

**LAVAGEM DE DINHEIRO E CORRETORAS DE VALORES
MOBILIÁRIOS: CONTEXTO, REGULAÇÃO E
IMPLEMENTAÇÃO DE KYC**

*MONEY LAUNDERING AND SECURITIES BROKERS: CONTEXT,
REGULATION AND KYC IMPLEMENTATION*

Paulo Coelho¹

Felipe Eduardo Hideo Hayashi²

RESUMO

A complexidade das normas regulatórias de prevenção à lavagem de dinheiro é grande geradora de riscos de conformidade para as instituições financeiras reguladas pelo Banco Central do Brasil e pela Comissão de Valores Mobiliários. Esta complexidade advém de vários fatores, como documentos internacionais, leis nacionais, realidade da evolução tecnológica e das práticas criminosas e as demandas de mercado. Por essa razão, para a gestão destes riscos, se faz necessária a adoção de metodologia robusta e adaptável à diversas realidades, capaz de prevenir lavagem de dinheiro sem impactar negativamente o negócio, criando para ele, inclusive, valor. O presente trabalho pretende

¹ Pós-graduado em Compliance e Governança Jurídica pela FAE Business School e Bacharel em Direito pela UFPR. Advogado com experiência profissional em Direito Criminal e Compliance no Mercado Financeiro. Membro da Comissão de Conformidade e Compliance da OAB/SC. Pesquisador do Instituto Brasileiro de Prevenção à Lavagem de Dinheiro. Contato: paulohcosta94@gmail.com.

² Mestre em Direito Econômico e Socioambiental pela Pontifícia Universidade Católica do Paraná - PUC/PR. Especialista em Ciências Criminais e Direito Processual. Graduado em Direito pela Universidade Federal de Santa Catarina - UFSC. Professor de Compliance da FAE Business School. Autor do livro "Corrupção: Combate Transnacional, Compliance e Investigação Criminal?". Delegado de Polícia Federal. Ex-Chefe da Delegacia de Repressão a Corrupção e Crimes Financeiros no Paraná. Ex-Diretor do Departamento de Justiça da Secretaria de Justiça, Família e Trabalho do Paraná. Chefe da Delegacia de Repressão a Crimes Contra o Meio Ambiente e o Patrimônio Histórico no Paraná. Contato: hayashi.fehh@gmail.com.

demonstrar através de exemplos a aplicabilidade do COSO *Internal Control Integrated Framework* para a construção de controles de KYC em uma Corretora de Câmbio, Títulos e Valores Mobiliários. Irá se realizar uma contextualização das normas que geram as obrigações para as Instituições, para depois, seguindo os pilares do COSO exemplificar como os controles podem ser construídos.

Palavras-chave: Compliance. Coso. Lavagem de dinheiro.

ABSTRACT

The complexity of Anti-money laundering regulatory standards is a major source of compliance risks for financial institutions regulated by the Central Bank of Brazil and the Brazilian Securities and Exchange Commission. This complexity arises from several factors, such as international documents, national laws, the reality of technological evolution and criminal practices, as well as market demands. For this reason, managing these risks requires the adoption of a robust and adaptable methodology to different contexts, capable of preventing money laundering without negatively impacting business operations, and even creating value for the organization. This paper aims to demonstrate, through examples, the applicability of the COSO Internal Control Integrated Framework in building Know Your Customer controls within a Foreign Exchange, Securities, and Brokerage Firm, under Brazilian laws and regulations. It will provide a contextualization of the regulations that generate obligations for institutions, and then, following COSO's pillars, illustrate how these controls can be constructed.

Keywords: Anti-money Laundering. Compliance. COSO.

1 INTRODUÇÃO

O presente trabalho possui o objetivo de apresentar uma ilustração da implementação da parte de KYC (Know Your Customer) de um programa de prevenção à lavagem de dinheiro (PLD) em uma Corretora de Câmbio, Títulos e Valores Mobiliários (CCTVM), tipo de instituição financeira regulada pela Comissão de Valores Mobiliários (CVM) e pelo Banco Central do Brasil (BACEN). O esforço aqui se dará contextualizando o instituto do *Compliance*, examinando as principais normas regulatórias aplicáveis e ilustrando a implementação de controles internos,

especialmente no quesito de *Know Your Customer* (KYC), a partir da metodologia COSO.

Pretende-se um exame dos principais pontos das normas regulatórias aplicáveis e demonstrar, por meio de exemplos, a aplicabilidade da metodologia escolhida para a construção de controles pelo departamento de *Compliance* de uma CCTVM.

2 CONTEXTO

O conceito de *Compliance* chega ao cenário corporativo brasileiro inicialmente através de empresas multinacionais que, em razão das jurisdições onde possuíam ações negociadas ou onde estavam estabelecidas suas sedes, eram obrigadas a manter programas e padrões a fim de garantir o cumprimento de legislações em todas as suas filiais³. *Compliance* significa, em tradução livre, “cumprimento”, podendo-se dizer que seu conceito é inerente às relações empresariais em um estado democrático de Direito, uma vez que todo aquele dotado de personalidade jurídica contrai o dever de cumprir a lei.

