui indicadas, elaboradas com base na Circula BACEN 3978/2020, estará em consonância com aquilo que existe de mais moderno e eficiente em boas práticas de PLD/FT no Brasil e ao redor do mundo.**

76. Com o objetivo de melhorar ainda mais a qualidade da informação, a referida Circular abandonou por completo o conceito de "*Check List*", uma espécie de critérios objetivos de notificação de operações suspeitas que historicamente gerou volumes enormes de COEs (1,3

---

57 Acessível em https://www.cfatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers. Acesso em 29 de junho de 2020.

58 Acessível em http://enccla.camara.leg.br/acoes. Acesso em 28 de junho de 2020.

59 A fala reproduzida entre aspas foi retirada de exposição do Procurador do BACEN Marcel Mascarenhas, quando de sua participação no evento "Diálogos entre os Setores Público e Privado", promovido pelo Instituto de Cooperação Jurídica Internacional (ICJI), em parceria com o Grupo de Estudos em Direito Penal Econômico da Fundação Getúlio Vargas em São Paulo (FGV-SP), em 25.2.2019, em São Paulo.

60 Nos termos do artigo 1º, da Circular 3978/2020

milhões em 2016)[61], sem qualquer efetividade para fins de persecução criminal, para passar a incorporar o conceito de ABR para instituições financeiras e demais entidades autorizadas a funcionar pelo órgão.[62]

77. Como explica o GAFI/GAT, em seu *Guideline* sobre o tema: *"uma abordagem baseada em risco significa que países, autoridades competentes e bancos identificam, avaliam e compreendem o risco de lavagem de dinheiro e financiamento ao terrorismo a que estão expostos e adotam as medidas de mitigação apropriadas de acordo com o nível de risco. Essa flexibilidade permite um uso mais eficiente dos recursos, pois bancos, países e autoridades competentes podem decidir sobre a maneira mais eficaz de mitigar os riscos de lavagem de dinheiro e financiamento do terrorismo que eles identificaram. Isso lhes permite concentrar seus recursos e tomar medidas aprimoradas em situações onde os riscos são maiores, aplicar medidas simplificadas em que os riscos são mais baixos e isentar atividades de baixo risco. A implementação da abordagem baseada em risco evitará as consequências de um comportamento de risco inadequado"*[63].

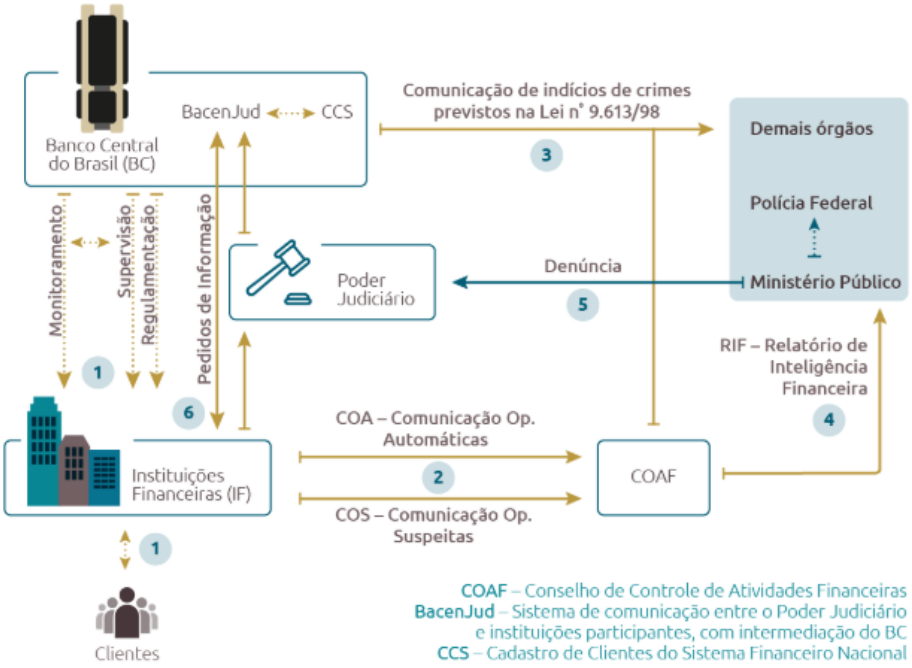
78. Para facilitar o entendimento a respeito do fluxo informacional no âmbito do BACEN, trazemos abaixo esquema elaborado pelo próprio regulador:

---

61 Acessível em https://www.valor.com.br/node/5225457. Acesso em 28 de junho de 2020.

62 Tal entendimento vai ao encontro do próprio E. CRSFN no julgamento do Recurso Voluntário nº 13.478-LD, datado de 22.7.2017, sobre coleta de informações de qualidade por uma UIF. O E. CRSFN entende que o excesso de informação "*sem organização, sem critério, sem completude pode simplesmente eliminar os efeitos do disclosure*" e, ainda, que não *"parece produtivo que uma quantidade enorme de informações seja encaminhada ao Conselho de Controle de Atividades Financeiras (COAF), órgão de prevenção e combate à lavagem de dinheiro, pois este muito provavelmente não terá condições de processar tamanha quantidade de informações*".

