ManagementSolutions
Making things happen

Crimes financeiros: tendências e desafios na era digital

P&D

www.managementsolutions.com

Design e diagramação
Departamento de Marketing e Comunicação
Management Solutions - Espanha

Fotograflas

Arquivo fotográfico da Management Solutions
iStock

Índice

Introdução

"Os crimes levam o castigo às costas"
Miguel de Cervantes[1]

O crime financeiro é um conceito geral que compreende um conjunto de atividades ilícitas. Embora existam diferenças entre jurisdições, em termos gerais, o crime financeiro inclui atividades como lavagem de dinheiro (ou seja, transformar em legal o dinheiro que vem de diferentes atividades ilegais), financiamento do terrorismo, violação de sanções econômicas, suborno e corrupção, fraude e abuso de mercado[2].

O crime financeiro e a lavagem de dinheiro (LD) representam uma grande ameaça que o setor financeiro enfrenta em suas estruturas de identificação, gestão e controle de riscos. Por exemplo, a quantidade de dinheiro lavado globalmente em um ano é estimada entre 2% e 5% do PIB global, ou entre $800 bilhões e $2 trilhões em dólares americanos atuais[3]. Entretanto, menos de 1% dele é apreendido ou congelado pelas agências de aplicação da lei[4].

Nos últimos anos, instituições financeiras de diferentes geografias investiram bilhões de dólares na melhoria de seus sistemas, pessoas e processos para poder enfrentar a crescente ameaça que o crime financeiro representa para sua estabilidade e sua reputação. De acordo com alguns relatórios do setor, o investimento anual das instituições financeiras em todo o mundo para cumprimento das normativas sobre o crime financeiro é estimado em mais de 200 bilhões de dólares[5].

Vários fatores tornam o combate ao crime financeiro cada vez mais desafiador, inclusive:

- Uma economia cada vez mais globalizada e um setor financeiro interconectado correspondente, dificulta a rastreabilidade completa do dinheiro.

- Abordagem local de supervisão. Historicamente, a abordagem ao crime financeiro, e em particular as atividades de PLD, tem sido conduzida por legisladores e supervisores locais, autoridades de aplicação da lei específicas de cada país e agências de inteligência financeira. Apesar da existência de órgãos intergovernamentais, como a Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FAFT)[6], não há plataformas operacionais, nem mecanismos regulatórios e de supervisão para colaboração efetiva e compartilhamento de informações.

- A progressiva sofisticação das estratégias de lavagem de dinheiro, envolvendo outros tipos de crimes como fraude ou crimes cibernéticos (por exemplo, roubo de identidade)[7] .

- A evolução da indústria de pagamentos em direção a mecanismos de pagamentos digitais mais fáceis, mais rápidos e mais flexíveis.

- A irrupção das criptomoedas e sua capacidade de evitar a rastreabilidade das fontes de recursos[8].

- Os avanços tecnológicos implementados como resultado da pandemia, que forçaram as instituições financeiras a reduzir as interações presenciais e substituí-las por processos digitais (incluindo o on-boarding remoto de novos clientes), mais suscetíveis ao crime digital que pode eventualmente levar ao crime financeiro.

Não obstante, as instituições financeiras contam com condições favoráveis que possibilitam a utilização de ferramentas mais robustas na luta eficaz contra o crime financeiro, identificando, monitorando, medindo e controlando estes tipos de atividades ilícitas, inclusive:

- Maior capacidade computacional para executar alertas e estratégias de identificação de riscos em tempo real envolvendo um conjunto muito mais completo de data points para identificar estratégias sofisticadas.

[1] Miguel de Cervantes Saavedra (1547-1616). Escritor espanhol. Autor da obra "O engenhoso fidalgo Dom Quixote de la Mancha".
[2] Financial Conduct Authority (2021).
[3] Escritório das Nações Unidas contra a Droga e o Crime (2011).
[4] Fórum Econômico Mundial.
[5] Lexis Nexis Risk Solutions (2021).
[6] Um grupo de ação intergovernamental que reúne mais de 200 países, e que atua como o grupo padrão global de lavagem de dinheiro e financiamento do terrorismo),
[7] Um exemplo paradigmático de dos criminosos cibernéticos Carbanak e Cobalt pode ser discutido: gangues de criminosos são capazes de (i) inserir um malware nas contas de trabalho dos funcionários dos bancos (através de técnicas de phishing padrão - ciberataque); (ii) usar credenciais para aumentar os saldos de certas contas (fraude); (iii) permitir que o dinheiro seja transferido além-fronteiras e/ou extraído através de caixas eletrônicos; e (iv) reinseri-lo no sistema usando técnicas clássicas de lavagem ecológica ou *greenwashing*. Ver o comunicado de imprensa da Europol https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
[8] Paesano, F. (2021).

- Modelagem matemática mais avançada, incluindo algoritmos de *machine learning* que podem ser executados mais rapidamente e são capazes de refinar as estratégias e melhorar a eficácia na detecção.

- Maior conscientização por parte dos diretivos e do Conselho de Administração sobre as implicações deste tipo de crimes, o que reflete em compromisso e investimento plurianuais. Ao mesmo tempo, maior visibilidade do custo total dos crimes financeiros (incluindo tanto os prejuízos diretos como os decorrentes da remediação e multas[9]), bem como a conscientização dos riscos que essas práticas acarretam, cada vez mais "conectados".

- Aumento da colaboração dentro da instituição, com a eliminação de silos e a colaboração entre departamentos (tecnologia, *compliance*, legal, fraude, prevenção à lavagem de dinheiro, etc.) para garantir que ocorra total compartilhamento de informações e transparência entre as equipes responsáveis por crimes financeiros.

- Desde os primeiros trabalhos da Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FAFT), e com o trabalho de outras organizações internacionais como o Escritório das Nações Unidas contra Drogas e Crime, há muito mais consciência sobre a importância da cooperação internacional.

Prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT)

Tendo em vista a série de casos notórios que afetaram bancos globais sistemicamente importantes e respectivo escrutínio regulatório[10,11], uma das atividades de prevenção ao crime financeiro que tem atraído investimentos importantes nos últimos anos é a luta contra a lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT). Apesar dos importantes progressos realizados para reforço dessas capacidades, a prevenção dessas atividades ilícitas segue sendo uma das principais preocupações para as entidades financeiras.

Dada a natureza transfronteiriça da lavagem de dinheiro e do financiamento do terrorismo, uma das ações mais assertivas é a maior cooperação internacional entre países e regiões o que permite realizar ações mais sincronizadas.

Nessa linha, os reguladores e supervisores estão desempenhando um papel fundamental para incentivar e permitir tal colaboração global e apoiar de modo geral a prevenção desses crimes. Alguns dos exemplos de ação regulatória incluem:

a. Reforçar os mecanismos de supervisão para atravessar as jurisdições. Por exemplo, a 5ª Diretiva contra lavagem de dinheiro da UE[12] exige que a CE realize uma avaliação semestral dos riscos de LD/FT que poderiam impactar o mercado interno na região[13]. Os resultados de tais avaliações são informados aos responsáveis políticos regionais e locais.

[9] Lexis Nexis Risk Solutions (2021).
[10] Sanction Scanner (2021).
[11] Comissão Europeia (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0373
[12] Parlamento Europeu e o Conselho (2015).
[13] Ver, por exemplo, o Relatório de Avaliação de Risco Supranacional da Comissão Europeia e o Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a avaliação do risco de lavagem de dinheiro e financiamento do terrorismo que afeta o mercado interno e está relacionado a atividades transfronteiriças. COM (2019) 370. Ver também a Avaliação Nacional de Risco de Lavagem de Dinheiro e Financiamento do Terrorismo do Reino Unido para 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf

b. Incentivar uma maior cooperação entre legisladores e supervisores locais, autoridades de aplicação da lei e agências de inteligência financeira específicas do país[14]. Por exemplo, a 5ª Diretiva contra a lavagem de dinheiro da UE[15] exige uma avaliação, pela CE, da estrutura de cooperação entre as Unidades de Inteligência Financeira da União Europeia e com terceiros. A Diretriz inclui a possibilidade de estabelecer um mecanismo de coordenação e apoio. Nessa linha, recentemente a UE anunciou a criação de uma nova autoridade da UE[16] para melhorar a supervisão e cooperação de PLD/FT entre as Unidades de Inteligência Financeira locais. A nova autoridade europeia contra a lavagem de dinheiro, AMLA[17] atuará como uma autoridade central e coordenará as autoridades nacionais para assegurar, entre outras coisas, que o setor privado de cada país aplique adequadamente as regras da UE. Como continuação desse esforço, a EBA publicou recentemente suas "Diretrizes sobre cooperação e troca de informações entre supervisores prudenciais, supervisores de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e unidades de inteligência financeira sob a Diretiva 2013/36/UE"[18].

c. Prosseguir com a colaboração entre a supervisão prudencial e a não prudencial[19].

d. Para riscos emergentes ou áreas de debilidade identificadas como parte de seu processo de supervisão, os reguladores em todo o mundo estão sendo muito ativos em termos de emissão de nova regulamentação. Uma das áreas de evolução mais rápida é a das das criptomoedas[20].

e. Incentivar o investimento em dados, modelagem avançada e IA incluindo análise externa avançada, e análise gráfica para a modelagem de redes e relações de ordem múltipla[21].

Neste contexto, o objetivo deste *white paper* é duplo:

- Definir o âmbito de crimes financeiros e analisar o contexto regulatório.
- Desenvolver um foco especial nas tendências e desafios em PLD/FT, incluindo a resposta das instituições financeiras para melhorar os *frameworks* de gestão e controle de riscos, e estabelecer algumas relações entre PLD/FT e outros riscos que compreendem o conceito de crime financeiro.

O documento está estruturado da seguinte forma: após um resumo executivo, a seção 2 contém uma visão abrangente do conceito e do cenário regulatório sobre crimes financeiros. A seção 3 cobre as principais tendências e desafios em PLD/FT, incluindo o *framework* e a governança, o desenho organizacional, as necessidades de dados, os processos empresariais e a infraestrutura tecnológica. E, por último, a seção 4 contém um foco específico nas capacidades avançadas de modelagem matemática e tendências usadas com o objetivo de melhorar a eficiência e a eficácia na detecção.

[14] Autoridade Bancária Europeia (2021).
[15] Parlamento Europeu e o Conselho (2015).
[16] Parlamento Europeu (2021).
[17] Não confundir com a Lei contra Lavagem de Dinheiro dos EUA (2020)
[18] Autoridade Bancária Europeia (2021).
[19] Mersch, Y. (2019). Anti-lavagem de dinheiro e combate ao financiamento do terrorismo - iniciativas recentes e o papel do BCE.
[20] Autoridade Bancária Europeia. (2021).
[21] Autoridade de Conduta Financeira (2022). Sandbox regulatório.

Resumo executivo

"O capital não é um mal em si mesmo, o mal reside em seu mau uso"
Mahatma Gandhi[22]

1. ***Definição.*** Crime Financeiro é um termo amplo que se refere a um conjunto de riscos não prudenciais que as organizações do setor financeiro enfrentam como parte de suas atividades de originação de negócios. Entre outros, o crime financeiro inclui lavagem de dinheiro proveniente de diferentes atividades ilegais (incluindo tráfico de drogas, armas ou seres humanos, escravidão, etc.), financiamento ao terrorismo, violação de sanções econômicas, suborno e corrupção, fraude e abuso de mercado. Recentemente, o risco cibernético e o crime digital também têm sido incluídos nesta categoria.

2. ***Foco.*** Embora todos esses subtipos de riscos tenham recebido muita atenção e investimento nos últimos anos, esta análise será focada em três subtipos de risco que tendem a ser tratados sob estruturas similares por organizações: lavagem de dinheiro, financiamento do terrorismo e sanções econômicas. Seguindo a convenção padrão da indústria e regulação, este documento se refere a ele genericamente como PLD/ FT (Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo). A razão para focar em PLD/FT, além de permitir uma análise mais profunda, também responde ao crescente escrutínio regulatório e de supervisão e à natureza evolutiva dos riscos (por exemplo, duas diretrizes PLD na UE em menos de 5 anos), e o correspondente aumento do investimento e importância que as instituições financeiras estão dando às seus *frameworks* de PLD/FT (ligados aos grandes danos à reputação e às multas econômicas de derivadas das deficiências em seu modelo de controle).

3. ***Desafios.*** As instituições financeiras enfrentam um ambiente desafiador quando se trata de PLD/FT. A economia global torna o rastreamento dos movimentos de dinheiro cada vez mais difícil. Isto se torna mais desafiador devido à irrupção de criptomoedas e à proliferação de multidões de tecnologias de pagamento. Além disso, abordagens locais à regulamentação e legislação, com capacidade limitada de compartilhar informações e inteligência além das fronteiras, permitiram que organizações criminosas internacionais encontrassem pontos fracos no sistema. Essas organizações criminosas desenvolvem continuamente suas estratégias e constroem esquemas que envolvem ciberataques com estratégias de fraude e lavagem de dinheiro, que as instituições financeiras que ainda operam em silos têm dificuldade de enfrentar. Além disso, a pandemia da Covid 19 e a necessidade de usar canais on-line e reduzir o contato presencial tornou os processos de Know Your Customer mais exigentes. As instituições financeiras precisam enfrentar esses desafios após um ambiente sustentado de baixas taxas de juros e forte pressão de custos.

4. ***Condições favoráveis.*** Apesar do exposto acima, existem condições favoráveis que as instituições financeiras estão utilizando para enfrentar esses desafios, incluindo o uso de tecnologia e dados. A automação avançada, o BPM *(Business Process Management)* e a robótica são alguns dos mais destacados e ajudam a agilizar os processos de negócio. Por outro lado, também é relevante o uso de mecanismos de *machine learning* e IA, que ajudam a perfilar os clientes e sua transacionalidade de uma maneira mais eficaz, com um menor número de alertas improdutivos ou falsos positivos. As empresas também estão evoluindo significativamente sua estrutura de governança, com maior treinamento e conscientização (do Conselho de Administração e do Comitê Executivo às equipes operacionais) e mais colaboração entre diferentes subtipos de riscos (especialmente fraude).

5. ***Entorno regulatório.*** Os reguladores também estão evoluindo significativamente suas estruturas e recursos. Primeiro criando órgãos supranacionais de colaboração ou supervisão, construindo bancos de dados comuns, realizando avaliações de risco em toda a jurisdição e fortalecendo o diálogo e a colaboração entre supervisão prudencial e não-prudencial. Os reguladores também estão sendo muito ativos em termos de publicação de novas políticas e orientações sobre riscos emergentes que são identificados como pontos fracos em sua capacidade de supervisão, bem como encorajando as empresas a usar a inovação para enfrentar os riscos de LD/FT.

6. ***Reação das instituições financeiras.*** As instituições financeiras estão fortalecendo seu estruturas de PLD/FT, por meio de redesenho total ou intervenções específicas em sua *framework* e governança (incluindo melhorias em sua avaliação de risco, políticas e normas, sua divisão de

[22] Mohandas Karamchand Gandhi (1869-1948) foi o principal líder do Movimento de Independência da Índia contra o Raj britânico, praticando a desobediência civil não violenta, assim como um pacifista indiano, político, pensador e advogado hindu.

responsabilidades entre 1ª, 2ª e 3ª linhas de defesa, bem como sua colaboração entre os subtipos de risco). Eles também estão desenvolvendo sua organização, dando maior importância hierárquica ao responsável do crime financeiro, realizando análises estratégicas de necessidades futuras, construindo funções especializadas ou centralizando capacidades. Outras áreas de forte foco incluem seus programas de cultura comportamento, infraestrutura de dados e Informações gerenciais, bem como a racionalização e automação dos principais processos empresariais básicos de PLD/FT (KYC, monitoramento contínuo, gerenciamento de alertas e investigações, até o envolvimento com a aplicação da lei e Relatórios de Atividades Suspeitas). Por último, a infraestrutura tecnológica que sustenta a estrutura está sendo significativamente melhorada, assim como as capacidades matemáticas e a taxonomia dos modelos.

7. ***Avaliação de risco.*** Uma avaliação de risco robusta está no centro do *framework* de PLD/FT de uma organização. As boas práticas no setor envolvem a realização de uma avaliação de risco em diferentes níveis, começando com uma avaliação de risco supranacional e nacional realizada por entidades internacionais e autoridades reguladoras, que definem o cenário dos riscos específicos regionais/de jurisdição associados à PLD/FT. Essas contribuições informam uma avaliação de risco específica do negócio das instituições financeiras. Isto incluirá a identificação e avaliação dos riscos associados ao perfil de sua base de clientes, produtos e canais, sua escala, geografia etc. geografia etc. Por último, a avaliação de risco individual para cada relacionamento com o cliente utiliza estes dados como um input e complementa com o conhecimento específico do cliente, estrutura da empresa, proprietários beneficiários, fontes de fundos e riqueza.

8. ***Apetite ao risco.*** Tal avaliação de risco abrangente informa o apetite ao risco e os limites a serem usados no lançamento de novos produtos ou serviços, novas iniciativas empresariais (por exemplo, fusões, aquisições, novas linhas de negócio etc.). Além disso, também determina uma pontuação de "new to bank" que estabelece uma expectativa preliminar em relação ao comportamento do cliente (tipo de transações, canais a serem utilizados etc.), e o risco de LD/FT associado ao relacionamento. Isto está associado a um conjunto de padrões em torno da frequência de revisão periódica do relacionamento, e limiares para monitoramento de pagamentos e transacionalidade que acionam alertas quando ocorrem desvios do comportamento esperado. Além disso, as organizações mais avançadas têm um loop de feedback regular entre os incidentes identificados em seu monitoramento comportamental e a avaliação de risco do cliente, de modo que o perfil de risco e as ações mitigadoras associadas possam ser atualizados imediatamente.

9. ***Escopo da cobertura de risco.*** A avaliação de risco precisa cobrir não apenas os clientes, mas também os fornecedores terceirizados. As instituições financeiras dependem de uma série de terceiros para executar suas atividades cotidianas. Dependendo da natureza do negócio, esses terceiros também podem expor a organização ao crime financeiro, incluindo LD/FT, e a corrupção.

10. ***Políticas e normas.*** Em um ambiente tão altamente regulado, é essencial que as instituições financeiras escrevam e formalizem políticas, padrões e melhores práticas que permitam à organização agir sob formas comuns de trabalho e processo comercial. Este corpo de conhecimento é também uma ação mitigadora instrumental, pois permite o treinamento, a conscientização e a comunicação em toda a organização. Algumas das organizações mais avançadas possuem uma arquitetura de políticas em vigor, com hierarquias formalizadas de documentos que são interligados e referenciados (rastreabilidade vertical), publicados em formato digital que permite fácil navegação, com principais idéias, resumos etc. Eles também têm um modelo operacional que garante o monitoramento contínuo de novas regulamentações e riscos emergentes, lições aprendidas com incidentes LD/FT (internos ou de seus pares) e a atualização oportuna desse conjunto de documentos.

11. ***Framework de governança.*** Um dos aspectos que exigem mais investimento e forte liderança é a *framework* de governança e o modelo de três linhas de defesa (LoD) para a identificação, gestão, controle e supervisão do risco LD/FT. É uma das áreas onde reguladores e supervisores têm dedicado mais tempo e esforço. A tendência no setor inclui uma clara definição e formalização do papel de cada uma das linhas de defesa, assinada pelo Comitê Executivo / Conselho como parte do *framework* de prevenção do risco de LD/FT.

12. ***Linhas de defesa.*** Em um dos arquétipos mais difundidos, a primeira linha de defesa que inicia o negócio e é responsável pelo relacionamento com o cliente, também é responsável pela identificação, gerenciamento e controle do risco. Isto inclui a implantação de uma *framework* de controle de risco para assegurar que o perfil de risco seja mantido dentro do apetite, e que as operações diárias estejam de acordo tanto com as políticas internas quanto com os regulamentos externos. As empresas também reforçaram sua segunda linha de defesa, com a nomeação formal de um responsável de *compliance* de PLD/FT, ou equivalente. Em algumas jurisdições, esta função obrigatória precisa ser formalmente aprovada pelo regulador e espera-se que tenha experiência suficiente para desempenhar um desafio independente e efetivo ao negócio. Em torno desta função, existem fortes equipes de compliance e supervisão que prestam serviços de consultoria à empresa em tópicos básicos de PLD/FT, emitem orientações, políticas e normas para a identificação, monitoramento e controle adequados dos riscos, e supervisionam a adoção e incorporação destes na atividade de negócios como de costume. A segunda linha de defesa nas organizações mais maduras tem um plano formal de supervisão de PLD/FT que envolve monitoramento dos indicadores-chave de risco (KRIs, *Key Risk Indicators*) e de controle (KCIs, *Key Control Indicators*), realização de testes de controle independentes, revisões temáticas e investigações práticas mais intrusivas de áreas que estão no radar regulatório ou para as quais há preocupações. Uma ferramenta fundamental desta segunda linha de defesa é a informação gerencial, tanto em termos de a própria informação produzida pela empresa e utilizada como input no plano de supervisão, como também sua própria informação independente que tende a ser a utilizada para reportar ao Comitê Executivo e aos Comitês delegados da Diretoria / Conselho. A terceira LoD, que costuma recair na função de Auditoria Interna, avalia o *framework* e o desafio efetivo adotado pela segunda linha, bem como o nível de adoção deste *framework* por parte da primeira LoD.

