AulaVirtual
Generando Conocimiento

ISSN: 2665-0398

MARCOS REGULATORIOS PARA LA IA EN CIBERSEGURIDAD FINANCIERA Y BANCA MÓVIL: EVIDENCIA DESDE UNA REVISIÓN SISTEMÁTICA

REGULATORY FRAMEWORKS FOR AI IN FINANCIAL CYBERSECURITY AND MOBILE BANKING: EVIDENCE FROM A SYSTEMATIC REVIEW

Tipo de Publicación: Articulo Científico
Recibido: 18/04/2026
Aceptado: 19/05/2026
Publicado: 26/05/2026
Código Único AV: e732
Páginas: 1(1196-1215)
DOI: https://doi.org/10.5281/zenodo.20411727

Autores:
Pablo Enrique Mazuelos-Soldevilla
Ingeniero Industrial
https://orcid.org/0000-0002-7856-8785
E-mail: pabmazueloss@upt.pe
Afiliación: Universidad Privada de Tacna
País: República del Perú

Percy Dario Mazuelos-Soldevilla
Ingeniero Comercial
Maestro en Contabilidad, Tributación y Auditoria
https://orcid.org/0000-0001-9678-3326
E-mail: permazuelos@upt.pe
Afiliación: Universidad Privada de Tacna
País: República del Perú

Rosa Mardely Roque Lanchipa
Contadora Pública, mención en Auditoría
Magíster en Dirección de Personas
https://orcid.org/0000-0001-9661-280X
E-mail: rroquel@upt.pe
Afiliación: Universidad Privada de Tacna
País: República del Perú

Carlos Augusto Lobatón Gutiérrez
Contador Público
Magister en Administración
https://orcid.org/0000-0001-8936-270X
E-mail: carlos.lobaton@unmsm.edu.pe
Afiliación: Universidad Nacional Mayor de San Marcos
País: República del Perú

Resumen

La digitalización acelerada de los servicios financieros y la expansión de la banca móvil han incrementado la exposición del sector bancario a fraudes, ataques cibernéticos, filtraciones de datos y decisiones automatizadas opacas. En este escenario, la inteligencia artificial se ha convertido en una herramienta estratégica para fortalecer la ciberseguridad, aunque su adopción plantea desafíos regulatorios, éticos y operativos que requieren análisis sistemático. El objetivo de este artículo fue identificar y clasificar los marcos regulatorios existentes a nivel global que abordan el uso de inteligencia artificial en la ciberseguridad del sector financiero y evaluar su aplicabilidad específica a plataformas de banca móvil. Se desarrolló un artículo de revisión sistemática siguiendo criterios de búsqueda, selección y síntesis de literatura científica especializada, organizada según marcos regulatorios, aplicabilidad móvil, desafíos éticos y brechas jurisdiccionales. Los resultados evidenciaron que los marcos existentes se agrupan en estándares de ciberseguridad, normas de protección de datos, esquemas de cumplimiento financiero y enfoques emergentes de gobernanza algorítmica. Sin embargo, su aplicación a banca móvil sigue siendo parcial, especialmente frente a biometría, autenticación adaptativa, IA generativa, datos conductuales y proveedores tecnológicos. Se concluye que la banca móvil requiere una gobernanza regulatoria integrada, adaptable y transfronteriza.

Palabras Clave Inteligencia artificial, ciberseguridad financiera, marcos regulatorios, banca móvil, gobernanza algorítmica.