63 Acessível em https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf. Acesso em 28 de junho de 2020.



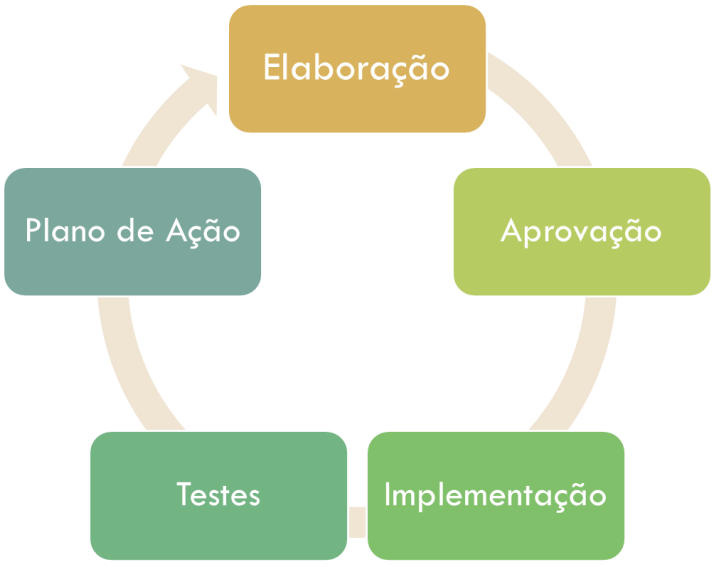
79. A Circular 3978/2020 prevê novas diretrizes a respeito (i) da governança e papéis da alta administração, (ii) da avaliação necessária e prévia de riscos e de efetividade da política de PLD/FT quando à oferta de novos produtos e serviços, (iii) de mecanismos, protocolos e indicadores pré-determinados e bem definidos envolvendo controles internos para que as 3 (três) linhas de defesa da organização venha a ser capazes de cumprir os seus papéis para fins de dar efetividade à política de PLD/FT, (iv) procedimentos relacionados à coleta de informações de clientes, funcionários, parceiros e subcontratados (v) registro de operações e serviços (vi) *search and screening* e notificações de operações suspeitas no Brasil. Tudo isso, deve ser permeado pelo conceito de ABR.

80. A fim de fornecer espécie de *overview* da nova Circular, **e especificamente das divisões e subdivisões que deve ter a Política de PLD/FT da Exchange,** elaboramos o quadro abaixo, que sistematiza todos os componentes da normativa:

Política de PLD/FT	
Diretrizes ● Papéis & Responsabilidades. ● Avaliação & Análise prévia de novos produtos serviços e tecnologias. ● Avaliação de risco & de efetividade.	**Procedimentos** ● Coleta de Informações: clientes, funcionários, terceirizados e subcontratados. ● Registro de operações e serviços. ● Search & screening operações suspeitas.

● Mecanismos de aferição do cumprimento da política, dos protocolos pré-determinados e controles internos. ● Promoção de cultura organizacional: KYE & KYP. ● Seleção e a contratação de funcionários e de prestadores de serviços terceirizados. **Divulgação** ● Aos funcionários e terceirizados, parceiros, fornecedores e prestadores de serviços terceirizados: detalhadamente. ● Documentada e atualizada após aprovações e alterações anuídas pelo Conselho de Administração ou Diretoria. **Avaliação Interna de Risco: aprovação e revisão** ● Do Conselho de Administração, ou Diretoria, Comitê de Auditoria, quando houver. ● Revisão: de 2 em 2 anos. **KYE & KYP** ● Classificar categorias de risco, obter informações sobre o contratado ou parceiro a respeito de sua reputação, certificar que o parceiro tem presença física onde está constituído ou licenciado, conhecer os seus procedimentos e a Diretoria da IF deverá aprovar o contrato de parceria.	● Reporte de operações suspeitas. **Comprometimento da alta administração** **Avaliação Interna de Risco: alvo** ● Dos clientes (classificação e qualificação), da instituição via modelo de negócio e área geográfica de atuação. ● Operações, transações, produtos e serviços, incluindo canais de distribuição. ● Dos funcionários e terceirizados, parceiros, fornecedores e prestadores de serviços terceirizados. ● Métrica e graduação (vetores macro): probabilidade de ocorrência & magnitude dos impactos financeiro, jurídico e reputacional. ● Métricas e graduação (vetores micro): processos, testes periódicos e eventuais, trilhas de auditoria, métricas e indicadores de avaliação de procedimentos, metodologia de identificação e correção de eventuais deficiências. ● Avaliação de Efetividade: metodologia, testes, qualificação dos avaliadores e trilha de deficiências e plano de ação para aplicar as devidas correções.

