RELATÓRIO DE VIAGEM

DADOS DO EVENTO

DATA DE INÍCIO	DATA DE TÉRMINO	NOME DO EVENTO	CIDADE/PAÍS
12 de maio de 2025	14 de maio de 2025	ACAMS The Assembly - Europe	Paris, França

RESUMO DO EVENTO

ENTIDADE ORGANIZADORA	PROCESSO	PARTICIPANTES
ACAMS	006.193/2025-0	Jetro Coutinho Missias

JUSTIFICATIVA (RESUMO)

A AudDefesa está conduzindo duas auditorias cujos assuntos foram contemplados pelo evento. Na primeira auditoria, Proteção da Pessoa Idosa contra Golpes Digitais, faz parte do escopo tratarmos dos crimes envolvendo roubo de celular. Parte da solução para o problema envolve processo de trabalho chamado Know Your Costumer (KYC), segundo o qual bancos, agentes de telefonia, polícia e formuladores de políticas de segurança pública aplicam ferramentas para verificar e confirmar a identidade do consumidor, atividades financeiras realizadas por eles, riscos, estabelecimento de compliance com a regulação e etc. O Workshop B tratou especificamente sobre o KYC. O evento principal também trouxe debates sobre o KYC (como a sessão "KYC: Entendendo Riscos, Confiando nas Decisões e Abertura de Oportunidades" e a sessão "Em guarda" que tratou especificamente de golpes e esquemas). A segunda Auditoria, sobre a atuação dos órgãos federais de segurança pública no combate a lavagem de dinheiro tendo em vista a recuperação de ativos, é um tema de vanguarda no TCU e demanda conhecimentos sobre as ameaças emergentes advindas dos crimes financeiros, as ferramentas que se tornaram recentemente utilizadas pelos criminosos e as diversas relações e implicações com o crime organizado. O Workshop A tratou especialmente sobre avaliação de riscos envolvendo crimes financeiros, a principal forma da Lavagem de Dinheiro e das dificuldades na recuperação de ativos. Além disso, houve apresentação de estudos de caso sobre lavagem de dinheiro e de recuperação de ativos pelas autoridades que as investigaram e as palestras envolvendo o futuro do combate aos crimes financeiros, a utilização da Inteligência Comportamental na internet no combate a este tipo de crime e as principais técnicas utilizadas nesse combate. Em ambas as auditorias, o evento ajudou a entender mais profundamente os objetos de auditoria relacionados, compreender melhor os riscos desses objetos, como se dá a atuação internacional no tema, qual o atual comportamento dos criminosos e como a comunidade internacional combate tais crimes e situações. Além disso, permite a identificação de critérios e a prospecção de alternativas de encaminhamento que, considerando o contexto brasileiro, possam aproximar o Brasil da realidade mundial referência na área.

RELATO

O evento da ACAMS reúne profissionais seniores voltados a questões relativas a fraudes, golpes, lavagem de dinheiro e financiamento de crimes e de terrorismo.

O primeiro dia foi formado por duas participações em Workshops. No Workshop A – Mastering Fraud Risk Assessments - foram apresentadas metodologias estruturadas para Avaliação de Risco de Fraude (Fraud Risk

Assessment - FRA), destacando a combinação de elementos quantitativos e qualitativos. Foram abordados dados recentes sobre fraudes na Europa, totalizando perdas de US$ 103,6 bilhões em 2023 e €11,7 bilhões com fraudes Authorized Push Payment (APP) em 2024. O workshop detalhou o framework de FRA, composto por identificação de riscos, análise de riscos e controles, avaliação do risco residual e tratamento do risco. Casos práticos demonstraram diferenças na implementação do FRA em diferentes organizações, destacando desafios como propriedade pouco definida dos riscos e uso de planilhas versus sistemas robustos.