13. ***Integração entre riscos.*** As organizações criminosas estão se tornando cada vez mais sofisticadas em seus esquemas de lavagem de dinheiro; frequentemente combinando Ciberataques (roubo de credenciais e personificação), uso ilícito desses acessos privilegiados para cometer uma fraude, e usando múltiplos mecanismos para lavar os lucros dessa. Como reação, as instituições financeiras estão evoluindo seus modelos para um *framework* cada vez mais integrado de prevenção ao crime financeiro, com um modelo unificado de governança que incorpora todos os subtipos de risco em um único modelo operacional (LD/FT, evasão fiscal e fraude, juntamente com o risco cibernético). Embora existam diferentes níveis de maturidade, isto geralmente envolve graus de taxonomia de risco comum, infraestrutura de dados e conjuntos de dados unificados, estratégias conjuntas que tentam detectar eventos sincronizados dos diferentes tipos de risco ou *fameworks* comuns para análise de alerta e investigações. Algumas organizações até mesmo centralizaram a responsabilidade sob uma única figura e criaram centros de excelência que fornecem capacidades operacionais em todos os subtipos de riscos.

14. ***Desenho organizacional.*** Mesmo que não exista um padrão industrial em torno da estrutura organizacional que implemente mais efetivamente as três linhas do modelo de defesa da PLD/FT, tanto os reguladores quanto as instituições financeiras têm uma forte expectativa de que os líderes dessas equipes tenham linhas de relatório que permitam o desafio independente para os negócios e a escalada direta para o nível executivo e do Conselho, se necessário. Além disso, que a senioridade e as habilidades certas estejam presentes e que as equipes tenham pessoas e recursos tecnológicos suficientes para serem eficazes em suas atividades. Na segunda linha de defesa, o chefe da supervisão de PLD/FT tende a se reportar para um nível executivo, que é o Chief Risk Officer, Chief Compliance Officer ou Head of Legal / General Council.

15. ***Planejamento da força de trabalho.*** Uma das tendências e melhores práticas do setor consiste em conectar a ambição alvo em torno de PLD/FT, apetite ao risco e estratégia, com um exercício de planejamento estratégico para avaliar as necessidades das pessoas em termos de volume, conjuntos de habilidades e conhecimentos, locais etc. Uma vez feita a análise, há uma execução rigorosa para garantir que tal capacidade esteja no lugar conforme e quando necessário. Isto inclui treinamento / reciclagem dos colegas existentes e contratação de novos talentos (parcialmente alimentado desde o fundo, através de programas de graduação, para

garantir um fornecimento contínuo de especialistas no assunto, independentemente das condições de mercado).

16. ***Capacidades analíticas.*** Como parte desse exercício de planejamento estratégico, a maioria das instituições financeiras está experimentando uma forte demanda por capacidades analíticas, já que muitos dos processos PLD/FT subjacentes se tornam mais orientados para dados (e ciência de dados) – análise de riscos, *screening* de nomes, monitoramento de transações, *screening* de falsos positivos etc. A maioria das organizações maduras está construindo fortes equipes analíticas avançadas (em alguns casos recrutando recursos do mercado e, em outros casos, reestruturando perfis de quantitativos de outras áreas - por exemplo, modelagem de risco prudencial - para aplicar seus conjuntos de habilidades a novos problemas comerciais). Há também forte demanda por perfis de pagamento especializados, incluindo indivíduos com conhecimento técnico detalhado de criptomoedas ou, de forma mais ampla, novas tecnologias de pagamento. Finalmente, outro perfil escasso no mercado e que normalmente é sinalizado nesses exercícios são os indivíduos com multiqualificações capazes de aportar valor em diferentes disciplinas no âmbito de crime financeiro. Estes perfis geralmente são muito úteis para detectar históricos de fraude e se tornam especialistas em assuntos de PLD/FT, atuando nas atividades de detecção de estratégias conjuntas de crimes financeiros e apoio aos centros de excelência multiuso que englobam todos os tipos de risco.

17. ***Quality Assurance.*** À medida que as organizações se tornam mais maduras, elas tendem a criar equipes especializadas para aumentar a eficácia, cortar através de diferentes negócios e garantir a profissionalização das atividades de controle de PLD/FT. Algumas dessas funções incluem equipes de controle e *quality assurance*, encarregadas de garantir que os principais processos empresariais onde os riscos podem surgir sejam executados adequadamente de acordo com a política e os procedimentos. Também equipes especializadas na segunda linha de garantia de defesa, para apoiar a execução eficaz do plano de supervisão.

18. ***Centros de excelência.*** Como parte desta especialização, um passo natural dado por instituições mais avançadas tem sido a criação de centros de excelência. A intenção geralmente é melhorar a eficácia e capturar sinergias na execução de processos operacionais tais como diligência devida do cliente (CDD, *Customer Due Diligence)*, diligência devida reforçada (EDD, *Enhanced Due Diligence)*, *screening* de nomes, monitoramento de transações, *screening* de pagamentos, mas também a produção de informações gerenciais, ou a entrega de melhorias e remediações contínuas. Algumas dessas instituições financeiras encontraram outras sinergias na incorporação desses centros de excelência aspectos operacionais relacionados à fraude, tanto interna (verificação de funcionários) quanto externa. Aspectos como o processo KYC e on-boarding (por exemplo, uma única equipe on-boarding, com a correspondente visão holística do crime financeiro, e simplificação da experiência do cliente), ou o desenvolvimento e parametrização de cenários para a detecção de lavagem de dinheiro, detecção de fraudes etc. são áreas comuns de sinergia.

19. ***Regionalização.*** Para os grandes grupos financeiros internacionais, uma evolução natural em sua jornada de centralização tem sido a regionalização das atividades. Nomeadamente, a criação de centros de excelência em nível regional, com os correspondentes benefícios em termos de melhor gestão do pool de recursos, eliminação de duplicidade, estrutura organizacional simplificada, estabelecimento de melhores caminhos de carreira e cruzamento de oportunidades de treinamento para a força de trabalho, com as correspondentes taxas de retenção mais elevadas. Na mesma linha de evolução, algumas grandes instituições financeiras que já operavam em países off-shore ou near-shore com menor custo de recursos humanos foram capazes de construir centros de excelência de sucesso nessas localidades para prestar serviços na região.

20. ***Terceirização.*** Finalmente, embora a terceirização de algumas das atividades operacionais ainda seja uma opção selecionada por diferentes instituições financeiras, há uma série de fatores que pressionam algumas dessas Instituições a ter internamente essas capacidades terceirizadas e a desenvolver esses conjuntos de habilidades dentro da organização. Não sendo o menor deles uma demanda regulatória cada vez maior em torno de atividades terceirizadas que são críticas para a organização e a necessidade associada de construir fortes estruturas de supervisão e controle em torno dos serviços terceirizados, o nível de excelência operacional esperado pelas diferentes partes interessadas (investidores, supervisores, sociedade), e o impacto reputacional das falhas operacionais.

21. ***Cultura e comportamentos.*** Uma área chave de investimento em programas estratégicos de PLD/FT é a concepção e incorporação da cultura correta, formas de trabalho e comportamentos de pessoal para combater os riscos de crimes financeiros subjacentes. O exame de supervisão está aumentando em todas as jurisdições, e a significativa redução nos perfis especializados de PLD/FT requer uma articulação e incorporação eficazes da cultura e comportamentos corretos

para os funcionários existentes e, especialmente, para os novos funcionários.

22. ***Treinamento.*** Como parte dos programas culturais de PLD/FT, as instituições financeiras estão investindo no fortalecimento dos processos de recrutamento e verificação de pessoal com responsabilidades em torno da PLD/FT. Também, no desenvolvimento de programas de treinamento e certificação de ambições (com modelos operacionais rigorosos a fim de manter os materiais atualizados, medir a eficácia e melhorar continuamente), e que estão ligados à progressão de carreira e remuneração. Isto também requer uma capacidade de monitorar e medir competências a fim de reagir à deterioração do conhecimento e da especialização. Estes programas também investem no desenvolvimento de mensagens claras e transparentes desde o topo (até Conselho de Administração e o nível Executivo), e fortes campanhas de comunicação dirigidas a diferentes segmentos da estrutura dos funcionários, com conteúdo direcionado para cada um deles. Finalmente, as instituições financeiras também estão dedicando tempo para projetar os incentivos certos e a medição de desempenho para sua força de trabalho, alinhados com o apetite ao risco e políticas associadas.

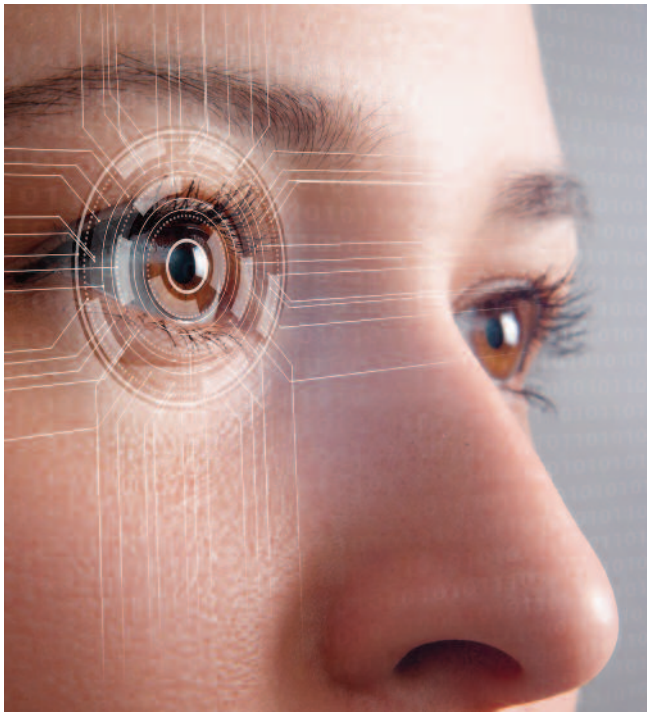
23. ***Infraestrutura de dados e informações gerenciais.*** Em uma economia cada vez mais orientada para os dados, uma das áreas-chave de desenvolvimento dentro do âmbito de PLD/FT é a infraestrutura de dados subjacente e as informações gerenciais utilizadas para a tomada de decisões. Da perspectiva da informação gerencial, uma tendência do mercado é incorporar, na Diretoria e nos relatórios de nível executivo, um conjunto abrangente de métricas e informações qualitativas para garantir que todos os riscos subjacentes (atuais e emergentes) associados ao negócio sejam levados em consideração. A informação gerencial detalha as mudanças na avaliação de riscos em nível de empresa, bem como uma representação dos riscos associados a novas relações comerciais (incluindo quantas novas relações comerciais por categoria de risco, qualquer nova relação de alto risco, qualquer PEP etc.). Para relacionamentos existentes, a alta administração da organização recebe informações sobre os resultados das atividades de monitoramento contínuo (por exemplo, monitoramento de transações, *screening* de pagamentos, revisões periódicas de clientes), bem como o resumo do relatório de atividades suspeitas que ocorreram, e estatísticas de acertos positivos acima e abaixo do limite determinado. A estrutura de relatórios também deve conter a saída dos relacionamentos existentes, e a lógica para estes. Finalmente, é uma prática avançada incorporar na gestão tanto questões em aberto provenientes do trabalho de *quality assurance,* auditoria interna ou ação investigativa de supervisão, como também uma seção sobre enlace regulatório ou envolvimento do setor (geralmente incluindo um elemento de varredura de horizonte para novos regulamentos ou exigências legais).

24. ***Informações externas.*** As informações gerenciais, o panorama de dados e a taxonomia subjacente ao *framework* estrutura de PLD/FT é muito abrangente e pode ser um desafio. Além dos dados de clientes e transações gerados pela organização, as empresas confiam mais do que nunca em informações externas (escritórios de renome, agências nacionais de crime, sentenças judiciais, registros públicos de proprietários beneficiários finais etc.) para complementar seus modelos analíticos. Esta informação externa, em vários casos, requer a ingestão, manutenção e comparação com listas para encontrar possíveis combinações dos clientes e transações atuais ou potenciais. Essas listas estão sendo enriquecidas com novas adições como ativos digitais proibidos (por exemplo, endereços de moedas virtuais ou carteiras digitais associadas a empresas ou indivíduos sob sanções). Além disso, a adoção das novas normas de mensagens sob a ISO20022 ajudará na triagem e comparação das transações.

25. ***Gerenciamento de listas e de sancionados.*** Especialmente no âmbito de sanções, o gerenciamento de listas é uma capacidade fundamental. As empresas mais maduras estão implementando uma plataforma de gestão de listas centralizada que agrega arquivos de diferentes departamentos de tesouraria e fornecedores, limpa os dados e depois os divulga entre todas as filiais de acordo com as regulamentações locais e a política do grupo, eliminando as duplicidades e aumentando a supervisão.

26. ***Conjuntos de dados heterogêneos.*** A natureza dos dados que estão sendo capturados também é muito variada e mutável. Uma taxonomia de dados padrão associados a PLD/FT pode incluir, além de informações transacionais padrão, IDs eletrônicos (por exemplo, eIDAS na UE), geolocalização, endereços IP ou mesmo IMEI e modelo de dispositivo dos dispositivos usados nas transações de moeda virtual conversível. Também listas contendo endereços IP não confiáveis, endereços IP de jurisdições sancionadas ou endereços IP marcados como suspeitos. Além disso, arquivos de mídia adversa e informações da mídia social podem incluir formato de áudio ou vídeo, o que destaca a demanda por informações não estruturadas e a infraestrutura subjacente correspondente para armazená-las e explorá-las.

27. ***Capacidades de gestão de dados.*** Estas demandas de dados exigem o desenvolvimento de capacidades de gestão de dados. Uma delas é uma capacidade de qualidade de dados para especificar proativamente regras comerciais e padrões de qualidade de dados em torno de dados críticos, e depois medir sistematicamente essas regras para identificar quaisquer violações. Além disso, um catálogo de dados que permite a harmonização da informação em diferentes repositórios e motores. Por fim, as instituições financeiras estão investindo fortemente na capacidade de linhagem de dados para permitir a rastreabilidade de ponta a ponta dos dados desde o ponto de consumo até o ponto de origem.



28. ***Harmonização da infraestrutura de dados.*** Um dos princípios mais importantes em termos de infraestrutura de dados tem sido a convergência para repositórios de dados únicos para que todos os componentes tecnológicos ou processos comerciais envolvidos no *framework* de PLD/FT alimentem e armazenem dados de volta para o repositório, tornando-os imediatamente disponíveis para o resto dos componentes. Esta centralização pode acontecer regionalmente ou mesmo em grupo. A fim de obter uma visão holística do risco do cliente e padronizar a investigação de alertas e relatórios, é indispensável consolidar os dados KYC, *screening*, monitoramento de transações, e gestão de alertas e casos em uma única plataforma. A consolidação das informações básicas necessárias para uma investigação antes que o alerta seja atribuído aumenta o tempo por alerta mais notificações automáticas à departamento de *compliance* quando um alerta está pendente de autorização.

29. ***Processos de negócio - on-boarding de clientes.*** Em relação aos processos de negócios para o *on-boarding* de novos clientes o KYC associados, a evolução do comportamento dos clientes, acelerada pela pandemia da Covid 19, alimentou o domínio dos canais digitais nas interações financeiras. As instituições estão investindo em soluções automatizadas de autosserviço através de canais digitais, acionáveis pelo usuário, usando uma identificação digital e dados biométricos, para capacitar os clientes durante o processo de *on-boarding*, revisões periódicas e recertificação. Além disso, permite a coleta de informações mais direcionadas e específicas ao risco (no *on-boarding* ou sempre que houver um gatilho), com questionários dinâmicos alinhados a uma segmentação pré-definida. Estes processos agora se conectam diretamente, através de APIs e micro serviços, a fontes externas de dados a fim de recuperá-los automaticamente e, portanto, simplificar a experiência do cliente, ao mesmo tempo em que validam os inputs de forma independentemente. Estas soluções também facilitam a manutenção automática de registros de suporte ao cliente durante o processo de *due diligence,* que pode ser fundamental em um processo de investigação potencial.

30. ***Processos de negócio - Monitoramento de transações.*** Outro processo que as instituições financeiras estão melhorando drasticamente é o monitoramento de transações que é muito exigente em termos de dados e perspectiva computacional para cálculo a probabilidade de cada cenário. As instituições financeiras estão investindo em tecnologia com maior capacidade computacional, alavancando a computação em nuvem. Além disso, estão refinando a execução de cenários baseados na segmentação dos clientes (em vez de executar todos os cenários para todos os dados disponíveis, os cenários são personalizados para se adaptarem ao perfil de risco da instituição e à realidade empresarial em termos de geografia, catálogo de produtos etc.). Outra opção para aumentar a

eficiência é realizar simulações (número de alertas, falsos positivos, falsos negativos, etc.) em um ambiente *sandbox* antes de implantar o cenário em produção ou cenários de execução apenas contra clientes suscetíveis, omitindo, por exemplo, o governo e órgãos públicos com risco muito baixo. Algumas instituições fazem uma triagem retroativa de lotes para identificar potenciais ligações com entidades sancionadas e sinalizar esses clientes como indivíduos de alto risco a serem investigados.

31. ***Processos comerciais - Avaliação em tempo real.*** Em termos de digitalização dos dados do cliente (nome durante o *on-boarding,* ou transações durante o negócio normal), a tendência do mercado é que estes sejam executados em tempo real. Portanto, existem exigências rigorosas sobre SLAs para manutenção de listas, e um processo técnico que garante que as verificações on-line não sejam impactadas pelo reprocessamento em lote do livro de todos os registros de clientes sempre que uma lista é atualizada. Além disso, a pegada digital é um método crescente para identificação de bandeiras vermelhas na *screening* de pagamentos. Nas organizações mais avançadas, os endereços IP coletados durante as operações do cliente, associados a transações e logins, são rotineiramente monitorados e comparados com os ingeridos durante o *on-boarding* para detectar o mau uso de uma conta de um país de alto risco/sanção ou roubo de conta. A detecção de endereços IP associados a uma rede Tor (que anonimiza o tráfego na web) é fundamental, pois pode revelar conexões entre o cliente e criminosos da *darknet*.

32. ***Processos de negócio - Reporting.*** Mesmo quando a detecção de risco é implementada com sucesso, a má comunicação poderia adulterar o processo. As instituições financeiras estão melhorando seus processos para garantir o cumprimento dos acordos de nível de serviço previstos por suas unidades de inteligência financeira locais (UIF) e que as mudanças nos formatos e exigências de relatórios sejam incorporadas rapidamente. Além disso, há oportunidades de automação na execução de etapas regulamentares que não requerem intervenção manual. Enfim, os canais de comunicação entre as funções de PLD/FT e as linhas de negócios devem ser muito dinâmicos, para garantir que as respostas às perguntas ou a coleta de informações adicionais sejam realizadas dentro dos prazos regulamentares.

33. ***Machine learning.*** Conforme discutido, tecnologias de detecção em tempo real estão sendo amplamente adotadas para evitar riscos associados a erros despercebidos e melhorar a experiência do cliente. Para o *screening* transacional e de nomes (ou casos fora da PLD/FT, como a detecção de áudio fraudulento) as instituições mais avançadas estão investindo em bibliotecas de *machine learning* para Processamento de Linguagem Natural (NLP) a fim de coletar, analisar e armazenar informações de áudio e criar alertas para as linhas de negócios que interagem com o cliente, finalizando a chamada imediatamente para evitar compartilhar qualquer informação pessoal.

34. ***Infraestrutura tecnológica.*** De uma perspectiva de infraestrutura tecnológica, o cenário de ferramentas de PLD/FT não pode mais depender unicamente de um *DataMart* relacional como um banco de dados central, pois agora recebe dados não estruturados (imagem, áudio, vídeo...) onde bases de dados NoSQL e *Data Lakes* são mais eficazes.

35. ***Distributed ledger technology.*** Os avanços tecnológicos também estão melhorando os sistemas de gerenciamento de listas, passando dos sistemas clássicos de gerenciamento de listas administrando tabelas e arquivos para a *Distributed Ledger Technology* (DLT) ou Tecnologia de registros distribuídos. . A DLT ajuda a salvaguardar a integridade dos dados, rastreabilidade, confidencialidade, criptografia e acordo entre as partes interessadas responsáveis. Além disso, permite aos reguladores auditarem o livro de transações, contendo a sequência de mudanças na lista com carimbo de data/hora para validar a conformidade.

36. ***Robótica avançada.*** Outra tendência tecnológica que as empresas têm usado para ganhar eficiência e melhorar a eficácia é a automação robótica de processos (RPA). Agentes virtuais, *chat-bots* e *call-bots* podem auxiliar os clientes com consultas estruturadas e repetitivas dia e noite sem interrupção, colocando-os em contato com um recurso humano para consultas que são mais complexas. O RPA também é uma melhoria crucial para o alerta e gerenciamento de casos, pois estes algoritmos podem ingerir mais dados, de mais fontes e mais rapidamente do que um investigador humano, permitindo uma análise mais rápida de uma base de evidências mais ampla e, consequentemente, gerando uma resolução mais precisa. Sistemas mais sofisticados automatizarão as etapas ou resultados com base em investigações e resultados anteriores.