81. A política de PLD/FT deve conter 5 (cinco) etapas que destacamos a seguir.

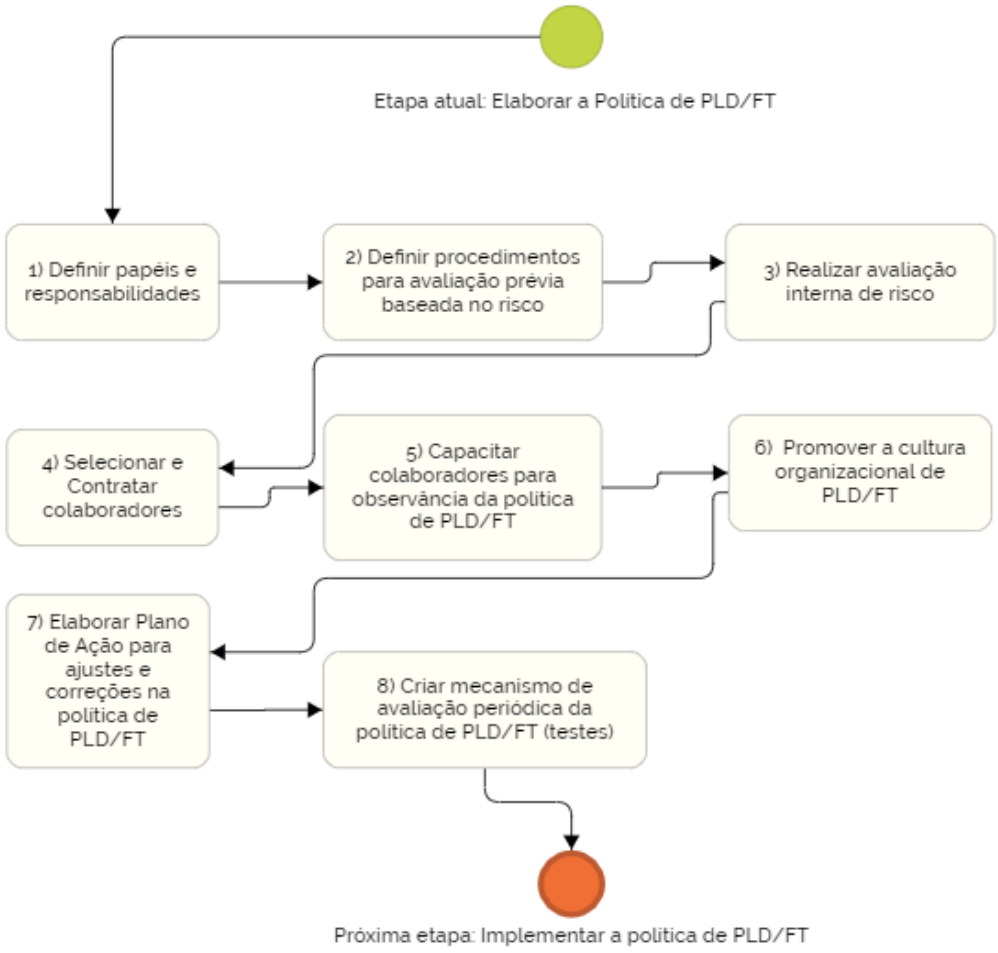


6.1 Etapa nº 1: Elaboração da Política de PLD/FT

82. A Exchange deverá definir: **(i)** os papéis e responsabilidades de cada integrante e parceiro da empresa para o cumprimento da política de PLD/FT; **(ii)** a seleção, contratação e capacitação dos empregados e parceiros; **(iii)** a promoção de cultura organizacional de PLD/FT; **(iv)** os procedimentos voltados à avaliação e à análise prévia de novos produtos e serviços, bem como da utilização de novas tecnologias, tendo em vista o risco de lavagem de dinheiro e de financiamento do terrorismo; **(v)** a avaliação interna de risco e a avaliação de efetividade; **(vi)** a verificação do cumprimento da política, dos procedimentos e dos controles internos de lavagem de dinheiro e financiamento ao terrorismo, bem como a identificação e a correção das deficiências verificadas, com definição de mecanismos de acompanhamento e de controle e a Governança da política de PLD/FT; e **(vii)** todas as diretrizes para implementação dos procedimentos de PLD/FT[64]. **Essas subetapas de elaboração devem seguir a ordem indicada neste fluxograma[65]:**

[64] **a)** de coleta, verificação, validação e atualização de informações cadastrais, visando a conhecer os clientes, os funcionários, os parceiros e os prestadores de serviços terceirizados; **b)** de registro de operações e de serviços financeiros; **c)** de monitoramento, seleção e análise de operações e situações suspeitas; e **d)** de comunicação de operações ao Conselho de Controle de Atividades Financeiras (Coaf).

[65] Conforme artigos 2º, 3º, 27, 38, 39, 43, 56 e 61, da Circular 3978/2020.



83. Como forma de avaliação interna de risco, nesta etapa precisarão estar bem definidos as formas pelas quais a política de PLD/FT formatará: (i) a classificação e qualificação dos clientes, da instituição via modelo de negócio e área geográfica de atuação; (ii) a detecção de operações, transações, produtos e serviços, incluindo canais de distribuição; (iii) a *approach* com seus funcionários e terceirizados, parceiros, fornecedores e prestadores de serviços terceirizados; (iv) métrica e graduação (vetores macro): de probabilidade de ocorrência & magnitude dos impactos financeiro, jurídico e reputacional; (v) métricas e graduação (vetores micro): processos, testes periódicos e eventuais, trilhas de auditoria, métricas e indicadores de avaliação de procedimentos, metodologia de identificação e correção de eventuais deficiências; e (vi) a "Avaliação de Efetividade" da própria política de PLD/FT: metodologia, testes, qualificação dos avaliadores e trilha de deficiências e plano de ação para aplicar as devidas correções.

6.2 Etapa nº 2: Aprovação da Política de PLD/FT

84. A aprovação da política de PLD/FT será realizada pelo comitê de auditoria[66], quando houver[67], e ao conselho de administração ou, se inexistente[68], à diretoria da instituição[69].

85. A Nota Interpretativa da Recomendação[7071] nº 1 do GAFI/FATF[72] determina que **a alta administração participe de todas as subetapas que compõem a aprovação da política de PLD/FT.**

6.3 Etapa nº 3: Implementação da Política de PLD/FT

86. O procedimento de implementação da política de PLD/DF deve ser endereçado ao setor de controles internos, como indicado em manuais internacionais, como o de COSO[73]. No âmbito desse setor, deve ainda haver indicação de pessoa responsável que responderá por esta etapa, perante a própria organização e o Estado.

---

66 *"A atuação do comitê de auditoria deve ser delimitada: sua função é de assessoramento, e não deliberativa. Ele presta apoio ao conselho de administração, a quem cabe a tomada de decisões e a responsabilidade última sobre os assuntos tratados no comitê. Este deve ser um órgão diretamente vinculado ao conselho, ao qual se reporta, não lhe competindo tomar decisões em nome do último. [...] O comitê de auditoria estatutário é uma exigência de regulamentação do BC e da Susep para instituições financeiras, entidades seguradoras, de capitalização e de previdência que atendam aos requisitos das normas vigentes. Para as demais organizações, ele é facultativo, mas sua importância é reconhecida por norma da CVM".* (http://www.ibracon.com.br/sib/gc/upload/1507212921.pdf)