Durante o workshop, as principais tendências debatidas foram: O uso de **IA generativa** para impulsionar golpes cibernéticos (*spearphishing*, *deepfakes*, etc.) e o **aumento de fraudes do tipo APP** (quando a própria vítima autoriza o pagamento) via esquemas de investimento falso, golpes românticos e esquemas de personificação.

Foram revisadas tipologias de fraude, a seguir explanadas:

Fraude de 1ª Parte: Cometida pelo próprio cliente (informações falsas, intenção deliberada de não pagar por produtos/serviços, fraude em empréstimos, etc.). Exemplos incluem fraude de crédito, fraude de documentos (documentação falsa) e simulação de perdas de mercadoria.

Fraude de 3ª Parte: Envolve um terceiro usando indevidamente dados de vítimas inocentes (ex.: roubo de identidade sem consentimento). Exemplos: account takeover (invasão de contas), roubo de identidade e fraude em pagamentos autorizados resultantes de golpes (como alguém ser convencido a transferir dinheiro).

Fraude de 2ª Parte: Situação híbrida em que um indivíduo compartilha voluntariamente seus dados com fraudadores, permitindo golpes (p.ex. money muling – "mulas" financeiras que emprestam suas contas a criminosos em troca de comissão).

Como desafios e oportunidades, os instrutores mencionaram que os riscos de fraude podem ficar "fragmentados" devido à própria estrutura matricial das organizações. O workshop listou dificuldades como: múltiplos tipos de fraude (internas, externas, cibernéticas, etc.), diferenças culturais para lidar com os riscos entre cada instituição, visibilidade limitada quando dados estão dispersos, e complexidade de mapeamento de riscos em tantos produtos e unidades. Além disso, funções relacionadas (operações de fraude, compliance, controles internos, TI, segurança) às vezes atuam de forma isolada, e unidades de negócio diversas podem enfrentar problemas de coordenação. Dados fragmentados e ausência de um "dono" único do risco em nível corporativo também dificultam a visão unificada. Diante disso, a recomendação foi clara: consolidar e centralizar o processo de FRA para obter uma visão completa dos riscos de fraude tanto no nível global do banco quanto em cada unidade de negócio.

Essa consolidação inclui compartilhar dados entre filiais, padronizar indicadores e centralizar relatórios, permitindo identificar padrões de fraude que transitam entre departamentos ou países. Para auditores, isso significa verificar se grandes conglomerados possuem algum comitê central ou função corporativa coordenando a gestão de fraude de todas as subsidiárias, evitando "silos" informacionais.

Já no workshop B – Navigating KYC Challenges in Virtual Asset Industry - foram destacados desafios específicos relacionados ao Know Your Customer (KYC) no setor de ativos. Foram abordadas definições do FATF/GAFI sobre ativos virtuais e prestadores de serviços relacionados (VASPs). Regulamentações internacionais, como a Travel Rule do FATF, exigindo coleta e compartilhamento de informações em transferências de criptoativos, por exemplo. A abordagem baseada em riscos foi recomendada, considerando fatores do produto, do cliente e geográficos. Também foram citados procedimentos contínuos de monitoramento de transações e atualizações periódicas dos dados dos usuários, bem como exemplos de falhas graves de KYC em casos reais (Block/Cash App, Coinbase Payments).

O workshop reforçou que VASPs devem aplicar os mesmos controles básicos de KYC/AML de instituições tradicionais. Isso inclui**: identificação formal de usuários e beneficiários finais, verificação documental, classificação de risco, monitoramento de transações, retenção de registros e reporte de atividades suspeitas**. Foi destacada também a importância do *Customer Due Diligence*, que impõe quatro requisitos centrais às instituições financeiras:

- Identificar e verificar a identidade dos clientes: coleta de dados cadastrais, documentos de identificação, validação de autenticidade.