No cenário global, a obrigação de implementação de programas de *Compliance* no setor privado, a padronização da prática e o *enforcement* específico, tem suas origens e desenvolvimento a partir de alguns casos emblemáticos.

Em 1972, durante a campanha eleitoral para as eleições daquele ano nos EUA, cinco pessoas foram detidas durante a tentativa de fotografar documentos e instalar aparelhos de escuta no escritório do Partido Democrata. O que ficou conhecido como “Caso Watergate”, culminou com a renúncia do presidente republicano, Richard Nixon, após as investigações provarem que o candidato

³ CARVALHO, André Castro Carvalho (org.). Manual de Compliance. Rio de Janeiro: Forense, 2019. p. 38.

vencedor tinha conhecimento das operações ilegais contra a oposição. Os desdobramentos do caso revelaram, além de situações de corrupção em solo norte-americano, esquemas de suborno de funcionários de alto escalão de governos de diferentes países, perpetrados por empresas nacionais, com o fim de obter vantagens na realização de negócios. Uma das respostas legislativas ao caso, especificamente com relação à corrupção extraterritorial, foi a edição do “*Foreign Corrupt Practices Act*”, diploma legal que, em síntese, obriga as empresas norte-americanas a cumprirem normas e manterem sistemas anticorrupção mesmo fora do território nacional⁴.

A Enron Corporation foi uma das empresas líderes no mundo em distribuição de energia e comunicações e no ano de 2001, investigações revelaram que a corporação havia manipulado seus balanços contábeis, inflando artificialmente seus lucros e escondendo dívidas de 25 bilhões de dólares por dois anos consecutivos. Em 2002, a resposta legislativa a este e outros escândalos financeiros foi a redação da Lei *Sarbanes-Oxley*, que criou um arcabouço de obrigações voltada à realização de auditoria e implementação de controles internos nas empresas para mitigar riscos e, sobretudo, evitar fraudes como a mencionada⁵.

No ano de 2008 o mundo foi afetado pela maior crise econômica desde a ocorrida em 1929, quando, em efeito dominó, diversas grandes instituições financeiras quebraram em razão, dentre diversas outras questões, do estouro de uma bolha que se criou no mercado imobiliário norte-americano. É colossal a complexidade da crise, mas ela também ganhou a alcunha de “crise dos *subprimes*” por ter sido consequência da concessão de empréstimos de alto risco que se espalharam no sistema financeiro

⁴ HAYASHI, Felipe Eduardo Hideo. *Corrupção: Combate Transnacional, Compliance e Investigação Criminal*. Rio de Janeiro: Lumen Iuris, 2015, p. 34.

⁵ ASSI, Marcos. *Gestão de riscos com controles internos: Certificações e métodos para garantir a eficiência dos negócios*. São Paulo: Saint Paul, 2019, E-book Kindle, local 906.

mundial muito em razão de análises fraudulentas a respeito do nível de risco de títulos que possuíam em sua composição dívidas cuja inadimplência era praticamente certa⁶. Uma das principais respostas globais para crise foi a edição do terceiro Acordo de Basileia (ou simplesmente Basileia III), iniciativa promovida pelo Fórum de Estabilidade Financeira e pelo G20 para reforçar o sistema financeiro mundial após a crise de 2008, que reforça principalmente os padrões de gestão de risco das instituições financeiras.

Conforme já mencionado, os desdobramentos dos referidos casos fazem desembarcar as práticas de *Compliance* no território brasileiro pela via da obrigação de multinacionais a cumprirem com determinados padrões em todo o mundo. Contudo, ao lado desta via privada, o cenário atual do *Compliance*, em especial no quesito PLD, evidentemente contou também com a ação do poder público, motivado por discussões de direito internacional.

Em 1988, em Viena, foi concluída a Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas, promulgada no Brasil pelo Decreto 154/1991, o documento inaugurou a previsão da lavagem de dinheiro em normas do gênero. Dentre as ações previstas na convenção para combater o tráfico de drogas, destaca-se a importância de “privar pessoas dedicadas ao tráfico ilícito do produto de suas atividades criminosas” e eliminar, assim, o principal incentivo a essa atividade.

A convenção de Palermo, do ano 2000, promulgada no Brasil pelo Decreto 5.015/2006, traz conjunto de regras para o combate das organizações criminosas, tratando especificamente da lavagem de dinheiro e da necessidade de sua prevenção e repressão.

A Convenção de Mérida, de 2003, promulgada nacionalmente pelo Decreto 5.687/2006, trata especificamente do combate à corrupção, dispendo sobre PLD e

⁶ PINHEIRO, Juliano Lima. OLIVEIRA, Virgínia Izabel (org.). Gestão de Riscos no mercado financeiro. São Paulo: Saraiva, 2018, p. 12-14.

instituinto rígidos controles administrativos sobre a atuação de setores sensíveis, como instituições financeiras.

No que diz respeito ao *Compliance*, a colaboração privada é tratada especificamente pela Convenção de Palermo, em seu artigo 7º, e pela Convenção de Mérida, em seu artigo 14.

Finalmente, neste cenário, em 1988 foi publicada a Lei 9.613/1988, primeiro texto normativo do país a respeito da lavagem de dinheiro. A Lei de lavagem de dinheiro será tratada com mais detalhe no tópico seguinte, contudo, neste momento é importante mencionar que, além da criminalização da prática, o diploma define as pessoas e entidades privadas obrigadas a colaborar com a fiscalização e identificação de práticas delitivas.