Abstract

The accelerated digitalization of financial services and the expansion of mobile banking have increased the banking sector's exposure to fraud, cyberattacks, data breaches, and opaque automated decisions. In this context, artificial intelligence has become a strategic tool for strengthening cybersecurity, although its adoption raises regulatory, ethical, and operational challenges that require systematic analysis. The objective of this article was to identify and classify existing global regulatory frameworks that address the use of artificial intelligence in cybersecurity within the financial sector and to assess their specific applicability to mobile banking platforms. A systematic review article was developed following criteria for the search, selection, and synthesis of specialized scientific literature, organized according to regulatory frameworks, mobile applicability, ethical challenges, and jurisdictional gaps. The results showed that existing frameworks are grouped into cybersecurity standards, data protection regulations, financial compliance schemes, and emerging approaches to algorithmic governance. However, their application to mobile banking remains partial, particularly in relation to biometrics, adaptive authentication, generative AI, behavioral data, and technology providers. It is concluded that mobile banking requires integrated, adaptable, and cross-border regulatory governance.

Keywords Artificial intelligence, financial cybersecurity, regulatory frameworks, mobile banking, algorithmic governance.

Introducción

La ciberseguridad en el sector financiero se configuró como un campo de análisis en permanente transformación, debido a la digitalización progresiva de los servicios bancarios y al aumento de amenazas cibernéticas más complejas. Oyeniyi et al., (2024) señalaron que los marcos tradicionales de ciberseguridad, aunque cumplieron una función inicial relevante, resultaron cada vez menos suficientes frente a ataques sofisticados, por lo que plantearon la necesidad de adoptar estructuras más flexibles, adaptativas y apoyadas en tecnologías emergentes.

En este escenario, la inteligencia artificial (IA) adquirió un papel estratégico en la protección de los sistemas financieros digitales. Faraji et al., (2024) evidenciaron que las técnicas de IA, entre ellas el aprendizaje automático y el aprendizaje profundo, contribuyeron a mejorar la detección de fraudes y la defensa frente a ciberataques en transacciones financieras. De forma complementaria, Vučinić & Luburić (2022) sostuvieron que las innovaciones fintech generaron beneficios relevantes para el sistema financiero, pero también incorporaron riesgos que exigieron marcos regulatorios y mecanismos de supervisión más precisos. Por ello, los autores destacaron la importancia de reducir el riesgo cibernético mediante la adopción de instrumentos legales adecuados.

Las investigaciones recientes aportaron elementos importantes para comprender la relación entre IA, ciberseguridad y regulación financiera. Waliullah et al., (2025), mediante una revisión sistemática de 78 artículos basada en la metodología PRISMA, evidenciaron que el cumplimiento de regulaciones internacionales, como GDPR, PSD2 y GLBA, fortaleció la seguridad bancaria digital. Sin embargo, también identificaron dificultades persistentes para equilibrar protección tecnológica, facilidad de uso y cumplimiento normativo.

Por su parte, Eskandarany (2024), a través de entrevistas cualitativas aplicadas a directivos bancarios saudíes, identificó que las tecnologías de IA ofrecieron beneficios relevantes en la detección de amenazas y la prevención de fraudes. No obstante, el estudio también reveló barreras asociadas con infraestructura tecnológica limitada, preocupaciones éticas sobre privacidad de datos y posibles sesgos algorítmicos. En una línea similar, Udeh et al., (2024) analizaron la incorporación de IA en medidas de ciberseguridad para plataformas financieras sostenibles, concluyendo que las soluciones basadas en IA fortalecieron la resiliencia frente a amenazas cibernéticas, aunque exigieron criterios éticos y garantías sólidas de privacidad durante su implementación.

Pese a los avances identificados, la literatura mostró vacíos relevantes que justificaron el desarrollo de la presente investigación. Kamuangu

ISSN: 2665-0398

(2025) evidenció que las infraestructuras actuales de ciberseguridad no siempre avanzaron al mismo ritmo que la adopción acelerada de tecnologías emergentes. Esta situación resultó más crítica en regiones en desarrollo, donde los marcos regulatorios presentaron limitaciones para proteger adecuadamente los datos de los consumidores.