- Identificar e verificar beneficiários finais (no caso de pessoas jurídicas): obter informação de quem detém >25% do capital ou controla a empresa, por exemplo.
- Entender a natureza e propósito do relacionamento: para traçar um perfil de risco do usuário (ex.: qual uso pretendido da conta, volume esperado, origem dos recursos), permitindo comparar comportamento real versus esperado.
- Conduzir monitoramento contínuo: acompanhar transações do usuário de forma contínua a fim de identificar atividades suspeitas e manter as informações atualizadas (incluindo revalidação periódica de dados do cliente conforme seu risco).

Tais pilares são aplicáveis globalmente **como boas práticas**. O *workshhop* enfatizou que VASPs precisam implementar procedimentos escritos para atender a todos esses pontos. Além disso, como parte do Monitoramento e Supervisão Contínuos, foram listados requisitos específicos, como:

Identificação do Cliente: verificar identidade incluindo coleta de dados pessoais e documentos de identificação antes de iniciar o relacionamento

Avaliação de Risco do Cliente: atribuir um nível de risco a cada cliente com base em padrão de transações, localização geográfica e atividades declaradas

Monitoramento Contínuo: monitorar transações em tempo real ou periódico para detectar atividades suspeitas e assegurar conformidade contínua com normas AML

Diligência Aprimorada: aplicar medidas reforçadas para clientes de risco elevado (p.ex. revisão mais frequente, requerer informações adicionais, aprovação sênior para certas transações)

Reporte de Operações Suspeitas: reportar prontamente às autoridades quaisquer indícios de lavagem ou financiamento do terrorismo

Guarda de Registros: manter registros detalhados de informações de clientes e histórico de transações por período mínimo definido em lei, de forma a suportar auditorias e investigações futuras.

Foram também citadas tipologias de lavagem de dinheiro, algumas clássicas, mas que continuam relevantes no mundo atual (com os novos desafios envolvendo criptomoedas e internacionalização do crime organizado):

- *Layering* de múltiplas conversões: enviar fundos através de várias exchanges/corretoras ou converter entre várias criptomoedas ("*chain-hopping*") para ofuscar a trilha e dificultar seguir a origem;
- Uso de jurisdições de alto risco: transacionar com países sem controles rigorosos, aproveitando arbitragem regulatória para reduzir a chance de reporte;
- Informações inconsistentes de usuários: dados cadastrais conflitantes ou comportamento incompatível com perfil (ex.: cliente de perfil renda baixa movimentando grandes quantias) podem sinalizar uso de laranjas ou contas de fachada;
- Movimentação rápida de fundos: depósitos seguidos de retiradas rápidas para outras plataformas ou conversão imediata para moeda fiduciária, visando evitar detecção antes que alarmes possam ser disparados.

Além destes, permanecem riscos como anonimização do usuário (especialmente no contexto pós legislação de privacidade), *Self-Hosted Transactions* (transações com organizações, países que não seguem regulações) e o uso de plataformas descentralizadas para pagamento, transferências, o que dificulta o rastreamento dos recursos de origem ilícita.

Foram também analisados 3 estudos de caso, envolvendo o contexto de ativos, lavagem de dinheiro e recuperação de recursos.

O segundo e o terceiro dias contaram com apresentações sobre os temas do evento. Algumas sessões foram simultâneas, o que impediu a participação na totalidade. De forma a evitar que o relatório fique mais extenso do que já está, foram selecionadas palestras para este relatório.

A sessão "*Preventing Financial Crime*" abordou técnicas inovadoras em inteligência comportamental e análise de vínculos para prevenção de fraudes e crimes financeiros. Foram apresentadas técnicas como monitoramento de comportamento digital dos usuários (biometria comportamental), detecção de dispositivos compartilhados, e análise de horários anômalos de acesso às contas. Ressaltou-se a importância de integração de dados entre diferentes áreas para identificação proativa de fraudes complexas e redes criminosas.