67 *"A regulamentação brasileira também passou a incluir a obrigatoriedade do comitê de auditoria estatutário para alguns casos. Sua existência é exigida para muitas das instituições financeiras e seguradoras µ desde 2004, em obediência à aplicação da regulamentação pelo Banco Central (BCB) e pela Superintendência de Seguros Privados (Susep)"* (http://www.ibracon.com.br/sib/gc/upload/1507212921.pdf)

"Com relação às instituições financeiras para as quais o comitê é obrigatório, as condições são dadas pela Resolução do Conselho Monetário Nacional (CMN) n. 3.198/04. Já as normas referentes às seguradoras sujeitas à obrigatoriedade do comitê de auditoria, assim como as condições que as regem, são dadas pela Resolução do Conselho Nacional de Seguros Privados (CNSP) n. 321/15." (http://www.ibracon.com.br/sib/gc/upload/1507212921.pdf)

68 Atenção ao disposto no artigo 9º, da Resolução CMN nº 4.595, de 28 de agosto de 2017

69 Conforme artigos 9º e 12º, da Circular 3978/2020

70 As Recomendações do GAFI/FATF visão à uniformização internacional das melhores práticas concernentes a prevenir a lavagem de dinheiro e o financiamento do terrorismo. Atualmente, existem 40 (quarenta) Recomendações do GAFI/FATF, as quais servem como norte para que os países criem as suas próprias diretrizes em atenção às suas especificidades.

71 As Notas Interpretativas do GAFI/FATF têm o condão de integrar as suas Recomendações do ponto de vista interpretativo, assim como as "Carta-Circulares" estão para as "Circulares" no âmbito da disciplina normativa de edições de normas via BACEN.

72 Acessível em http://www.fazenda.gov.br/orgaos/coaf/arquivos/as-recomendacoes-gafi. Acesso em 28 de junho de 2020.

73 Acessível em https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf. Acesso em 28 de junho de 2020.

87. Nesta etapa, é importante que se leve em conta itens como:

- a elaboração de organograma que aclare quais são as linhas de subordinação funcional e a segregação de funções para a regular implementação da política de PLD/FT;
- a elaboração de um manual de procedimentos contendo práticas de autorizações, aprovações, processuais e de rotinas;
- a sistematização de estrutura contábil adequada, incluindo: técnicas orçamentárias e de custos; e
- a determinação de estrutura de auditoria interna, que seja capaz de verificar, avaliar e aperfeiçoar o procedimento de implementação.

88. Deve-se também levar em consideração a implementação da política para filiais estrangeiras e subsidiárias, que deve ter o mesmo rigor do procedimento de implementação utilizado no Brasil, como informa a Recomendação nº 18 do GAFI/FATF[74]. A Nota Interpretativa desta Recomendação aponta que essas empresas operantes no exterior devem: estabelecer programa de controles internos nos mesmos padrões dos utilizados na empresa brasileira; adotar programa contínuo de treinamento de seus colaboradores para cumprimento das determinações da política de PLD/FT elaborada pela empresa brasileira; e estabelecer auditoria independente para teste do sistema. **As informações constantes dos registros das filiais e subsidiárias devem ser compartilhadas, para fins de PLD/FT.**

89. Nesse contexto, a nova Circular criou ainda a obrigação de compartilhamento de informações intragrupo envolvendo o beneficiário final das operações e pessoas politicamente expostas, em linha com o que previu o *Guideline "Private Sector Information Sharing"*[75], publicado pelo GAFI/FATF em novembro de 2017[76].

---

74 Acessível em http://www.fazenda.gov.br/orgaos/coaf/arquivos/as-recomendacoes-gafi. Acesso em 28 de junho de 2020.

75 Acessível em https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf. Acesso em 28 de junho de 2020.

76 Conforme ao artigo 27, §6º, da Circular 3978/2020: *"no caso de relação de negócio com cliente residente no exterior que também seja cliente de instituição do mesmo grupo no exterior, fiscalizada por autoridade supervisora com a qual o Banco Central do Brasil mantenha convênio para troca de informações, admite-se que as informações de qualificação de pessoa exposta politicamente sejam obtidas da instituição no exterior, desde que assegurado ao Banco Central do Brasil o acesso aos respectivos dados e procedimentos adotados".*

90. Esta etapa – como todas as outras – deve ter como base **a avaliação baseada no risco**, a fim de que haja laço entre os expedientes adotados pela área de controles internos e a realidade fática das operações e dos clientes envolvidos com a Exchange.

91. A Exchange deve separar em 3 (três) fases o procedimento de implementação: **a coleta (**momento de registro e armazenamento de informações), **a análise** (quando a empresa deve implementar procedimentos que assegurem a avaliação da política de PLD/FT); e **a resposta** (subetapa em que se deve apontar quais são os mecanismos da empresa para a resolução de possíveis irregularidades na política de PLD/FT, com base na probabilidade e impacto do risco[77] e do custo-benefício[78]).

6.4 Etapa nº 4: Testes da Política de PLD/FT

92. A etapa de testes é de grande importância, porque serve como modo de análise do grau de *accuracy* da Política de PLD/FT. Por meio dessa avaliação, a Exchange realizará ajustes que deverão corrigir inconstâncias, sem a necessidade de qualquer movimentação do lado do Estado.

