Anti-Money Laundering Controls in the Era of Digital Banking

Maria Fernanda Montoya Ruiz[1]; Sheyla Dayana Paredes García[1]; Alisson Alicia Saravia Puchuc[1], Renato Oswaldo Martínez López[1]; Wilfredo Galindez Azorza[1]

[1]Facultad de Ciencias Empresariales, Carrera de Contabilidad y Finanzas, Universidad de Lima, Perú

20211766@aloe.ulima.edu.pe, 20194412@aloe.ulima.edu.pe, 20194594@aloe.ulima.edu.pe, romartin@ulima.edu.pe, wgalinde@ulima.edu.pe

Abstract- This study analyzes the role of internal controls in the prevention of money laundering within digital banking platforms. Based on a systematic literature review (SLR) of articles indexed in Scopus between 2019 and 2025, it examines the risks associated with the digital environment, the technological tools applied, and the main challenges for financial institutions. The theoretical framework is based on the COSO model and GAFILAT recommendations, highlighting the importance of components such as the control of the environment, risk assessment, and staff training. The results show that, although digital technologies offer efficiency and accessibility, they also increase the complexity of detecting illicit operations. Consequently, the need to adapt internal controls to the new digital dynamics through automated systems, robust compliance policies and an organizational culture oriented to risk management is reinforced.

Keywords- Internal Control, Money Laundering, Artificial Intelligence, Digitalization

Controles Anti-Lavado de Dinero en la Era de la Banca Digital

Resumen- El presente estudio analiza el papel de los controles internos en la prevención del lavado de activos dentro de las plataformas digitales bancarias. A partir de una revisión sistemática de literatura (SLR) de artículos indexados en Scopus entre 2019 y 2025, se examinan los riesgos asociados al entorno digital, las herramientas tecnológicas aplicadas, y los principales desafíos para las entidades financieras. El marco teórico se apoya en el modelo COSO y en las recomendaciones del GAFILAT, destacando la importancia de componentes como el entorno de control, la evaluación de riesgos y la capacitación del personal. Los resultados evidencian que, si bien las tecnologías digitales ofrecen eficiencia y accesibilidad, también incrementan la complejidad en la detección de operaciones ilícitas. En consecuencia, se refuerza la necesidad de adaptar los controles internos a las nuevas dinámicas digitales mediante sistemas automatizados, políticas de cumplimiento robustas y una cultura organizacional orientada a la gestión del riesgo.

Palabras clave- Control Interno, Lavado de Activos, Inteligencia Artificial, Digitalización.

I. INTRODUCCIÓN

En los últimos años, el crecimiento masivo de las plataformas digitales en el sector bancario ha transformado radicalmente la forma en que los usuarios acceden y gestionan productos financieros. Esta evolución, impulsada por la digitalización y el uso intensivo de tecnologías como la inteligencia artificial, Big Data y la automatización de procesos, ha permitido una mayor inclusión financiera y eficiencia operativa. Sin embargo, también ha incrementado los riesgos asociados al lavado de activos, especialmente por el uso de canales digitales que pueden facilitar el anonimato, la fragmentación de transacciones y la velocidad de movimientos sospechosos.

De esta manera, aunque los gobiernos han implementado medidas para combatir el lavado de dinero, sus efectos sobre los métodos y precios de blanqueo siguen siendo en gran parte desconocidos. Esto es relevante al considerar los desafíos que enfrentan las plataformas digitales en la detección de actividades ilícitas [1].

Siendo así, el lavado de activos representa una de las principales amenazas para la integridad del sistema financiero, ya que permite incorporar al circuito económico formal recursos provenientes de actividades ilícitas. En respuesta, las instituciones bancarias están obligadas a implementar controles internos sólidos, orientados a la identificación, monitoreo y reporte de operaciones sospechosas, en línea con estándares internacionales como los del Grupo de Acción Financiera Internacional [GAFI] y las normativas locales como las emitidas por la Superintendencia de Banca, Seguros y AFP [SBS]

Este trabajo tiene como objetivo identificar los controles internos implementados para la prevención del lavado de activos en la era de la banca digital. La investigación se desarrollará bajo un enfoque cualitativo y documental, con base en normativa vigente, literatura académica y casos referenciales de aplicación práctica.

II. MARCO TEÓRICO

A. Lavado de activos

Según el glosario de definiciones de GAFILAT [2], el lavado de activos es un procedimiento utilizado para dar una apariencia legítima a dinero obtenido de actividades ilegales. Su objetivo es ocultar la fuente original del dinero, permitiendo que pueda ser usado sin que se detecte su origen delictivo.

Este proceso consta de tres etapas:

1. Colocación: Esta es la primera etapa, donde el dinero obtenido de actividades ilegales se introduce en el sistema financiero. Esto puede hacerse mediante depósitos bancarios, compras de bienes de alto valor, o incluso a través de negocios que manejan grandes cantidades de efectivo, como casinos o restaurantes. El objetivo es colocar el dinero en el sistema sin levantar sospechas.
2. Estratificación: En esta etapa, se realizan múltiples transacciones para distanciar aún más el dinero de su origen ilícito. Esto puede incluir transferencias bancarias entre diferentes cuentas, tanto nacionales como internacionales, compra y venta de activos, o cualquier otra actividad que complique el rastreo del dinero. La estratificación busca crear una compleja red de movimientos financieros que dificulte a las autoridades seguir la pista del dinero.
3. Integración: Finalmente, el dinero regresa a la economía formal como si fuera legítimo. En esta etapa, los fondos "limpios" se utilizan para inversiones legales, como la compra de propiedades, negocios o activos financieros. A este punto, el dinero se presenta como ingresos legítimos, permitiendo a los lavadores disfrutar de sus ganancias sin despertar sospechas.

B. Control interno

Según el marco COSO**,** los controles internos son políticas, procedimientos y actividades implementadas por una organización para garantizar la gestión adecuada de riesgos, la confiabilidad de la información financiera y el cumplimiento normativo. Estos controles se agrupan en cinco componentes [3]:

1. Entorno de control: Establece la base ética y cultural, determinando la actitud organizacional hacia el control.
2. Evaluación de riesgos: Identifica y prioriza riesgos internos y externos, permitiendo anticiparse a desafíos.
3. Actividades de control: Implementa políticas y procedimientos para mitigar riesgos.

4. Información y comunicación: Asegura que la información relevante se transmita de manera oportuna y precisa.

5. Monitoreo: Verifica la eficacia continua de los controles internos y permite ajustes necesarios.

C. Exposición de las plataformas digitales al lavado de activos

El lavado de activos en entornos digitales ha aumentado debido a la rapidez y anonimato que ofrecen las nuevas tecnologías financieras [4]. Esta situación ha obligado a organismos como el GAFI a exigir controles más estrictos y enfoques preventivos, especialmente sobre activos virtuales y servicios financieros digitales, ante el creciente riesgo de operaciones ilícitas.

Las entidades financieras, como principales intermediarios en el flujo de capital dentro de la economía formal, enfrentan un riesgo significativo de lavado de activos debido a la naturaleza de sus operaciones asociado a la ciberseguridad. Manejan grandes volúmenes de dinero, tanto en efectivo como electrónico, y participan en una amplia gama de operaciones nacionales e internacionales [5]. Con la introducción y expansión de plataformas digitales, estas entidades han transformado su forma de operar, ofreciendo servicios a través de aplicaciones móviles, banca en línea, billeteras digitales y otras herramientas tecnológicas avanzadas.