Especialmente no setor das CCTVMs, os esforços de prevenção e definição de obrigações estendem-se às normas dos órgãos reguladores, que serão tratadas em tópicos específicos.

Cabe mencionar que, relacionadas à PLD, encontram-se também a prevenção ao financiamento do terrorismo e da proliferação de armas de destruição em massa. A principal diferença entre as questões de lavagem de dinheiro e as outras duas citadas é que nas demais a origem dos recursos pode ser lícita. Contudo, em que pese a complexidade particular das citadas questões, uma estrutura de controles de cumprimento de normas única pode abarcar ambos os temas, devendo apenas a instituição levar em consideração, por exemplo, um risco mais elevado de financiamento ao terrorismo a depender da atuação em determinadas regiões, ou outros fatores que façam a atividade mais exposta ao risco de financiamento do terrorismo.

3 A LEI 9.613/1988

Foi dentro do mencionado contexto internacional, somado à ocorrência doméstica de casos de corrupção relacionados com lavagem de dinheiro e a um diverso processo de expansão do direito penal brasileiro, que surgiu a Lei 9.613/1988.

O diploma legal possui tripla natureza, contendo dispositivos de natureza penal material, processual penal e administrativa. A natureza penal pode ser tida como elemento central da Lei, uma vez que tipifica especificamente conduta anteriormente combatida através de tipos penais tradicionais, como favorecimento e receptação, ampliando o alcance do *jus puniendi* através de um núcleo típico mais amplo e elementares próprias da prática de lavagem de dinheiro. Por sua vez, a natureza processual penal da Lei trata de medidas cautelares e mecanismos de persecução, produção de provas, e localização de bens, valendo mencionar aquele do § 5º do artigo 1º, que dispõe sobre a redução de pena daquele autor, coautor ou partícipe que colaborar espontaneamente com as autoridades, prestando esclarecimentos que conduzam à apuração das infrações penais, à identificação de demais autores, coautores e partícipes, ou à localização dos bens, direitos ou valores objeto do crime. Finalmente, a natureza administrativa, foco deste trabalho, elenca pessoas sujeitas a mecanismos de controle — aquelas obrigadas a colaborar com a política criminal de combate à lavagem de dinheiro —, determina sanções administrativas e cria a Unidade de Inteligência Financeira brasileira, o Conselho de Controle de Atividade Financeira (COAF), tópicos estes que serão aprofundados em seguida.

O Brasil, como membro pleno do Grupo de Ação Financeira (FATF-GAFI), órgão intergovernamental de prevenção à lavagem de dinheiro, no cumprimento da 29ª recomendação do grupo, possui constituído, na forma das Leis 9.613/1998 e 13.974/2020, o COAF. A Unidade de Inteligência Financeira brasileira possui jurisdição nacional e autonomia operacional para realização de atividades de inteligência financeira, as quais consistem em realizar a análise de informações a fim de identificar suspeitas e ocorrências de lavagem de dinheiro, exame este que gera

Relatórios de Inteligência Financeira, os quais são encaminhados às autoridades competentes para abertura de investigação e ações penais. O COAF também recebe, por meio de mecanismos de cooperação, informações sobre investigações em curso as quais são confrontadas com dados já existentes na unidade.

Adotando um modelo de autorregulação, a Lei de lavagem de dinheiro brasileira, em seu artigo 9º, elenca pessoas físicas e jurídicas sujeitas à mecanismos de controle que, pela sensibilidade de suas atividades em relação à prática de mascaramento de capitais, tornaram-se obrigadas a colaborar com o Estado no combate desta criminalidade.

Dentre um extenso rol de setores e pessoas sujeitas, referido artigo 9º, em seu inciso I a III, dispõe que são sujeitas aos mecanismos de controles as pessoas que tenham como atividade a captação, intermediação e aplicação de recursos financeiros de terceiros, em moeda nacional ou estrangeira, bem como a compra e venda de moeda estrangeira ou ouro como ativo financeiro ou instrumento cambial e a custódia, emissão, distribuição, liquidação, negociação, intermediação ou administração de títulos ou valores mobiliários. Notadamente, as CCTVMs, objeto deste trabalho, caracterizam-se como pessoas sujeitas aos mecanismos de controle.

Uma vez que a natureza do crime de lavagem de dinheiro é o afastamento dos recursos de sua origem ilícita, identificar precisamente seus portadores iniciais e seu destino constitui o método basilar de combate ao delito.

O brocado em inglês *Follow the Money* sugere que a criminalidade organizada pode ser perseguida através da análise de movimentações financeiras e é neste sentido que o artigo 10º, inciso I, da Lei em tela, define que as pessoas sujeitas “identificarão seus clientes e manterão cadastro atualizado, nos termos de instruções emanadas das autoridades competentes”. Assim, as CCTVMs são obrigadas a garantir que os clientes são quem realmente dizem ser, evitando a abertura de contas

falsas, para interpostas pessoas (os “laranjas”) e, também, angariando informações suficientes para realização da avaliação de risco de seus clientes.