A abordagem envolve analisar aplicativos atípicos instalados em conjunto com apps de pagamento ou bancário, de forma a identificar eventual ligação com o crime organizado. Também envolve analisar aspectos como:

- Horário de uso (*Nocturnal Users*): Analisando grandes volumes de dados, identificam-se "usuários noturnos" (atividade concentrada na madrugada) em contraste com padrões normais de uso da base. Um cliente legítimo médio teria poucas sessões em horários muito tardios, ao passo que contas fraudulentas (controladas por quadrilhas muitas vezes operando de outros fusos horários) mostram acessos predominantes em horários incomuns. Detectar essa discrepância de horário pode sinalizar contas invadidas ou *bots* executando transações automatizadas fora do expediente do usuário real.
- Dispositivos Compartilhados ("*Communal device*"): Situações em que múltiplas contas bancárias reportadas por fraude acessam o serviço a partir de um mesmo dispositivo (mesmo tablet ou telefone). Isso indica que o dispositivo pode estar sendo usado em esquema organizado – por exemplo, um *fraud farm* onde agentes alternam entre várias credenciais roubadas num só aparelho. Identificar essa situação pode ajudar a desvendar redes de fraude (ligando contas aparentemente distintas).
- Padrões de digitação e comportamento do cursor: Analisar dados como velocidade de digitação, pressões de tecla, movimentos do mouse etc. para diferenciar usuário legítimo de impostor/*hacker*.

Além de outros aspectos, esta sessão mostrou que compreender bem o usuário (por meio do KYC) e com quem e onde ele transaciona pode ajudar a identificar red *flags*.

Já a sessão "*Putting the "P" into KYC*" destacou o conceito de KYC Perpétuo (pKYC), recomendando monitoramento contínuo e em tempo real das informações e atividades dos clientes, em contraste com revisões periódicas tradicionais. O uso de tecnologias integradas, automação e segmentação por risco foram sugeridos para aumentar eficiência operacional e conformidade regulatória, prevenindo fraudes e lavagem de dinheiro de forma mais dinâmica e eficaz.

A premissa foi que os programas tradicionais de KYC, baseados em revisões periódicas fixas, são muitas vezes ineficientes e não capturam mudanças rápidas no perfil de risco – daí a necessidade de incorporar um monitoramento contínuo impulsionado por dados em tempo real e automação.

Dessa forma, o KYC precisa ser "perpétuo", avaliando não só desvios transacionais, mas também mudança de jurisdição, alterações de comportamento, com novas checagens anti-lavagem de dinheiro a cada alteração no cadastro da conta. Houve também debate intenso sobre a inovação e a conformidade regulatória.

A sessão "*New Tech, New Rules: Reining in AI*" discutiu o impacto da inteligência artificial (IA) em crimes financeiros, incluindo riscos associados a fraudes sofisticadas, ataques cibernéticos e exposição de dados pessoais. Destacou-se o novo marco regulatório europeu, o AI Act, que classifica os sistemas de IA por nível de risco e estabelece exigências proporcionais, especialmente para aplicações de alto risco em setores críticos, como o financeiro. A apresentação sugeriu o uso de tecnologias avançadas para reforçar autenticação e monitoramento, enfatizando a necessidade de governança robusta sobre modelos de IA.

As recomendações envolveram usar a IA contra a IA, especialmente:

Autenticação Reforçada:

IA para verificação de identidade: uso de reconhecimento facial, de voz e outras biometrias com algoritmos avançados para autenticação de usuários (por exemplo, comparando *selfie* com documento de identidade de modo automatizado). Essas IAs conseguem detectar sutilezas (padrões faciais) e até sinais de *deepfake* (ex.: ausência de piscada natural).

Autenticação multifator & *Blockchain*: implementação de sistemas baseados em *blockchain* para autenticar identidades ou dispositivos de forma distribuída.

Detecção de Atividades Ilícitas:

Machine Learning nos alertas: IAs podem vasculhar transações e contas em tempo real identificando padrões complexos de lavagem, muito além de regras fixas. Modelos treinados com casos históricos aprendem anomalias sutilmente correlacionadas (sequências de transferências, estruturação de depósitos, etc.) e priorizam alertas verdadeiros.