37. ***Melhorias end-to-end.*** Todas essas melhorias tecnológicas combinadas significam que modelos de *machine learning* são usados para pontuar alertas, a fim de discriminar possíveis falsos positivos. O departamento de *compliance* deveria ter estabelecido um fluxo de trabalho claramente definido e objetivo para a revisão dos alertas, com um critério de priorização para analisar os alertas (por exemplo, baseado em perfis de risco, quantidade de transações ou pontuação correspondente). Este processo só é possível se for realizado por equipes especializadas em PLD/FT que se encarreguem de detectar organizações complexas e gerenciem listas brancas.

Definição do risco de crimes financeiros e contexto regulatório

"Os criminosos calcularam que o crime realmente compensa por tempo demais"
Ronald Reagan[23]

O crime financeiro refere-se a atos ilegais cometidos por um indivíduo ou grupo de indivíduos para obter ganhos financeiros pessoais utilizando os meios de serviços financeiros ou mercados financeiros. Embora existam diferentes definições do que o Crime Financeiro[24] dá direito a , sob este conceito as ações de LD/FTP, suborno, abuso de mercado, ou fraude são consideradas[25].

Duas definições de crime financeiro da Financial Conduct Authority (FCA, Autoridade de conduta financeira do Reino Unido) e da Federal Deposit Insurance Corporation (FDIC, Corporação Federal de Seguro de Depósitos dos Estados Unidos) são destacadas::

> *"Qualquer tipo de conduta criminosa relacionada a dinheiro ou a serviços ou mercados financeiros, incluindo qualquer ofensa envolvendo: (a) fraude ou desonestidade; ou (b) má conduta ou uso indevido de informações relacionadas a um mercado financeiro; ou (c) manuseio dos produtos do crime; ou (d) financiamento do terrorismo"*[26].

> *"Abuso de Pessoas jurídicas para disfarçar o envolvimento no financiamento do terrorismo, lavagem de dinheiro, evasão fiscal, corrupção, fraude e outros crimes financeiros"*[27]

A criação dos meios para identificar e processar crimes financeiros ilícitos em suas diferentes formas desencadeou a promulgação de diferentes iniciativas de supervisão e regulamentação. As duas ações críticas que promoveram uma maior coordenação global na regulamentação do LD foram a constituição do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FAFT)[28] e a ratificação pela ONU da Convenção sobre Crime Organizado Transnacional[29], o primeiro tratado de PLD/FT. Como parte do GAFI, os Estados Membros são obrigados a cumprir com as normas globais de prevenção destes riscos. Estas normas[30] definem amplamente os componentes centrais de qualquer programa moderno de PLD/FT em qualquer instituição financeira:

- Implementar medidas de verificação de identidade de *Know Your Customer* (KYC).
- Executar as medidas de diligência recomendadas pelo GAFI.
- Manter registros adequados de clientes de alto risco.
- Monitorar regularmente as contas em busca de atividades financeiras suspeitas e relatar essa atividade à autoridade nacional apropriada.
- Aplicar sanções eficazes contra pessoas jurídicas e entidades obrigadas que descumpram as recomendações do GAFI.

Por outro lado, os princípios do GAFI e os acordos da Convenção da ONU criaram um consenso para começar a trabalhar na identificação das práticas de LD/FT e, mais importante ainda, para detê-las.

Durante as últimas décadas, o conceito de PLD/FT evoluiu de forma diferente, assim como as várias regulações, em função, entre outras coisas, da natureza mutável das atividades financeiras. As principais tendências observadas nas atividades de crimes financeiros internacionais incluem:

- Restrições rigorosas às transações na maioria das jurisdições, o que aumenta o apetite dos criminosos financeiros para se desviarem para outros tipos de atividades como criptoativos em estágios incipientes de controle e regulação.
- Atitudes, preferências e comportamento dos clientes mudando, com foco crescente nos serviços bancários digitais[31], que serão alvo de criminosos financeiros (por

[23] Ronald Wilson Reagan (1911-2004) foi um ator, estadista e político americano que serviu como 40º Presidente dos Estados Unidos (1981-1989) e 33º Governador da Califórnia (1967-1975).

[24] Alguns órgãos reguladores ou supervisores, como a FCA, fornecem uma definição "fechada" do termo "crime financeiro" e das ações consideradas dentro dele, enquanto outros podem reivindicar responsabilidade pela avaliação, regulamentação e supervisão de certos atos ilegais que podem ser qualificados como crime financeiro (por exemplo, FINCEN). As ações identificadas do ML e TF são, no entanto, essenciais para qualquer programa de supervisão de crimes financeiros.

[25] Outros atos ilegais com ganhos financeiros implícitos que estão sujeitos à regulamentação geral incluem: roubo de identidade, corrupção, evasão fiscal, desvio de fundos, falsificação, falsificação, falsificação.

[26] Autoridade de Conduta Financeira (2021).

[27] Anexo A ao § 1010.230-Certificação referente a proprietários beneficiários de clientes com personalidade jurídica, Lei FDIC, Regulamentos, Atos Relacionados.

[28] FATF (2019).

[29] Escritório da ONU sobre Drogas e Crime (2005).

[30] Apesar da complexidade do tema e da constante evolução das técnicas ML e da tecnologia disponível para ele, estas normas seguem sendo o núcleo dos programas de PLD em todo o mundo e abordam os requisitos de avaliação de PLD estabelecidos pelo setor: avaliação da classificação de risco do cliente, programa de monitoramento de transações e programa de monitoramento de sanções. As normas relacionadas aos clientes de alto risco são especialmente importantes, pois a abordagem baseada no risco é quintessencial para a definição de qualquer programa de PLD.

[31] Esta tendência tem sido exacerbada como resultado da pandemia COVID-19.

exemplo, ativos virtuais, carteiras de custódia, moedas fiduciárias, cartões pré-pagos).

- O aumento das atividades financeiras internacionais facilitado pelas tecnologias disponíveis promoveu novas exigências de consumo global, o que cria canais para atividades financeiras ilícitas.

A complexidade do ambiente atual está forçando as autoridades reguladoras a tomar medidas e abordar a modernização dos programas de Crimes Financeiros à luz desses elementos transformadores.

As mudanças regulatórias associadas ao crime financeiro durante os últimos anos (2021-2022) focaram em::

- Restrições mais rígidas para evitar a lavagem de dinheiro em circuitos "não tradicionais", por exemplo, novas regras para transações digitais.
- Aumentar o foco nos fundamentos do programa KYC para monitorar os riscos e perfis dos clientes e para reforçar, portanto, a regulação de PLD/FT.
- Introdução de novas tecnologias e análises (por exemplo, serviços em nuvem, modelo de *machine learning/artificial intelligence,* analítica avançada) para passar à identificação em tempo real e ao uso otimizado de recursos.
- Coordenação entre jurisdições para melhorar os programas de prevenção de crimes financeiros.
- Corporação pública e privada e desenvolvimento de plataforma para o compartilhamento de informações.

Uma das tendências reguladoras mais importantes tem sido o fortalecimento da colaboração interbancária e entre países com o objetivo de aumentar as capacidades de compartilhamento de dados e informações sobre crimes financeiros e criar regras homogêneas que poderiam atuar em coordenação[32]. Embora estas iniciativas estejam nas primeiras etapas, elas estão se mostrando bem-sucedidas (como foi visto, por exemplo, na reação de diferentes regiões à invasão russa da Ucrânia e nas sanções correspondentes impostas aos interesses econômicos russos).

Panorama regulatório em diferentes jurisdições

Os Estados Unidos vêm desenvolvendo regulação a este respeito desde 1970. Entretanto, nos últimos anos, foi emitida nova regulamentação para atualizar o arcabouço existente:

- A Lei AML de 2020[33] modernizou a Lei de 1970 (BSA/AML) incorporando elementos críticos para abordar a questão de LD e fraude em alinhamento com as tendências atuais..
- A mesma regulação agiu de acordo com as exigências dos proprietários beneficiários finais. Os bancos terão melhor visibilidade sobre o beneficiário final de uma transação, o que promulgará o reforço da due diligence do cliente e reduzirá as atividades de lavagem e fraude.
- As bolsas de criptomoedas devem completar o processo KYC para cada cliente[34].

No caso da União Europeia, a CE apresentou um pacote com quatro propostas legislativas relacionadas à PLD/FT[35]. O objetivo deste novo pacote legislativo é abordar as diferenças nas regulamentações nacionais e aumentar a coordenação entre os estados membros.

O governo britânico está trabalhando ativamente para cumprir as normas internacionais de PLD/FT e considerando a introdução de prioridades nacionais na Lei de PLD[36]. O governo está progredindo em seu Plano de Crimes Econômicos de 2019-2022[37] para fortalecer as estruturas do crime financeiro. Em sua última declaração de progresso sobre este Plano, foram desenvolvidas várias ações centrais que se baseiam nas ações originais dentro do Plano de Crimes Econômicos[38,39].

Na China, a CBIRC emitiu novas medidas[40] para encorajar as instituições financeiras a cumprir efetivamente suas obrigações de PLD/FT e regular a sua supervisão e administração.

O Japão emitiu recentemente diretrizes PLD/FTP[41] que também prescrevem uma abordagem baseada no risco que está em conformidade com as normas internacionais, tais como o GAFI.

Em Cingapura, a Lei de Serviços de Pagamento[42] foi atualizada em janeiro de 2021. Este regulamento fornece uma estrutura flexível para os sistemas de pagamento e prestadores de serviços de pagamento no país. Recentemente a Autoridade Monetária de Cingapura (MAS) também publicou dois documentos de consulta que procuram fortalecer o marco regulatório em torno da lavagem de dinheiro[43].

[32] O GAFI incluiu em sua agenda a iniciativa da parceria público-privada (PPP). Diferentes reguladores também lançaram iniciativas semelhantes.
[33] FinCEN.gov (2020).
[34] Além desta importante adição às regras do KYC, outras regulamentações sobre ativos virtuais foram emitidas pela U.S. Securities and Exchange Commission, Commodity Futures Trading Commission e FinCEN para reforçar a estrutura de controle destes ativos nos EUA.
[35] Regulamento para estabelecer uma autoridade de PLD/FT da UE; Regulamento para regras aplicáveis a PLD/FT (single rulebook) e entidades sujeitas a elas; Diretiva 6 sobre PLD/FT (AMLD6) substituindo a anterior, a ser transposta para a legislação nacional com regras para supervisores nacionais e UIFs nos Estados Membros e Regulamento sobre transferência de fundos.
[36] O Instituto de Finanças Internacionais e a Deloitte (2021).
[37] Governo do Reino Unido (2019).
[38] Governo do Reino Unido (2021).
[39] i) Conceber e entregar um Plano de Ação contra Fraude abrangente; ii) Reforçar a ação operacional público-privada para enfrentar as vulnerabilidades conhecidas, permitindo o fluxo de financiamento ilícito dentro e fora do Reino Unido; iii) Melhorar a eficácia e eficiência de toda a resposta do sistema ao crime econômico, aumentando a inteligência de alto valor para a aplicação da lei e reduzindo a atividade de baixo valor que custa aos negócios e proporciona poucos benefícios; iv) Continuar a entregar a reforma dos RAS, incluindo os próximos estágios de implantação da nova infraestrutura de TI e o aumento do pessoal da Unidade de Inteligência Financeira do Reino Unido; v) Finalizar o modelo de recursos sustentáveis para apoiar a reforma do crime econômico; vi) Desenvolver propostas legislativas para combater a fraude, ML, apreender mais ativos criminosos e fortalecer a transparência corporativa; e vii) Capitalizar a Presidência do G7 para fortalecer a resposta internacional global às finanças ilícitas e à luta contra a corrupção.
[40] Banco Popular da China (2020).
[41] Agência de Serviços Financeiros (2021).
[42] República de Cingapura (2019).
[43] Veja: Documento de consulta sobre a Proposta de Avisos de PLD para Arranjos Comerciais Transfronteiriços de Intermediários do Mercado de Capitais sob Proposta de Estrutura de Isenção. Autoridade Monetária de Cingapura. 12 de maio de 2021, e Documento de Consulta sobre a Plataforma de Compartilhamento de Informações FI-FI para PLD/FT. Autoridade Monetária de Cingapura. Outubro de 2021.


19

A lista a seguir são mostrados os principais órgãos supervisores e reguladores que atuam na implementação do programa de crimes financeiros e os principais regulamentos e diretrizes. A evolução histórica explica o foco principal em PLD/FT.

Estados Unidos – Órgão Regulador: FinCEN

- *Lei de Segredo Bancário (BSA), Lei de Relatório de Moeda e Transações Estrangeiras de 1970* | 26-Out-70. Define o marco regulatório para que as instituições financeiras americanas ajudem as agências governamentais americanas a detectar e prevenir a lavagem de dinheiro, incluindo transações que excedam os 10.000 dólares, informem atividades suspeitas que possam significar lavagem de dinheiro, evasão fiscal ou outras atividades criminosas.
- *Título III do USA PATRIOT Act de 2001* | 26-Out-01. A seção 314 ajuda na identificação, interrupção e prevenção de atos terroristas e atividades de lavagem de dinheiro.
- *Lei de transparência corporativa de 2019* | 11-Jun-19. Requer que entidades novas e existentes reportem informações de titularidade efetiva à Financial Crimes Enforcement Network ("FinCEN"), cria um banco de dados de titularidade efetiva e institui penalidades civis, multas e sanções criminais por descumprimento.
- *AML Act de 2020 (Lei AMLA dos EUA)* |1-Jan-21. Requer que o FinCEN estabeleça prioridades nacionais em PLD/FT para que as instituições financeiras as incorporem em seus programas, e coletar e relatar informações adicionais sobre os titulares de conta, incluindo informações sobre propriedade e controle. Também requer que os reguladores e examinadores as incorporem em suas normas, orientações e exames.
- *Prioridades Nacionais contra a lavagem de dinheiro e combate ao financiamento do terrorismo* | 30-Jun-21. Prioridades governamentais para combater a lavagem de dinheiro e o financiamento do terrorismo.

Reino Unido - Órgão Regulador: Governo do Reino Unido

- *Lei de 2002 sobre os produtos do crime* | 24-Jul-02. Criou a Agência de Recuperação de Ativos e tomou providências sobre a nomeação de seu Diretor e suas funções (incluindo funções relacionadas a receitas) e estabelece o esquema legislativo para a recuperação de origem criminal.
- *Lei de finanças criminais de 2017* | 27-Abr-17. Uma lei para emendar a Lei de 2002 sobre produtos de crimes; fazer provisões em conexão com propriedade terrorista; criar ofensas corporativas para casos em que uma pessoa associada a uma pessoa jurídica ou sociedade facilita a comissão por outra pessoa de uma ofensa de evasão fiscal; e para propósitos relacionados.
- *O Regulamento sobre lavagem de dinheiro, financiamento do terrorismo e transferência de fundos de 2017* | 28-Jun-17. O Tesouro Nacional é designado para os fins da seção 2(2) da Lei das Comunidades Europeias de 1972 em relação à prevenção da lavagem de dinheiro e do financiamento do terrorismo.

Reino Unido - Órgão Regulador: FCA

- *Lei de Serviços Financeiros de 2012* | 19-Dez-12. Lei para emendar a Lei do Banco da Inglaterra de 1998, a Lei de Serviços e Mercados Financeiros de 2000 e a Lei Bancária de 2009; para fazer outras provisões sobre serviços e mercados financeiros; para fazer provisões sobre o exercício de certas funções estatutárias relacionadas às sociedades de crédito hipotecário, sociedades de socorro mútuos e outras sociedades mútuas; para emendar a seção 785 da Lei de Empresas de 2006; para fazer provisões que permitam ao Diretor de Poupança prestar serviços a outros órgãos públicos; e para propósitos relacionados.

Reino Unido - Órgão Regulador: JMLSG

- *Orientação para a prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo* |20-Dez-21. Define o que se espera das empresas e seu pessoal em relação à prevenção da lavagem de dinheiro e ao financiamento do terrorismo, mas lhes permite alguma discrição sobre como aplicam os requisitos do regime britânico de PLD/FT nas circunstâncias particulares da empresa, e seus produtos, serviços, transações e clientes.

União Europeia - Órgão Regulador: EC

- *Diretiva contra a lavagem de dinheiro* | 9-Jun-18. Estabelecer fatores que as empresas devem considerar ao avaliar o risco LD/FT associado a uma relação comercial ou a uma transação ocasional. Além disso, fornecem orientação sobre como as instituições financeiras podem ajustar as medidas de due diligence de seus clientes para mitigar o risco de LD/FT que identificaram, de modo a torná-las mais apropriadas e proporcionais. Finalmente, elas apoiam os esforços de supervisão PLD/FT das autoridades competentes ao avaliar a adequação das avaliações de risco das empresas e das políticas e procedimentos de PLD/FT.
- *Regulamento Delegado da Comissão (UE) 2019/758* | 31-Jan-19. As normas técnicas regulamentares para a ação mínima e o tipo de medidas adicionais que as instituições de crédito e financeiras devem tomar para mitigar o risco de lavagem de dinheiro e financiamento do terrorismo em certos países terceiros.
- *Proposta de uma 6ª Diretiva sobre PLD/FT (AMLD 6)* | 20-Jul-21. Diretiva sobre os mecanismos a serem implementados pelos Estados-Membros para a prevenção do uso do sistema financeiro para fins de lavagem de dinheiro ou financiamento do terrorismo e que revoga a Diretiva (UE) 2015/849.
- *Pacote legislativo de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo* | 20-Jul-21. O pacote inclui uma proposta para a criação de uma nova autoridade da UE para combater a lavagem de dinheiro. É parte do compromisso da Comissão de proteger os cidadãos da UE e o sistema financeiro da UE contra a lavagem de dinheiro e o financiamento do terrorismo. O objetivo é melhorar a detecção de transações e atividades suspeitas, e fechar brechas usadas por criminosos para lavar produtos ilícitos ou financiar atividades terroristas através do sistema financeiro.

União Europeia - Órgão Regulador: EBA

- *Diretrizes sobre políticas e procedimentos em relação à gestão de compliance e o papel e responsabilidades do responsável de Compliance de PLD/FT* | 14-Jun-22. As diretrizes abordam de forma abrangente, pela primeira vez no nível da UE, toda o *framework* de governança de PLD/FT. Estas diretrizes especificam o papel, tarefas e responsabilidades do responsável de *compliance* de PLD/FT, do órgão de administração e do executivo sênior encarregado da *compliance* de PLD/FT, bem como das políticas, controles e procedimentos internos. Elas complementam, mas não substituem, as diretrizes relevantes emitidas pelas Autoridades Supervisoras Europeias sobre acordos mais amplos de governança e verificações de adequação.

União Europeia - Órgão Regulador: ESMA

- *Relatório Anual 2020 sobre as sanções de abuso de mercado da UE* | 20-Out-21. O Relatório descreve um aumento no número de sanções e medidas administrativas em 2020 em comparação com 2019, chegando a 541 de 279 no ano anterior. Entretanto, também constatou que as sanções financeiras impostas são significativamente menores, atingindo apenas 17,5 milhões de euros em 2020, em comparação com os 82 milhões de euros em 2019.
- *Plano de ação para uma política abrangente da União sobre a prevenção da lavagem de dinheiro e do financiamento do terrorismo* | 13-Maio-20. Em sua comunicação "Rumo a uma melhor implementação da estrutura da UE contra a lavagem de dinheiro e o financiamento do terrorismo" e relatórios complementares de julho de 2019, a Comissão estabeleceu as medidas necessárias para assegurar uma política abrangente da UE sobre prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo (PLD/FT). Estas

incluem melhor implementação das regras existentes, um livro de regras mais detalhado e harmonizado, supervisão de alta qualidade e consistente, inclusive conferindo tarefas de supervisão específicas a um órgão da UE, interconexão de registros centralizados de contas bancárias e um mecanismo mais forte para coordenar e apoiar o trabalho das Unidades de Inteligência Financeira (UIF).

China - Órgão Regulador: CBIRC

- *Medidas para a supervisão e administração da prevenção à lavagem de dinheiro e do combate ao financiamento do terrorismo de instituições financeiras* | 1-Ago-21. A fim de fazer com que as instituições financeiras cumpram efetivamente suas obrigações de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e regular a supervisão e administração do combate à lavagem de dinheiro e ao financiamento antiterrorista, o Banco Popular da China formulou as medidas de supervisão e administração da prevenção à lavagem de dinheiro e ao financiamento do terrorismo (as "Medidas") de acordo com a Lei de prevenção à lavagem de dinheiro da República Popular da China, a Lei bancária da República Popular da China e a Lei contra o terrorismo da República Popular da China.

Japão - Órgão Regulador: FSA

- *Diretrizes para a prevenção à lavagem de dinheiro e o combate ao financiamento do terrorismo* | 19-Fev-21: A Agência de Serviços Financeiros ("FSA"), com as medidas de supervisão necessárias, deverá monitorar as medidas PLD/FT de cada Instituição Financeira, compartilhar o resultado com as instituições financeiras e instá-las a melhorar a gestão de risco. As Diretrizes esclarecem as ações necessárias e as ações esperadas a serem implementadas por cada Instituição Financeira e como a FSA conduzirá o monitoramento no futuro.