Las plataformas digitales bancarias han traído consigo una serie de beneficios, como la conveniencia y accesibilidad para los usuarios, quienes pueden realizar operaciones financieras desde cualquier lugar y en cualquier momento sin necesidad de acudir a una sucursal física. Sin embargo, esta virtualización también ha incrementado la exposición a riesgos de lavado de activos. La naturaleza digital de estas plataformas permite la realización de transacciones de alto volumen con un nivel de anonimato superior al de las operaciones tradicionales, lo cual puede ser explotado para integrar dinero ilícito en el sistema financiero de manera rápida y discreta.

El entorno digital incrementa los riesgos debido a lo siguiente [6]:

1. Las plataformas digitales permiten realizar un gran número de transacciones rápidamente y, a menudo, con un nivel de anonimato mayor que en las operaciones bancarias tradicionales. Esta capacidad de mover fondos de manera rápida y discreta puede ser explotada para integrar dinero ilícito en el sistema financiero.

2. La facilidad con la que se pueden abrir cuentas digitales, a menudo sin necesidad de presencia física, incrementa el riesgo de que individuos malintencionados establezcan múltiples cuentas bajo identidades falsas o robadas para mover fondos ilícitos sin levantar sospechas.

3. Algunas plataformas digitales permiten transacciones con criptomonedas, que son menos reguladas y ofrecen un mayor grado de anonimato. Esto dificulta el rastreo de fondos y puede ser aprovechado para ocultar el origen de activos ilícitos.

4. Las plataformas digitales operan a nivel global, lo que permite a los delincuentes transferir fondos a través de múltiples jurisdicciones rápidamente. Esto complica el rastreo y la recuperación de fondos, especialmente cuando se trata de países con regulaciones más laxas.

5. La capacidad de realizar operaciones complejas, como transferencias entre múltiples cuentas y conversiones rápidas de moneda, proporciona a los lavadores de dinero herramientas efectivas para ocultar y mover activos ilícitos sin detección inmediata.

6. Las plataformas digitales son vulnerables a ciberataques que podrían comprometer la seguridad de las cuentas y permitir el acceso no autorizado para mover fondos ilícitos.

7. Automatización y falta de interacción humana: La automatización de procesos en las plataformas digitales puede reducir la capacidad de detectar comportamientos anómalos que podrían indicar lavado de dinero, ya que falta la intervención humana que podría notar irregularidades sutiles.

8. Innovación tecnológica rápida: La rápida adopción de nuevas tecnologías en el sector bancario digital puede superar la capacidad de los sistemas de cumplimiento para adaptarse, dejando brechas que los delincuentes pueden explotar antes de que se implementen controles efectivos.

9. Desafíos regulatorios: Las diferencias en las regulaciones de lavado de dinero entre diferentes jurisdicciones pueden ser aprovechadas por los lavadores de dinero para diseñar esquemas que eviten la detección, especialmente cuando las plataformas digitales operan a través de fronteras internacionales.

III. METODOLOGÍA

La presente investigación posee un enfoque cualitativo, que según Hernández-Sampieri [7], se refiere a aquella investigación que busca estudiar fenómenos de manera sistemática enfocándose en una revisión de la literatura. Asimismo, se aplica la técnica de Revisión Sistemática de Literatura [SLR], por sus siglas en inglés, con el objetivo de recopilar, analizar y sintetizar de manera rigurosa los estudios académicos existentes sobre los controles internos frente al lavado de activos en plataformas digitales bancarias. Este enfoque permite obtener una visión global, ordenada y crítica del estado actual del conocimiento en el tema.

Para reforzar la validez del proceso de búsqueda y selección de artículos, se aplicó la Declaración PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), la cual establece un conjunto de pasos y diagramas que aseguran la transparencia en la inclusión y exclusión de estudios, así como en la identificación de sesgos, tal como se muestra en la Tabla 1.

TABLA 1
ECUACION DE BUSQUEDA PARA SCOPUS

Ecuación de la búsqueda para Scopus
"internal control" OR "compliance" OR "regulation" OR "oversight") AND ("money laundering" OR "AML" OR "financial crime" OR "illicit finance") AND ("digital banking" OR "online banking" OR "e-banking" OR "fintech") AND ("risk management" OR "fraud prevention" OR "security measures" OR "monitoring") AND ("transaction monitoring" OR "due diligence" OR "reporting" OR "audit"

Como se aprecia en la Tabla 1, el uso combinado de términos permitió abarcar literatura tanto académica como práctica.

A. Planeamiento de la investigación y estrategia de búsqueda

En esta etapa se presenta la identificación del objetivo de la investigación el cual es identificar los controles internos para la prevención de lavados de activos en la era de la banca digital. Para ello, se realizó una búsqueda automática en la base de datos de Scopus. Para esta revisión se consideró desde el año 2019 al año 2025 con el propósito de tener artículos recientes y de relevancia.

Siendo así, con el fin de obtener los artículos más importantes se definieron los términos de búsqueda "control", "compliance", "financial crime", "money-laundering", "digital banking", "Fintech", resultando en la ecuación de la búsqueda presentada en la Tabla 1.

B. Criterios de selección de estudios

Tras aplicar los términos de búsqueda en la base datos bibliográficos de Scopus, obtuvimos un total de 195 artículos relacionados con el objetivo de la investigación a los cuales se les aplicó los criterios de inclusión y exclusión con fines de identificar los artículos adecuados llegando a un total de 121 artículos y, por último, se le aplicó criterios de calidad (Tabla 3) resultando con 36 artículos a los cuales se les realizó el análisis detalladamente.

TABLA 2
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

N°	Inclusión	Exclusión
1	Documentos del tipo artículo y artículos de conferencias	Documentos del tipo capítulo de libro, artículos cortos, resúmenes y posters
2	Artículos en inglés o español	Artículos en un idioma diferente al inglés o español
3	Artículos de los años 2019 al 2025	Artículos con acceso restringido
4	Artículos relacionados al lavado de activos en banca digital.	

De acuerdo con la Tabla 2, se excluyeron artículos con acceso restringido o en idiomas distintos al inglés y español.

Con el fin de garantizar la validez de los artículos seleccionados, se aplicaron los criterios de calidad que se muestran en la Tabla 3.

TABLA 3
CRITERIOS DE CALIDAD

N°	Criterios
1	¿El artículo es claro en su desarrollo?
2	¿Las técnicas del estudio están adecuadamente definidas?
3	¿El artículo tiene relación con el tema establecido?

La Tabla 3 evidencia que la claridad metodológica fue un criterio determinante en la selección final

C. Extracción de los datos y síntesis.

Luego de aplicar los criterios de selección y calidad, obtuvimos un total de 36 artículos. A partir de estos, se extrajo un archivo de datos en formato .csv para su posterior procesamiento, los datos se descargaron directamente de Scopus para realizar el metaanálisis.

IV. RESULTADOS

A. Metaanálisis de la literatura

Esta sección presenta los controles internos para la prevención de lavado de activos en la era de la banca digital mediante casuística. Se examinaron artículo publicados desde el año 2019 al año 2025. En referencia a la cantidad de artículos publicados, como se visualiza en la Figura 1, el período con menos publicaciones fue el 2021 y posterior a dicho año, el número de publicaciones ha ido en aumento. Ello se puede explicar al crecimiento intensivo del uso de la tecnología en la banca digital lo cual se relaciona con el aumento del riesgo al haber mayor exposición para el lavado de activos.