Asimismo, Oyewole et al., (2024) señalaron que la relación entre fintech y las normas de privacidad de datos expuso un "trilema de innovación", en el cual la expansión tecnológica entró en tensión con la integridad del mercado y la claridad regulatoria. Esta situación permitió advertir la falta de marcos específicos orientados al uso de IA en plataformas bancarias móviles. De manera concordante, Ali et al., (2024) confirmaron que, aunque la IA y el aprendizaje automático fueron incorporados progresivamente como herramientas de mitigación en la ciberseguridad fintech, todavía persistió la necesidad de afrontar desafíos regulatorios, técnicos y organizacionales para que estas tecnologías desarrollaran plenamente su potencial. En ese sentido, se identificó una carencia de marcos regulatorios integrados y específicos para la banca móvil.

Ante los vacíos identificados, el presente artículo de revisión sistemática tuvo como objetivo identificar y clasificar los marcos regulatorios existentes a nivel global que abordan el uso de inteligencia artificial en la ciberseguridad del sector financiero, así como analizar su aplicabilidad específica a las plataformas de banca móvil.

Metodología

La presente investigación adopta un enfoque de revisión sistemática de la literatura, siguiendo las directrices del protocolo PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), el cual constituye un estándar metodológico ampliamente reconocido para garantizar la transparencia, reproducibilidad y rigor en la identificación, selección y síntesis de estudios relevantes.

La búsqueda se realizó en la base de datos Scopus, empleando la siguiente cadena booleana: (("artificial intelligence" OR "machine learning" OR "deep learning") AND ("cybersecurity" OR "cyber security" OR "information security") AND ("regulatory framework" OR "regulation" OR "compliance" OR "governance" OR "ethical") AND ("banking" OR "financial sector" OR "fintech" OR "mobile banking"))

Para orientar la revisión sistemática, se formularon las siguientes preguntas de investigación: PI1: ¿Cuáles son los marcos regulatorios existentes a nivel global que abordan el uso de inteligencia artificial en ciberseguridad del sector financiero? PI2: ¿En qué medida estos marcos regulatorios contemplan disposiciones específicas aplicables a plataformas de banca

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

móvil? PI3: ¿Cuáles son los principales desafíos éticos identificados en la literatura respecto a la implementación de IA en ciberseguridad bancaria móvil? PI4: ¿Qué brechas regulatorias se identifican entre las diferentes jurisdicciones en relación con la gobernanza de la IA aplicada a la ciberseguridad de servicios financieros móviles?

Se seleccionó Scopus como base de datos principal debido a que constituye una de las fuentes bibliográficas más exhaustivas y multidisciplinarias, con amplia cobertura de publicaciones en ciencias computacionales, finanzas y regulación, lo cual permite capturar la intersección temática entre IA, ciberseguridad y marcos regulatorios del sector financiero.

La estrategia de búsqueda se fundamentó en la combinación de palabras clave derivadas del objetivo de investigación, organizadas en cuatro bloques temáticos: a) inteligencia artificial (artificial intelligence, machine learning, deep learning); b) ciberseguridad (cybersecurity, cyber security, information security); c) regulación y ética (regulatory framework, regulation, compliance, governance, ethical); y d) sector financiero y banca móvil (banking, financial sector, fintech, mobile banking)

Criterios de inclusión	Criterios de exclusión
Artículos publicados entre 2019 y 2026.	Estudios fuera del periodo 2019-2026.
Artículos originales y revisiones en revistas indexadas con revisión por pares.	Actas, capítulos, tesis, informes, editoriales y cartas al editor.
Publicaciones en idioma inglés.	Publicaciones en idiomas distintos al inglés.
Estudios sobre IA aplicada a autenticación biométrica o detección de fraude en banca móvil.	Estudios sin aplicación específica en banca móvil o servicios financieros móviles.
Estudios con métricas de rendimiento o análisis de limitaciones.	Estudios teóricos sin métricas ni evaluación de limitaciones.
Artículos con texto completo disponible.	Artículos sin acceso al texto completo.
Estudios con rigor metodológico suficiente.	Estudios con baja calidad metodológica.