Índia - Órgão Regulador: FIU

- *Lei de Prevenção da lavagem de dinheiro* | 17-Jan-03. Uma Lei do Parlamento da Índia promulgada pelo governo da NDA para evitar a lavagem de dinheiro e prever o confisco de bens derivados da lavagem de dinheiro.

Austrália - Órgão Regulador: AUSTRAC

- *Lei de Relatórios de Transações Financeiras (FTR) 1988* | 16-Abr-18. A Lei FTR foi introduzida para auxiliar na administração e aplicação das leis tributárias, bem como de outras legislações da Commonwealth, do estado e do território.

- *Lei de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo* | 12-Dez-06. Prevê medidas para detectar, deter e interromper a lavagem de dinheiro, o financiamento do terrorismo e outros crimes financeiros graves; e fornece aos órgãos governamentais australianos relevantes e seus homólogos internacionais as informações necessárias para investigar e processar crimes de lavagem de dinheiro, crimes constituídos pelo financiamento do terrorismo e outros crimes graves.

África do Sul - Órgão Regulador: FIC

- *Lei do Centro de Inteligência Financeira* | 28-Mar-03. Estabelece o Centro de Inteligência Financeira do país (FIC) e introduz um framework básico para alinhar os regulações de PLD/FT do país com os da comunidade internacional em geral. Esta lei foi reforçada pela Lei 1 de Emenda do Centro de Inteligência Financeira de 2017, introduzindo uma abordagem baseada no risco para o *due diligence* do cliente.

Global - Organismo regulador: ONU

- *Convenção contra o Crime Organizado Transnacional e seus Protocolos* | 15-Nov-00. O objetivo desta Convenção é promover a cooperação para prevenir e combater o crime organizado transnacional de forma mais eficaz.

Global - Órgão Regulador: OCDE

- *Cooperação internacional contra crimes fiscais e outros crimes financeiros* | 14-Jun-12. Este relatório da OCDE contém uma compilação de uma variedade de regulamentações internacionais sobre crimes financeiros.

Global - Órgão Regulador: GAFI

- *Recomendações do GAFI 2012* | Out-21. As recomendações do GAFI estabelecem um framework abrangente e consistente de medidas que os países devem implementar para combater a lavagem de dinheiro e o financiamento do terrorismo, assim como o financiamento da proliferação de armas de destruição em massa. Os países têm diversas estruturas jurídicas, administrativas e operacionais e diferentes sistemas financeiros, e, portanto, não podem todos tomar medidas idênticas para combater essas ameaças.

- *Metodologia do GAFI 2013* | *Nov-20.* O GAFI conduz avaliações mútuas dos níveis de implementação das Recomendações do GAFI por parte de seus membros de forma contínua. Estas são avaliações por pares, onde membros de diferentes países avaliam outro país. A metodologia do GAFI para avaliar o cumprimento das Recomendações do GAFI e a eficácia dos sistemas PLD/FT estabelece o processo de avaliação.

- *Procedimentos para a Quarta Rodada de Avaliações Mútuas PLD/FT do GAFI* | Jan-21. O GAFI está conduzindo uma quarta rodada de avaliações mútuas para seus membros com base nas Recomendações do GAFI (2012) e na Metodologia para Avaliar o Cumprimento das Recomendações do GAFI e a Eficácia dos Sistemas de PLD/FT (2013), conforme emendado periodicamente. Este documento estabelece os procedimentos que são a base para essa quarta rodada de avaliações mútuas.

- *Processos e procedimentos consolidados para avaliações mútuas e acompanhamento*| Jan-21. Os Processos e Procedimentos Consolidados para Avaliações Mútuas e Acompanhamento estabelecem os elementos centrais que formam a base para todas as avaliações e se baseiam nos Procedimentos para a 4ª Rodada de Avaliações de PLT/FT do GAFI.

Global - Órgão Regulador: BCBS

- *Princípios básicos para uma supervisão bancária eficaz* | Out-06. Os Princípios Fundamentais têm sido utilizados pelos países como referência para avaliar a qualidade de seus sistemas de supervisão e para identificar o trabalho futuro a ser feito para atingir um nível de base de práticas de supervisão sólidas.

- *Guias sobre a gestão prudencial dos riscos relacionados à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT)* | Jul-20. Estas diretrizes têm por objetivo melhorar a eficácia da supervisão da gestão do risco de lavagem de dinheiro e financiamento do terrorismo (FT) dos bancos, em consonância e como complemento das metas e objetivos das normas publicadas pelo Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Tessorismo (GAFI/FAFT) e dos princípios e diretrizes publicados pelo Comitê de Basileia.

- *Diretrizes atualizadas para uma abordagem baseada no risco em relação aos ativos virtuais e aos provedores de serviços de ativos virtuais* | Out-21. O Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/(FATF) publicou em outubro de 2021 uma série de diretrizes que estabelecem como devem ser aplicadas as recomendações do GAFI no contexto da tecnologia de contabilidade distribuída e das criptomoedas.

Tendências e desafios na prevenção à lavagem de dinheiro e ao financiamento do terrorismo

"As empresas devem aproveitar o poder da ética que está assumindo um novo nível de importância e poder "

James Joseph[44]

Há um conjunto de capacidades que podem ser consideradas sob um mapa de PLD/FT para instituições financeiras, que se destinam a permitir a identificação, gerenciamento, controle e supervisão de PLD/FT. Este mapa inclui (i) o framework e governança; (ii) a estrutura organizacional; (iii) os processos de negócios (incluindo KYC, avaliação de risco do cliente, screening de sancionados, assim como monitoramento de transações ou screening de pagamentos, entre outros); (iv) a infraestrutura tecnológica; e (v) a infraestrutura de dados e capacidades analíticas (ver figura 1).

Framework e governança

Na base de seus programas de PLD/FT, as instituições financeiras estão aprimorando seu *framework* de risco e modelos de governança para garantir tanto um escopo abrangente, quanto uma integração efetiva no negócio. Para este fim, o *framework* inclui o processo de avaliação de risco, estabelecendo padrões e políticas, e garantindo uma gestão de risco robusta através de um modelo de três linhas de defesa

Avaliação de riscos

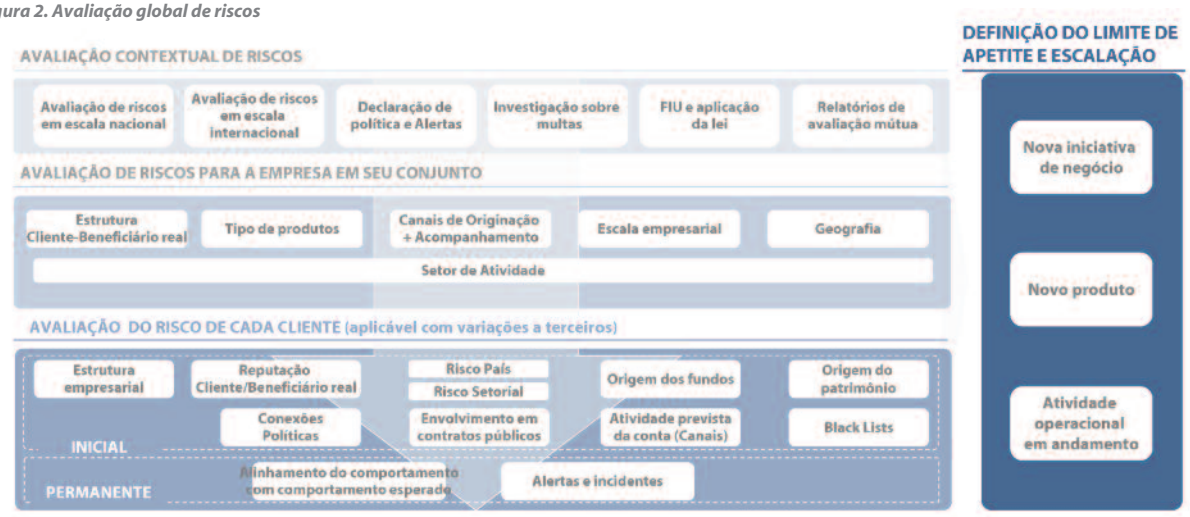
A avaliação de riscos é um mecanismo para compreender as fontes de risco, e é um dos componentes centrais da abordagem de uma empresa à PLD/FTP.

O processo de avaliação de risco tem quatro componentes principais que podem ser implementados: avaliação de risco contextual, empresarial, do cliente e de terceiros.

[44] James Joseph Sylvester (1814-1897) foi um matemático inglês que fez contribuições importantes para o campo das matrizes (ele cunhou os termos matriz, invariante e discriminante, entre outros), bem como para a teoria das invariantes algébricas (em colaboração com A. Cayley), determinantes, teoria dos números, partições e combinatórias.

Figura 1. Mapa genérico das capacidades de PLD/FTP em uma instituição financeira avançada

Figura 2. Avaliação global de riscos



Avaliação do risco contextual

O ponto de partida da Avaliação de Riscos é uma revisão abrangente do modelo de negócios, assim como do contexto no qual tais negócios são conduzidos. Há muitos fatores para esta análise (ver Figura 2). Além disso, uma contribuição importante para este processo é a avaliação de Riscos regional / local fornecida pela autoridade reguladora correspondente. Em muitos países, a autoridade supervisora tem o mandato de realizar uma avaliação de risco exaustiva de PLD/FT[45,46,47].

Avaliação de risco do negócio

A Avaliação de Riscos a nível de negócio é o mecanismo que permite às instituições financeiras avaliar, para cada parte de seu negócio e dentro dele[48], onde se encontram os principais riscos.

Além disso, a Avaliação de Riscos em toda a empresa fornece o *framework* e o contexto para avaliar os riscos de PLD/FT no desenho de novos produtos, bem como nas relações comerciais individuais, permitindo uma revisão abrangente do relacionamento através dos diferentes fatores de risco que impactam a instituição.

Estabelecer um processo formal, envolvendo os especialistas no assunto certo no negócio, e garantir que a avaliação de risco seja revista continuamente são algumas das práticas do setor em organizações mais avançadas[49].

Avaliação do risco do cliente

No nível mais granular, as instituições financeiras realizam Avaliações do Risco do Cliente – Client Risk Assessment (CRAs) individuais para analisar os riscos decorrentes no ponto de *on-boarding* de um novo cliente, bem como durante todo o ciclo de vida do cliente. Esta avaliação deve incluir um conjunto mínimo de fatores que os reguladores tenham fornecido (por exemplo, fontes de riqueza e fundos ou fatores de risco específicos do país e do setor)[50,51].

Historicamente, os dados e capacidades matemáticas dedicadas a esta avaliação têm sido limitados, desencadeando classificações de clientes que nem sempre discriminavam clientes de alto risco, ou que classificavam inadequadamente muitos clientes em grupos de médio ou alto risco, com o correspondente esforço operacional necessário à supervisão, e o impacto na experiência do cliente.

Como resultado, as instituições financeiras têm dedicado investimentos significativos para obter uma abordagem mais precisa baseada no risco e em sua gestão. Atualmente, os esforços estão concentrados em simplificar a taxonomia de modelos alinhados a um conjunto comum de famílias de variáveis (por exemplo, cliente, transação, canal, produto, região), que são utilizadas consistentemente em toda a organização, para garantir a completude e discriminação adequada[52].

[45] Ver, por exemplo, o Artigo 6(5) da (UE) 2015/849 (Quarta Diretiva da UE contra a lavagem de dinheiro), que exige que a EBA emita um parecer sobre os riscos de LD e FT que afetam o setor financeiro da UE a cada dois anos.
[46] Ver o "Parecer sobre os riscos de lavagem de dinheiro e financiamento do terrorismo que afetam o setor financeiro da União Europeia".
[47] GAFI (2013). https://www.fatf-gafi.org/documents/documents/nationalmoneylaunderingandt e rroristfinancingriskassment.html
[48] Depende de seu risco setorial, escala comercial, perfil e estrutura de clientes e dos beneficiários finais, tipos e complexidade dos produtos, canais utilizados para distribuição ou serviço, transações e geografias.
[49] Este processo permite incluir formalmente PLD/FT na estrutura de Apetite ao Risco, uma vez que impulsiona as atividades operacionais nos negócios e as decisões estratégicas nos comitês de aprovação de novos produtos, novas iniciativas comerciais (como fusões, aquisições etc.) e novos projetos de transformação.
[50] EBA (2017a) https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70
[51] FCA (2022), https://www.handbook.fca.org.uk/handbook/FCG.pdf
[52] As instituições financeiras mais avançadas já utilizam algoritmos de *machine learning* e modelos comportamentais para avaliar o risco do cliente. Estes algoritmos são treinados e calibrados com dados históricos e, quando necessário, com julgamento especializado, com melhorias significativas de precisão em relação aos modelos tradicionais, que consideram fundamentalmente juízo especialista.

Avaliação de riscos de terceiros

Por último, algumas instituições financeiras dependem de terceiros para executar parte de suas atividades diárias, desde corretores e intermediários até atividades operacionais de terceirização, prestação de treinamento, assessoria, serviços de infraestrutura tecnológica, etc. Dependendo da natureza do negócio, estes terceiros também podem expor a organização à PLD/FT[53] (ou outra forma de crime financeiro).

Portanto, é prática comum ter uma abordagem totalmente integrada ao gerenciamento de riscos de fornecedores terceiros para avaliar os riscos subjacentes de lavagem de dinheiro e do financiamento do terrorismo. Para este fim, as equipes de compras realizam treinamento específico para poder atuar como uma "primeira linha de defesa" e realizar a avaliação integral.

Normas e políticas

Uma documentação exaustiva que especifica os padrões a serem seguidos em toda a organização é um dos pilares estratégicos de qualquer *framework* de PLD/FT, e um dos mecanismos mais eficazes para mitigar o risco.

As organizações mais avançadas dispõem dos seguintes elementos:

- Uma arquitetura de política que, partindo de uma estrutura de documentação, progressivamente desce em cascata para padrões específicos de negócios, bem como procedimentos e instruções de orientação[54].
- Mecanismos adequados para comunicar efetivamente e incorporar essas políticas na atividade real da organização. Estes podem incluir a existência de um portal web onde a documentação é acessível aos funcionários relevantes, juntamente com um programa abrangente de treinamento e conscientização e um processo de comunicação eficaz para garantir que qualquer adição ou mudança relevante ao cenário de políticas seja imediatamente comunicada em toda a organização.
- Um modelo operacional bem estabelecido que permite que as políticas sejam revistas e atualizadas regularmente, de modo que a nova regulamentação e os riscos emergentes no negócio, ou as lições aprendidas com os incidentes relacionados a PLD/FT, sejam adequadamente e oportunamente atualizados nos documentos, e comunicados em toda a organização. A alta administração deve conduzir esta atualização, e a integração efetiva das políticas nos processos de negócio[55].

O modelo das três linhas de defesa

Como em outros riscos, um modelo robusto de três linhas de defesa (LoD) é um dos pilares do *framework* de gestão de PLD/FT, uma vez que estabelece as responsabilidades pela identificação, gestão, controle e supervisão dos riscos subjacentes.

As instituições financeiras reforçaram seu modelo de linhas de defesa ao realizar uma divisão mais granular de responsabilidades e responsabilidades entre elas.

Primeira linha de defesa

A primeira linha de defesa é, em última instância, responsável pela identificação, gestão e controle dos riscos originados na

[53] EBA (2017b). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

[54] Cada documento contém referências aos riscos aos quais se refere (ligadas à Avaliação de Riscos quando aplicável), bem como às referências externas (regulamentação e legislação, orientação da indústria, etc.) que permitem a conformidade e a rastreabilidade.

[55] EBA (2017c). https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf/66ec16d9-0c02-428b-a294-ad1e3d659e70

condução dos negócios, bem como por estar em conformidade com a regulamentação interna e externa. Ela mantém o relacionamento com o cliente, o que envolve a realização das atividades básicas da KYC[56] , e o monitoramento do perfil de risco[57]. Também é responsável por coordenar o *off-boarding* de clientes com a anuência da segunda linha..

A fim de garantir a profissionalização, padronização nas formas de trabalho e recursos adequados, as instituições mais avançadas formalizaram o papel de uma função ou unidade de PLD/FT no negócio que apoia as equipes de negócios no exercício de suas responsabilidades (ver seção sobre estrutura organizacional).

Segunda linha de defesa

A segunda linha de defesa é responsável pela criação do *framework* de PLD/FT, emitindo políticas (para adaptar a regulação externa à realidade interna do negócio) e por fim supervisionar sua adequada aplicação. Na maioria das instituições financeiras, tende a haver também um elemento de assessoria à primeira linha em casos complexos de *on-boarding* e *off-boarding* de clientes, bem como no caso de desenvolvimento de novos produtos / serviços etc.

Em instituições financeiras avançadas, a segunda linha de defesa desenvolve um plano formal de supervisão com diferentes ações que combina a contribuição obtida de diferentes fontes com o conhecimento especializado sobre a avaliação de risco do negócio e de toda a empresa ou áreas de preocupação regulatória. A ação dentro do plano pode incluir a emissão de nova política ou orientação, informações gerenciais mais frequentes de tópicos particulares, maior amostragem de casos ou revisões temáticas mais "intrusivas" e inspeções especializadas no local.

A segunda linha de defesa também produz informações gerenciais e relatórios periódicos para os órgãos internos de governanaça, para mantê-los informados sobre a evolução do perfil de risco da organização e qualquer ponto relevante para a escalada (por exemplo, brechas no ambiente de controle, novos relacionamentos de alto risco etc.).

O responsável da supervisão de PLD/FT geralmente se reporta a um nível executivo: *Chief Risk Officer, Chief Compliance Officer ou Head of Legal* / Conselho Geral, ou no seu caso, um membro do Conselho de Administração[58] ou dentro da Alta Administração. Tal profissional designado[59] é um indivíduo com responsabilidade final pela supervisão do *framework* e toda a atividade associada à PLD/FT. Este indivíduo e sua equipe atuam como ponto central de referência tanto para o desafio independente e eficaz, como também para o aconselhamento sobre tópicos específicos e complexos.

Terceira linha de defesa

A terceira linha de defesa geralmente se encontra com a função de Auditoria Interna da organização. Como com os demais riscos, esta é uma função independente do negócio e da organização de risco, reportando-se diretamente ao Comitê de Auditoria do Conselho, e com responsabilidades para avaliar e avaliar a amplitude e eficácia do *framework* definido pela segunda linha de defesa, seu nível de adoção pela primeira linha de defesa e o nível de supervisão independente e desafio efetivo realizado pela segunda linha.

A terceira linha de defesa tem seu próprio plano de auditoria independente que parte da informação gerencial da primeira e segunda linha de defesa a partir da qual desenvolve seu próprio conjunto de auditorias.

Estrutura organizacional

Funções especializadas

Na última década, as instituições financeiras estiveram sob intensa pressão para reduzir custos, dado o período sustentado de baixas taxas de juros a que foram submetidas, e o impacto financeiro adicional da pandemia. Ao mesmo tempo, espera-se que melhorem a eficácia e eficiência de suas operações para aumentar o número de alertas produtivos e a detecção de tentativas de lavagem de dinheiro.

Em termos de eficácia, há uma tendência para profissionalizar ainda mais certas funções dentro da função PLD/FT. Alguns exemplos incluem:

1. A criação de equipes especializadas de Controle de Qualidade / *Quality Assurance* na primeira linha de defesa, que utilizam um conjunto completo de técnicas para realizar amostragem avançada, a fim de identificar falhas no cumprimento de políticas e procedimentos e levantar recomendações para melhorias.

2. A criação de funções específicas de garantia e supervisão na segunda linha de defesa. Em linha com a discussão acima, estas equipes atuam como uma camada de execução do plano de supervisão e realizam mergulhos profundos na forma de trabalho de revisão detalhada e especializada sobre assuntos específicos.

[56]Por exemplo, coleta de informações do cliente, identificação e validação, a CDD (ou *Due Diligence* Reforçado, quando necessário) e Avaliação de Risco do Cliente.

[57]Isto inclui o monitoramento contínuo das transações (usando em geral modelos avançados para detectar comportamento estranho e estratégias conhecidas de lavagem de dinheiro), triagem de pagamentos contra listas de vigilância etc. Como no caso do *on-boarding*, a análise e liberação de alertas de baixo nível tende a acontecer também no negócio, e a escalada para a segunda linha de definições acontece apenas nos casos de suspeita de verdadeiros positivos.

[58]Em certas jurisdições é exigido que a instituição designe formalmente um membro do Conselho de Administração ou da Alta Administração como o responsável final pelo cumprimento da regulação. Ver, por exemplo, as Diretrizes da EBA sobre a função dos responsáveis de *compliance* de PLD/FT, EBA/CP/2021/31. Ver também The Financial Conduct Authority ML 7.1 The money laundering reporting officer.

[59]O oficial nomeado não é necessariamente considerado um papel formal. Por exemplo, a regulação do Reino Unido reconhece a função de um "funcionário designado", da mesma forma que a função de um funcionário encarregado de informar sobre a lavagem de dinheiro (ambas as funções podem recair sobre a mesma pessoa, ver o Manual da Autoridade de Conduta Financeira).