Além da identificação de clientes, a manutenção de registros de transação, nos termos de instruções regulatórias (artigo 10, inciso II), também constitui obrigação, a qual visa dificultar o sucesso da fase de ocultação da lavagem de dinheiro, de modo que seja possível desemaranhar complexas transações financeiras, desvendando assim, por meio dos referidos registros, a origem ilícita dos recursos.

A figura da autorregulação se faz presente por excelência no inciso III do mesmo artigo 10, que dispõe da obrigação das pessoas sujeitas a “adotar políticas, procedimentos e controles internos, compatíveis com seu porte e volume de operações, que lhes permitam atender ao disposto neste artigo e no art. 11, na forma disciplinada pelos órgãos competentes”.

Por fim, as pessoas sujeitas são também obrigadas à manutenção de registro perante o órgão regulador e a atender requisitos do COAF.

Além da identificação de clientes e manutenção de registros, as pessoas sujeitas aos mecanismos de controle devem, nos termos do artigo 11 da Lei, monitorar e avaliar este conjunto de informações a fim de comunicar ao COAF a ocorrência de situações que “possam constituir-se em sérios indícios” de lavagem de dinheiro ou com o delito estarem relacionadas. No caso das CCTVMs, os padrões requeridos para os procedimentos de comunicação são delineados em regulações específicas do BACEN e da CVM, razão pela qual se deixará para tratar deste assunto com mais profundidade nos tópicos a respeito das referidas normas.

O descumprimento das obrigações supracitadas é passível de sanção administrativa. A primeira sanção aplicável é a advertência, que é combinada a irregularidades relacionadas às obrigações de identificação de clientes e manutenção de registros. A pena de multa pecuniária — cujo limite será o dobro do valor da operação; o dobro do lucro real obtido; o valor que presumivelmente seria obtido pela

realização da operação ou R\$ 20.000.000,00 (vinte milhões de reais) — será aplicada quando i) deixarem as pessoas obrigadas de sanar irregularidades apontadas em sede de advertência; ii) pelo descumprimento das obrigações de identificação de clientes, manutenção de registros, implementação de políticas e controles internos, falha em satisfazer as requisições do COAF e iii) deixarem de fazer a comunicação de operações financeiras a que se refere o art. 11 da Lei. A pena de inabilitação temporária, pelo prazo de até dez anos, para o exercício do cargo de administrador de pessoas jurídicas que constem no rol de pessoas sujeitas será aplicada quando forem verificadas infrações graves quanto ao cumprimento das obrigações ou quando ocorrer reincidência específica em atos anteriormente punidos com multa. Por fim, a cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento, será aplicada quando da reincidência específica de infrações anteriormente punidas com inabilitação temporária.

4 A CIRCULAR 3.978/2020 DO BACEN

Dentro da estrutura do Sistema Financeiro Nacional, o BACEN figura como órgão supervisor das instituições financeiras, e sua Circular 3.978, de 23 de janeiro de 2020 dispõe sobre a política, os procedimentos e os controles internos a serem adotados para a prevenção da utilização do sistema financeiro como meio dos crimes de “lavagem” ou ocultação de bens, direitos e valores. A norma prevê diretrizes sob as quais as instituições autorizadas pelo BACEN a funcionar devem: a) implementar e manter política de prevenção à lavagem de dinheiro e financiamento do terrorismo; b) organizar a governança da política e seus controles; c) realizar avaliação interna de risco; d) realizar procedimentos destinados a conhecer os clientes; d) realizar registro de operações; e) tratar da ocorrência de operações suspeitas; f) proceder a comunicação de operações suspeitas ao COAF g) realizar procedimentos destinados

a conhecer empregados, parceiros e fornecedores; h) implementar mecanismos de acompanhamento e controle dos procedimentos e i) realizar avaliação de efetividade.

Notadamente, a característica marcante e, também, maior avanço da referida norma, foi a adoção da Abordagem Baseada em Risco, em uma clara lógica de autorregulação. O artigo 2º, § único, por exemplo, dispõe que a Política de PLD das instituições deve ser compatível com os perfis de risco a) dos clientes; b) da instituição; c) das operações, transações, produtos e serviços; e d) dos funcionários, parceiros e prestadores de serviços terceirizados. Portanto, não há uma regra geral para a elaboração da política e execução de controles, devendo as instituições fazer como mais eficazmente e eficientemente se der em suas respectivas realidades.

Pretendendo que as instituições realizem seus controles de forma eficiente, tendo em mente que os recursos são escassos, cria-se um ambiente regulatório em que elas estão autorizadas a despende de maiores esforços para situações de maior risco, e adotar controles simplificados para as de menor risco. Assim, em simplificado exemplo, uma instituição que oferece apenas produtos conservadores, mas possui boa parte de seus clientes em regiões fronteiriças notadamente mais suscetíveis a abrigarem agentes criminosos, deveria dispor de controles mais robustos de KYC ao passo que permite-se adotar controles simples para análise de transações.