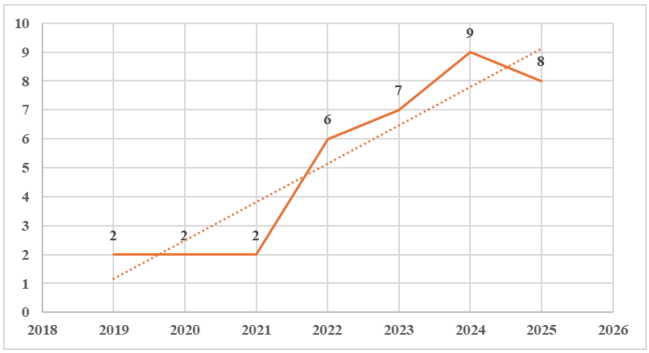

Fig. 1: Cantidad de publicaciones anuales.

En esa línea, cabe mencionar que, de los 36 documentos, el 58.7% son artículos académicos y el 41.3% son conference papers.

Por otra parte, se observa que hay una variedad amplia en relación con las áreas sujetas de las respectivas investigaciones siendo las más relevante, la de Computer Science (23.7%) y la de Social Sciences (15.7%) lo cual se explicaría con que los controles internos implementados cada vez son en su mayoría automáticos, es decir que la tecnología va en aumento.

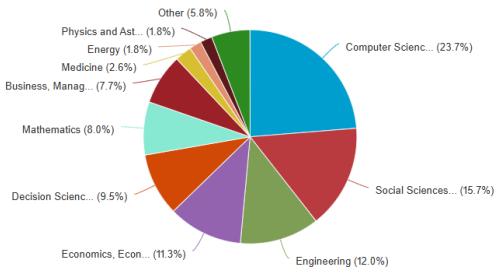

Fig. 2: Publicaciones por área

En correspondencia con el origen de las publicaciones científicas, en la figura 3 se evidencia que, del total de las 36 publicaciones, en gran parte pertenecen a países asiáticos siendo India el líder (24%) e Indonesia (15%) lo cual radica con que la mayoría de los controles automáticos según lo investigado han sido implementados allá en el sector financiero.

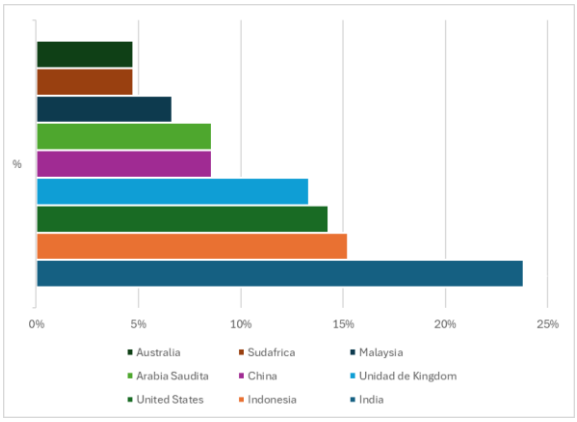

Fig. 3: Publicaciones por país de origen de las publicaciones.

A continuación, se analizará los papers más relevantes acorde a su asociación con el marco COSO para luego examinar el rol de la tecnología en este estudio.

B. Ambiente de control y establecimiento de objetivos

De acuerdo con las 40 recomendaciones del GAFI [8], el principio 18, Programas de cumplimiento interno y auditoría, establecen que las instituciones financieras deben tener programas de cumplimiento sólidos que incluyan políticas, procedimientos y controles internos diseñados para prevenir y detectar el lavado de dinero y el financiamiento del terrorismo. Deben realizar auditorías internas y externas para asegurar la efectividad de estos programas. Este principio se asocia al componente de "Ambiente Interno", ya que promueve un ambiente organizacional que valora el cumplimiento y establece una cultura de riesgo sólida dentro de la organización.

Asimismo, el principio 1: Evaluaciones de riesgo y políticas nacionales enfatiza la necesidad de que los países identifiquen, evalúen y entiendan los riesgos de lavado de dinero y financiamiento del terrorismo, desarrollando políticas nacionales para mitigarlos. Esto requiere un enfoque basado en el riesgo. Por otro lado, el principio 15: Nuevas tecnologías se centran en la necesidad de que las instituciones evalúen los riesgos asociados con el desarrollo de nuevos productos y prácticas de negocio, especialmente aquellos que involucran nuevas tecnologías.

Estos principios aseguran que los objetivos estratégicos de una organización estén alineados con la gestión de riesgos. Para el principio 1, se garantiza que los objetivos estratégicos se definan claramente antes de proceder a la identificación y evaluación de los riesgos, alineándose con la mitigación de estos riesgos. En cuanto al principio 15, se asegura que los objetivos relacionados con la innovación tecnológica consideren los riesgos potenciales desde el inicio, integrando la gestión de riesgos en el proceso de desarrollo e implementación de nuevas tecnologías.

El establecimiento de objetivos, como componente del COSO, es crucial para definir metas claras que alineen el crecimiento organizacional con la mitigación de riesgos asociados al lavado de activos. Establecer objetivos claros permite a las plataformas digitales bancarias priorizar tanto el cumplimiento normativo como la innovación responsable. Al integrar estos principios, el componente de "Ambiente Interno" del marco de control se fortalece significativamente, promoviendo un entorno organizacional que valora el cumplimiento y establece una cultura de riesgo sólida. Esto crea una base sólida para que las organizaciones definan objetivos claros que no solo promuevan el crecimiento y la innovación, sino que también prioricen la mitigación de riesgos.

En el contexto de las plataformas digitales bancarias, establecer un ambiente de control sólido es fundamental para gestionar los riesgos de lavado de dinero y financiamiento del terrorismo, componentes clave del COSO. Este ambiente de control debe incorporar tecnologías avanzadas que permitan un monitoreo efectivo y continuo. Herramientas como la inteligencia artificial y el aprendizaje automático son esenciales para analizar datos en tiempo real y detectar transacciones sospechosas. Un ambiente de control robusto asegura que las plataformas digitales bancarias cumplan con las normativas vigentes, protegiendo la integridad y seguridad de las transacciones y, en última instancia, aumentando la confianza de los usuarios. Esto crea una cultura de cumplimiento y gestión de riesgos que permea toda la organización, alineada con el principio 18 de las recomendaciones del GAFILAT, que promueve un entorno organizacional comprometido con la ética y la transparencia.

Los desafíos que enfrenta la banca india ante fraudes financieros y activos no productivos, destacando cómo las tecnologías emergentes pueden mejorar los sistemas de control y gestión de riesgos. Este enfoque es particularmente relevante para el control del lavado de activos en plataformas digitales bancarias, especialmente en aplicaciones móviles que actualmente concentran gran parte de las transacciones financieras. Los autores subrayan el papel de herramientas digitales como la inteligencia artificial, la automatización robótica de procesos (RPA) y el blockchain para fortalecer los controles internos y prevenir actividades ilícitas [9].