3. A criação de equipes analíticas PLD/FT. Elas tendem a incorporar outros subtipos de riscos, além de PLD/FT. (por exemplo, fraude) e são geralmente equipes muito orientadas para os negócios, identificando qualquer nova tendência no mercado.

4. A criação de capacidades especializadas em torno da mudança e remediação no negócio. O efeito combinado das múltiplas camadas de controle e supervisão se traduz em um portfólio de recomendações, emitidas pelas equipes de *quality assurance,* equipes de auditoria interna e revisões de supervisão.

Centralização e criação de centros de excelência

Em conexão com a busca para operações mais eficientes, diversas instituições financeiras de grande porte puxaram a alavanca da centralização de algumas das atividades operacionais dentro de suas equipes PLD/FT, criando centros de excelência. Algumas das atividades operacionais que foram centralizadas incluem a due diligence do cliente, que incorpora as verificações e controles em torno da KYC, o desempenho da Avaliação de Risco do Cliente etc[60]. Essas equipes geralmente têm uma especialização de Varejo e Empresas, para contabilizar as diferenças nos processos KYC / KYB *(Know Your Business)*. Algumas instituições têm uma equipe especializada em KYS *(Know Your Supplier)* e realizam a PLD/FT, bem como a avaliação de Fraude anti-suborno e corrupção (ABC, *Anti Bribery and Corruption*) de seus Fornecedores em uma única equipe.

Para grandes grupos financeiros internacionais, uma evolução natural em sua jornada de centralização tem sido a regionalização das atividades (ou seja, a criação de centros de excelência em nível regional), com os correspondentes benefícios em termos de melhor gestão do conjunto de recursos, eliminação da duplicação, estrutura organizacional simplificada e melhores caminhos de carreira e cruzar oportunidades de treinamento para a força de trabalho.

Embora a terceirização de algumas das atividades operacionais seja uma opção, há uma série de fatores que empurram algumas instituições financeiras a incorporar as capacidades terceirizadas e desenvolver os conjuntos de habilidades dentro da organização. Alguns dos fatores são a crescente demanda regulatória em torno das atividades terceirizadas que são críticas para a organização, a necessidade associada de construir fortes estruturas de supervisão e controle em torno dos serviços terceirizados, o nível de excelência operacional esperado pelas diferentes partes interessadas, ou o impacto reputacional das falhas operacionais.

[60]Há outros exemplos como: a execução de triagem de nome e manutenção associada de listas de vigilância; o desempenho do Monitoramento de Transações (como no caso do CDD, com uma divisão natural entre varejo e empresas); a execução de triagem de pagamentos; os procedimentos operacionais associados às saídas de clientes; a produção de informações gerenciais e relatórios padronizados e algumas das atividades especificadas acima, incluindo *quality assurance,* alteração e correção e análise de dados.

Abordagem integrada para a gestão do risco de crime financeiro

Alguns dos casos recentes mais complexos de crimes financeiros envolvem uma combinação de roubo de credenciais e falsificação de identidade, uso ilícito de acesso privilegiado para cometer uma fraude e múltiplos mecanismos para lavar os lucros.

Neste sentido, uma tendência comum em algumas das instituições financeiras mais avançadas, de acordo com o assessoramento regulatórios[1], consiste em alcançar uma convergência em direção a um modelo unificado de Governança que incorpora todos os subtipos de riscos (lavagem de dinheiro, financiamento do terrorismo, evasão fiscal, fraude e crimes cibernéticos) em um único *framework*.

As sinergias naturais que surgem ao abordar os diferentes subtipos de riscos de crime financeiro sob um modelo unificado que consequentemente a dão origem a oportunidade de eficiência é explicado na adoção deste modelo:

- Há uma forte análise de um novo cliente no ponto de origem do relacionamento, com uma quantidade significativa de informações comuns que abrangem a identificação do cliente, validação, *screening* do nome, avaliações de risco do cliente etc.
- Há um componente de monitoramento contínuo, também com conjuntos de dados sobrepostos em torno de informações sobre transações e pagamentos, que podem ser fundidos em um único repositório de dados para fins de exploração.
- Por fim, há pesquisas que exigem ferramentas de fluxo de trabalho, uma sólida manutenção de registros , documentação e relatórios.

Em grandes instituições financeiras há um certo nível de integração. No entanto, ainda há espaço para melhorias em termos de alcançar a integração total. Algumas das melhores práticas do setor incluem:

- Um framework único para identificação, gestão e controle de riscos. Inclui uma taxonomia de risco comum a todos os tipos de risco, uma autoavaliação comum de risco e controle etc.
- Infraestrutura de dados subjacente comum, visando uma única "visão 360" do cliente e de seus dados, juntamente com sua transacionalidade.
- *Framework* comum e infraestrutura tecnológica para implementação e detecção de alerta, assim como para fua gestão.
- Organizações centralizadas, que incentivam o compartilhamento de informações e uma abordagem holística da propriedade e gestão de riscos, sem lacunas que os criminosos financeiros possam explorar.
- Centros operacionais de excelência capazes de fornecer capacidades operacionais através dos diferentes tipos de risco, com recursos multidisciplinares capazes de gerenciar esses casos.

Dado o número significativo de pessoas operacionais atualmente encarregadas da identificação e gestão das diferentes equipes de crimes financeiros, e a abordagem silos com a qual elas foram originalmente montadas, as oportunidades desta jornada rumo à integração em termos de eliminação da duplicação, aumento da eficiência e eficácia é especialmente significativa.

[1]Ver, por exemplo, *A firm's guide to countering financial crime risks da* FCA, https://www.handbook.fca.org.uk/handbook/FCG.pdf

Planejamento da força de trabalho e competências

As instituições financeiras mais avançadas foram capazes de conectar sua ambição em torno da PLD/FT, conforme refletido na sua estratégia e apetite por ao risco, com as necessidades de suas equipes. Nesses casos, há uma análise abrangente:

i. Começa com a Avaliação de Risco em toda a empresa, crescimento esperado do negócio e mudanças no perfil de risco e iniciativas estratégicas que se espera que mudem as formas de trabalho.

ii. Faz uma projeção informada sobre a capacidade necessária para lidar com a estratégia PLD/FT[61]. Algumas das melhores práticas no setor envolvem a construção de modelos de dimensionamento para que as equipes operacionais possam conectar, em nível operacional, a demanda por capacidade com a oferta.

iii. A seguir, se desenha e aplica uma estratégia para assegurar a existência dessa capacidade. Isto inclui treinamento ou reciclagem do pessoal existente e a contratação de novos talentos.

Nos últimos anos, os exercícios de planejamento da força de trabalho em algumas das organizações mais avançadas identificaram a necessidade de reforçar as equipes com:

1. Perfis quantitativos e analíticos capazes de compreender o negócio e os riscos subjacentes e construir modelos matemáticos usando técnicas de *machine learning*.
2. Conhecimento de novas tecnologias especializadas em pagamento, incluindo as criptomoedas.
3. Pessoas polivalentes capazes de capitalizar a experiência anterior em diferentes subtipos de riscos dentro do âmbito do crime financeiro, que se tornam especialistas no assunto PLD/FT.

Processos de negócio

As instituições financeiras têm dedicado tempo e esforço significativos para racionalizar os processos empresariais associados à PLD/FT. A pressão para reduzir custos e melhorar a eficiência, abriu as portas para o avanço das tecnologias de automação, plataformas de gerenciamento de processos comerciais e modelagem avançada. Além disso, essas melhorias também têm um impacto positivo na experiência do cliente, "pedir as coisas uma única vez", etc. Processos como o KYC foram significativamente simplificados e fortalecidos.

KYC: Avaliação de Risco, due diligence do cliente e due diligence reforçado

Os canais de distribuição passaram de um modelo focado em agências para um modelo de autoatendimento remoto, fomentado por tecnologias capacitadoras, instituições que buscam reduções de custos e a pandemia da Covid-19. A gestão digital do risco do cliente passa de um fator penalizador e se tornar o meio usual de gerenciamento, o que requer um controle mais rigoroso sobre a comunicação entre banco e cliente. Infelizmente, é mais difícil para as instituições financeiras verificar com quem estão fazendo negócios e os objetivo reais das relações comerciais. Novas tecnologias e procedimentos modernos permitem às instituições financeiras mitigar sua exposição PLD/FT através de mecanismos de due diligence melhorados. No entanto, algumas dessas melhorias também se tornaram extenuantes para o cliente devido às constantes solicitações de documentação, muitas vezes via papel, sem alternativa digital.

Soluções automatizadas de autosserviço[62] através de canais digitais, acionáveis pelo usuário, usando uma identificação digital e dados biométricos, capacita os clientes durante o processo de on-boarding, revisões periódicas e recertificação. Além disso, facilita a manutenção de registros automatizados de suporte ao cliente durante o processo de due diligence, o que pode ser determinante em um processo de investigação potencial. Da mesma forma, a identificação digital e os dados biométricos combaterão a fraude de identidade.

Estas soluções de autosserviço reconhecem a distribuição dos clientes por segmentos, definidos e calculados pelos departamentos de Compliance apoiados por técnicas de IA. Como resultado, a segmentação de clientes pode melhorar a captura de informações de KYC, auxiliada por questionários dinâmicos de bordo. Como resultado, é fundamental simplificar o ciclo de desenvolvimento e vida da jornada do cliente, para garantir um tempo rápido para de lançamento no mercado de novas melhorias no processo de KYC e adaptar-se de forma rápida às novas regulações.

As políticas e procedimentos de KYC devem ser revistas periodicamente para mitigar os riscos e aumentar a inclusão financeira. A este respeito, alguns cidadãos não podem abrir contas bancárias ou ter acesso à ajuda pública devido à dificuldade de obter a identificação necessária. Portanto, as instituições financeiras devem evitar medidas rígidas de CDD e apostar em avaliações comportamentais e contextuais.

Supervisão contínua (monitoramento de transações, screening de sanções, screening de pagamentos)

O monitoramento das transações é um processo muito pesado[63]. Agregar todas as transações, contas e clientes a fim de calcular a probabilidade de cada cenário requer grandes quantidades de poder de computação e memória. A análise de custo-benefício é um tópico polêmico entre os departamentos de compliance regulatório. Sistemas legados podem ser aprimorados para lidar com as demandas de desempenho, mas há uma necessidade crescente de tecnologias de ponta com maior capacidade de provisionamento à medida que mais dados são integrados nos modelos.

[61] Esta capacidade é articulada em termos de número de pessoas, conjuntos de habilidades e conhecimentos, localizações, etc.
[62] Ver Guia EBA sobre o uso de soluções de *on-boarding* de clientes à distância. https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/guidelines-use-remote-customer-onboarding-solutions
[63] Autoridade Bancária Europeia. (2021).

Elementos da gestão de recursos humanos

Cultura e comportamentos

Cultura corporativa refere-se às crenças e ideias que uma empresa tem e à forma como elas afetam a forma como ela faz negócios e como seus funcionários se comportam [Cambridge Dictionary].

A cultura, formas de trabalho e os comportamentos dos colaboradores foram identificados em várias revisões temáticas, ações de fiscalização por supervisores, reguladores e agências nacionais como uma das causas fundamentais das lacunas no framework de PLD/FT.

Por esta razão, as instituições financeiras que têm programas PLD/FT avançados tendem a incorporar uma cultura ambiciosa, destinada a incorporar os comportamentos corretos na condução dos negócios. Alguns dos componentes da estrutura cultural da organização incluem capacidades em torno dos seguintes elementos:

Recrutamento e seleção de pessoal

Antes de sua incorporação, os indivíduos que terão qualquer responsabilidade associada à PLD/FT (tanto a força de trabalho interna quanto a de terceiros) devem passar por um processo de verificação, para validar, na medida do possível, que têm a ética de trabalho e integridade corretas, e que nada em seu histórico os exporia como alvos do crime organizado[1].

Treinamento e certificação

Os programas de treinamento e conscientização envolvem cursos genéricos para todos os funcionários do banco, treinamento específico para a função PLD/FT e treinamento para membros do Comitê Executivo e do Conselho de Administração, abrangendo toda a gama de crimes e estratégias criminais que são pertinentes à organização[2].

Compromisso da administração

A alta administração desempenha um papel fundamental em termos de incorporação da cultura. Em instituições financeiras avançadas, os indivíduos que estão próximos aos níveis operacionais de execução do *framework* de risco sentem-se seguros em relação a questões e preocupações crescentes associadas à atividade comercial, e esses relatórios são tratadas de forma anônima e diligente. Existem mecanismos de denúncia de irregularidades e são utilizados regularmente pelos funcionários para levantar preocupações, ou debates em fóruns de tomada de decisão.

Em nível de Conselho, em instituições financeiras avançadas, os membros do Conselho têm tanto o conhecimento quanto as informações gerenciais para compreender os riscos de LD/FT e realizar um desafio efetivo para as funções executivas.

Incentivos e mensuração de resultados

Os mecanismos de incentivo e remuneração devem ser alinhados aos comportamentos desejáveis da força de trabalho e uma entrega adequada das responsabilidades individuais, de acordo com o modelo de governança da empresa. Além disso, o esquema de incentivos não deve encorajar a tomada de riscos inaceitáveis que estejam acima do apetite da organização.

As instituições financeiras mais avançadas têm um mecanismo de definição de objetivos que incorpora indicadores-chave de risco e desempenho associados à PLD/FT que são quantificáveis, bem como indicadores qualitativos que refletem os comportamentos desejados.

Comunicações

Como um dos mecanismos para propagar a cultura e aumentar a conscientização entre o pessoal, algumas instituições financeiras constroem fortes programas de comunicação em torno de seu framework de PLD/FT. Estes são executados como campanhas de comunicação profissional, com uma clara segmentação do público, seleção do conteúdo a ser direcionado a cada segmento de público, canal de entrega etc.

[1] As instituições mais avançadas têm um processo de verificação personalizado para as diferentes funções dentro da organização, incluindo diferentes níveis de senioridade e responsabilidade, assim como diferentes riscos aos quais estarão mais expostas dependendo de sua função (por exemplo, clientes que enfrentam clientes, unidade de investigação financeira, segunda linha de especialistas em defesa etc.).

[2] Os programas de treinamento podem incluir um processo de revisão e aprimoramento contínuo. Além disso, há responsabilidades específicas de revisar formalmente os materiais de treinamento para incorporar novas evoluções da política interna e do cenário regulatório, riscos emergentes, novas publicações regulatórias, etc. Há também programas para certificações do setor, que podem ser ligados a caminhos de carreira e incentivos ao desenvolvimento de carreira.

Uma configuração para aumentar o desempenho sem investimento em infraestrutura é a execução de cenários baseados na segmentação do cliente, em vez de executar todos os cenários para todos os dados disponíveis. Isto é harmonizado com uma Avaliação Baseada em Risco, pois os cenários são customizados para se adaptarem ao perfil de risco da instituição e à realidade do negócio (clientes, geografia, catálogo de produtos etc.). Outra opção para aumentar a eficiência sem alocação de recursos adicionais é a simulação de desempenho (número de alertas, falsos positivos, falsos negativos etc.) em um ambiente sandbox antes de implantar o cenário em Produção. Uma terceira opção é executar os cenários apenas contra clientes suscetíveis, omitindo, por exemplo, o governo e órgãos públicos com risco muito baixo. Por outro lado, os possíveis vínculos com entidades ou pessoas sancionadas poderiam ser identificadas através de um processo batch de *screening* sobre a carteira completa de clientes, considerando esses clientes como indivíduos de alto risco a serem investigados.

Os processos de negócio em torno das sanções sofreram uma transformação significativa nos últimos meses, como resultado da invasão russa da Ucrânia, e das ações legislativas associadas a União Europeia, EUA, Reino Unido[64] e outras geografias tomaram. As instituições financeiras investiram recursos tanto na interpretação das restrições quanto em melhorias operacionais em termos de gerenciamento de listas. Em alguns casos, isto significou uma aceleração dos programas destinados a implementar uma plataforma de gestão de listas centralizada que agrega arquivos de diferentes departamentos de tesouraria e fornecedores, limpa os dados e depois os divulga entre todas as entidades do grupo de acordo com seus regulamentos locais e a política do grupo elimina duplicidades e aumenta a supervisão do programa de Sanções[65].

O *screening* transacional[66] e o *screening* de nomes de clientes durante o *on-boarding* devem ser executados em tempo real. Portanto, são necessários acordos de nível de serviço (SLAs) rigorosos para o carregamento da lista, já que a maioria dos sistemas não pode escanear durante uma atualização da lista. Por outro lado, quando listas proibidas ou cinzas são atualizadas, uma varredura em lote é necessária para todos os registros de clientes contra alterações nas listas. Este processo não deve interferir com os processos on-line e deve ser executado em uma fila separada, já que as mudanças nas listas são muito frequentes, mesmo várias vezes por semana, e consomem tempo, dado o elevado número de registros de clientes.

Gestão e investigação de alertas

A implementação de uma solução de fornecedor especializado por módulo, e às vezes, mais de uma ferramenta por módulo de diferentes fornecedores, isola os alertas, já que os sistemas de gestão de casos não são integrados. Além disso, os Compliance Officers não têm acesso a todos os dados e seus procedimentos podem variar devido à sua ferramenta. Para obter uma visão holística do risco do cliente e padronizar a investigação de alertas e relatórios, é indispensável consolidar os dados KYC, *Screening*, monitoramento de transações, e Gestão de Alertas e Casos em uma única plataforma. A consolidação das informações básicas necessárias para uma investigação antes que o alerta seja atribuído aumenta o tempo por alerta, além das notificações automáticas à funçao de *compliance* quando um alerta está pendente de autorização.

Os modelos baseados em *machine learning* são úteis para pontuar alertas, a fim de discriminar os possíveis falsos positivos. Na sequência, o departamento de *compliance* deve ter estabelecido um fluxo de trabalho claramente definido e objetivo para a revisão dos alertas, com um critério de priorização para analisá-los[67].

Compromisso com a aplicação da lei a relatórios de atividades suspeitas

Mesmo que a detecção de risco seja implementada com sucesso, uma má comunicação poderia adulterar o processo. As instituições financeiras devem cumprir os SLAs esperados de suas UIF, adaptando seus relatórios a um formato específico que está sujeito a mudanças. Alguns passos regulamentares que não requerem intervenção manual, por exemplo, os relatórios de transações monetárias (CTRs), aplicáveis nos EUA, deixam margem para a automação. Ao mesmo tempo, a detecção proativa de isenções de CTR é uma melhora rápida da função. No entanto, a administração da prevenção de lavagem de dinheiro deve rever periodicamente o processo de tomada

[64] Ver a Lei de Crime Econômico (Transparência e Execução) 2022 (a Lei ECTE) no Reino Unido, Perguntas Frequentes 1007 e 1010 da OFAC, ou os até oito pacotes de sanções impostas pela UE a indivíduos e empresas russas.

[65] As plataformas de sanções precisam de regras de personalização para evitar escaneamento de valores irrelevantes (PO Box, #, espaços duplos...).

[66] Além da análise da transferência de dinheiro, a pegada digital é um método crescente para as bandeiras vermelhas. Os endereços IP coletados durante as operações do cliente, associados a transações e logins, devem ser rotineiramente monitorados e comparados com os coletados durante o *on-boarding* para detectar o mau uso de uma conta de um país de alto risco/sanção ou roubo de conta. A detecção de endereços IP associados ao Tor é fundamental, pois pode revelar conexões entre o cliente e criminosos *darknet*.

[67] Por exemplo, com base em perfis de risco, montante da transação ou pontuação correspondente). Este processo só é possível se realizado por equipes especializadas em AML para lidar com a investigação de organizações complexas e gerenciar listas brancas.

de decisão das exceções para obter controle e compreensão.

A comunicação com as linhas de negócios, que têm um contato direto com os clientes, exige canais dinâmicos para resolver questões e transferir documentação dentro do prazo do regulador, aplicando penalizações nos gestores de cliente em caso de erros repetidos frequentemente ao coletar informações do cliente. Por fim, avisos repetidos e fundamentos de relatórios rejeitados requerem detecção e perfil de dados para compreender a causa raiz e resolvê-la. A qualidade dos dados entre plataformas de sistemas de ATMs e bancos de dados bancários com informações de clientes previamente registradas é importante, mas também de identificar erros de relatórios e duplicidades antes de apresentá-los ao órgão regulador.

Informações e dados gerenciais

Informações gerenciais

As informações gerenciais sobre PLD/FT permitem a mensuração, visualização, comunicação e gestão eficaz dos riscos subjacentes. Nesse sentido, a melhor prática no setor inclui a adoção de padrões do setor em torno de práticas de governança e gestão de dados e relatórios (por exemplo, BCBS 239[68]).

As informações gerenciais produzidas devem detalhar as mudanças na Avaliação de Risco em nível de empresa, assim como uma representação dos riscos associados a novas relações comerciais (incluindo novas relações comerciais por categoria de risco, qualquer nova relação de alto risco etc.). Para relacionamentos existentes, a alta administração da organização deve receber informações oportunas sobre os resultados das atividades de monitoramento em andamento (por exemplo, monitoramento de transações, *screening* de pagamentos, revisões periódicas de clientes), bem como o resumo de relatórios de atividades suspeitas *(suspicious activity reports*, ou SARs) e estatísticas sobre os resultados positivos acima e abaixo de um limite específico. A estrutura de relatórios também deve conter a saída dos relacionamentos existentes, e sua fundamentação.