Análise de *Blockchain*: Rastreio de movimentações em cadeias públicas, ligando endereços a entidades conhecidas (ex.: associando um endereço Bitcoin a uma *exchange*, ou a um *dark market* identificado). Isso permite seguir o rastro de fundos suspeitos de/para instituições e detectar conexões com esquemas ilegais.

Monitoramento em tempo real: Combinação de IA e automação para acompanhar fluxos conforme acontecem, sinalizando atividades fora do normal instantaneamente. Por exemplo, análise de transações financeiras em milissegundos com bloqueio das com alta probabilidade de fraude antes da conclusão.

Na Sessão "Smells Suspicious: Prestige Perfumes Money Laundering" foi relatado caso real de lavagem de dinheiro envolvendo a empresa Prestige Perfumes, investigada pelo Ministério Público dos Países Baixos com cooperação internacional. A lavagem foi realizada por meio de operações comerciais fictícias com empresas de fachada em diversos países. Indicadores de alerta incluíram transações incompatíveis com atividades declaradas, pagamentos de entidades opacas, e diferenças entre fluxos financeiros e físicos. A investigação comprovou a origem criminosa dos fundos ligados ao tráfico internacional de drogas, destacando a importância da cooperação internacional e análise de inteligência financeira detalhada.

As autoridades holandesas começaram as investigações em 2021, comparando fluxos financeiros da empresa com os fluxos reais de mercadorias. Ao aprofundar as investigações, abriram-se duas novas rotas: uma francesa (pela empresa *Societé Nova*) e outra paraguaia (*Classica Company*), o que levou à comprovação da origem criminosa dos recursos, além da apreensão de dinheiro, ouro e drogas.

Os principais alertas (*red flags*) do caso envolveram:

- Incompatibilidade entre transações financeiras e atividade econômica declarada: A Prestige Perfumes (e empresas relacionadas) apresentavam fluxos de pagamento que não batiam com seu ramo/natureza empresarial. Perfume é um produto relativamente estável e com margens limitadas; movimentações em milhões de euros fugiam do padrão.
- Pagadores/recebedores terceiros sem relação aparente com o cliente: Muitos pagamentos à Prestige vinham de terceiros sem conexão lógica (empresas de setores distintos, países distintos). Não havia justificativa comercial para tais transações, indicando interposição de laranjas.
- Referências de pagamento incoerentes com bens/serviços fornecidos: Descrições de transferências mencionavam itens sem ligação com perfumes ("segurança", "limpeza", "produção"), sugerindo tentativa de maquiar finalidade.
- Diferenças entre valores de faturas e montantes pagos: Pagamentos maiores ou em número diferente do que constava em faturas comerciais (indicando trocas financeiras travestidas de pagamento comercial).
- Origem dos fundos divergindo do destino das mercadorias: dinheiro vindo de país X para pagar suposta exportação para país Y, sem conexão, ou montantes vindo de vários países enquanto os produtos físicos teriam destino diferente.
- Mudanças frequentes e não explicadas nos terceiros pagadores: A rede trocava constantemente as empresas usadas para enviar dinheiro, em uma tentativa de diluir e confundir o rastreamento.
- Pagamentos de entidades opacas sediadas em jurisdições de alto risco: Uso de contas em países com alto risco.
- Beneficiário final desconhecido: Estruturas societárias complexas ou acionistas de fachada tornavam difícil identificar quem se beneficia dos valores.

Já a sessão "Fraud Prevention Lifecycle" apresentou abordagem integrada para prevenção de fraudes, enfatizando a necessidade de quebrar silos internos e unificar processos como análise de fraudes, tecnologia, estratégia e operações antifraude. Foi ressaltado que criminosos estão utilizando múltiplos canais, exigindo maior coordenação e integração das equipes de prevenção. Também foi discutido o uso de inteligência artificial generativa para melhorar eficiência operacional, aprimorar detecção de fraudes e automatizar processos.