La investigación revela que muchas fallas en los sistemas tradicionales, como la desconexión entre plataformas o la escasa trazabilidad, permiten que operaciones sospechosas no sean detectadas a tiempo. En este sentido, la incorporación de tecnologías avanzadas en las aplicaciones bancarias puede facilitar una supervisión más eficiente y en tiempo real, esencial para identificar patrones irregulares asociados al lavado de dinero. Además, el estudio destaca que el éxito de estas herramientas depende de que el personal bancario tenga las competencias técnicas adecuadas para interpretar alertas y aplicar medidas correctivas.

Por tanto, el artículo refuerza la idea central de que las aplicaciones bancarias deben contar con controles internos robustos para prevenir el lavado de activos en un entorno cada vez más digitalizado y expuesto a riesgos operacionales.

Un sistema de control interno sólido es crucial para mitigar el riesgo de lavado de activos, especialmente en el contexto de las plataformas digitales bancarias. La comunicación interna efectiva y un entorno organizacional bien estructurado son esenciales para identificar y responder rápidamente a posibles amenazas [10]. En las plataformas digitales, donde las transacciones ocurren a gran velocidad, una cultura organizacional que fomente un flujo claro de información es vital para abordar las vulnerabilidades de manera proactiva y eficiente. Aunque la evaluación de riesgos no arrojó resultados concluyentes, un ambiente interno que promueva una comunicación clara y eficaz es clave para enfrentar los desafíos del entorno digital. De la misma manera,

estudios evidencian que durante la pandemia de COVID-19, el ambiente de control en las instituciones financieras de Malasia se vio desafiado por el auge del delito digital y el bajo cumplimiento normativo preexistente [11]. La situación expuso la necesidad urgente de fortalecer los controles internos mediante sistemas digitales resilientes, mayor supervisión automatizada y capacitación del personal para enfrentar eficazmente el lavado de activos en la banca digital.

Por otro lado, estudios examinan el papel de los bancos comerciales en el control del lavado de activos, con un enfoque en el Commercial Bank of Jordan. Este análisis es particularmente relevante para las plataformas digitales bancarias, donde las transacciones son rápidas y complejas [12]. A partir de una muestra significativa de empleados, los autores identifican cinco dimensiones clave que afectan la efectividad de las medidas contra el lavado de dinero: verificación de clientes, cumplimiento de leyes e instrucciones del banco central, procedimientos de control interno, claridad de la evidencia y capacitación del personal. Aunque la verificación de clientes fue altamente valorada, la formación del personal fue considerada de menor prioridad, revelando una debilidad institucional crítica. El estudio subraya que el éxito de los controles internos no solo depende de políticas y normativas, sino también de la capacitación continua del personal. En el entorno digital, donde las operaciones bancarias son más susceptibles al abuso por parte de lavadores de dinero, es fundamental que el personal esté preparado para identificar y manejar actividades sospechosas de manera eficaz, reforzando así la integridad de los controles internos en las plataformas digitales.

En esa misma línea, sobre el control interno del dinero electrónico en las empresas profundizan en el ambiente de control, enfatizando que la existencia de regulaciones claras y procedimientos organizacionales precisos como la verificación documental, la distribución adecuada de responsabilidades y la aprobación por la alta dirección, la cual es esencial para sostener una supervisión confiable de las transacciones digitales [13]. El trabajo destaca que dichos elementos deben estar formalmente integrados en el reglamento interno, que este sea completo, inequívoco y aprobado por la gerencia, de modo que el personal actúe con responsabilidad y ética. Además, subrayan la balanceada aplicación del control: éste debe ser periódico, objetivo y completo, pero sin sobrecargar ni inhibir la iniciativa del personal; la automatización, recomendada por los autores, fortalece la eficiencia y consistencia del ambiente de control, al reducir costos y aumentar fiabilidad. Por último, es importante destacar que el ambiente de control –base del control interno– en el sector financiero se fortalece cuando se adoptan marcos sólidos de gobernanza de IA [14]. El estudio resalta la necesidad de implementar regulaciones explícitas, transparencia en los algoritmos, supervisión humana constante y entornos controlados como los "regulatory sandboxes". Estas prácticas garantizan que la integración de IA en procesos críticos —como detección de fraudes y cumplimiento normativo— no se traduzca en opacidad o riesgo sistémico, sino que promuevan un entorno ético, vigilado y resiliente frente al lavado de activos en la banca digital.

Por otra parte, se examina la incidencia del gobierno corporativo en la eficacia de las medidas contra el lavado de activos en el sector bancario. Los autores concluyen que una estructura de gobernanza robusta, basada en la supervisión activa del directorio, la definición clara de políticas de cumplimiento y la implementación de mecanismos de control, desempeña un papel determinante en la prevención del uso indebido del sistema financiero [15]. Asimismo, resalta la necesidad de realizar evaluaciones periódicas de riesgos por parte de la alta dirección. El artículo también identifica limitaciones significativas en la implementación de las normas antilavado, como la interferencia política, la escasez de personal técnico especializado, la exclusión financiera y el rezago tecnológico.

Este enfoque se articula directamente con la investigación, al evidenciar que los controles internos tradicionales deben ser reformulados y fortalecidos para responder adecuadamente a los riesgos emergentes en entornos digitales. En este sentido, el gobierno corporativo no solo se constituye como un elemento normativo, sino también como una herramienta estratégica para garantizar la integridad operativa de las plataformas bancarias, prevenir el ingreso de fondos ilícitos y promover una cultura organizacional orientada a la transparencia y al cumplimiento normativo.

C. Monitoreo

El principio 26 del GAFI requiere que las instituciones financieras estén reguladas y supervisadas adecuadamente, asegurando que cumplan con los estándares de prevención de lavado de dinero y financiamiento del terrorismo. Esto implica el monitoreo continuo de prácticas y controles para mantener su efectividad. Un monitoreo efectivo asegura que las políticas y procedimientos se apliquen correctamente, permitiendo que las organizaciones detecten y respondan a irregularidades de manera oportuna. Por su parte, el principio 27 establece la necesidad de supervisar grupos financieros para asegurar que todas las partes del grupo cumplan con los requisitos y estándares necesarios. Se debe asegurar que el monitoreo se extienda a todas las entidades dentro de un grupo financiero promueva la coherencia y el cumplimiento en toda la organización, fortaleciendo su capacidad para prevenir el lavado de activos en un entorno global complejo y dinámico.

Autores proponen una infraestructura de transacciones bancarias basada en blockchain con algoritmos de consenso de inmediata finalización, lo que aporta un monitoreo estilo "panóptico" capaz de fortalecer significativamente el control interno en la prevención del lavado de activos [16]. Al almacenar representaciones digitales verificadas de la identidad del cliente (KYC) en una red con transparencia total, se reduce la duplicación de procesos y se automatiza el monitoreo de transacciones, facilitando la identificación de contrapartes, el rastreo de fuentes de fondos y la generación de alertas tempranas. Esta trazabilidad inalterable crea una vigilancia continua donde los potenciales delincuentes saben que sus movimientos pueden revisarse en cualquier momento, lo que disminuye el incentivo para actividades ilícitas, reduce costos laborales en cumplimiento AML y promueve una supervisión bancaria más efectiva en entornos digitales de alta velocidad.