Em particular, as Instituições Financeiras mais avançadas incorporam, nos relatórios ao Conselho, Comitês delegados do Conselho e Comitês Executivos, um conjunto abrangente de métricas e informações qualitativas para assegurar que todos os riscos subjacentes associados ao negócio sejam levados em consideração. Além disso, para equipes mais operacionais, as instituições desenvolveram painéis de controle contendo métricas KPI e KRI em tempo real, com a opção de extrair insights sobre os dados com mais detalhes para facilitar a identificação de pontos fracos no processo e elaborar estratégias de longo prazo.

Outras boas práticas do setor incluem a incorporação, na gestão regular de informações escalonadas à alta administração, das questões em aberto em nível de carteira declaradas pela Garantia de Qualidade, Auditoria Interna ou ação investigativa da Supervisão[69]. Esta visão também sobrepõe, além da ação corretiva, as informações sobre a transformação estratégica das operações PLD/FT e fornece, desta forma, uma visão única da mudança em toda a disciplina.

Gestão e qualidade dos dados

Os dados têm sido uma das principais áreas de evolução e investimento das instituições financeiras nos últimos anos. Sabe-se que dados insuficientes ou de baixa qualidade[70] é um dos fatores mais relevantes que afetam a capacidade de uma Instituição Financeira de identificar, gerenciar e controlar os riscos PLD/FT. Além da clássica remediação manual da qualidade dos dados, as empresas estão fazendo amplo uso de técnicas avançadas para a descoberta de dados, bem como métodos analíticos como lógica difusa ou processamento de linguagem natural para realizar a correspondência e harmonização de dados.

Há várias capacidades de gestão de dados que suportam as funções PLD/FT que são instrumentais. Uma delas é uma capacidade de Qualidade de Dados para especificar proativamente regras comerciais e padrões de qualidade de dados em torno dos elementos críticos de dados usados na identificação e gerenciamento de riscos. Além disso, um Catálogo de Dados que permite a harmonização dos dados em diferentes repositórios e motores e permite aos administradores

[68]Comitê de Basileia (2013a). https://www.bis.org/publ/bcbs239.pdf
[69]Nas organizações mais avançadas, os relatórios para a alta gerência incluem uma seção sobre o enlace com a regulação ou o compromisso com o setor. Isto geralmente contém um elemento de exploração do horizonte para novas regulações ou requisitos legais (e o impacto previsto na organização).
[70]Comitê de Supervisão Bancária de Basileia (2013b).

de dados compreender melhor o significado comercial dos dados, classificar os dados coletados e consumidos em cada processo e alertar as partes interessadas apropriadas no caso de um problema de dados. Além disso, as instituições financeiras estão investindo fortemente em capacidades de linhagem de dados para permitir a rastreabilidade de ponta a ponta dos dados desde o ponto de uso até o ponto de origem.

Mesmo os sistemas mais avançados de detecção automática PLD/FT não são confiáveis se os dados estiverem errados. As regras de qualidade implementadas nos sistemas transacionais de front office assegurarão a geração correta de dados e as regras de consistência confirmarão a correta alimentação de dados nos sistemas PLD/FT.

Infraestrutura de dados e demandas sobre um modelo de dados PLD/FT

A necessidade de informações gerenciais implica uma infraestrutura de dados exigente[71]. É desejável capturar, armazenar, processar e gerenciar informações sensíveis com os mais altos padrões. Os módulos tecnológicos usados para PLD/FT podem se sobressair em suas capacidades analíticas, mas a duplicação de fluxos de dados para diferentes componentes tecnológicos em silos é altamente ineficiente do ponto de vista de transmissão.

Por este motivo, é importante ter um repositório de dados único acessado por todos os componentes tecnológicos e processos de negócios envolvidos no *framework* de PLD/FT. Desta forma, cada processo (por exemplo, Classificação de Risco do Cliente, Alertas, Resultados de Casos, SAR, etc.) utiliza dados do repositório central e armazena seus resultados, tornando-os imediatamente disponíveis para outros processos e os *diferentes* envolvidos no momento. Instituições financeiras que operam em vários países podem centralizar suas ferramentas e repositórios para regiões inteiras ou mesmo globalmente. Estas soluções melhorarão a supervisão de *compliance* e reduzirão os custos em departamentos duplicados nas entidades do grupo, licenças de fornecedores ou infraestrutura.

O aproveitamento de fontes precisas de informações externas para complementar as informações internas disponíveis é uma tendência na maioria das instituições financeiras.

Entretanto, as instituições financeiras não podem mais obter por si mesmas todas as informações necessárias para identificar e avaliar adequadamente os riscos potenciais inerentes à sua atividade. Em uma indústria centrada no digital, os dados acumulados podem ser vendidos ou compartilhados com outras partes. Portanto, fontes externas, tais como escritórios de renome, agências nacionais de combate ao crime, sentenças judiciais e registros públicos são fontes recomendadas para o enriquecimento de modelos.

As tecnologias disruptivas, o comportamento dos clientes modernos e os desastres naturais exigem que as instituições financeiras redesenhem suas estratégias de monitoramento de transações. Os modelos subtreinados nas novas técnicas de PLD/FT não oferecem a capacidade de responder rapidamente ao risco de Crimes Financeiros. Consequentemente, certos cenários devem ser executados automaticamente quando determinados eventos externos ocorrem (novos produtos, lockdowns, catástrofes, conflitos etc.).

A análise histórica é uma prática chave nestes casos. Mesmo que a instituição financeira perca qualquer cenário durante uma crise, ainda podem ser encontradas bandeiras vermelhas contra esses cenários temporários e SAR apresentados. O monitoramento comportamental é uma das tendências atuais no setor, apoiado pelas mais novas técnicas de *machine learning*. O monitoramento comportamental define primeiro como os produtos e serviços devem ser utilizados. Em segundo lugar, ele analisa o comportamento histórico, comportamento esperado, comportamento do grupo de pares e identifica mudanças de comportamento, consumindo todos os dados disponíveis para detectar riscos de crimes financeiros.

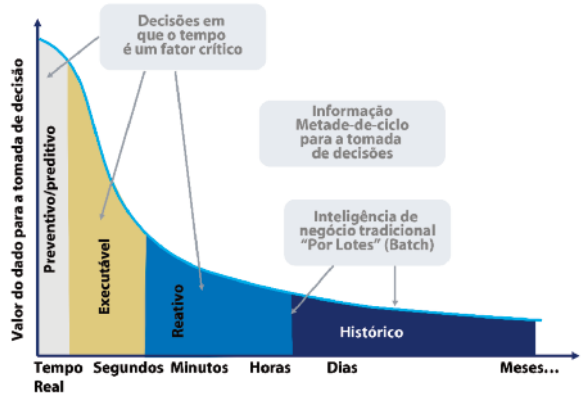
Na área de gestão de casos, o amplo uso das redes sociais está novamente exigindo a ingestão de dados não estruturados e o uso de gráficos para encontrar possíveis conexões entre clientes e criminosos. Finalmente, modelos padronizados de relatórios usando ferramentas de agrupamento de dados, que combinam conjuntos de dados de múltiplas fontes, e geração automatizada de SAR irão acomodar quaisquer mudanças de formato exigidas pelas UIFs, reduzindo as rejeições.

Infraestrutura tecnológica

As ferramentas de PLD/FT não podem mais depender apenas de um *DataMart* relacional como um banco de dados central, pois agora ele está recebendo dados não estruturados onde as bases de dados NoSQL e *Data Lake* se tornam mais eficazes. É de suma importância implementar tecnologias de detecção em tempo real para evitar riscos associados a erros despercebidos e melhorar a experiência do cliente (ver figura 3). As instituições financeiras ainda dependem de sistemas de gerenciamento de arquivos e filas de espera para enviar transações e notificações entre aplicações. O *screening* transacional e de nomes (ou casos fora de PLD/FT, como a detecção de áudio de fraude) se beneficiam da análise em tempo real. Para este último, as bibliotecas de *machine learning* para Processamento de Linguagem Natural (NLP) são apropriadas para coletar, analisar e armazenar informações de áudio e criar alertas para as linhas de negócios que interagem com o cliente, finalizando a chamada imediatamente para evitar compartilhar qualquer informação pessoal.

[71] Comitê de Supervisão Bancária de Basileia (2013c).

Figura 3: Redução do valor dos dados para a tomada de decisão



Source: Perishable insights, Mike Gualtieri, Forrester

As melhorias de dados em tempo real e não estruturadas resultam em picos na atividade de transmissão, processamento e armazenamento, com grandes investimentos em novas opções de armazenamento e migração de dados. Por este motivo, a migração para uma infraestrutura de *cloud* é uma boa solução para acessar novos recursos de gerenciamento de dados.

Com relação à detecção de endereços IP, as instituições financeiras precisam coordenar entre elas e os reguladores para sistematizar a geração de listas contendo endereços IP não confiáveis, endereços IP de jurisdições sancionadas ou endereços IP marcados como suspeitos. Além disso, ferramentas analíticas estão disponíveis no mercado para detectar se os clientes estão usando uma Rede Privada Virtual (VPN) para distorcer sua localização real. Interfaces de programação de aplicativos (APIs) desempenham um papel significativo neste novo monitoramento, pois seus logs devem capturar dados IP que podem ser analisados em tempo real, empregando ferramentas como AWS *OpenSearch* ou Splunk.

A automação robótica de processos (RPA) é uma das principais tendências tecnológicas que aumenta a experiência do cliente através de soluções automatizadas de autosserviço. Agentes virtuais, *chat-bots* e *call-bots* podem auxiliar os clientes com consultas estruturadas e repetitivas dia e noite sem interrupção, colocando-os em contato com um recurso humano para consultas mais complexas. O RPA também é uma melhoria crucial para a gestão de alertas e casos, pois estes algoritmos podem ingerir mais dados de mais fontes mais rapidamente do que um investigador humano, permitindo uma análise mais rápida de uma base de evidências mais ampla e, em última instância, uma resolução mais precisa[72].

[72]Por exemplo, a coleta e agregação dos dados necessários para uma investigação, economiza tempo para o oficial da PLD procurar a documentação. Outras tarefas repetitivas estão sujeitas à automatização, por exemplo, sinalizando alertas duplicados de um único cliente. Sistemas mais sofisticados automatizarão etapas ou resultados com base em investigações e resultados anteriores.

Alguns exemplos de requisitos e práticas em termos de dados

Algumas jurisdições como a UE (por exemplo: eIDAS) exigem que as instituições financeiras de qualquer Estado membro capturem e gerenciem as identificações eletrônicas para fins de PLD/FT, o que se espera reduzir custos e erros humanos com melhor experiência do cliente. Isto é significativo para serviços de confiança, que são considerados de maior risco devido à sua estrutura, ciclos de vida curtos e propósitos variados.

A este respeito, durante qualquer relação comercial, as instituições financeiras coletam informações sobre geolocalização e endereço IP para posteriormente detectar atividades de locais indesejáveis ou roubo de conta. Uma capacidade robusta de Integração de Dados conecta corretamente os diferentes campos com as perguntas mostradas nos questionários dinâmicos, segmentando assim o cliente. A FinCen[1] recomenda até mesmo a coleta do IMEI *(International Mobile Equipment Identity)* é um número de identificação único de 15 dígitos que é atribuído a cada aparelho de telefone celular e do modelo de dispositivo do celular do cliente para operações de moeda virtual conversível. As instituições financeiras armazenam suas interações digitais com os clientes implantando bancos de dados semiestruturados e não-estruturados.

Como mencionado, as instituições financeiras têm que integrar informações de fontes externas para enriquecer seus modelos. Algumas dessas informações são fáceis de ingerir, tais como as bandeiras dos proprietários beneficiários finais em registros públicos ou registros de uma lista PEP. Por outro lado, arquivos de mídia adversa podem incluir formato de áudio ou vídeo, o que novamente destaca a demanda por informações não estruturadas. Além disso, algumas jurisdições exigem mecanismos automatizados para reportar quaisquer desalinhamentos entre registros públicos e dados coletados por instituições obrigadas.

Em termos de listas de controle, há também algumas boas práticas do setor que merecem destaque. A lista proibida não deve ser modificada, exceto para enriquecimento e agregação, enquanto as listas normais e cinzas devem ser rápida e facilmente atualizadas pelos departamentos de conformidade para melhorar o desempenho e cumprir com as políticas internas. Esta perspectiva deve ser refletida na construção de um sistema centralizado de gerenciamento de listas juntamente com notificações automáticas quando as listas são recebidas, agregadas e divulgadas. Estatísticas sobre contagens de registros devem estar disponíveis e o sistema deve esperar notificação automática dos sistemas de detecção, relatando as mesmas contagens de registros de listas carregadas em seus bancos de dados.

A parte deste ponto, em 2018, a OFAC incluiu os primeiros endereços de moeda virtual na lista SDN *(Specially Designated Nationals and Blocked persons)*. São carteiras digitais vinculadas a indivíduos e empresas sancionadas com as quais os negócios são proibidos, cuja estrutura é a descrita.

Na medida em que mais jurisdições incluem listas de ativos virtuais proibidos, as instituições financeiras devem fazer uma varredura contra essas carteiras durante as transações em moeda virtual.

Uma das tendências mais relevantes do setor é a adoção da ISO20022 sobre pagamentos SWIFT, que melhora a triagem e o monitoramento do desempenho através da inclusão de tags XML. Ao contrário das atuais mensagens de formulário livre, os pagamentos SWIFT especificarão claramente o significado dos campos, reduzindo os falsos positivos. As instituições financeiras são obrigadas a atualizar seus sistemas de triagem e monitoramento para analisar esses novos tags e armazená-los em tabelas e colunas apropriadas em seus bancos de dados.

Referência de novas tags XML de informação em transações SWIFT

Digital Currency Address	*XBT*	*158treVZBGMBThoaympxccPdZPtqUfYfT9*
▼	▼	▼
SDN list column	*Currency*	*Wallet ID*

[1]A Financial Crimes Enforcement Network of US procura proteger o sistema financeiro do uso ilícito, combater a lavagem de dinheiro seus crimes relacionados, incluindo o terrorismo, e promover a segurança nacional.

Modelagem analítica e técnicas avançadas para a PLD/FT

"Um modelo é sempre parcial, mas oferece recursos para o avanço do conhecimento"
Jean-Pierre Changeux[73]

Esta seção descreve algumas das tendências e práticas mais inovadoras do setor baseadas em modelagem analítica e técnicas avançadas para a identificação, gerenciamento, controle e supervisão da lavagem de dinheiro.

O contexto para a abordagem analítica da avaliação da PLD/FT

Com o surgimento de uma regulamentação mais restritiva, visando uma identificação mais rápida e melhor dos riscos, e novas tecnologias disponíveis, as instituições financeiras estão se movendo ao longo de uma nova jornada transformadora em relação à implementação da adoção de análises avançadas de PLD/FT[74]. As três principais ferramentas usadas para detectar a lavagem de dinheiro incluem a avaliação do de risco do cliente, o monitoramento das transações e as regras de *screening* de sanções.

Avaliação do risco do cliente

A avaliação do risco do cliente é um modelo baseado nos fatores de risco associados à identificação da lavagem de dinheiro, tais como país do cliente, ocupação e salário, produtos bancários etc.

Os modelos estatísticos se tornaram a prática principal para a classificação de risco do cliente, através da aplicação de diferentes técnicas para resolver o problema da detecção de anomalias. Entretanto, este problema é complexo para identificar ou reproduzir, e produz amostras desbalanceadas.

A aplicação de métodos avançados de dados nos permite superar estas limitações, melhora a precisão da avaliação do risco do cliente e fomenta sua relevância ao longo do programa de PLD/FT. A avaliação do risco do cliente evolui progressivamente para uma avaliação do risco comportamental do cliente na qual os dados contínuos são atualizados e enriquecem o processo de identificação de riscos[75]. Além disso, os próprios modelos estão incorporando o benefício do uso de técnicas de *machine learning*. Métodos supervisionados, tais como o *random forest*, são os primeiros a serem implementados para desvendar relações ocultas entre os fatores de risco em um conjunto aumentado de fatores.

À medida em que o poder computacional, a riqueza e a profundidade dos dados aumentam, estes modelos comportamentais também podem incorporar gatilhos para a estruturação de transações potenciais, ou seja, estratégias coletivas para lavar dinheiro por vários indivíduos através de pequenas quantias, para evitar a detecção por estratégias clássicas de detecção estática. A capacidade de construir algoritmos e estratégias que funcionam não com base em um cliente individual ou cliente mais transação, mas em conjuntos de clientes, permite a identificação da estruturação da transação de forma mais proativa e eficaz. Estes chamados algoritmos gráficos[76,77] aproveitam as conexões potenciais provenientes de diferentes fontes de informação[78]. Além disso, a capacidade de construir uma representação de rede abrangente de todos os clientes traz o valor adicional de racionalizar o processo de investigação de alerta, entre outros.

Monitoramento de transações

A abordagem mais comum de monitoramento de transações consiste em um sistema baseado em regras, no estilo de uma árvore de decisão. Cada regra é configurada para identificar um comportamento definido desmascarando as atividades LD potenciais dos clientes e entidades envolvidas na transação[79].

[73] Jean-Pierre Changeux (b.1936)) é um neurocientista francês conhecido por suas pesquisas em vários campos da biologia, desde a estrutura e função das proteínas, ao desenvolvimento precoce do sistema nervoso, até as funções cognitivas.

[74] Entretanto, não há uniformidade no grau de adoção destas técnicas de análise avançadas. Enquanto algumas entidades financeiras estão experimentando soluções inovadoras, aplicações simples são mais comuns no setor, e a confiança no apoio analítico está no início para outras. No entanto, o presente e o futuro dos programas PLD/FT não podem ser entendidos sem se olhar para as novas tecnologias e metodologias disponíveis.

[75] Por exemplo, incorporação de informações de monitoramento de transações, triagem de pagamentos ou análise outlier em torno de canais, volumes, geolocalização, etc.

[76] Soltani, Reza & Nguyen, Uyen & Yang, Yang & Faghani, Mohammad & Yagoub, Alaa & An, Aijun (2016). 1-7. 10.1109/UEMCON.2016.7777919

[77] Aprendizagem de gráficos escalonáveis para a luta contra a lavagem de dinheiro: A First Look; Weber, M; Chen, J.; Suzumura, T.; Pareja, A.; Ma, T.; Kanezashi, H., Kaler, T.; Leisersen C.E.; Schardl, Tao B

[78] Por exemplo, circuitos fechados de transacionalidade - transferências regulares -, para a propriedade conjunta de contas, endereço único, filial de escolha ou a maioria das filiais visitadas ou caixas eletrônicos, geoposicionamento via aplicativos móveis, coincidência de comerciantes, etc.

[79] Este comportamento suspeito será muito provavelmente baseado em valores anômalos em termos de localização, contagem de transações ou os valores das mesmas.

Essas regras são geralmente identificadas como "cenários". Regras e cenários mais complexos tentam abordar a identificação de contas aninhadas e relações mais sofisticadas entre as partes, mas a base da identificação anterior permanece, de modo geral, no nível da transação individual, analisando os dados recebidos durante o processo transacional. Quando um outlier é identificado, um alerta é acionado, o que posteriormente requer uma avaliação de um especialista[80].

Neste processo, o conjunto inicial de regras é dividido em uma segmentação mais profunda dos comportamentos nos quais a linha de negócios, o nível de atividade transacional e a avaliação de risco do cliente determinam os outliers comportamentais finais, ou seja, os alertas que seriam acionados.

Os métodos analíticos de dados podem ser aproveitados para detectar mais alertas de qualidade, aumentando os verdadeiros positivos e reduzindo os falsos negativos, ou seja, mais alertas verdadeiros são identificados sem aumentar o ruído na identificação. As técnicas de análise de dados e de *machine learning* são implementadas para otimizar a segmentação proporcionando uma identificação mais precisa dos padrões graças à exploração de dados históricos[81].

Entretanto, as entidades financeiras que procuram ativamente incorporar métodos avançados em seu programa PLD/FT podem decidir concentrar-se na priorização de alerta. A abordagem de regras gera grandes quantidades de alertas mesmo quando o ajuste adequado dos limites do cenário é implementado, e a segmentação foi otimizada. Para resolver isto, muitos bancos implementam métodos de aprendizagem supervisionados para classificar os alertas em termos de produtividade[82]. O aspecto chave que determina o sucesso desta abordagem é a utilização de métricas diferenciais, além das variáveis esperadas e inamovíveis disponíveis no nível da transação.

A abordagem mais disruptiva para a identificação de riscos de PLD/FT consiste em abandonar a abordagem tradicional de regras individuais para revelar uma relação oculta com análises avançadas. Entretanto, poucas instituições financeiras estão explorando a utilização de metodologias alternativas. Algumas delas são:

- A análise gráfica, que ocupa seu espaço na identificação das relações de rede e é cada vez mais determinante para as atividades de lavagem no mundo financeiro interconectado
- Técnicas de *clustering*, que ajudam a identificar os valores atípicos sem assumir comportamentos específicos; portanto, capturando com mais frequência novas atividades ilícitas potenciais.