Dessa forma, foi destacada a importância da integração das etapas do ciclo de prevenção a fraudes, ressaltando que essas práticas criminosas estão cada vez mais sofisticadas e distribuídas por diversos canais. Foi salientado que criminosos iniciam ataques por canais externos, como redes sociais, antes de atingir canais internos. Assim, sistemas tradicionais, separados por canais, mostram-se inadequados para identificar conexões relevantes que poderiam impedir esquemas maiores.

Para enfrentar esse cenário complexo, foi proposta a unificação das equipes internas de prevenção a fraudes, como operações, *analytics*, TI e segurança, sob uma coordenação centralizada, criando maior probabilidade de prevenção e resposta. Essa integração permite visão holística do cliente, otimizando processos como análise preditiva, desenvolvimento de tecnologia antifraude, estratégias alinhadas à tolerância ao risco e operações que continuamente aperfeiçoam os sistemas com base no feedback das investigações realizadas.

Além disso, foram destacadas áreas prioritárias de investimento que refletem tendências globais, incluindo uso de inteligência artificial para melhorar detecção, monitoramento de "mulas financeiras", educação preventiva de usuários e controles rigorosos na abertura de contas. Por fim, foi sugerido o uso de IA generativa como potencial inovação, embora com ressalvas quanto à maturidade e riscos associados. Para auditorias, foi recomendado verificar se as instituições adotam essa abordagem integrada e se estão investindo adequadamente nas áreas identificadas como de maior risco.

ENCAMINHAMENTOS POSSÍVEIS, NO ÂMBITO DO TCU, DECORRENTES DESTA AÇÃO

Como o propósito da participação do evento era desenhar melhor as auditorias da AudDefesa nesses temas, os encaminhamentos são:

- Considerar o setor financeiro e o Banco Central como *stakeholders* essenciais no processo de KYC e contra lavagem de dinheiro.
- Incorporar como risco dos objetos das auditorias a existências das "mulas financeiras".
- Incluir como critérios nas auditorias: *Framework FRA, Perpetual KYC* (com todos os seus requisitos), *Travel Rule* FATF/GAFI, *Customer Due Diligente* (CDD), tipologias de fraude, tipologias de lavagem de dinheiro, *Fraud Prevention* Cycle (FPC).
- Incorporar os alertas (*red flags*) do caso Prestige Perfumes nas avaliações a serem realizadas.
- Adotar como boa prática a estrutura de regulação de fraude (TFEU, LOCAF, EPPO, PSD2/PSD3, IPR, MiCA), bem como as diretivas anti lavagem de dinheiro da União Européia.
- Incentivar o uso de Análise Comportamental de Dados para prevenção de golpes digitais e lavagem de dinheiro.
- Incentivar o uso de IA para combater golpes e fraudes gerados com IA, seguindo o princípio de "paridade de armas", bem como análise *blockhain*, *machine learning* e outras tecnologias.
- Avaliar organismos governamentais responsáveis por procedimentos aduaneiros e comerciais e sua capacidade de detectar sinais de lavagem de dinheiro baseada em comércio.
- Promover cooperação técnica internacional com as autoridades financeiras europeias para trocas de melhores práticas e informações
- Incentivar mudança regulatória que impulsione integração entre as áreas de prevenção de fraudes nas instituições financeiras.
- Incentivar mudança regulatória que oriente o processo de KYC de acordo com os riscos do produto, do cliente e geográfico.
- Avaliar práticas de monitoramento contínuo do COAF e outros reguladores.
- Incentivar que os controles de prevenção a fraude contenham análises de *device sharing*, detecção de *bots*/automação e perfil comportamental.
- Identificar maneiras de fornecer segurança jurídica aos órgãos que combatem fraude, dado o cenário trazido pela LGPD.
- Incentivar melhor governança de dados no setor público, abrangendo *data quality*, centralização de cadastro e compartilhamento de dados e informações.