D. Evaluación de Riesgo

El principio 1 del GAFI se centra en la evaluación integral de riesgos tanto a nivel nacional como organizacional. Este principio es fundamental para asegurar que los riesgos se

identifiquen y evalúen correctamente antes de desarrollar respuestas adecuadas [17]. Al realizar una evaluación exhaustiva, las organizaciones pueden priorizar sus recursos y esfuerzos en áreas que presentan mayor riesgo de lavado de dinero y financiamiento del terrorismo, fortaleciendo así sus defensas contra estas amenazas. De manera complementaria, el principio 22 destaca la importancia de evaluar los riesgos específicos de actividades y profesiones no financieras designadas (APNFDs), como abogados, contadores y agentes inmobiliarios, debido a su potencial para ser utilizadas en el lavado de dinero. La identificación y evaluación de riesgos en estos sectores no financieros ayudan a las instituciones a implementar medidas de mitigación efectivas, asegurando una cobertura integral en la lucha contra el lavado de activos.

El principio 21 del GAFI establece medidas adicionales para identificar y gestionar los riesgos asociados con ciertas personas y entidades, como aquellas incluidas en listas de sanciones o personas políticamente expuestas (PEPs). Este principio permite a las instituciones financieras identificar eventos específicos que podrían suponer riesgos adicionales para la organización, facilitando la toma de medidas preventivas y correctivas adecuadas. La capacidad de reconocer estos eventos es crucial para mitigar los riesgos potenciales que podrían derivarse de las interacciones con estas entidades. Por su parte, el principio 12 requiere que las instituciones financieras implementen medidas para identificar y gestionar los riesgos asociados con las PEPs, dado su potencial involucramiento en actividades de corrupción o abuso de poder. Esto facilita la identificación de eventos que podrían afectar negativamente los objetivos organizacionales.

De acuerdo con, el principio 6 del GAFI espera que las jurisdicciones implementen medidas proporcionadas a los riesgos identificados, ajustando los controles y procedimientos según la evaluación del riesgo. Este principio proporciona un marco para desarrollar respuestas específicas a los riesgos, alineadas con la tolerancia al riesgo de la organización [18]. Al adaptar las respuestas a los riesgos particulares que enfrenta la organización, se asegura una gestión de riesgos más efectiva y eficiente. Por otro lado, el principio 19 impone sanciones efectivas, proporcionadas y disuasivas para combatir el lavado de dinero y el financiamiento del terrorismo, asegurando que las violaciones sean tratadas adecuadamente. Informar sobre cómo responder a riesgos específicos mediante la aplicación de sanciones regulatorias permite a las organizaciones mantener la integridad y cumplimiento de sus operaciones.

En este mismo sentido, y considerando el contexto actual de la banca digital, donde las transacciones son masivas, automáticas y descentralizadas, se destaca una propuesta de un enfoque avanzado de control interno basado en redes neuronales gráficas a nivel de aspectos (*Aspect-Level Graph Neural Networks*) para la identificación de riesgos de lavado de activos [19]. Su modelo construye grafos dinámicos que integran múltiples dimensiones —características del cliente, ubicación geográfica, actividad comercial y contexto industrial— permitiendo detectar patrones de riesgo que no son evidentes con métodos estadísticos convencionales. Esta arquitectura permite representar de forma estructurada y contextualizada las relaciones financieras entre cuentas, mejorando la detección automática de comportamientos anómalos. En consecuencia, el estudio demuestra que, mediante este tipo de inteligencia artificial, los sistemas de control interno pueden anticiparse al lavado de activos incluso en entornos digitales complejos, fortaleciendo la supervisión y reduciendo significativamente los niveles de exposición institucional al riesgo.

E. Actividades de control

Las actividades de control representan un eje esencial en la prevención del lavado de activos dentro del sistema financiero. En esta línea, el principio 10 del GAFI establece que las instituciones deben implementar procedimientos de debida diligencia para identificar, verificar y monitorear a sus clientes, garantizando que los servicios no sean utilizados con fines ilícitos. Esto implica la aplicación de controles que aseguren tanto la integridad de las transacciones como la correcta identificación del cliente. La debida diligencia se configura, por tanto, como una herramienta preventiva clave para evitar el uso indebido del sistema financiero.

En complemento, el principio 11 dispone que las instituciones deben conservar registros de transacciones y otra información relevante por un período mínimo, facilitando así las investigaciones relacionadas con actividades sospechosas. El aseguramiento de controles que respalden la documentación adecuada de información crítica permite rastrear y analizar transacciones potencialmente ilícitas, reforzando de este modo la eficacia del sistema de control interno.

De forma coherente con estos lineamientos, destacan que las actividades de control interno aplicadas en el sector bancario especialmente en lo que respecta al entorno de control y al monitoreo continuo son fundamentales para mitigar los riesgos de lavado de activos [20]. A través de un estudio realizado en 108 sucursales bancarias en Malasia, los autores evaluaron cómo los cinco componentes del marco COSO (2013) inciden sobre la efectividad de las estrategias antilavado. En particular, identificaron que un entorno de control sólido, caracterizado por la ética organizacional, la integridad del personal y el compromiso de la alta dirección posibilita que las políticas contra el lavado no solo se diseñen de manera adecuada, sino que también se ejecuten con disciplina y coherencia.

Adicionalmente, el componente de monitoreo, aplicado mediante auditorías periódicas, supervisión de actividades sospechosas y retroalimentación continua, garantizó que las debilidades operativas fueran detectadas y corregidas oportunamente. Las actividades específicas de control incluyeron: programas de capacitación en prevención de lavado de activos, aplicación de procedimientos de conocimiento del cliente (KYC), uso de sistemas automatizados de seguimiento y presentación obligatoria de reportes de operaciones sospechosas. Aunque los componentes de evaluación de riesgos y comunicación no reflejaron un impacto directo significativo, su interacción con las políticas AML fortaleció el sistema de control en su conjunto. En consecuencia, la evidencia empírica sugiere que el fortalecimiento del entorno ético y el monitoreo sistemático en plataformas bancarias digitales son factores determinantes para la eficacia de los controles internos frente al lavado de activos.

Por último, en el contexto de Zimbabwe, el control interno en la banca digital se consolida como un pilar esencial para mitigar el riesgo de lavado de activos. Este refuerzo permite a los bancos identificar operaciones inusuales y cumplir con los estándares regulatorios AML/CFT. En esta línea, estudios evidencian que los sistemas de control que

incluyen monitoreo digital, debida diligencia del cliente, auditoría independiente y funciones de cumplimiento han permitido a las entidades financieras reducir su exposición al uso indebido de las plataformas digitales. No obstante, desafíos estructurales como la insuficiencia tecnológica, la escasez de personal calificado y la interferencia política debilitan significativamente la eficacia de dichos controles. En este escenario, la gobernanza corporativa se muestra como un factor crítico, al orientar el diseño, la supervisión y la sostenibilidad de los sistemas internos, configurando un marco preventivo robusto frente a los riesgos emergentes en la banca digital.

F. Información y Comunicación

El principio 20 del GAFI exige a las instituciones reportar actividades sospechosas de lavado de dinero o financiamiento del terrorismo, asegurando una comunicación eficaz y oportuna para gestionar riesgos. Por su parte, el principio 3 impulsa la cooperación internacional y el intercambio de información, esenciales para enfrentar amenazas globales de manera conjunta y efectiva.

