

El uso de las Tecnologías Emergentes en la Prevención de Lavados de Activos y Financiamiento del Terrorismo (Resumen del Artículo de difusión fin del Máster en Compliance, Fraude y Blanqueo especialidad en Análisis Forense e Inteligencia Financiera)



Autores (por el orden de fotos): Yurissa Bibely Chez Gastón, CCO., MBA., MCFB., Eduardo Antonio Risk Hernández, Lcdo., MCFB., Karla Escaño Hidalgo, Lcda., MCFB., Alexis Olivo, CPA., AFA, MBA., MCFB.

Las tecnologías emergentes, como blockchain, inteligencia artificial y machine learning, están transformando la forma en que las empresas operan, sin embargo, al mismo tiempo, están proporcionando nuevas herramientas y oportunidades para el lavado de activos y financiamiento del terrorismo.

La combinación de estas tecnologías puede generar un ecosistema robusto para la detección y la prevención del LA/FT, ofreciendo un enfoque eficaz y proactivo para la adaptación de los sujetos obligados a un entorno que es cada vez más complejo y en evolución constante. La implementación de estas tecnologías no solo mejora la detección y la prevención del LA/FT, sino que también fortalece la confianza en el sistema macroeconómico mundial.

El Blockchain proporciona un sistema novedoso que mejora de manera significativa la capacidad de los sujetos obligados en la prevención de LA/FT, creando un entorno con mayor seguridad y eficiencia para gestionar todo tipo de transacciones financieras, sin embargo de la misma forma presenta riesgos que benefician el LA/FT como son:

- Anonimato en transacciones
- Dificultad para rastrear flujos de fondos digitales como las criptomonedas que utilizan blockchain
- Uso de plataformas descentralizadas que pueden operar sin intermediarios, dificultando la identificación de los actores involucrados.

La Inteligencia Artificial es aplicada en la prevención de LA/FT a través de tecnologías avanzadas para identificar y mitigar actividades sospechosas en las transacciones de negocios. Con la IA, los sistemas de procesamientos de datos pueden analizar grandes volúmenes de transacciones para identificar patrones inusuales con indicios de LA/FT e incluso predecir comportamientos sospechosos generando alertas automáticas sobre los mismos.

De igual forma la Inteligencia Artificial representa una herramienta poderosa para las actividades ilícitas ya que la misma puede utilizar datos para ocultar la identidad de beneficiarios finales, manipular los algoritmos de legitimación de fondos, entre otras aplicaciones para dificultar la trazabilidad de las operaciones.

El Machine Learning es una dimensión de la inteligencia artificial a través de la cual las computadoras “aprenden” sobre el procesamiento de datos para mejorar tareas específicas sin ser programadas específicamente para ello. Con la utilización de algoritmos analiza patrones en los datos para hacer predicciones y tomar decisiones.

La inteligencia artificial se apoya en el machine learning en la prevención del LA/FT

Esta permite a los sujetos obligados gestionar los riesgos de manera proactiva y efectiva, automatizando y optimizando los procesos de detección contribuyendo así a un sistema de gestión de riesgo más integro y seguro.

Al igual que las tecnologías mencionadas anteriormente, esta puede presentar riesgos en algunas aplicaciones de esta para el área de cumplimiento, tales como:

- **Tecnologías de Contratos Inteligentes:** impone un riesgo en la complejidad de la comprensión de los contratos y la posibilidad del uso malintencionado en proyectos no regulados.
- **Redes Sociales y Marketing Digital:** pueden promocionar productos o servicios usados para el lavado de activos, ayudando en la creación de perfiles empresariales falsos para sustentar sus operaciones fraudulentas.
- **Tecnologías de Identificación Digital:** permiten la posibilidad de suplantación de identidad, dificultando el uso de la verificación de identidades en línea.

Uno de los desafíos principales de las mencionadas tecnologías es el uso responsable y ético de las mismas, no solo del capital humano que los supervisa y regula, sino también de la dependencia hacia la tecnología y la deshumanización de los procesos, haciendo crucial el balance entre la automatización y la intervención humana para la aplicación del juicio y ética en determinadas circunstancias.

La Unión Europea (UE) ha tomado la delantera en la formulación de marcos regulatorios y directrices éticas para garantizar que estas tecnologías se utilicen de una manera responsable y beneficiosa para la sociedad. Los principios éticos establecidos por la Comisión Europea para el uso de la inteligencia artificial deben considerar: a) Humanos como el centro (considerando en su diseño y uso el respeto y la dignidad humana), b) Transparencia (Ser comprensibles y los resultados explicables), c) No discriminación (debe evitar sesgos y discriminación), d) Seguridad y protección (debe operar de manera segura y proteger los datos sensibles).

Otro desafío es la recopilación y análisis de grandes volúmenes de datos, lo que implica un riesgo latente de privacidad y protección de datos. Por su parte, la falta de supervisión y monitoreo de los algoritmos utilizados en la inteligencia artificial y el machine learning pueden perpetuar sesgos existentes o malintencionados en los parámetros predictivos, debido a que, a su vez, el riesgo de ciberataques y violaciones de seguridad aumenta cuando se implementan este tipo de tecnologías en los sistemas de información.

Concluimos el presente artículo con la siguiente anécdota y reflexión:

“Tomando en su mano a una pequeña mariposa y cerrando su puño, alguien pregunto a un sabio, ¿la mariposa que tengo en las manos vive o muere? Si el sabio respondía que vivía la apretaría hasta que muriera aplastada y si respondía que estaba muerta simplemente abriría su mano para que esta se fuera volando; la respuesta del sabio como tal fue muy atinada, le respondió: Esta en tus manos y en la intención de tu corazón el que viva o muera”.

El uso de la tecnología puede ser un gran aliado o formidable adversario en la lucha contra el crimen organizado, la diferencia la marca el compromiso ético y buen grado de conciencia asumido por parte de sus originadores y usuarios.

Referencias

Prevención de Lavado de Activos, Financiamiento del Terrorismo y Proliferación de Armas de Destrucción masiva. (2019)

<https://dgii.gov.do/legislacion/prevencionLavado/informacionEspecializada/Documents/BrochureLavadoDeActivos.pdf> ¿Qué es lavado de activos? (2019). - <https://www.uaf.cl/lavado/> Tecnologías

Emergentes. (2023) -<https://startupeable.com/glosario/tecnologías-emergentes/> 'Machine learning': ¿qué es y cómo funciona el maestro en reconocer patrones? (2024). -

<https://www.bbva.com/es/innovacion/machine-learning-que-es-y-como-funciona/> Mariano Sánchez y Luisa Caicedo. Nuevas tecnologías en IA para la prevención del LA/FT. (2023).-

<https://www.compliance.com.co/nuevas-tecnologias-en-ia-para-la-prevencion-del-la-ft/> FATF (Financial Action Task Force). (2021). “Guidance on Digital Identity”. Recuperado de: FATF. FATF. (2020).

"Guidance on Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers". Recuperado de: FATF. United Nations Office on Drugs and Crime (UNODC). (2020). "The Use of Artificial

Intelligence in Crime Prevention and Criminal Justice". Recuperado de: UNODC. European Union Agency for Cybersecurity (ENISA). (2020). “Blockchain and Virtual Currencies: Risks and Reporting Obligations”. Recuperado de: ENISA.