Um segundo elemento que merece destaque na referida norma são as diretrizes que determinam o tratamento de operações suspeitas. A norma anterior (Circular 3.461/2009) dispunha apenas a respeito da necessidade de comunicação de operações suspeitas, enquanto a Circular 3.978/2020 determina a condução de procedimentos de monitoramento, seleção e análise de operações suspeitas, os quais levam a uma decisão fundamentada de comunicação ou de não comunicação. Segundo Sólon Cícero Linhares, tais diretrizes solucionam a existência de um dilema de agência quando da comunicação de operações suspeitas a respeito de, por

exemplo, um cliente muito lucrativo⁷. Em suma, as diretrizes de procedimento determinadas pela atual norma — a qual evidentemente transmite a ideia de utilização de sistemas automatizados para realização do monitoramento e seleção⁸ —, determinam a execução de procedimentos mais refinados no tratamento de operações suspeitas, especialmente pela necessidade de fundamentação das decisões. Por exemplo, quando a seleção de uma operação pelos parâmetros pré-definidos (baseados em risco) resultar em eventual análise como falso positivo, mesmo assim deverá ser realizada uma decisão de não comunicação, nos termos do artigo 43 § 2º, devendo esta ser formalizada em dossiê e mantido à disposição do BACEN.

5 A RESOLUÇÃO 50/2021 DA CVM

A CVM, na figura de órgão supervisor do Mercado de Capitais, portanto da atividade das CCTVMs, possui norma específica que dispõe sobre PLD.

Cumprе ressaltar que, conforme jurisprudência consolidada (vide PAS 01/2011, que apurou a conduta de administradores do Banco Panamericano), as competências da CVM e do BACEN são originárias e concorrentes. O entendimento é de que são distintas as searas de supervisão da CVM — como órgão responsável pela proteção ao investidor e regular funcionamento do mercado de valores mobiliários — e do BACEN — como órgão que resguarda a higidez do sistema

⁷ LINHARES, Sólón Cícero. Manual de Prevenção à lavagem de dinheiro. São Paulo: Tirant lo Blanch, 2021, p. 57.

⁸ Evidente pela redação do artigo 40, § 1º e 2º: “Art. 40 [...] § 1º As instituições devem manter documentação detalhada dos parâmetros, variáveis, regras e cenários utilizados no monitoramento e seleção de operações e situações que possam indicar suspeitas de lavagem de dinheiro e de financiamento do terrorismo. § 2º Os sistemas e os procedimentos utilizados no monitoramento e na seleção de operações e situações suspeitas devem ser passíveis de verificação quanto à sua adequação e efetividade.”

financeiro —, atraindo ambas as competências regulatórias e sancionatórias a atividade das CCTVMs.

Em seu conteúdo, a norma da CVM é bastante similar à já examinada Circular do BACEN, tratando em seus capítulos de: a) implementação de Política de PLD/FTP, realização de Avaliação Interna de Risco e implementação de procedimentos e controles internos visando o cumprimento da norma; b) determinação da indicação de diretor estatutário como responsável pelo cumprimento da resolução, bem como suas responsabilidades; c) monitoramento, análise e comunicação de operações e situações suspeitas; d) registro de operações e manutenção de arquivos; e) cumprimento de sanções impostas por resoluções do CSNU.

Em nota explicativa à Resolução 50⁹, a CVM expõe ser característica de destaque da norma a inserção da Abordagem Baseada em Risco como principal ferramenta de governança de PLD, deixando clara a afinidade do órgão pela via da autorregulação.

O documento também expõe a preocupação do órgão regulador com a comunicação organizacional e atuação de executivos. Lê-se que o diretor estatutário, deve dispor de todas as informações necessárias para o cumprimento de sua função de garantir o *Compliance* à norma, não podendo em situação alguma as instituições supervisionadas alegarem qualquer restrição de acesso a qualquer dado corporativo ao referido diretor. Por sua vez, ao mencionar a Alta Administração, é exposto o dever destes órgãos de garantir a independência do diretor estatutário e da implantação da política e controles, prover o departamento de *Compliance* de recursos suficientes para execução de suas atividades e fazer-se ciente da exposição a riscos de PLD.

Finalmente, a nota explicativa demonstra a importância dada pelo órgão regulador aos procedimentos de KYC, tidos como “um dos principais pilares da PLD”

⁹ Disponível em https://conteudo.cvm.gov.br/legislacao/notas-explicativas/nota_resol050.html. Acesso em 11 de outubro de 2024.

notando-se, inclusive, ser a norma da CVM mais exigente se comparada com a do BACEN, requerendo a coleta de um rol maior de dados de clientes.

6 COMPLIANCE COMO GESTÃO DE RISCO LEGAL

O risco é algo inerente aos fatos da vida, relacionando-se à possibilidade de perdas, mas também ao aproveitamento de oportunidades. O sociólogo alemão Ulrich Beck traduz a atual sociedade como sendo uma “sociedade do risco”, na qual as maiores ameaças da vida em sociedade surgem não da natureza alheia ao ser humano — como a erupção de um vulcão —, mas do que chamou de modernização reflexiva: a criação do homem, no cenário de elevado desenvolvimento tecnológico, acaba por se tornar gradativamente um foco maior de risco do que a natureza¹⁰. Alamiro Velludo Salvador Netto, exemplifica constatando que “o avanço tecnológico permitiu, por exemplo, o melhor e mais eficiente escoamento urbano de águas pluviais, enquanto esse mesmo avanço tecnológico, paradoxalmente, tornou todos suscetíveis aos simples humores do mercado”¹¹.