93. O endereçamento de reparos na Política de PLD/FT (realizáveis pelos procedimentos descritos no Plano de Ação) deve ter lastro em testes definidos pela própria Exchange, de acordo com o risco das operações, a diversidade de sua base de clientes, a localização geográfica e outras variáveis atinentes à possibilidade de utilização da instituição para fins de lavagem de dinheiro e financiamento do terrorismo. Encaixam-se nesse conceito: **(i) testes conceituais,** que consistem em avaliar a adequação entre os expedientes adotados pela

---

77 *"Na avaliação das opções de resposta, a administração considera o efeito da probabilidade e do impacto do risco, reconhecendo que uma determinada resposta poderá afetar, de forma diferente, a probabilidade e o impacto do risco. [...] Ao analisar as respostas, a administração poderá considerar eventos e tendências anteriores, e o potencial de situações futuras. Via de regra, ao avaliar as respostas alternativas, a administração determina o seu efeito em potencial, utilizando as mesmas unidades de medida ou as compatíveis com as empregadas para o objetivo correspondente."* (https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf)

78 *"Em razão das limitações de recursos, as organizações devem considerar os custos e os benefícios relativos às opções de respostas alternativas ao risco. As medições de custo-benefício para a implementação de respostas a riscos são realizadas com diversos níveis de precisão. De um modo geral, é mais fácil tratar do aspecto custo da equação, que, em muitos casos, pode ser quantificado com bastante precisão. Habitualmente, consideram-se todos os custos diretos associados ao estabelecimento de uma resposta, e os custos indiretos, caso sejam mensuráveis na prática. Algumas organizações também incluem os custos de oportunidade associados à utilização dos recursos."* (https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf)

empresa e as previsões legais e infralegais; **(ii) testes sistêmicos,** nos quais se realizada espécie de "varredura" nos cadastros internos da empresa, a fim de checar a completude da base cadastral da Exchange. Para tanto, a empresa pode comparar as suas informações com as constantes em cadastros da Receita Federal Brasileira ("RFB") e em cadastros de outras empresas privadas; e **(iii) testes de fidedignidade de informações,** em que se compara dados em meio físico com dados em bases digitais da empresa.

94. Outros testes podem e **devem** ser empregados, para possibilitar a ágil correção dos expedientes dispostos na política de PLD/FT .

6.5 Etapa º 5: Plano de Ação da Política de PLD/FT

95. O Plano de Ação consiste em uma série de procedimentos que devem ser acionados para corrigir eventuais irregularidades na efetividade da política de PLD/FT, dos procedimentos e controles internos previstos pela empresa. Esse documento deve ser revisto em duas hipóteses: (i) **quando se passam dois anos da elaboração da política de PLD/FT;** e (ii) **quando, na fase de testes, nota-se alguma irregularidade na política de PLD/FT.**

96. A implementação do Plano de Ação deverá ser documentada por meio de relatório de acompanhamento, que deve ser encaminhado à ciência: (i) do comitê de auditoria, quando houver; (ii) da diretoria da instituição; e (iii) do conselho de administração, quando existente.

97. Por final, a fim de exemplificar o regramento sancionador em PLD/FT, destacamos que a Circular BACEN n°. 3.858, de 14 de novembro de 2017 ("Circular BACEN 3858/17"), ajuda a identificar, pelo lado do consequencialíssimo, quais serão os custos da inobservância, caso não se atenda à Circular 3978/2020. Para facilitar o entendimento a esse ponto, preparamos o quadro a seguir no que tocam todas as obrigações administrativas:

Irregularidades	***Penalidades: Multa***	***Inabilitação***
1.) Deixar de cadastrar ou atualizar cadastro	a) R$ 20 mil a R$ 50 mil b) R$ 30 mil a R$ 80 mil, quando grave	3 a 5 anos
2.) Omissão de Comunicação Automática	a) R$ 50 mil a R$ 100 mil	3 a 5 anos

	b) R$ 60 mil a R$ 150 mil, grave	
3.) Deixar de identificar cliente, atualizar cadastro e de manter registro das transações	a) R$ 250 mil a R$ 1 milhão b) R$ 500 mil a R$ 2 milhões, grave	3 a 5 anos
4.) Deixar de adotar procedimentos relacionados a controles internos	a) R$ 500 mil a R$ 3 milhões b) R$ 1 milhão a R$ 6 milhões, grave	6 a 8 anos
5.) Comunicar de forma inadequada ou fora do prazo operações de Comunicação Automática	a) 1% a 2% das operações b) 2% a 4%, grave	4 a 6 anos
6.) Deixar de comunicar operações de Comunicação Automática	a) 2% a 5% b) 3% a 6%, grave	4 a 6 anos
7.) Comunicar de forma inadequada ou fora do prazo, propostas ou operações que contenham indícios de crimes ou que com eles se relacionem	a) 5% a 7% b) 6% a 8%, grave	6 a 8 anos
8.) Administrador que não deixar de dar ciência do ato de comunicação a outras pessoas, inclusive àquelas objeto da comunicação	a) 7% a 9% b) 8% a 10%, grave	4 a 6 anos
9.) Deixar de reportar propostas ou operações que contenham indícios de crime ou que com eles se relacionem	a) 10% a 15% b) 15% a 20%, grave	6 a 8 anos

7. Dever de diligência do administrador de Exchange

98. Para a elaboração deste Manual, valemo-nos da Circular 3978/2020, para fins de parametrização metodológica de estabelecimento de Política de PLD/FT por Exchanges, e da Resolução nº 4.595, de 28 de agosto de 2017, do Conselho Monetário Nacional ("Resolução CMN 4595/17"), que traz exigências quanto à necessidade de implementação, cumprimento, revisão e gerenciamento de diretrizes que digam respeito ao Compliance[79], como parâmetro normativo.

[79] Art. 9º da Resolução nº 4595/2017: *"O conselho de administração deve, além do previsto no art. 4º desta Resolução: I - assegurar: a) a adequada gestão da política de conformidade na instituição; b) a efetividade e a continuidade da aplicação da política de conformidade; c) a comunicação da política de conformidade a todos os*

99. Nesse sentido, ressaltamos: **os deveres destacados nos tópicos anteriores integram o chamado dever de diligência,** mencionado pelo legislador infraconstitucional, no artigo 153, da Lei nº 6.404, de 16 de dezembro de 1976 ("Lei das S.A")[80].