En el contexto del control interno frente al lavado de activos en la banca digital, el componente de información y comunicación resulta crucial para garantizar la detección oportuna de operaciones sospechosas y el cumplimiento normativo. Además, estudios demuestran que la integración de tecnologías de la información y comunicación (TIC) e inteligencia artificial (IA) en los sistemas financieros africanos ha mejorado significativamente los canales de comunicación interna y externa, optimizando la recolección, procesamiento y transmisión de datos relevantes para la prevención del lavado de dinero. [21]. Estas herramientas permiten establecer alertas automatizadas, mejorar la trazabilidad de las transacciones y generar reportes de riesgo más eficientes, fortaleciendo así uno de los pilares esenciales del control interno.

Asimismo, autores abordan la prevención del lavado de activos desde una perspectiva práctica enfocada en la organización de controles internos dentro del sistema bancario. El estudio propone un modelo basado en tres líneas de defensa: la primera línea, encargada de la debida diligencia y la gestión operativa del riesgo; la segunda, correspondiente a la unidad de cumplimiento (AML), responsable de supervisar, detectar y corregir deficiencias; y la tercera, que recae en la función de auditoría interna, la cual evalúa de forma independiente la eficacia del entorno de control [22]. Se destaca la necesidad de establecer procedimientos claros, una estructura de gobierno robusta, y el uso de herramientas tecnológicas como sistemas automatizados de monitoreo de transacciones y análisis de alertas.

Como aporte central, el estudio introduce el concepto de Repositorio de Controles AML, una herramienta estructurada que consolida las acciones de control críticas, permitiendo clasificarlas según su nivel de riesgo, periodicidad y función (preventiva o retrospectiva). Este sistema facilita la trazabilidad y la respuesta ante riesgos regulatorios y reputacionales, promoviendo una cultura de cumplimiento dentro de la organización. El artículo concluye que el fortalecimiento de los controles internos en los bancos no solo mitiga el riesgo de lavado de dinero, sino que también mejora la eficiencia operativa y la credibilidad institucional en el marco del cumplimiento internacional.

G. Tecnología

Continuando con el análisis de la literatura encontrada, en el contexto de un sistema bancario cada vez más digitalizado y expuesto a riesgos complejos, la incorporación de tecnologías como la inteligencia artificial, el blockchain y el Internet de las Cosas ha redefinido la estructura y eficacia de los controles internos. Si bien estas herramientas han optimizado procesos clave como la gestión de datos y la toma de decisiones en tiempo real, su valor más estratégico reside en la capacidad de fortalecer la detección de operaciones sospechosas y mitigar el riesgo de lavado de activos. Blockchain, por ejemplo, ofrece una trazabilidad segura e inmutable de las transacciones, mientras que la inteligencia artificial permite identificar patrones anómalos con mayor precisión [23]. No obstante, el estudio advierte que estas innovaciones tecnológicas solo serán eficaces si se integran dentro de un marco estratégico adaptable, que considere los desafíos regulatorios, éticos y de ciberseguridad propios del entorno financiero actual.

Asimismo, una evaluación rigurosa sobre cómo la aplicación del marco COSO en entidades bancarias puede mitigar el riesgo de lavado de activos [24]. A través de evidencia empírica, el autor demuestra que la adopción efectiva de los cinco componentes del modelo —particularmente el entorno de control y el monitoreo continuo— permite establecer una cultura organizacional sólida, centrada en el cumplimiento normativo y la detección temprana de operaciones inusuales.

Profundizando el caso del blockchain, se ha convertido en un recurso estratégico, esta tecnología permite una trazabilidad e inmutabilidad de las transacciones, facilitando el monitoreo automático de operaciones sospechosas y reduciendo la intervención manual que puede dar lugar a errores o corrupción interna [25]. Además, los contratos inteligentes permiten automatizar procesos de cumplimiento como la verificación de identidad y el reporte de actividades inusuales, mejorando la eficiencia del sistema de control. No obstante, su efectividad depende de la calidad de los datos ingresados y del respaldo normativo que regule su aplicación.

En esa misma línea, el uso de sistemas automatizados basados en inteligencia artificial [IA] y aprendizaje automático [ML] para el monitoreo de transacciones sospechosas se ha convertido en una herramienta clave para reforzar los controles internos contra el lavado de activos en plataformas digitales bancarias, estos sistemas permiten mejorar la eficiencia operativa y la capacidad de detección en tiempo real, pero presentan retos significativos relacionados con la transparencia, la aplicabilidad de los algoritmos y el cumplimiento normativo [26]. La investigación evidencia que los bancos aún prefieren modelos más simples y controlables, debido al alto riesgo regulatorio asociado a errores en modelos complejos de IA.

Además, se destaca que la incorporación de tecnologías como el análisis forense digital y el procesamiento avanzado de bases de datos fortalece directamente el control interno frente al lavado de activos en la banca digital [27]. Al automatizar la detección de patrones inusuales y preservar evidencia digital de forma legalmente admisible, estas herramientas permiten una supervisión continua, trazabilidad robusta y respuesta oportuna ante transacciones sospechosas. Así, la tecnología no solo complementa, sino que transforma el control interno en un sistema proactivo y eficaz para mitigar el riesgo de lavado en

entornos financieros altamente digitalizados. Posteriormente, autores proponen el sistema MLD como refuerzo al control interno en la banca digital, al comparar datos bancarios con registros fiscales para detectar inconsistencias que podrían indicar lavado de dinero [28]. Esta automatización mejora la vigilancia interna y permite identificar operaciones sospechosas de forma más eficiente y alineada con regulaciones.

Adicionalmente, las plataformas de pago virtual, como PayPal, han facilitado el comercio, pero también presentan riesgos de lavado de dinero. Para combatir esto, es esencial establecer controles internos robustos. Por ejemplo, PayPal ha implementado políticas AML y KYC para identificar transacciones sospechosas y cumplir con normativas internacionales, destacando la necesidad de medidas efectivas para prevenir actividades ilícitas [29]. Esto se complementa con estudios realizados en años anteriores, proponen un sistema basado en filtros automáticos para detectar lavado de dinero, que ayuda a fortalecer el control interno en la banca digital [30]. Usando un índice que combina varios criterios, como movimientos inusuales y patrones numéricos sospechosos, el modelo permite identificar operaciones irregulares de forma más rápida y precisa.

Por último, autores proponen un nuevo marco para la prevención del lavado de activos en bancos mediante el mapeo de los procesos de COBIT (Control Objectives for Information and Related Technology) con los componentes del modelo COSO, buscando fortalecer la gobernanza y los controles tecnológicos en el sector financiero. Esta propuesta surge de la necesidad de integrar tecnología de la información con las mejores prácticas de control interno, para dar respuesta a los requisitos establecidos por leyes como el Bank Secrecy Act estadounidense [31].

El diseño metodológico unifica COBIT y COSO para definir procesos tecnológicos con objetivos de control claros en instituciones financieras. Este marco permite gestionar datos, generar informes y detectar fraudes de forma eficiente y controlada. Los autores destacan su eficacia en la gestión de riesgos y cumplimiento, considerándolo una herramienta viable contra el lavado de activos. No obstante, señalan la necesidad de validarlo en distintos contextos y adaptarlo a regulaciones como Basilea III. Se recomienda aplicar controles adecuados a cada realidad, no de forma general. En conjunto, ofrece una guía práctica para integrar tecnología y cumplimiento en el sector bancario.

V. DISCUSIÓN DE RESULTADOS

A. Marco COSO

Los resultados de la sección IV muestran que la literatura reciente sobre control interno en banca digital se concentra principalmente en el Monitoreo y las Actividades de control, mientras que componentes como Evaluación de riesgos e Información y comunicación tienen menor desarrollo.