Ao tratar do risco na atividade corporativa, Marcos Assi define risco como “uma ou mais condições de variáveis com potencial necessário de causar dano ao patrimônio da empresa”, sendo a competência do profissional de gestão de risco a “seleção de quais riscos a empresa deve tratar”¹². Especificamente a respeito de

¹⁰ BECK, Ulrich. Sociedade de risco: rumo a uma outra modernidade. Trad. Sebastião Nascimento. 2. ed. São Paulo: Editora 34, 2011.

¹¹ NETTO, Alamiro. 1. Política Criminal, Pessoa Jurídica e Direito Penal In: NETTO, Alamiro. Responsabilidade Penal da Pessoa Jurídica - Ed. 2023. São Paulo (SP): Editora Revista dos Tribunais. 2023. Disponível em: <https://www.jusbrasil.com.br/doutrina/responsabilidade-penal-da-pessoa-juridica-ed-2023/2085628301>. Acesso em: 5 de dezembro de 2025.

¹² ASSI, Marcos. Gestão de riscos com controles internos: Certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2019, E-book Kindle, local 95.

Compliance, o mesmo autor citado anteriormente define a atividade de *Compliance* como a gestão dos riscos legais da empresa¹³.

Em linhas gerais, a gestão de risco se dá através da identificação dos riscos — mediante a noção de que toda atividade gera algum risco —, da análise destes riscos e da implementação de controles mitigadores, sendo importante frisar que sempre restará um risco residual, que deve também ser levado em consideração e monitorado¹⁴.

As normas de PLD são uma grande fonte geradora de risco legal para as CCTVMs, tanto devido à sua grande complexidade, que pode gerar inúmeras situações de possível desconformidade, quanto pelo elevado impacto em razão das possíveis graves penalidades, entre elevadas multas e ameaça de perda de licença, além do impacto reputacional.

Dentre os controles a serem implementados para PLD, os controles de KYC constituem grande desafio operacional dada as inúmeras vezes que serão executados e visto que serão aplicados a todo e qualquer cliente que a Instituição venha a receber, o que inerentemente eleva a probabilidade de falha. Por esta razão o KYC foi escolhido como foco da ilustração de implementação realizada neste trabalho.

7 IMPLEMENTAÇÃO DE CONTROLES DE KYC EM UMA CCTVM UTILIZANDO O COSO INTERNAL CONTROL INTEGRATED FRAMEWORK

¹³ ASSI, Marcos. *Compliance: como implementar*. São Paulo: Saint Paul, 2018, p. 29.

¹⁴ AVALOS, José Miguel Aguilera. *Auditoria Interna e Gestão de Riscos*. São Paulo: Saraiva, 2009, p. 35.

O COSO (*Committee of Sponsoring Organizations*) é uma organização privada criada no ano de 1985, nos EUA, com o objetivo de estudar as causas da ocorrência de fraudes em relatórios financeiros e contábeis, patrocinada por cinco das principais associações de classe de profissionais ligados à área financeira e de auditoria dos EUA¹⁵, sendo a sua metodologia “*Internal Control Integrated Framework*”, a mais aceita entre as companhias abertas norte-americanas, tendo também sido a estrutura recomendada pelo PCAOB (*Public Company Accounting Oversight Board*) e pela SEC (*Securities Commission*). No Brasil, é a metodologia recomendada nos materiais do PQO (Programa de Qualificação Operacional) da B3, que certifica profissionais das áreas de Riscos e *Compliance*, e é utilizada pela própria bolsa de valores na gestão de seus riscos corporativos¹⁶ e, evidentemente serviu de base para a norma de controles internos do BACEN, a Resolução CMN nº 4.968/2021.

Controle interno é definido pelo COSO como “processo conduzido pela estrutura de governança, administração e outros profissionais da entidade para propiciar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade” (COSO, 2013).

Vale destacar que o COSO é perfeitamente aplicável para a implementação de controles de *Compliance*, tendo a própria organização, inclusive, publicado o

¹⁵ O COSO é patrocinado pelas seguintes instituições: AICPA (*American Institute of Certified Public Accounts*); AAA (*American Accounting Association*); FEI (*Financial Executives International*) e IIA (*The Institute of Internal Auditors*) e IMA (*Institute of Management Accountants*).

¹⁶ Princípios para infraestruturas o mercado financeiro divulgação de informações da B3 março 2020, p. 46. Disponível em: https://www.b3.com.br/data/files/C5/32/B9/07/898A2710547B5127AC094EA8/B3_PFMI_DISCLOSURE_-_Portugues_-_Atualizacao_-_Consolidado_-_PUBLICADO_-_202006.pdf. Acesso em 11 de outubro de 2024.

documento de título "*Compliance Risk Management: Applying the COSO ERM Framework*", que trata dessa intersecção.

Nos tópicos seguintes serão brevemente expostos os conceitos dos cinco componentes de um sistema de controles internos para em seguida, ilustrar-se como podem ser aplicados para a construção de controles de KYC, a fim de mitigar o risco de uma CCTVM encontrar-se em desconformidade, neste quesito, com a Resolução CVM 50 e a Circular 3.978 do BACEN.