100. O dever de diligência é um conceito abstrato que implica um padrão de comportamento[81]. Em jurisdições estrangeiras, é conhecido como *duty of care*, dever segundo o qual os administradores precisam cumprir com diligência as obrigações derivadas das suas funções, resultando da regra moral subjacente denominada *law of negligence*[82]. Nesse sentido, os administradores das Exchanges devem aplicar nas atividades de controle, decisão e condução da companhia, o tempo, esforço e conhecimentos demandados pela natureza das funções, competências específicas e determinadas circunstâncias[83].

101. Nas fases de implementação e de revisão da política de PLD/FT, é importante que o administrador da Exchange tenha o cuidado de coordenar as suas atuações, com clareza, com base nos deveres e obrigações previstos no estatuto social da instituição supervisionada. Essa preocupação parte da análise minuciosa da jurisprudência do Conselho de Recursos do Sistema Financeiro Nacional ("CRSFN"), que indica maior potencial de responsabilização dos administradores quando as suas obrigações são genéricas[84].

---

empregados e prestadores de serviços terceirizados relevantes; e d) a disseminação de padrões de integridade e conduta ética como parte da cultura da instituição; II - garantir que medidas corretivas sejam tomadas quando falhas de conformidade forem identificadas; e III - prover os meios necessários para que as atividades relacionadas à função de conformidade sejam exercidas adequadamente, nos termos desta Resolução".

80 "*Art. 153. O administrador da companhia deve empregar, no exercício de suas funções, o cuidado e diligência que todo homem ativo e probo costuma empregar na administração dos seus próprios negócios".*

81 CARVALHOSA, Modesto. Comentários à lei das sociedades anônimas. 3º Vol. 4ª ed. São Paulo: Saraiva, 2009, p. 274.

82 Como ensina Pedro Caetano Nunes, em sua obra "*Corporate governance*", o ideário de *law of negligence* impõe àquele que assume uma função que comporta um risco de provocação de danos a obrigação moral de cumprir o seu dever com diligência .

83 ABREU, J. M. Coutinho de. Responsabilidade civil dos administradores de sociedades. 2ª ed. Coimbra, Almedina, 2010, p. 19.

84 Por exemplo, no Recurso nº. 12.533 do CRSFN, julgado em 25.8.2015, foi decidido que: (i) apesar de o disposto no artigo 44, da Lei nº. 4.595/64 e no Decreto-Lei nº. 448 ser considerado norma aberta para fins de caracterização de falta grave (ausência de legalidade, portanto), estes dispositivos estariam inseridos no conceito de norma de "terceira geração" (CR/88), com a finalidade de preservar o interesse da coletividade, o que justificaria portanto, a manutenção da condenação como infração grave; e (ii) a simples assinatura individual da ata de reunião colegiada bastaria como elemento probatório para a caracterização da responsabilidade e culpa dos administradores do banco.

102. No dia a dia, tem-se visto o BACEN interpretar o artigo 153, da Lei das S.A., de forma ampliativa. Para a Procuradoria Geral da Fazenda Nacional, que atua junto ao CRSFN, o dever de diligência do administrador está relacionado com postura e conduta proativas para identificar se um determinado assunto é ou não irregular do ponto de vista jurídico. Dessa forma, o administrador da Exchange deve ter o mínimo de cuidado e diligência ao participar das reuniões da instituição e ter uma postura proativa. **A ressalva em Ata**, indicando uma eventual discordância com o que foi decidido, pode, por exemplo, **isentá-lo de culpa quando diante de eventual cenário limítrofe sobre prática regular versus irregular.**

103. Deve-se ter especial atenção, portanto, nos casos particularmente sensíveis para o futuro da Exchange, como, por exemplo, em momentos de **alienação de controle acionário** ou de **emissão de novas ações**. Isso quer dizer que, além da verificação das informações disponíveis, deverá o conselheiro exigir solicitações adicionais, conforme o caso, sob pena de descumprir seu dever fiduciário de diligência.

104. Tem-se visto em demais julgados, por outro lado, que não será considerada a "quebra" do dever de diligência pelo administrador, nos casos em que:

i. as decisões negociais da companhia, ainda que fracassadas, tenham respeitado os procedimentos de deliberação e averiguação esperados do Conselho de Administração[85];
ii. a conduta seja configurada como descumprimento no dever de lealdade. Não poderá um mesmo ato se configurar como quebra ao dever de lealdade e de diligência. Por exemplo, se o administrador sabe que sua omissão será perniciosa à companhia, mas benéfica a si próprio, a omissão dolosa configura descumprimento do dever de lealdade, porém não descumprimento do dever de diligência[86];
iii. os conselheiros não possuem ciência de informações que outros detêm, os quais sim podem ser punidos por conta do conhecimento. Ou seja, o Conselho de Administração é órgão da companhia, todavia a apuração de responsabilidades é individual e depende das circunstâncias atinentes a cada membro, que poderão ter uma competência estatutária específica[87];

85 Recurso nº. 11.832/2012 do CRSFN
86 Recurso nº 11.833/2013 do CRSFN
87 Recurso nº. 11.958/2012 do CRSFN

iv. se trate de ocorrências rotineiras da companhia, que estão mais próximas dos diretores executivos. O conselheiro não poderá ser punido quando essa distância natural lhe obsta o acesso a determinadas informações[88]; e

v. ocorra a conduta proativa do conselheiro, ainda que inadequada ou ineficaz, podendo até ser alvo de alguma outra imputação, mas não na caracterização do descumprimento do dever de diligência[89].

105. Especificamente quanto a possíveis inobservâncias de dever de diligência que impliquem em prejuízo para consumidores, os administradores das Exchanges devem estar atentos à possibilidade de propositura de ação civil pública, pelo Ministério Público, com base na Lei nº 7.913, de 7 de dezembro de 1989, que é a ação civil pública, de competência do Ministério Público.

