Desafios e tendências 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

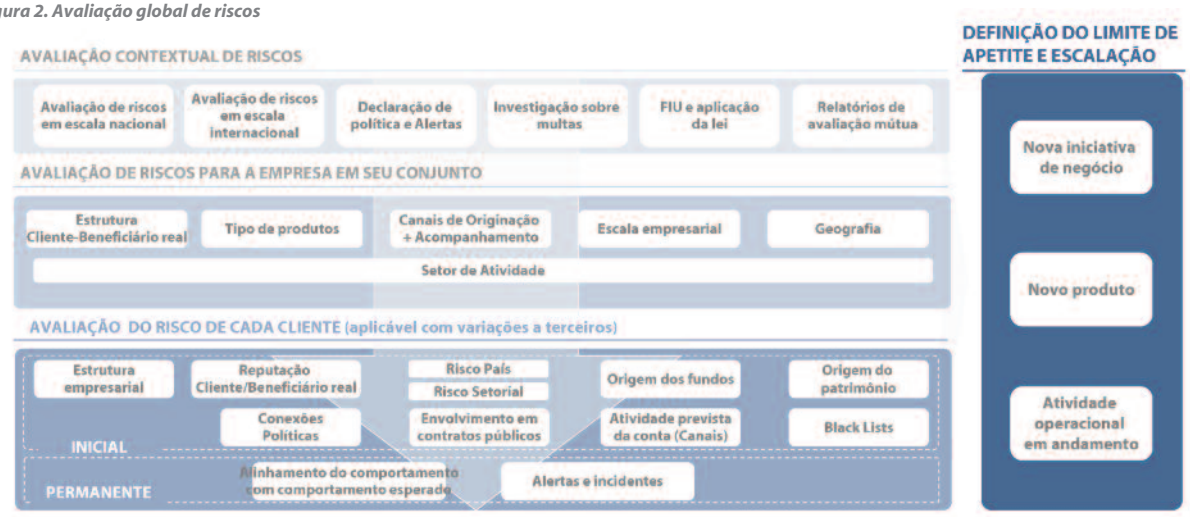
A avaliação de riscos é um mecanismo para compreender as fontes de risco, e é um dos componentes centrais da abordagem de uma empresa à PLD/FTP.

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 funcionário designado não deve considerar necessariamente como tendo o papel formal reconhecido. 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. Fazer 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 do canal 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 Função de PLD/FT 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 *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 notificação 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 de decisão das exceções para obter controle e compreensão.

[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.

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 digna, 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 da notificação de atividades suspeitas 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 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

[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).

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, *Suspicious Activity Report,* 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 *Suspicious Activity Report* 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.

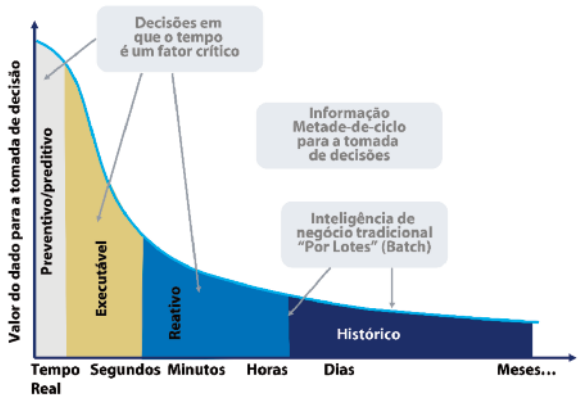
Infraestrutura tecnológica

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.

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.

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

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



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.