7.1 AMBIENTE DE CONTROLE

O ambiente de controle é um conjunto de normas, processos e estruturas que fornece a base para a condução do controle interno por toda a organização, por meio de elementos como criação de cultura de integridade, disciplina e delegação de autoridade. Possui como principal fator a alta gestão, podendo ser ilustrado pelo brocado corporativo "*tone from the top*" ou "o exemplo vem de cima".

Em geral, as instituições financeiras constroem uma área de cadastro, responsável pela execução de controles de KYC, como a condução de atividades para garantir a completude e validade dos dados cadastrais de um novo cliente, isto, contudo, não esgota os controles necessários nas atividades da organização. Uma vez que o que move uma CCTVM é a atividade da clientela, em maior ou menor proporção, de forma mais ou menos direta, quase todas as áreas deste tipo de instituição estarão envolvidas com os clientes e, portanto, podem ter em suas atividades implementados controles de KYC. Neste sentido, os artigos 17, VII, b), da Resolução CVM 50 e 18, § 4º, da Circular 3.978 do BACEN, determinam a necessidade de acompanhamento da evolução do relacionamento com o cliente, atividade holística que só é possível mediante o trabalho conjunto de diversas áreas. A exemplo, o relacionamento com o cliente envolverá a área de cadastro quando da

verificação de seus dados, envolverá a área comercial quando do oferecimento e contratação de produtos, envolverá a área de *Compliance* quando do monitoramento de operações e envolverá a mesa de operações quando da execução de ordens. Em última todas as áreas estarão envolvidas quando da identificação de atividade suspeita passível de reporte ao COAF, pois estas podem ser percebidas em diversos momentos, por diferentes pessoas e devem ser reportadas no decorrer de todo ciclo do relacionamento com cliente.

O exposto, portanto, gera a necessidade de um reforçado ambiente de controle em toda a CCTVM para que os controles de KYC sejam adequadamente executados em todas as áreas.

7.2 AVALIAÇÃO DE RISCOS

A avaliação de riscos é um processo dinâmico e iterativo para identificar e avaliar os riscos existentes quando da persecução dos objetivos da organização.

Este componente é *conditio sine qua non* à implementação de controles adequados. Em especial, no caso das CCTVMs, as normas regulatórias dispõem justamente de uma lógica de abordagem baseada em risco, na qual as instituições devem implementar seus controles baseados na sua própria e específica exposição a riscos de lavagem.

Os controles devem ser planejados, implementados e executados baseando-se na realidade de exposição ao risco da instituição, desde o perfil de carteira de clientes até a disposição de recursos. Neste passo, deve-se avaliar os riscos de descumprimento com as exigências de KYC: Uma instituição com uma quantidade de clientes elevada deverá preocupar-se com a possibilidade de incapacidade na coleta e armazenamento de uma grande massa de dados cadastrais, ao passo que uma corretora focada em clientes corporativos deverá preocupar-se com a inabilidade de

identificar os beneficiários finais ou acompanhar o relacionamento com os clientes em razão da eventual complexidade das estruturas societárias ou das operações realizadas.

7.3 ATIVIDADES DE CONTROLE

Atividades de controle são ações estabelecidas por meio de políticas e procedimentos que auxiliam no cumprimento das diretrizes definidas pela alta administração para mitigar os riscos gerados pela busca aos objetivos da organização.

Realizada a análise dos riscos, implementam-se os controles, focando maiores esforços nas situações de maior risco e permitindo poupar-se nas situações de menor risco. Seguindo o exemplo dado no tópico anterior, a corretora possuidora de uma quantidade elevada de clientes optará pela contratação de mais profissionais na área de cadastro, investimento em um sistema mais robusto de validação de dados e implementação de rotinas com maior periodicidade de revisão da completude das informações de KYC. Em sentido contrário, a corretora focada em clientes corporativos, imaginando que não possuirá uma carteira e rotatividade tão grande de clientes, em comparação com a primeira, poderá se preocupar em menor medida com o processamento de dados cadastrais em quantidade, mas deverá direcionar seus esforços em identificar beneficiários finais, em compreender cadeias societárias e operações complexas, relacionando-as com o cliente para, entre outras situações, decidir se há ou não de indício de lavagem.

7.4 INFORMAÇÃO E COMUNICAÇÃO

As instituições obtêm, geram ou utilizam importantes informações, advindas de fontes internas ou externas, as quais devem possuir qualidade a fim de apoiar a

execução dos controles internos, sendo a comunicação o meio pelo qual tais informações são transmitidas.

Não só para a execução de controles de KYC, a comunicação é elemento essencial ao sucesso de qualquer empresa. Uma comunicação efetiva será necessária entre a área de cadastro e o agente comercial que captou determinado cliente caso esclarecimentos sejam necessários para a completude de um cadastro, assim como eventuais alterações nas normas de KYC deverão ser prontamente comunicadas às áreas afetadas. Notadamente, aquele agente comercial que tem contato próximo com o cliente terá valiosas informações quando da análise de uma operação suspeita.

Conforme examinado no tópico específico, a CVM determina que as CCTVMs não poderão alegar qualquer restrição de acesso a qualquer dado corporativo ao diretor responsável pelos controles de PLD, portanto faz-se mandatário um efetivo sistema de comunicação entre as áreas da instituição para que se executem adequadamente os controles e se mitigue o risco de desconformidade com as normas de KYC.