Avançar para uma abordagem não baseada em regras não implica automaticamente o abandono de boas práticas de otimização previamente identificadas. De fato, a confiança em análises avançadas para melhorar a segmentação do cliente, combinada com a detecção de rede e outliers, e a utilização de priorização de alerta pode ser vista como uma solução integral.

Screening de sanções

Os motores de *screening* de sanções comparam indivíduos ou empresas contra uma lista de sanções designada, utilizando técnicas de coincidência difusa. As abordagens mais simples são baseadas em uma ampla gama de transformações aplicadas aos "nomes" (mudança de ordem de nomes, iniciais, transliteração,

[80] Ver Scalable Graph Learning for Anti-Money Laundering: A First Look; Weber, Chen, Suzumura, Pareja, Ma, Kanezashi, Kaler, Leisersen Schardl, Tao.

[81] O ajuste do limiar de dados permite otimizar os baldes de aumento de produtividade ao longo das variáveis utilizadas nos cenários (mais verdadeiros positivos), enquanto fornece medidas do risco potencial não identificado (limitando os falsos negativos). Estas abordagens comuns se baseiam nos motores existentes baseados em regras.

[82] Esta abordagem pode ser vista como uma imitação da revisão dos alertas por analistas de nível 1; no entanto, esta poderia ser uma identificação mais complexa a ser abordada e nem todas as entidades têm sucesso neste esforço.

Um exemplo de avaliação nacional de riscos

O governo britânico publica regularmente uma avaliação nacional de riscos[1], que informa sobre os riscos de crimes financeiros enfrentados a nível nacional. Através desta avaliação nacional de riscos são incluídas referências sobre as técnicas mais habituais utilizadas na LD/FT e seu nível de implantação no país e são uma referência importante para as próprias instituições em sua avaliação do risco.

Uma empresa deve realizar uma avaliação de risco de Crimes Financeiros e usá-la para informar o projeto de seus controles de PLD/FT. A avaliação de risco nacional serve, portanto, como uma base sólida para construir esta avaliação, com a empresa tomando medidas extras para compreender, mais especificamente, os riscos que eles enfrentam.

Isto levaria em conta, mas não limitado à sua carteira de clientes e aos produtos que eles têm - contas correntes pessoais servem como meio de evasão fiscal para muitas pequenas empresas, bem como a introdução de exposição a muitas outras técnicas de lavagem de dinheiro devido à sua capacidade de rápidas transferências de fundos e aceitação de transações em dinheiro. Além disso, uma revisão da atividade criminal histórica pode ajudar a entender quaisquer tipologias adicionais enfrentadas pelo banco.

As transações de dinheiro que entram e saem das contas, servem como uma maneira fácil para os lavadores de dinheiro quebrarem os rastros das transações. Embora o uso de dinheiro em espécie na lavagem de dinheiro seja generalizado e esteja incluído em muitas das estratégias utilizadas, os controles em torno dos riscos de dinheiro em espécie são geralmente os mais simples, em grande parte devido a pouca informação disponível para transações em espécie.

As mulas de dinheiro são terceiros que são usadas, consciente ou inconscientemente para fazer transações adicionais em dinheiro e transferências de fundos que mascaram os rastros de transações. Isto pode ser usado em conjunto com outras estratégias, por exemplo, compra de ativos de alto valor e revenda, para remover quase completamente as suspeitas sobre a origem dos fundos, onde as contas temporárias poderiam ser as de uma rede de mula. Isto é difícil de detectar usando métodos tradicionais, pois nenhuma conta única, e nenhum cliente único, pode jamais ser usado para grandes volumes das transações usadas em qualquer etapa deste processo.

Da mesma forma, os negócios com uso intensivo de dinheiro servem como outro desafio para os métodos tradicionais de detecção. Negócios como salões de beleza, bancas de jornais e lavadoras de carros são utilizados por lavadores de dinheiro para documentar o dinheiro proveniente de atividades criminosas como receita comercial legítima, de modo que grandes volumes de fundos ilícitos das redes criminosas possam ser centralizados em uma conta. Isto se mostra difícil de detectar, pois a renda em dinheiro da empresa pode parecer consistente com sua própria história, bem como com a renda de seus pares e, portanto, pode não haver suspeitas levantadas pelas transações em dinheiro da empresa. Esses negócios, no entanto, são normalmente também ligados ao tráfico de pessoas e à escravidão moderna, que incluem seus próprios comportamentos transacionais que podem ser mais fáceis de detectar. Como no caso do uso de mulas de dinheiro, estas tipologias geralmente envolvem uma rede de terceiros aparentemente não relacionados. Estes terceiros podem ser os facilitadores ou mesmo as vítimas destes crimes e, portanto, há comportamentos específicos que se espera ver. Transações em múltiplas cidades diferentes, especialmente em cidades com centros de transporte, uso intensivo de restaurantes de fast-food, múltiplas transações no mesmo hotel no mesmo dia, múltiplos pagamentos a provedores de telefonia móvel, transferências de fundos entre contas com comportamentos similares e transações internacionais, especialmente em dinheiro e transferências de fundos, são todos fortes indicadores destas tipologias. Se estas partes puderem ser vinculadas ao negócio de caixa intensivo, então a rede completa poderá ser descoberta.

As transações internacionais são outras operações de alto risco identificadas na avaliação de risco nacional. Elas são vistas em uma variedade de técnicas de lavagem de dinheiro, bem como apresentam um risco em outros aspectos da criminalidade financeira. Isto é visto no tráfico de pessoas, que é estimado como um dos maiores geradores de receita criminal em todo o mundo. O tráfico de pessoas requer o envio para o exterior de membros da quadrilha de crime organizado associada nos países associados ao tráfico. Isto pode ser como dinheiro levantado no Reino Unido e movimentado fisicamente para o exterior ou através de mulas de dinheiro de forma semelhante ao comportamento associado aos depósitos em dinheiro descritos anteriormente.

O financiamento do terrorismo é identificado como uma tipologia de alto risco dentro do Reino Unido. A captação e movimentação de recursos não é considerada um objetivo primordial dos terroristas, especialmente porque a maioria dos recentes ataques terroristas tem sido de baixo orçamento e baixa sofisticação, frequentemente planejados, financiados e feitos por um indivíduo. O financiamento do terrorismo é comumente utilizado para mover fundos para o exterior através de métodos relativamente simples, tais como a movimentação física de dinheiro para o exterior ou o emprego de empresas de serviços monetários (MSBs). Portanto, a detecção do financiamento do terrorismo requer uma coleta de indicadores-chave da mesma forma que é requerido para o uso de empresas com uso intensivo de dinheiro na lavagem de dinheiro.

O risco associado aos criptoativos cresce ano após ano à medida que os criptoativos se tornam mais comuns e de fácil acesso, mas os controles em torno deles permanecem relativamente novos com o Reino Unido introduzindo regulamentações em torno do uso de criptoativos para lavagem de dinheiro somente em janeiro de 2020. Gangues criminosas organizadas usam criptoativos para lavagem de dinheiro comprando primeiro os criptoativos com seus fundos ilícitos, potencialmente após um estágio inicial de estratificação, antes de vender os ativos para fornecer uma fonte legal de seus fundos. Além disso, os criptoativos podem ser facilmente movimentados através das fronteiras, permitindo que os criminosos movimentem fundos significativos internacionalmente com facilidade significativa em comparação às moedas fiduciárias.

Isto serve como um exemplo de novos riscos emergentes na criminalidade financeira que representam outro desafio para as instituições desenvolverem e agirem regularmente novos controles para acompanharem as mudanças e desenvolvimentos encontrados pelos lavadores de dinheiro.

[1] HM Treasury: National risk assessment of Money laundering and terrorist financing 2020. December 2020.

erros vocais ou consonantes comuns etc.). Os nomes transformados são padronizados como cadeias e comparados com os nomes da lista de sanções, também padronizados seguindo as mesmas regras. As regras ou lógicas correspondentes medem o grau de separação entre as duas cadeias. O motor pode retornar uma pontuação da correspondência, ou um alerta baseado em uma regra pré-definida de correspondência, entretanto, a lógica subjacente é a mesma, ou seja, as duas cadeias são similares o suficiente para conceder uma revisão especializada.

Como no caso do monitoramento de transações, estas regras produzem muitos falsos positivos[83]. Além disso, o potencial de otimização com base no ajuste é menor do que no caso do monitoramento de transações.

Por esta razão, as instituições estão explorando métodos alternativos para melhorar a qualidade da identificação baseada em tecnologias de tradução e transliteração, e a aplicação de técnicas de processamento de linguagem natural (NLP) para melhorar a correspondência do nome. A melhoria dos métodos analíticos de *screening* de sanções ocorre paralelamente à exploração dessas técnicas na identificação de notícias negativas.

Os próximos passos em abordagens analíticas para a avaliação de PLD/FT

A aplicação de métodos e tecnologias inovadoras não se restringe aos destacados acima. O processamento de linguagem de natureza ampliada e o aprendizado profundo, aplicações em cadeia de bloqueio, verificação eletrônica de identidade, reconhecimento de voz e fala, biometria ou geolocalização são outras tecnologias que podem contribuir para a identificação de atividades ilícitas.

Subjacentes a todas estas abordagens potenciais, podem ser encontradas várias tendências na análise PLD/FT:

- Uma análise mais profunda dos dados existentes tanto no momento da transação, quanto do cliente e seus relacionamentos são implementados. Algumas das opções analíticas descritas acima tornam-se impotentes se os dados diferenciais não estiverem disponíveis e incorporados à análise.

- Dados suplementares das fontes internas e das diferentes dimensões do programa PLD/FT (isto é, classificação de risco do cliente, due diligence, identificação de sanções, transações) e fontes externas (dados públicos sobre PEP, relações de propriedade, fontes reputacionais, buscas abertas) são necessários para criar uma abordagem holística para a identificação de risco PLD/FT.

- As tecnologias e métodos podem ser tão complexos quanto a inovação permite, porém o dimensionamento dos mais adequados à natureza do negócio e a avaliação de risco da instituição é fundamental para otimizar o uso de recursos tecnológicos e humanos e, ao mesmo tempo, garantir a conformidade regulatória.

Os supervisores e reguladores estão em geral relutantes a mudanças repentinas e favorecem metodologias bem estabelecidas antes de abraçar completamente as mudanças revolucionárias. Entretanto, para as instituições dispostas a

[83] Os motores podem ser mais ou menos complexos na incorporação de transformações inovadoras aplicadas a nomes, ou incorporar mais fontes de sanções de qualidade melhoradas com informações PEP, no entanto, todos eles apresentam os mesmos pontos fracos.

embarcar em um programa completo de transformação da análise de PLD/FT, uma série de avanços tem ocorrido nos últimos anos[84]: desde desenvolvimentos específicos de aplicações de coincidências difusas ou detecção de PEP em colaborações conjuntas, até a constituição de centros de inovação e *sandboxes*.

Na jornada rumo a uma identificação de risco mais sofisticada, a interpretabilidade e o controle de risco apropriado permanecem no centro das preocupações do regulador (e das instituições).

O uso de análises avançadas no programa de PLD/FT está vinculado a que as regras implementadas seja consideradas modelos e estejam, portanto, sujeitos às práticas de identificação, monitoramento e controle que as instituições implementaram sob a função de gestão do risco de modelo (MRM). Embora a distinção para a classificação de risco do cliente seja clara, pois cumpre todas as condições tipicamente estabelecidas no *framework* de gestão do risco de modelo (MRM) para ser um modelo ou pelo menos uma ferramenta do usuário que deve ser monitorada, motores de regras de PLD/FT não foram inicialmente vistos como modelos. A assimilação dos motores de PLD/FT na disciplina de gerenciamento de risco do modelo não aconteceu uniformemente entre jurisdições e principais atores querem evitar o peso de um escrutínio incremental dos programas de PLD/FT[85].

No entanto, as tecnologias de *machine learning* para melhorar a identificação de riscos estão ampliando a concepção do que se entende como modelo sujeito ao MRM. Apesar de sua vontade de fomentar sua aplicação aos programas PLD/FT, os supervisores deixam clara a necessidade de garantir um grau adequado de compreensão e interpretabilidade das metodologias implementadas e dos resultados obtidos. Os modelos de caixa preta devem ser evitados. Os modelos de *machine learning* podem sofrer com a falta de transparência na seleção e explicabilidade dos recursos, avaliação do desempenho dos modelos etc. Uma documentação apropriada, teste do modelo, módulos de interpretabilidade; os princípios básicos de um *framework* robusto de MRM apoiarão a adequação desses modelos para o uso de PLD/FT.

Estudo de caso: melhoria a detecção de padrões suspeitos através da análise de redes

Uma das técnicas aplicadas com sucesso para detectar fraudes é a chamada análise de rede. Esta técnica pode ajudar a identificar, detectar e caracterizar comportamentos suspeitos usando métricas, técnicas de *machine learning* e algoritmos fuzzy.

Para desenvolver a análise da rede, há três etapas relevantes a serem consideradas (i) coletar dados relevantes e construir um gráfico que represente os relacionamentos entre as entidades; (ii) decidir sobre a estratégia de identificação que irá identificar o cluster de entidades e relacionamentos suspeitos; e (iii) caracterizar estes clusters através de métricas apropriadas a serem usadas como características dos modelos de detecção (ver figura 4).

Etapa 1. Representação da rede

Uma rede permite o exame de relacionamentos complexos entre entidades relacionadas, seja através de vínculos de dados internos, tais como transações, ou externos, tais como

Figura 4. Etapas para a detecção através da análise de redes.

[84] Nas palavras do recente documento emitido pelo GAFI, "as novas tecnologias têm o potencial de tornar as medidas de PDL/FT sejame mais rápidas, mais baratas e mais eficazes". Além disso, o GAFI enumera as múltiplas iniciativas de supervisores e instituições de todo o mundo que constituem a vanguarda da evolução do setor: Opportunities and challenges of new technologies for AML/CTF, disponível em https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CTF.pdf

[85] Uma declaração conjunta da FRS, FDIC e OCC abordou questões da indústria sobre como a orientação de MRM deve ser aplicada aos modelos de compliance de BSA/AML. Os supervisores consideram que nem todos os sistemas devem ser classificados como modelos, e o próprio banco pode categorizar os modelos como entenderem. Mais importante ainda, eles declararam que os bancos não são obrigados a ter processos duplicados ou a conduzir atividades de testes duplicados para cumprir com a regulaão da BSA. Embora fornecendo certo grau de manobra às instituições financeiras, a declaração reforça a visão do banco abordando os riscos associados aos sistemas de PLD (com ou sem modelos).

endereços e titularidades (ver Figura 5). A construção de redes requer computação de pontos de dados granulares suficientes que possam conectar entidades a diferentes objetos, tais como empresas, endereços, usos digitais, etc., e para considerar a força destes relacionamentos (por exemplo, conexão transacional). Esta rede pode ser estruturada como um grafo (tanto direcionado como não direcionado, e ponderado ou não ponderado). A rede construída e as informações nela contidas determinarão a idoneidade de determinadas técnicas (por exemplo, um grafo não direcionado ponderado poderia ser tratado nas seguintes etapas usando técnicas de agrupamento, tais como o agrupamento espectral).

Etapa 2. Estratégia de identificação

É necessária uma estratégia de identificação para desvendar possíveis padrões de lavagem de dinheiro ou outras atividades ilícitas dentro da rede identificada. Há diferentes estratégias que podem ser usadas, por exemplo:

- Abordagens heurísticas baseadas na proximidade de casos ou entidades suspeitas confirmadas.
- Abordagens probabilísticas e reconhecimento de padrões.
- Abordagem de detecção de comunidades baseada em técnicas de *machine learning*.

Ao aplicar a abordagem de detecção de comunidades, é necessário descobrir diferentes comunidades. Uma comunidade é um subgrafo da rede com um número maior e uma relação mais intensa entre os membros da comunidade, em comparação com subgrafos aleatórios e pouco informativos (ver figura 6). A detecção de comunidades é uma abordagem útil para detectar e caracterizar as estruturas-alvo, o que pode exigir o uso de algoritmos como k-means, clustering hierárquico, clustering espectral, algoritmos evolutivos ou otimização da modularidade[86].

Para encontrar as comunidades ótimas, uma função específica é otimizada: a função de modularidade. Dada uma rede representada como um grafo ponderado e dividido em comunidades ou módulos, esta esta fórmula depende da estrutura específica da representação gráfica, e expressa a definição matemática de modularidade em termos de pesos:

$$Q = \frac{1}{2w}\sum_i\sum_j\left(w_{ij} - \frac{w_i w_j}{2w}\right)\delta(C_i, C_j)$$

Onde C_i é a comunidade para a qual o nó i é atribuído, w_{ij} representa o valor do peso na ligação entre os nós i e j (0 se não houver ligação), $w_i = \sum_j w_{ij}$, e $w = \sum_i w_i$. Por último, a função δ corresponde à função delta de kronecker delta: $\delta(i,j)$ toma o valor 1 se os nós i e j estiverem no mesmo módulo e 0 caso contrário.

Etapa 3. Uso de funções

Uma vez identificadas as comunidades objetivo dentro da rede, métricas ou características específicas podem ser definidas para avaliar a profundidade e a importância dos relacionamentos ou o risco das conexões entre entidades. Estas características podem ser usadas em regras ou algoritmos de *machine learning* para melhorar a capacidade de previsão dos modelos, reduzindo os falsos positivos e identificando melhor os padrões suspeitos. A abordagem baseada em regras com incorporação de características "enriquecidas" pode ser útil para produzir alertas qualitativos, já que incorporam novas

[86] Vários autores desenvolveram algoritmos ótimos para a detecção de padrõesão de padrões. Ver L. Alsedà, A. Awasthi, Jörg Lässig (2012).

Figura 5. Representação do algoritmo de detecção de comunidades (etapas (a) a (d) usando a otimização da modularidade.
A comunidade superior contém um comportamento suspeito (objetivo) que corresponde, neste caso de uso, à rede do Cliente A da Etapa 1 (representado na figura 7 na próxima página).

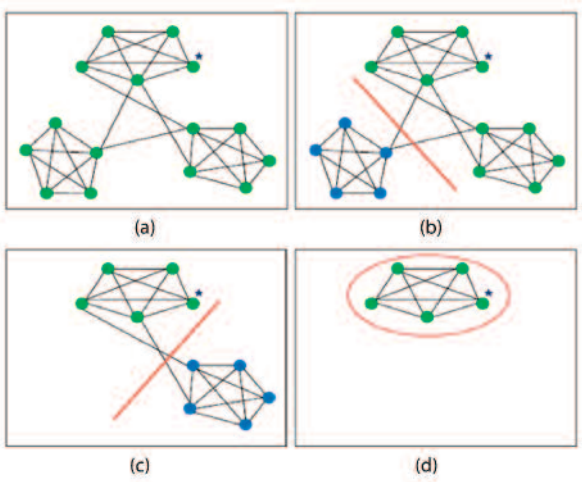
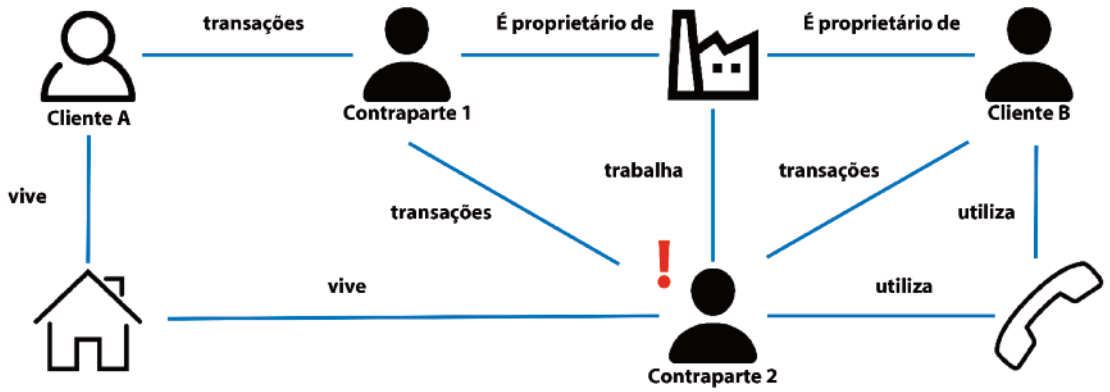


Figura 6. Lógica simplificada para um cenário baseado em características obtidas através da análise da rede. Outras características, tais como valores de transações, podem ser incorporadas de acordo com o padrão ou combinação de padrões a serem detectados. Este exemplo é meramente ilustrativo.

Lógica e parametrização das regras de detecção com características de rede:

- Se tipo de entidade = **Individual**
- Se comunidade suspeita identificada: conexões suspeitas identificadas = **Sim**
- Se o número de rotas para o nó suspeito >= **num_rotas_para_no_suspeito**
- Se a distância até o nó suspeito for <= **distancia_maxima_ate_no_suspeito**
- Se as conexões primárias com o nó suspeito = **tipo_conexao_principal**

Figura 7. Representação dos relacionamentos de rede relacionados ao Cliente A incluindo um nó suspeito (a Contraparte 2 está na blacklist) e possíveis entidades sintéticas (nós relacionados à Companhia)



informações além da base transacional tradicional relacionada com o cliente (ver figura 8). No entanto, as técnicas de *machine learning* podem desvendar relações mais sólidas que permitem separar os verdadeiros alertas positivos dos falsos.