Tabla 1. Criterios de inclusión y exclusión

La aplicación sistemática de estos criterios de inclusión y exclusión, junto con el protocolo PRISMA, garantiza la reproducibilidad del proceso de selección y la calidad de la evidencia sintetizada, elementos fundamentales para una revisión sistemática rigurosa orientada a identificar y clasificar los marcos regulatorios globales sobre IA en ciberseguridad financiera y su aplicabilidad a la banca móvil (Ver Figura 1).

ISSN: 2665-0398

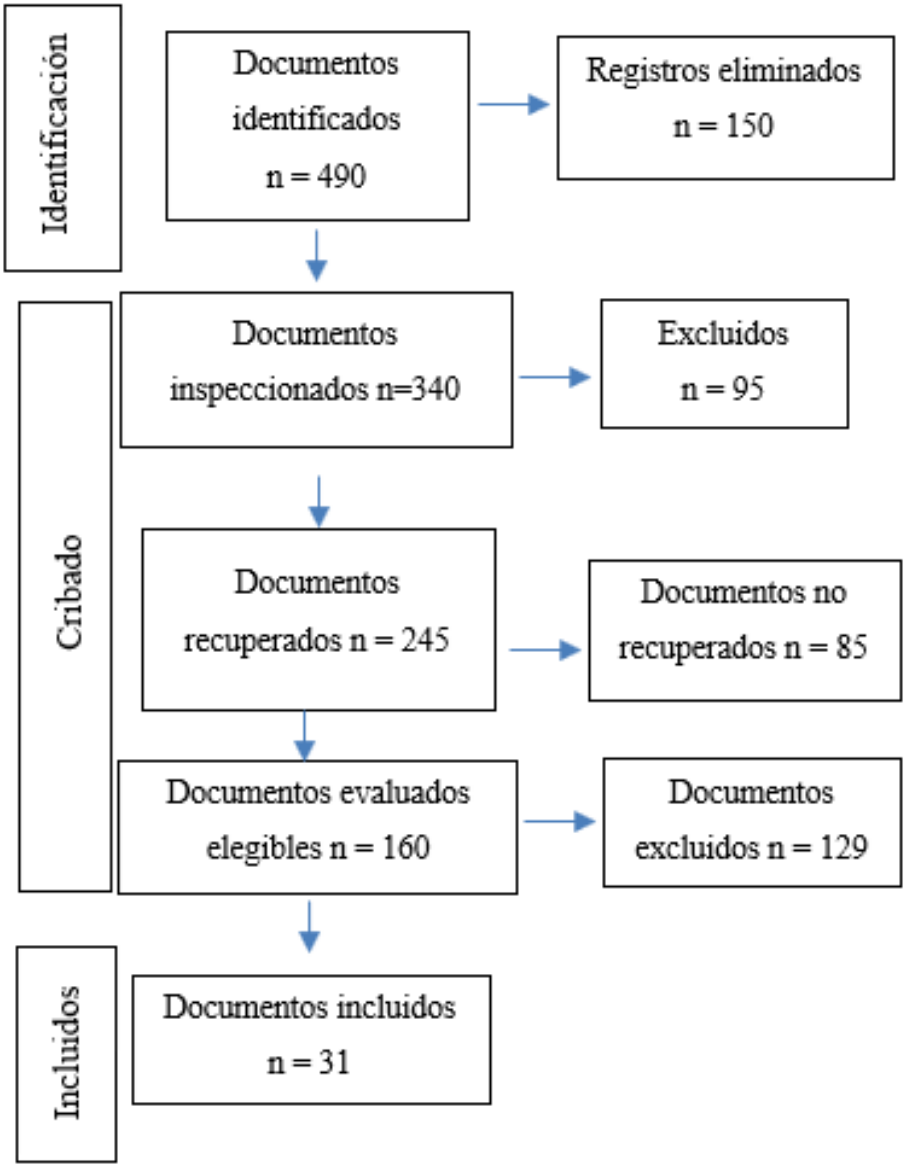

Figura 1. Flujograma del método PRISMA

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Resultados

Autor	Marco o enfoque regulatorio	Aporte
Al Batayneh et al., (2021)	ISO 27002, ISO 27014, COBIT, FFIEC, ISACA e ISGF	Los marcos de gobernanza de seguridad funcionan como instrumentos preventivos para evaluar controles, auditoría, supervisión y madurez institucional antes de adoptar IA en bancos.
Bui (2026)	Normativa vietnamita sobre ciberseguridad, datos, AML/CFT y banca digital	Propone una trazabilidad normativa que transforma obligaciones legales en controles auditables para IA, ciberseguridad, datos y banca en línea.
Chitimira & Ncube (2021)	Cybercrimes Bill, ECTA, RICA, POPIA y política nacional de ciberseguridad	Evidencia que los marcos tradicionales resultan insuficientes si no incorporan IA y 5G para prevenir ciberdelitos financieros.
Kumari (2026)	GDPR, CCPA, PSD2, PIPL, DPDPA y LGPD	La gobernanza de IA en banca digital exige articular privacidad, autenticación, protección de datos, trazabilidad y cooperación regulatoria.
Mota Makore (2024)	Modelos regulatorios de IA de la Unión Europea, Reino Unido y Sudáfrica	La regulación de IA debe equilibrar inclusión financiera, responsabilidad, ciberseguridad y prevención de exclusión algorítmica.
Nadella et al., (2025)	NIST CSF, ISO/IEC 27001, privacidad diferencial y cifrado	Integra estándares clásicos con IA generativa, datos sintéticos y detección adaptativa para fortalecer privacidad y ciberseguridad empresarial.
Sayari et al., (2025)	Políticas de IA, protección del consumidor y gobernanza de riesgos	Los marcos regulatorios deben asegurar transparencia, control humano, mitigación de sesgos y estabilidad del sistema financiero.