106. Por fim, é importante ressaltar que o artigo 159, da Lei das S.A., prevê a possibilidade de ajuizamento de ação de responsabilidade civil em face de administradores, atribuindo à companhia, mediante deliberação da assembleia geral, a competência para promovê-la, a fim de reaver os prejuízos causados ao seu patrimônio. Existe ainda a possibilidade de ação interposta individualmente por acionistas ou terceiros diretamente prejudicados pelo administrador.

88 Recurso nº. 11.417/2012 do CRSFN

89 Recurso nº 11.969/2012 do CRSFN

ANEXO A –Autorregulação de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo

Brasília-DF, Julho de 2020

ÍNDICE

CAPÍTULO I – OBJETO E ÂMBITO DE APLICAÇÃO

Art. 1º. Esta Norma de Autorregulação dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas Exchanges brasileiras, visando à prevenção da utilização do segmento de criptoeconomia 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.

§ 1º Para os fins desta Norma de Autorregulação, os crimes referidos no caput serão denominados genericamente "lavagem de dinheiro" e "financiamento do terrorismo".

§ 2º Para os fins desta Norma de Autorregulação, denominaremos “Exchanges” a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos, em conformidade com o disposto na Instrução Normativa RFB nº 1.888, de 3 de maio de 2019.

CAPÍTULO II - DA POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO

Art. 2º. As Exchanges devem implementar e manter política formulada com base em princípios e diretrizes que busquem prevenir a sua utilização para as práticas de lavagem de dinheiro e de financiamento do terrorismo.

Parágrafo único. A política de que trata o caput deve ser compatível com os perfis de risco:

I - dos clientes;

II - da instituição;

III - das operações, transações, produtos e serviços; e

IV - dos funcionários, parceiros e prestadores de serviços terceirizados.

Art. 3º. A política referida no art. 2º deve comtemplar:

I - as diretrizes para:

a) a definição de papéis e responsabilidades para o cumprimento das obrigações de que trata esta Norma de Autorregulação;

b) a definição de procedimentos voltados à avaliação e à análise prévia de novos produtos e serviços, bem como da utilização de novas tecnologias, tendo em vista o risco de lavagem de dinheiro e de financiamento do terrorismo;

c) a avaliação interna de risco e a avaliação de efetividade;

d) a verificação do cumprimento da política, dos procedimentos e dos controles internos de que trata esta Norma de Autorregulação, bem como a identificação e a correção das deficiências verificadas;

e) a promoção de cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, contemplando, inclusive, os funcionários, os parceiros e os prestadores de serviços terceirizados;

f) a seleção e a contratação de funcionários e de prestadores de serviços terceirizados, tendo em vista o risco de lavagem de dinheiro e de financiamento do terrorismo; e

g) a capacitação dos funcionários sobre o tema da prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

II - as diretrizes para implementação de procedimentos:

a) de coleta, verificação, validação e atualização de informações cadastrais, visando a conhecer os clientes, os funcionários, os parceiros e os prestadores de serviços terceirizados;

b) de registro de operações e de serviços financeiros;

c) de monitoramento, seleção e análise de operações e situações suspeitas; e

d) de comunicação de operações ao Conselho de Controle de Atividades Financeiras (Coaf); e

III - o comprometimento da alta administração com a efetividade e a melhoria contínua da política, dos procedimentos e dos controles internos relacionados com a prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

Art. 4º. A política referida no art. 2º deve ser:

I - documentada;

II - aprovada pelo conselho de administração ou, se inexistente, pela diretoria da Exchange; e

III - mantida atualizada.

CAPÍTULO III – DA AVALIAÇÃO INTERNA DE RISCO

Art. 5º. As Exchanges devem realizar avaliação interna com o objetivo de identificar e mensurar o risco de utilização de seus produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.

§ 1º Para identificação do risco de que trata o caput, a avaliação interna deve considerar, no mínimo, os perfis de risco:

I - dos clientes;

II - da Exchange, incluindo o modelo de negócio e a área geográfica de atuação;

III - das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e

IV - das atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados.

§ 2º Devem ser utilizadas como subsídio à avaliação interna de risco, quando disponíveis, avaliações realizadas por entidades públicas do País relativas ao risco de lavagem de dinheiro e de financiamento do terrorismo.

Art. 6º. A avaliação interna de risco deve ser:

I - documentada e aprovada por diretor responsável;

II - revisada a cada dois anos, bem como quando ocorrerem alterações significativas nos perfis de risco mencionados no art. 5º.

CAPÍTULO IV – DOS PROCEDIMENTOS DESTINADOS A CONHECER OS CLIENTES

Art. 7º. As Exchanges devem implementar procedimentos destinados a conhecer seus clientes, incluindo procedimentos que assegurem a devida diligência na sua identificação, qualificação e classificação.

§ 1º Os procedimentos referidos no caput devem ser compatíveis com:

I - o perfil de risco do cliente, contemplando medidas reforçadas para clientes classificados em categorias de maior risco, de acordo com a avaliação interna de risco referida no art. 5º;

II - a política de prevenção à lavagem de dinheiro e ao financiamento do terrorismo de que trata o art. 2º; e

III - a avaliação interna de risco de que trata o art. 5º.

Art. 8º. As Exchanges devem adotar procedimentos de identificação que permitam verificar e validar a identidade do cliente.

§ 1º Os procedimentos referidos no caput devem incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação do cliente, inclusive, se necessário, mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

§ 2º No processo de identificação do cliente devem ser obtidos, no mínimo:

I - o nome completo, o endereço residencial e o número de registro no Cadastro de Pessoas Físicas (CPF) ou registro similar, no caso de pessoa natural; e

II - a firma ou denominação social, o endereço da sede e o número de registro no Cadastro Nacional da Pessoa Jurídica (CNPJ) ou registro similar, no caso de pessoa jurídica.

Art. 9º. As informações referidas no art. 8º devem ser mantidas atualizadas.