No exemplo da figura 7, cuja infomação de redes é apresentada na figura 8, o cliente A e o cliente B pertencem ao mesmo cluster suspeito com conexões com a entidade suspeita (Contraparte 2), mas o cliente B tem a relação mais forte, tanto pessoal quanto profissionalmente com a Contraparte 2. Com base nesse cenário, se os limites forem calibrados para ser num_rotas_para_no_suspeito = 1, distancia_maxima_ate_no_suspeito = 5 e tipo_conexao_principal = "all" (seja transacional, pessoal ou de qualquer outro tipo), então tanto o Cliente A como o B serão marcados como entidades suspeitas (ou suas transações relacionadas, etc.). No entanto, considerando uma abordagem mais tradicional, sem a análise de redes, somente o cliente B seria marcado como tal; o cliente A não tem conexões transacionais com a Contraparte 2.

Características complexas podem ser avaliadas e diferentes tipos de algoritmos de *machine learning* podem ser treinados, permitindo atribuir um risco maior ao Cliente B e às transações associadas. A adição de novas características aos modelos também permite maior precisão e maior detecção de comportamentos potencialmente arriscados (reduzindo falsos alertas negativos), enquanto se discrimina melhor o risco entre os comportamentos identificados (reduzindo os falsos alertas positivos).

Figura 8. Informação sobre os clientes para a identificação de conexões suspeitas

Empresa	Distância mínima para o nó suspeito	Conexão primária com o nó suspeito	Conexão de dados pessoais	Número de rotas para o nó suspeito	Cluster identificado	Conexões suspeitas identificadas
Cliente A	2	Transacional	Sim	2	1	Sim
Cliente B	1	Transacional	Sim	4	1	Sim

Conclusões

Os crimes financeiros (em seu sentido amplo, que inclui lavagem de dinheiro, financiamento do terrorismo, não cumprimento de sanções econômicas, suborno e corrupção, fraude e abuso de mercado) continuam a ser uma grande ameaça para o setor financeiro no mundo inteiro, e especificamente, a lavagem de dinheiro como uma das áreas a prestar maior atenção. De acordo com o Escritório das Nações Unidas sobre Drogas e Crime, estima-se que o montante de dinheiro lavado no mundo em um único ano é estimado entre 2% e 5% do PIB mundial, ou seja entre 800 bilhões e 2 trilhões de dólares americanos. Entretanto, menos de 1% desse dinheiro é apreendido ou congelado pelas forças da lei.

As instituições financeiras, reguladores e agências de combate ao crime estão trabalhando em conjunto para aproveitar um maior poder computacional, uma modelagem matemática mais avançada, uma maior consciência no topo e coordenação mais estreita combater a lavagem de dinheiro em todas as jurisdições para combater esse crime econômico.

Nesse contexto, as instituições financeiras estão investindo na melhoria de suas capacidades para a identificação, gestão, mensuração, controle e supervisão de seus riscos::

1. *Framework* e governança, com avaliações de risco mais formais e abrangentes, normas e políticas mais detalhadas, um modelo melhor definido e mais coordenado de 3 linhas de defesa e abordagens mais integradas para a gestão de riscos (entre os diferentes riscos de crimes econômicos).

2. Estrutura organizacional, com equipes especializadas e totalmente dedicadas, dirigidas por especialistas no assunto. Também a centralização das capacidades para assegurar uma ação eficiente e eficaz, e o planejamento estratégico de pessoal para assegurar não apenas o atual fornecimento de especialistas no assunto, mas também a identificação de futuras necessidades de competências (por exemplo, cientista de dados). As instituições financeiras estão também investindo fortemente para assegurar a adequada incorporação da cultura e dos comportamentos corretos para lidar com esse crime.

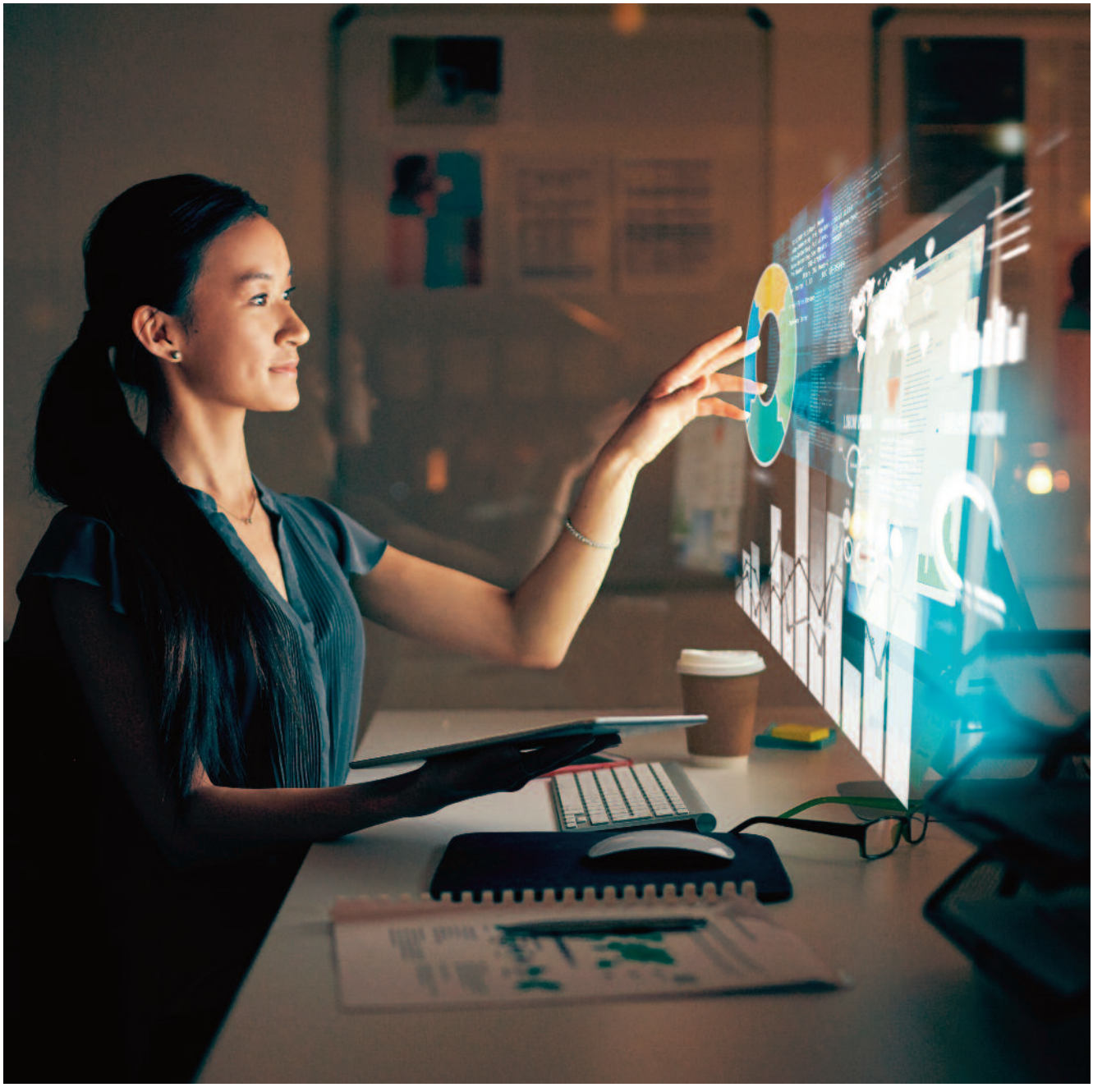
3. Processos de negócio, incluindo as avaliações de risco em toda a empresa, assim como o due diligence e avaliação de risco de cada cliente. Também o investimento na racionalização e fortalecimento do monitoramento das transações, detecção das sanções e pagamentos, pesquisa da gestão de alertas, assim como colaboração com os órgãos de aplicação da lei.

4. Melhoria dos dados subjacentes que respalda a identificação e a mensuração de riscos, incluindo a melhoria das fontes de dados, a melhoria da qualidade dos dados e da capacidade de governança dos dados.

5. Investimento em infra-estrutura tecnológica, com particular atenção à capacidade de lidar com novas ameaças, tais como lavagem de dinheiro através através de criptomoedas, assim como o aumento das capacidades e a automação dos processos tecnológicos.

Uma das principais áreas de investimento, que também está provando ser uma das mais eficazes, é o desenvolvimento de processos analíticos avançados para aumentar a eficácia da detecção de ameaças. Este é um dos pilares do futuro de uma função eficaz contra a lavagem de dinheiro (e crimes financeiros em geral): uma função em que os dados e a modelagem e análise avançadas são capazes de identificar padrões em tempo quase real e desencadear alertas produtivos e respostas automatizadas.

Glossário



AMLA: A Lei de Prevenção a Lavagem de Dinheiro de 2001 é a principal lei contra a lavagem de dinheiro. Ela permite que as autoridades investiguem a lavagem de dinheiro e outros crimes financeiros a fim de proteger as instituições financeiras e deter os criminosos.

Avaliação da classificação de risco do cliente: Eles são uma das três principais ferramentas utilizadas pelas instituições financeiras para detectar a lavagem de dinheiro. Os modelos implantados pela maioria das instituições hoje são baseados em uma avaliação dos fatores de risco como a ocupação do cliente, salário e os produtos bancários utilizados.

BPM: Business Process Management. BPM é uma metodologia de trabalho baseada, em um sistema de gestão que se encarrega de controlar a modelagem, a visibilidade e a gestão dos processos produtivos da empresa.

BSA (Bank Secrecy Act): A partir de 1970, é uma das primeiras leis a combater a lavagem de dinheiro nos Estados Unidos. A BSA exige que as empresas mantenham registros e relatórios que estão determinadas a ter muita utilidade em assuntos criminais, tributários e regulatórios.

CFT (Countering the Financing of Terrorism) ou FT (Financiamento do Terrorismo): Este termo envolve o uso de fundos que podem ser de origem lícita ou ilícita e a utilização desses fundos para apoiar a atividade terrorista.

Convenção sobre o Crime Organizado Transnacional: foi adotada pela resolução 55/25 da assembleia Geral de 15 de novembro de 2000, e é o principal instrumento internacional na luta contra o crime organizado transnacional.

GAFI/FAFT (Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo): É uma instituição intergovernamental criada em 1989 pelo então G8. O objetivo do GAFI é desenvolver políticas para ajudar a combater a lavagem de dinheiro e o financiamento do terrorismo.

KCI (Key Control Indicator): Indicador chave de controle.

KYB (Know Your Business): Estas estratégias se concentram em estabelecer relações ótimas com outras empresas que podem ser clientes ou fornecedores, para mitigar o risco de fazer negócios com uma entidade não confiável ou que esteve envolvida em uma situação comprometedora no passado.

KYC (Know Your Customer): Estes procedimentos são estabelecidos em torno de um processo de identificação e verificação da identidade de um cliente no qual uma série de controles e verificações são aplicados para evitar relações comerciais com pessoas ligadas ao terrorismo, corrupção ou lavagem de dinheiro.

KYS (Know Your Supplier): Esta prática proporciona mais percepção e transparência sobre fornecedores e riscos relacionados à cadeia de fornecimento, a fim de abordar tópicos como desempenho do fornecedor, continuidade dos negócios, sustentabilidade, fraude e suborno, risco de segurança, lavagem de dinheiro, trabalho infantil e outros requisitos de conformidade legal/organizacional.

KRI (Key Risk Indicator): Indicator chave de risco.

Modelo de linhas de defesa: As três linhas de defesa representam uma abordagem para fornecer um *framework* em torno da gestão de riscos e controles internos dentro de uma organização, definindo papéis e responsabilidades em diferentes áreas e a relação entre elas.

Mula de dinheiro: Uma pessoa que transfere ou movimenta dinheiro adquirido ilegalmente em nome de outra pessoa.

PEP: Politically Exposed Person. Pessoa politicamente exposta.

PLD: Significa Anti Money Laundering ou Prevenção à Lavagem de Dinheiro (PLD) e é usado principalmente no setor financeiro, legal e de conformidade para se referir aos controles padrão que as empresas e organizações devem ter em vigor para prevenir, identificar e relatar comportamentos suspeitos de lavagem de dinheiro.

Programa de supervisão de transações: Ele ajuda as instituições financeiras a detectar automaticamente transações suspeitas, tais como depósitos em dinheiro de alto valor ou atividades incomuns na conta.

Screening: É um processo que visa identificar e conduzir a due diligence do cliente sobre qualquer pessoa politicamente exposta como parte de um robusto programa Prevenção a Lavagem de Dinheiro e Know Your Customer (PLD/KYC).

Screening de sanções: é uma combinação de políticas, procedimentos e tecnologias que permitem uma instituição financeira garantir que ela não forneça nenhuma forma de serviços para sancionar as partes sancionadas, direta ou indiretamente.

Unidades de Inteligência Financeira (UIFs): Unidades de investigação estabelecidas por países individuais para centralizar a coleta de relatórios de atividades suspeitas relacionadas à atividade financeira criminosa e compartilhar os resultados da análise com agências governamentais pertinentes.

Bibliografia

Autoridade de Conduta Financeira. Manual da FCA. https://www.handbook.fca.org.uk/handbook/glossary/G416.html

Escritório das Nações Unidas sobre Drogas e Crime. Lavagem de dinheiro. https://www.unodc.org/unodc/en/moneylaundering/overview.html

Fórum Econômico Mundial. Global Coalition to Fight Financial Crime (Coalizão Global de Combate ao Crime Financeiro). https://www.weforum.org/projects/coalition-to-fight-financial-crime

Lexis Nexis Risk Solutions (2021). Custo global de compliance.

Paesano, F. (2021). As criptomoedas e as investigações de lavagem de dinheiro. Instituto da Basileia sobre Governança.

Europol. (2018). Preso na Espanha o autor intelectual por trás de um roubo cibernético de 1 bilhão de euros. https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain#downloads

Sanction Scanner. (2021). Multas contra a lavagem de dinheiro (PLD) de 2021. https://sanctionscanner.com/blog/anti-money-laundering-aml-fines-of-2021-561

Comissão Europeia. (2019). Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a avaliação de casos recentes de suposta lavagem de dinheiro envolvendo instituições de crédito da UE.

Parlamento Europeu e o Conselho. (2015). Diretiva (UE) 2015/849.

Autoridade Bancária Europeia. (2021). Diretrizes sobre cooperação e troca de informações entre supervisores prudenciais, supervisores da PLD/FT e unidades de inteligência financeira sob a Diretiva 2013/36/UE.

Mersch, Y. (2019). Prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo - iniciativas recentes e o papel do BCE. https://www.bankingsupervision.europa.eu/press/speeches/date/2019/html/ssm.sp191115~a435dd398e.en.html

Autoridade Bancária Europeia. (2019). Parecer da Autoridade Bancária Europeia sobre as comunicações às entidades supervisionadas relativas aos riscos de lavagem de dinheiro e financiamento do terrorismo na supervisão prudencial.

Parlamento Europeu. (2021). Proposta de Regulamento do Parlamento Europeu e do Conselho sobre as informações que acompanham as transferências de fundos e certos criptoativos (reformulada).

Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FAFT). (2014). Definições-chave das moedas virtuais e potenciais riscos PLD/FT.

Parlamento Europeu. (2021). Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece a Autoridade para o Combate à Lavagem e ao Financiamento do Terrorismo e que altera os Regulamentos (UE) No 1093/2010, (UE) 1094/2010, (UE) 1095/2010.

Holman, D.; Stettner, B. (2018). Regulamento Anti-Lavagem de Dinheiro de Criptomoedas: Abordagens Estadunidenses e Globais. Allen & Overy, LLP.

Autoridade Bancária Europeia. (2021). Relatório final sobre o projeto de normas técnicas de regulação sob o Artigo 9a (1) e (3) do Regulamento (UE) No 1093/2010.CTF.

Financial Conduct Authority (2022). Empresas aceitas pelo Regulatory Sandbox. https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms

Conselho de Governadores do Sistema da Reserva Federal (2018). Declaração Conjunta sobre Esforços Inovadores para Combater a Lavagem de Dinheiro e o Financiamento do Terrorismo.
https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms

Conselho de Governadores do Sistema da Reserva Federal (2021). Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning.
https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence

Federal Deposit Insurance Corporation (2021). Anexo 1010.230 Requisitos de titularidade efetiva para clientes com personalidade jurídica. Lei FDIC, regulações, leis relacionadas.

Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FAFT). (2019). Os Ministros do GAFI dão a este organismo um mandato de duração indefinida.

Escritório das Nações Unidas sobre Drogas e Crime. (2005). Convenção das Nações Unidas contra o Crime Organizado Transnacional e seus Protocolos.

Escritório das Nações Unidas sobre Drogas e Crime. (2011). Estimar os fluxos financeiros ilícitos resultantes do tráfico de drogas e outros crimes organizados transnacionais. Relatório de pesquisa. Outubro de 2011.

Rede de Execução de Crimes Financeiros. (2020). A Lei de Combate à Lavagem de Dinheiro de 2020.

Instituto de Finanças Internacionais; Deloitte. (2021). A eficácia da reforma do gerenciamento de riscos de crimes financeiros e os próximos passos em uma base global.

Banco Popular da China. (2021). Medidas para a Supervisão e Administração da Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo de instituições financeiras.

Agência de Serviços Financeiros. (2021). Diretrizes para o Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

República de Cingapura. (2019). Lei de Serviços de Pagamento.

Autoridade Monetária de Cingapura. (2021). Documento de consulta sobre a Proposta de Avisos de PLD para Acordos Comerciais Transfronteiriços de Intermediários do Mercado de Capitais em virtude dos marcos de isenção propostos.

Autoridade Bancária Europeia. (2021). Parecer da Autoridade Bancária Europeia sobre os riscos de lavagem de dinheiro e financiamento do terrorismo que afetam o setor financeiro da União Europeia.

Grupo de Ação Financeira Internacional. (2013). Avaliação de risco de lavagem de dinheiro e do financiamento do terrorismo.

Autoridade Bancária Europeia. (2022). Diretrizes sobre o papel dos responsáveis de compliance de PLD/FT.

Autoridade Bancária Europeia. (2021). Diretrizes sobre o uso de soluções de on-boarding de clientes remotos.

Comitê de Supervisão Bancária de Basileia. (2013). Princípios para a agregação eficaz de dados de risco e relatórios de risco.

Soltani, R.; Nguyen, U.; Yang, Y.; Faghani, M. (2013). Um novo algoritmo para detecção de lavagem de dinheiro baseado em similaridade estrutural.

Weber, M; Chen, J.; Suzumura, T.; Pareja, A.; Ma, T.; Kanezashi, H., Kaler, T.; Leisersen C.E.; Schardl, Tao B. (2018). Aprendizagem de gráficos escaláveis para a prevenção à lavagem de dinheiro.

HM Treasury: National risk assessment of money laundering and terrorist financing. December 2020.

Nosso objetivo é superar as expectativas dos nossos clientes sendo parceiros de confiança

A Management Solutions é uma empresa internacional de serviços de consultoria com foco em assessoria de negócios, riscos, organização e processos, tanto sobre seus componentes funcionais como na implementação de tecnologias relacionadas.

Com uma equipe multidisciplinar (funcionais, matemáticos, técnicos, etc.) de mais de 3.300 profissionais, a Management Solutions desenvolve suas atividades em 41 escritórios (17 na Europa, 20 nas Américas, 2 na Ásia,1 na África e 1 na Oceania).

Para atender às necessidades de seus clientes, a Management Solutions estruturou suas práticas por setores(Instituições Financeiras, Energia e Telecomunicações) e por linha de negócio, reunindo uma ampla gama de competências de Estratégia, Gestão Comercial de Marketing, Gestão e Controle de Riscos, Informação Gerencial e Financeira, Transformação: Organização e Processos, e Novas Tecnologias.

A área de P&D presta serviço aos profissionais da Management Solutions e a seus clientes em aspectos quantitativos necessários para realizar os projetos com rigor e excelência, através da aplicação das melhores práticas e da prospecção contínua das últimastendências em *data science*, *machine learning*, modelagem e *big data*.

Juan G. Cascales
Sócio da Management Solutions
juan.garcia.cascales@msunitedkingdom.com

Antonio Tazón
Sócio da Management Solutions
antonio.tazon@msnorthamerica.com

Patricia Pajuelo
Diretora da Management Solutions
patricia.pajuelo@msnorthamerica.com

Luke Harrison
Experienced Senior da Management Solutions
luke.harrison@msunitedkingdom.com

Management Solutions, erviços profissionais de consultoria

Management Solutions s é uma firma internacional de serviços de consultoria focada na assessoria de negócio, riscos, finanças, organização e processos

Para mais informações acesse **www.managementsolutions.com**

Nos siga em:

www.managementsolutions.com

Madrid Barcelona Bilbao Coruña London Frankfurt Düsseldorf Paris Amsterdam Copenhagen Oslo Warszawa Zürich Milano Roma Bologna Lisboa Beijing Istanbul Johannesburgo Sydney Toronto New York New Jersey Boston Pittsburgh Atlanta Birmingham Houston San Juan de Puerto Rico San José Ciudad de México Monterrey Querétaro Medellín Bogotá Quito São Paulo Lima Santiago de Chile Buenos Aires