7.5 ATIVIDADES DE MONITORAMENTO

As organizações utilizarão avaliações contínuas para se certificar da presença e do adequado funcionamento dos controles internos.

O monitoramento dos controles é a atividade própria da área de *Compliance*, como supervisora da efetividade dos controles. Os artigos 6º da Resolução CVM 50 e 62 da Circular 3.978 do BACEN, determinam a produção de relatórios que tratam do monitoramento de efetividade dos controles de PLD, constituindo, inclusive, risco de conformidade o mero descumprimento com os prazos determinados para tais relatórios.

Notadamente, o monitoramento possui o objetivo de identificação de falhas e proposição de melhoras, então, a corretora que identificar falhas no processamento de dados incluirá em seu plano de ação, por exemplo, a implementação de sistema mais robusto de cadastro, enquanto uma instituição na qual houve uma evasão à seleção de operações suspeitas em razão da complexidade das operações deverá rever seus parâmetros de alerta.

8 CONCLUSÃO

O contexto mundial de mudanças e complexidade das atividades empresariais demanda uma resposta contra os fatores criminal advindos disto. As leis penais, como a Lei de lavagem de dinheiro, fixam a incidência da resposta mais incisiva do Estado para coibir tais práticas não sendo, contudo, suficientes para lidar totalmente com a questão. Embora a expansão da Lei penal para tratar de questões de crimes empresariais e econômicos deva ser entendida como legítima, é crucial que esta incidência se dê em *ultima ratio*, sob pena de violação de conquistas democráticas. Diante disto, a Lei penal serve também como referência para demais medidas extrapenais que contribuem para a resolução das questões, sendo a principal delas, no tema aqui discutido, a colaboração com entes privados em medidas de prevenção.

A criação de obrigações de colaboração de entes privados na prevenção à lavagem de dinheiro é medida justa, necessária e eficiente. Justa, pois significa a contribuição dos agentes econômicos na resolução de uma externalidade negativa criada pelos produtos com os quais lucram. É do mesmo modo necessária, pois o Estado não dispõe sozinho de todos os aparatos para lidar com o problema, seja por questões materiais ou de legitimidade. Por fim, adequada, uma vez que não há ninguém melhor para colaborar com a resolução da problemática do que aqueles que tem todo o *Know-how* e estão próximos dos riscos.

Sendo legítimas as normas regulatórias a respeito de PLD, elas geram também elevado risco legal para as CCTVMs, diante das sanções aplicáveis em caso de não cumprimento, razão pela qual é necessária a construção de tal programa por meio de uma metodologia adequada.

Conforme demonstrou-se, a metodologia do COSO se mostra adequada para a gestão do risco de conformidade para com as normas da CVM e BACEN, em razão de equilibrar robustez e prestígio técnico com a maleabilidade que se adequa às mais diversas realidades empresariais.

REFERÊNCIAS

ASSI, Marcos. Compliance: como implementar. São Paulo: Saint Paul, 2018.

ASSI, Marcos. Gestão de riscos com controles internos: Certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2019. E-book Kindle.

AVALOS, José Miguel Aguilera. Auditoria Interna e Gestão de Riscos. São Paulo: Saraiva, 2009.

BADARÓ, Gustavo Henrique, BOTTINI, Pierpaolo Cruz. Lavagem de Dinheiro. Aspectos Penas e Processuais Penais. São Paulo: Thomson Reuters, 2019.

BECK, Ulrich. Sociedade de risco: rumo a uma outra modernidade. Trad. Sebastião Nascimento. 2. ed. São Paulo: Editora 34, 2011.

CARVALHO, André Castro Carvalho (org.). Manual de Compliance. Rio de Janeiro: Forense, 2019.

COSO, Compliance Risk Management: Applying the COSO ERM Framework, 2020. Disponível em: <https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf>. Acesso em 22 de janeiro de 2025.

COSO, Executive Summary, 2013. Disponível em : <https://auditoria.mpu.mp.br/pgmq/COSOIIICIF_2013_Sumario_Executivo.pdf>. Acesso em 22 de janeiro de 2025.

PINHEIRO, Juliano Lima. OLIVEIRA, Virgínia Izabel (org.). Gestão de Riscos no mercado financeiro. São Paulo: Saraiva, 2018.

HAYASHI, Felipe Eduardo Hideo. Corrupção: Combate Transnacional, Compliance e Investigação Criminal. Rio de Janeiro: Lumen Iuris, 2015.

LINHARES, Sólton Cícero. Manual de Prevenção à lavagem de dinheiro. São Paulo: Tirant lo Blanch, 2021.

NETTO, Alamiro. 1. Política Criminal, Pessoa Jurídica e Direito Penal In: NETTO, Alamiro. Responsabilidade Penal da Pessoa Jurídica - Ed. 2023. São Paulo (SP): Editora Revista dos Tribunais. 2023. Disponível em: <https://www.jusbrasil.com.br/doutrina/responsabilidade-penal-da-pessoa-juridica-ed-2023/2085628301>. Acesso em: 5 de dezembro de 2025.