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 - SAR). 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, e com tomadas rápidas, 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 o desgaste significativo 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).

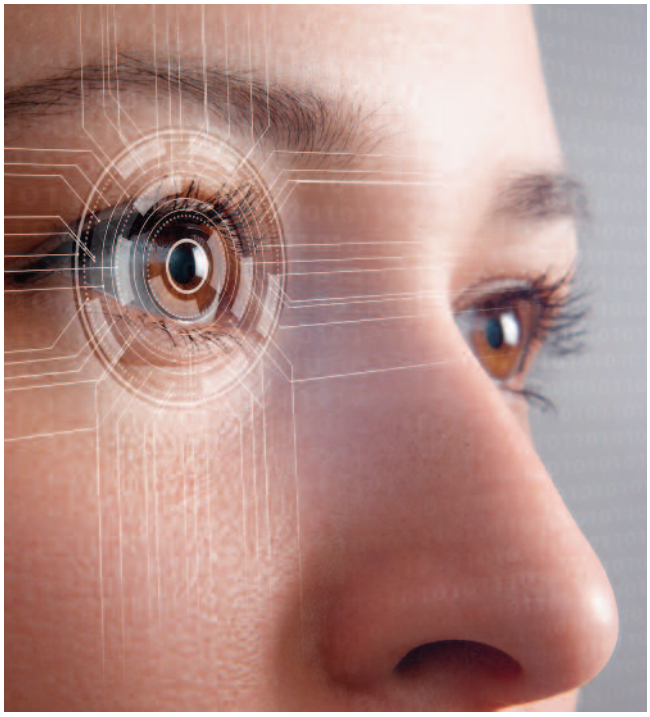
24. ***Informações externas.*** As informações gerenciais, o panorama de dados e a taxonomia subjacente ao *framework* estrutura de PLD/FT é muito abrangente e pode ser um desafio. Além dos dados de clientes e transações gerados pela organização, as empresas confiam mais do que nunca em informações externas (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 Diretoria de Compliance Regulatório 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 Avançada de Processos Robóticos (ARPA). 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 ARPA 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 responsável 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.