Ullah et al., (2024)	Gramm-Leach-Bliley Act, FISMA, CISA, FS-ISAC y políticas bancarias globales	La regulación bancaria requiere capacitación, cooperación internacional, MFA, blockchain e IA para enfrentar amenazas emergentes.

Tabla 2. Marcos regulatorios sobre IA y ciberseguridad financiera

Autor	Aplicación en banca móvil/digital	Aporte
Al-Dosari et al., (2024)	IA para phishing, fraude, DDoS, KYC, chatbots y ciberdefensa multicanal	La banca móvil requiere reglas específicas para IA defensiva, privacidad, gestión de terceros y protección frente a ataques adversariales.
Asmar & Tuqan (2024)	ML, IDS, IPS, fraude, ransomware, phishing y amenazas internas	Las plataformas digitales exigen gobernanza algorítmica, autenticación, cifrado, monitoreo continuo y respuesta en tiempo real.
Dasari & Kaluri (2024)	ML jerárquico para clasificación de ataques DDoS	La disponibilidad de la banca móvil depende de IDS robustos, modelos predictivos y mecanismos de continuidad operativa.
Ilyasov (2025)	MFA en la nube, OAuth 2.0, FIDO2, biometría y MFA adaptativo	La banca móvil necesita autenticación fuerte, interoperabilidad cloud, biometría y estándares técnicos de seguridad.
Manta et al., (2025)	ATMs, chatbots, robo-advisors, RPA, IA y banca por internet	La automatización bancaria combina componentes físicos y digitales, por lo que requiere regulación diferenciada sobre datos, fraude y atención automatizada.
Parveen et al., (2025)	IA, ML, fintech, open banking, blockchain, RPA y banca móvil	La banca móvil opera como ecosistema digital integrado donde IA y automatización intervienen en crédito, fraude, cumplimiento y servicio al cliente.

ISSN: 2665-0398

Autor	Aplicación en banca móvil/digital	Aporte
Shahzadi et al., (2025)	Gamificación, e-banking, phishing, malware, APTs y monitoreo con IA	La seguridad de banca digital debe incorporar formación del usuario, detección conductual y prevención personalizada.
Udayakumar et al., (2023)	Deep Fraud Net para fraude financiero y amenazas digitales	Las plataformas móviles requieren modelos adaptativos capaces de reducir falsos positivos y responder a patrones dinámicos de fraude.