Art.10º As Exchanges devem adotar procedimentos que permitam qualificar seus clientes por meio da coleta, verificação e validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócio.

§ 1º Os procedimentos de qualificação referidos no caput devem incluir a coleta de informações que permitam avaliar a capacidade financeira do cliente, incluindo a renda, no caso de pessoa natural, ou o faturamento, no caso de pessoa jurídica.

§ 2º A necessidade de verificação e de validação das informações referidas no § 1º deve ser avaliada pelas Exchanges de acordo com o perfil de risco do cliente e com a natureza da relação de negócio.

§ 3º Nos procedimentos de que trata o caput, devem ser coletadas informações adicionais do cliente compatíveis com o risco de utilização de produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.

§ 4º A qualificação do cliente deve ser reavaliada de forma permanente, de acordo com a evolução da relação de negócio e do perfil de risco.

§ 5º As informações coletadas na qualificação do cliente devem ser mantidas atualizadas.

Art. 11º Os procedimentos de qualificação do cliente pessoa jurídica devem incluir a análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como seu beneficiário final, sempre que a participação seja igual ou maior que o percentual de 20%.

§ 1º Devem ser aplicados à pessoa natural referida no caput, no mínimo, os procedimentos de qualificação definidos para a categoria de risco do cliente pessoa jurídica na qual o beneficiário final detenha participação societária.

§ 2º É também considerado beneficiário final o representante, inclusive o procurador e o preposto, que exerça o comando de fato sobre as atividades da pessoa jurídica.

CAPÍTULO V – DOS PROCEDIMENTOS DESTINADOS A CONTROLES INTERNOS

Art. 12º Os controles internos, independentemente do porte da Exchange, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações por ela realizadas.

Art. 13º Os controles internos, cujas disposições devem ser acessíveis a todos os funcionários da Exchange, de forma a assegurar sejam conhecidas a respectiva função no processo e as responsabilidades atribuídas aos diversos níveis da organização, devem prever:

I - a definição de responsabilidades dentro da Exchange;

II - meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da instituição;

III - a existência de canais de comunicação que assegurem aos funcionários, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

IV - a contínua avaliação dos diversos riscos associados às atividades da instituição;

V - O acompanhamento sistemático das atividades desenvolvidas, de forma a que se possa avaliar se os objetivos da instituição estão sendo alcançados, bem como a assegurar que quaisquer desvios possam ser prontamente corrigidos; e

VI - a existência de testes periódicos para os sistemas de informações, em especial para os mantidos em meio eletrônico.

VII - a existência de canais de comunicação que assegurem aos funcionários, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

VIII - a contínua avaliação dos diversos riscos associados às atividades da instituição;

§ 1º Os controles internos devem ser periodicamente revisados e atualizados, de forma a que sejam a eles incorporadas medidas relacionadas a riscos novos ou anteriormente não abordados.

CAPÍTULO VI – DA COMUNICAÇÃO AO COAF

Art. 14º As Exchanges devem implementar procedimentos de monitoramento, seleção e análise de operações e situações com o objetivo de identificar e dispensar especial atenção às suspeitas de lavagem de dinheiro e de financiamento do terrorismo.

Parágrafo único. Os procedimentos mencionados no caput devem:

I - ser compatíveis com a política de prevenção à lavagem de dinheiro e ao financiamento do terrorismo da Exchange;

II - ser definidos com base na avaliação interna de risco; e

III - considerar a condição de pessoa exposta politicamente, bem como a condição de representante, familiar ou estreito colaborador da pessoa exposta politicamente.

Art. 15º As Exchanges devem implementar procedimentos de análise das operações e situações selecionadas por meio dos procedimentos de monitoramento e seleção de que, com o objetivo de caracterizá-las ou não como suspeitas de lavagem de dinheiro e de financiamento do terrorismo.

§ 1º O período para a execução dos procedimentos de análise das operações e situações selecionadas não pode exceder o prazo de quarenta e cinco dias, contados a partir da data da seleção da operação ou situação.

§ 2º A análise mencionada no caput deve ser formalizada em dossiê, independentemente da comunicação ao Coaf.

Art. 16º As Exchanges devem comunicar ao Coaf as operações ou situações suspeitas de lavagem de dinheiro e de financiamento do terrorismo.

§ 1º A decisão de comunicação da operação ou situação ao Coaf deve:

I - ser fundamentada com base nas informações contidas no dossiê mencionado no art. 15, § 2º;

II - ser registrada de forma detalhada no dossiê mencionado no art. 15, § 2º; e

III - ocorrer até o final do prazo de análise referido no art. 15, § 1º.

CAPÍTULO VII – DOS MECANISMOS DE ACOMPANHAMENTO E DE CONTROLE

Art. 17º As Exchanges devem instituir mecanismos de acompanhamento e de controle de modo a assegurar a implementação e a adequação da política, dos procedimentos e dos controles internos de que trata esta Norma de Autorregulação, incluindo:

Parágrafo único. Os procedimentos mencionados no caput devem:

I - a definição de processos, testes e trilhas de auditoria

II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

Art. 18º As Exchanges devem elaborar plano de ação destinado a solucionar as deficiências identificadas por meio de avaliação de efetividade da política, dos procedimentos e dos controles internos de que trata esta Norma de Autorregulação.

§ 1º O acompanhamento da implementação do plano de ação referido no caput deve ser documentado por meio de relatório de acompanhamento.

§ 2º O plano de ação e o respectivo relatório de acompanhamento devem ser encaminhados para ciência e avaliação, até 30 de junho de cada ano:

I - do comitê de auditoria, quando houver;

II - da diretoria da Exchange; e

III - do conselho de administração, quando existente.

CAPÍTULO VIII – DAS DISPOSIÇÕES FINAIS

Art. 19º Esta Norma de Autorregulação entre em vigor em 14 de agosto de 2020.