Esto se alinea con en una cobertura parcial del modelo COSO:

1. Monitoreo: reforzado por estudios que incorporan transaction monitoring, trazabilidad de operaciones y alertas automatizadas.
2. Actividades de control: robustecidas con prácticas de KYC, auditorías internas y retención de registros.
3. Entorno de control y objetivos: son abordados en menor medida, vinculados a cultura ética y gobernanza corporativa.
4. Evaluación de riesgos e Información y comunicación: menos explorados, lo que evidencia una brecha en mecanismos preventivos y de coordinación interna.

Si bien los avances en monitoreo y actividades de control son consistentes, persiste un rezago en la evaluación de riesgos y la información/comunicación, lo cual limita la cobertura integral del marco COSO en la banca digital.

B. Estándares GAFI

Los resultados guardan relación con algunas recomendaciones del GAFI:

1. R10 (Debida diligencia del cliente): fortalecida por estudios sobre KYC y verificación digital.
2. R18 (Controles internos): representadas por el énfasis en auditorías y monitoreo continuo.
3. R26 (Regulación y supervisión): menos cubierta en la literatura, lo que muestra una falta de evidencia en mecanismos regulatorios aplicados a banca digital.
4. R15 (Nuevas tecnologías): algunos estudios reconocen los desafíos de la IA y blockchain, pero sin estandarización de métricas de efectividad.

Lo anterior evidencia que la literatura vincula parcialmente los estándares internacionales, pero aún carece de validaciones empíricas y reportes de impacto.

C. Implicancias para la banca digital

Los resultados sugieren que:

1. La adopción de IA y blockchain puede fortalecer la trazabilidad y reducir los falsos negativos en la detección de operaciones sospechosas.
2. Los controles KYC deben evolucionar hacia un modelo continuo (no solo en onboarding de clientes), acompañado de auditorías independientes.
3. La gobernanza de modelos de IA es un desafío pendiente: se requieren protocolos de validación, ética y supervisión humana.
4. En Latinoamérica, la evidencia escasa subraya la urgencia de implementar pilotos en entornos regulados (sandboxes).

D. Comparación con literatura previa

En países como India e Indonesia se observa una mayor producción académica, vinculada a la rápida digitalización de sus sistemas financieros. En contraste, la literatura latinoamericana es limitada, lo que restringe la comparabilidad.

Estudios previos han señalado que la efectividad de los programas AML depende de la madurez tecnológica y de la fortaleza institucional, lo cual explica la divergencia regional.

De los puntos señalados anteriormente aún queda una agenda pendiente, que incluye la estandarización de métricas

de efectividad, el desarrollo de estudios empíricos en Latinoamérica, la gobernanza de modelos de IA y blockchain, y la evaluación los efectos en el tiempo de los controles internos en la banca digital.

VI. CONCLUSIONES

Los controles internos constituyen un pilar fundamental en la prevención del lavado de activos en la banca digital. Su adecuada implementación asegura que las operaciones financieras se realicen conforme a la normativa vigente y a los estándares internacionales, fortaleciendo la integridad del sistema financiero y reduciendo los riesgos exposición.

La revisión de 36 estudios publicados entre 2019 y 2025 muestra que el 58.7% corresponde a artículos académicos y el 41.3% a conference papers, con predominio en las áreas de Computer Science (23.7%) y Social Sciences (15.7%), siendo India (24%) e Indonesia (15%) los países con mayor producción. En cuanto a los componentes del marco COSO, la evidencia se concentra en Monitoreo (alrededor del 40% de los artículos) y Actividades de control (35%), mientras que la Evaluación de riesgos (15%) y la Información y comunicación (10%) aparecen escasamente representadas.

Estos resultados evidencian cierta asimetría en la literatura, que prioriza la detección y supervisión de transacciones sobre la prevención temprana y la comunicación efectiva. Por tanto, resulta necesario un enfoque más integral que combine controles tecnológicos con los de gobierno.

Dado que las plataformas digitales se caracterizan por la alta velocidad y volumen de transacciones, se requiere avanzar hacia una mayor automatización, incorporando herramientas de inteligencia artificial, blockchain y análisis avanzado de datos para identificar patrones inusuales y emitir alertas oportunas. Sin embargo, su adopción debe acompañarse de marcos de validación, ética y supervisión humana que reduzcan sesgos y garanticen su alineación con las recomendaciones del GAFI.

La efectividad de los controles internos depende de un monitoreo y evaluación constante, capaz de ajustarse a cambios regulatorios y tecnológicos.

En adelante, será clave generar evidencia empírica en el contexto latinoamericano y adaptar los marcos internacionales de control a la realidad digital de la región, asegurando así la efectividad y resiliencia de los programas anti-lavado.

VII. RECOMENDACIONES

Es relevante que las plataformas digitales bancarias desarrollen controles internos diseñados específicamente para abordar los riesgos inherentes al entorno digital. A diferencia de los sistemas tradicionales, las plataformas digitales operan en un ecosistema dinámico y altamente automatizado, por lo que requieren mecanismos que permitan monitorear grandes volúmenes de transacciones en tiempo real. La implementación de sistemas automatizados que analicen patrones de comportamiento puede ser clave para detectar actividades sospechosas de manera oportuna y precisa.

Además, se recomienda la incorporación de herramientas tecnológicas avanzadas, como el análisis de datos y la inteligencia artificial, dentro del marco de control interno. Estas tecnologías permiten una detección más eficiente de anomalías, así como una mejor capacidad de respuesta ante riesgos emergentes. Su aplicación no solo mejora la capacidad preventiva, sino que también optimiza los recursos operativos y reduce el margen de error humano en los procesos de monitoreo.

Por último, resulta esencial fortalecer los protocolos de auditoría interna como parte integral de la estrategia de control. Las auditorías deben ser frecuentes, exhaustivas y orientadas tanto a evaluar la eficacia de los controles como a verificar el cumplimiento normativo. Un sistema robusto de auditoría contribuye a mantener la transparencia operativa, facilita la identificación de debilidades en los controles existentes y promueve una cultura organizacional orientada al cumplimiento y la mejora continua.

REFERENCIAS

[1] M. Levi y P. Reuter, “Money laundering”, *Crime and Justice*, vol. 34, pp. 289–375, 2006, doi: 10.1086/501508;WGROUP:STRING:PUBLICATION.

[2] GAFILAT, “Glosario de Definiciones”.

[3] Committee of Sponsoring Organizations of the Treadway Commission, “Lograr un control interno efectivo sobre la presentación de informes de sostenibilidad (ICSR): Generar confianza y fiabilidad a través del Marco Integrado de Control Interno COSO”, Committee of Sponsoring Organizations of the Treadway Commission.

[4] P. G. Caraballo, “Lavado de activos: orígenes, situación actual, y su problemática en entornos digitales (Money Laundering: Origins, Current Status, and Its Problematic on Digital Environments)”, SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3582257.

[5] A. Patil, B. Mishra, S. Chockalingam, S. Misra, y P. Kvalvik, “Securing financial systems through data sovereignty: a systematic review of approaches and regulations”, *Int J Inf Secur*, vol. 24, núm. 4, ago. 2025, doi: 10.1007/S10207-025-01074-4.

[6] M. Jullum, A. Løland, R. B. Huseby, G. Ånonsen, y J. Lorentzen, “Detecting money laundering transactions with machine learning”, *Journal of Money Laundering Control*, vol. 23, núm. 1, pp. 173–186, ene. 2020, doi: 10.1108/JMLC-07-2019-0055/FULL/PDF.

[7] R. Hernández-Sampieri y C. Mendoza, *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta*. Ciudad de México: Mc Graw Hill Education, 2018.

[8] GAFILAT y FATF, “ESTÁNDARES INTERNACIONALES SOBRE LA LUCHA CONTRA EL LAVADO DE ACTIVOS, EL FINANCIAMIENTO DEL TERRORISMO, Y EL FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA”.

[9] N. K. Bhasin y A. Rajesh, “The role of emerging banking technologies for risk management and mitigation to reduce non-performing assets and bank Frauds in the Indian Banking System”, *International Journal of e-Collaboration*, vol. 18, núm. 1, ene. 2022, doi: 10.4018/IJEC.290293.

[10] O. O. Fabiyi, O. D. Aregbesola, O. Wright, S. O. Omojola, y P. E. Kolawole, “Internal Control System and Fraud Prevention in Nigerian Deposit Money Banks”, *International Journal of Economics and Financial Issues*, vol. 15, núm. 3, pp. 179–183, abr. 2025, doi: 10.32479/ijefi.17537.

[11] A. H. Jamil, Z. Mohd Sanusi, N. M. Yaacob, Y. Mat Isa, y T. Tarjo, “The Covid-19 impact on financial crime and regulatory compliance in Malaysia”, *J Financ Crime*, vol. 29, núm. 2, pp. 491–505, mar. 2022, doi: 10.1108/JFC-05-2021-0107.

[12] K. Abdulwahab y M. Abdel-Mohdi, “The Role of Commercial Banks in Controlling Money Laundering Operations: A Case Study of the Commercial Bank of Jordan”, *International Journal of Innovation, Creativity and Change.*, 2019.

[13] S. Tkachenko, N. Dashchenko, y Z. Shatskaya, “Organizational Maintenance of Internal Control of Electronic Money at the Enterprise”. Consultado: el 5 de julio de 2025. [En línea]. Disponible en: https://www.abacademies.org/articles/organizational-maintenance-of-internal-control-of-electronic-money-at-the-enterprise-8408.html

[14] N. N. Ridzuan, M. Masri, M. Anshari, N. L. Fitriyani, y M. Syafrudin, “AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility”, *Information (Switzerland)*, vol. 15, núm. 8, ago. 2024, doi: 10.3390/INFO15080432.

[15] S. Abel, T. H. M. Makoni, J. Mukarati, R. Manenge, T. Mokumako, y P. Le Roux, "CORPORATE GOVERNANCE AND ANTI-MONEY LAUNDERING IN THE BANKING SECTOR", *International Journal of Economics and Finance Studies*, vol. 15, núm. 4, pp. 373–390, 2023, doi: 10.34109/IJEFS.202315418.

[16] T. Vinther Daugaard, J. Bisgaard Jensen, R. J. Kauffman, y K. Kim, "Blockchain solutions with consensus algorithms and immediate finality: Toward Panopticon-style monitoring to enhance anti-money laundering", *Electron Commer Res Appl*, vol. 65, may 2024, doi: 10.1016/J.ELERAP.2024.101386.

[17] FATF, "GUIDANCE ON DIGITAL IDENTITY".

[18] FATF, "RISK-BASED APPROACH GUIDANCE FOR THE BANKING SECTOR", 2014, Consultado: el 5 de julio de 2025. [En línea]. Disponible en: www.fatf-gafi.org

[19] Y. Yu, Y. Xu, J. Wang, Z. Li, y B. Cao, "Anti-Money Laundering Risk Identification of Financial Institutions based on Aspect-Level Graph Neural Networks", *Proceedings - 2022 IEEE 22nd International Conference on Software Quality, Reliability and Security Companion, QRS-C 2022*, pp. 542–546, 2022, doi: 10.1109/QRS-C57518.2022.00086.

[20] S. Vijeyan y M. Rahmat, "EFFECTS OF INTERNAL CONTROL TOWARDS MONEY LAUNDERING PREVENTION: AN INTERRELATION PERSPECTIVE", *Asian Journal of Accounting and Governance*, vol. 17, 2022, doi: 10.17576/ajag-2022-17-02.

[21] M. K. Couchoro, K. Sodokin, y M. Koriko, "Information and communication technologies, artificial intelligence, and the fight against money laundering in Africa", *Strategic Change*, vol. 30, núm. 3, pp. 281–291, may 2021, doi: 10.1002/JSC.2410.

[22] M. Milojičić, S. Knežević, y S. Milojević, "Organization of Internal Control in Banks Towards Money Laundering Prevention: A Practical Approach", *REVIZOR*, vol. 27, núm. 108, pp. 141–151, dic. 2024, doi: 10.46793/REV24108141M.

[23] R. A. Oleiwi, "The Impact of Using Digital Technologies on Internal Control Systems in the Banking Sector", *Lecture Notes in Networks and Systems*, vol. 923 LNNS, pp. 254–264, 2024, doi: 10.1007/978-3-031-55911-2_24.

[24] M. M. A. Alqudah, S. Al-Tahat, y L. T. Y. Almarabha, "The Effect of Implementing Internal Control Systems According to the COSO Committee in Reducing Money Laundering in Jordanian Commercial Banks", *Journal of Ecohumanism*, vol. 3, núm. 4, pp. 3330–3342, ago. 2024, doi: 10.62754/JOE.V3I4.3847.

[25] S. L. Hota, A. Kumar, A. Kumar, K. Ali, y S. S. Sakuntala, "Blockchain Technology and its Potential to Mitigate Corruption in Banking", *2024 4th International Conference on Advancement in Electronics and Communication Engineering, AECE 2024*, pp. 1029–1034, 2024, doi: 10.1109/AECE62803.2024.10911834.

[26] U. Turksen, V. Benson, y B. Adamyk, "Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI", *Journal of Banking Regulation*, vol. 25, núm. 4, 2024, doi: 10.1057/s41261-024-00233-2.

[27] D. A. Flores, O. Angelopoulou, y R. J. Self, "Combining digital forensic practices and database analysis as an anti-money laundering strategy for financial institutions", *Proceedings - 3rd International Conference on Emerging Intelligent Data and Web Technologies, EIDWT 2012*, pp. 218–224, 2012, doi: 10.1109/EIDWT.2012.22.

[28] B. Bidabad, "Money laundering detection system (MLD) (a complementary system of Rastin banking)", *Journal of Money Laundering Control*, vol. 20, núm. 4, pp. 354–366, oct. 2017, doi: 10.1108/JMLC-04-2016-0016.

[29] J. E. Correa Echevarría, "El Control Interno como herramienta para combatir el Lavado de Activos en las Entidades Financieras de la provincia de Trujillo, 2021-2022", 2024.

[30] S. Yang y L. Wei, "Detecting money laundering using filtering techniques: A multiple-criteria index", *Journal of Economic Policy Reform*, vol. 13, núm. 2, pp. 159–178, jun. 2010, doi: 10.1080/17487871003700796.

[31] V. Pramod, J. Li, y P. Gao, "A framework for preventing money laundering in banks", *Information Management & Computer Security*, vol. 20, núm. 3, pp. 170–183, jul. 2012, doi: 10.1108/09685221211247280.