Tabla 3. Aplicabilidad regulatoria a banca móvil y digital

Autor	Desafío ético central	Implicancia
Alnaabi & Al Mahruqi (2026)	Ambigüedad regulatoria, explicabilidad limitada e infraestructura heredada	La banca móvil puede generar decisiones automatizadas opacas y difíciles de auditar en fraude, autenticación o control de amenazas.
Alrafi & Mishra (2024)	Privacidad, transparencia, responsabilidad y justicia algorítmica	El perfilamiento de clientes y la detección automatizada de fraude requieren salvaguardas sobre datos personales y financieros.
Garad et al., (2024)	Seguridad de datos, cumplimiento y gobernanza de información	La innovación financiera debe incorporar privacidad, trazabilidad y gobernanza ética, no solo eficiencia tecnológica.
Gaviyau & Godi (2025)	Ética de datos, ciberseguridad, regulación y sistemas heredados	Banking 5.0 exige responsabilidad institucional ante decisiones automatizadas, billeteras digitales y servicios inteligentes.
Matlala (2026)	Calidad de datos, ciberseguridad, brechas regulatorias y capacidades técnicas	La GenAI puede mejorar chatbots y fraude, pero también amplifica sesgos, errores, exposición de datos y exclusión digital.
Rodríguez-Barboza et al., (2024)	Privacidad, sesgo algorítmico, ciberseguridad y acceso equitativo	La combinación IA-nube aumenta riesgos por dependencia de proveedores, almacenamiento remoto y uso masivo de datos financieros.
Sung et al., (2026)	Seguridad de información, gobernanza AIoT y sostenibilidad	La integración de IA, IoT y big data exige controles internos, transparencia operativa y alineación organizacional.
Vdovichena et al., (2025)	Vulnerabilidades de IA, ataques adversariales y políticas adaptativas	La IA debe evaluarse tanto como herramienta defensiva como posible fuente de nuevos riesgos en ciberseguridad bancaria.

Tabla 4. Desafíos éticos en IA para ciberseguridad bancaria móvil

Autor	Brecha identificada	Interpretación
Alazzam et al., (2026)	Diferencias de madurez normativa entre EAU y Jordania	La gobernanza de IA depende de regulación, ciberresiliencia, capacidad institucional y confianza digital.
Aysan et al., (2024)	Desigualdad institucional en riesgo, AML/CFT, datos y cumplimiento	Las brechas regulatorias son también metodológicas e institucionales, no solo normativas.
Fahimifar & Momenzadeh (2025)	Desfase entre seguridad tradicional e IA, ML, fintech y aprendizaje federado	La literatura avanza hacia detección inteligente de fraude más rápido que los marcos regulatorios.
Leelavathi et al., (2024)	Brecha entre banca tradicional y plataformas cripto	Los entornos cripto tienen riesgos descentralizados y regulación menos homogénea frente a la banca tradicional.
Maashi et al., (2023)	Desfase entre modelos deep learning y auditoría regulatoria	La detección algorítmica de fraude requiere explicabilidad, supervisión y evaluación de calidad de datos.

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

Autor	Brecha identificada	Interpretación
Nefla & Jellouli (2025)	Brechas éticas, regulatorias, de ciberseguridad, sesgo e inclusión	La gobernanza requiere estándares globales, control de sesgos, seguridad de sistemas descentralizados y coordinación internacional.
Sujadmiko et al., (2025)	Brecha entre jurisdicciones offshore y onshore	La trazabilidad digital, IA y cooperación internacional son necesarias para superar secreto bancario y vacíos regulatorios.

Tabla 5. Brechas regulatorias sobre gobernanza de IA y ciberseguridad financiera

Discusión de resultados

Los hallazgos de esta revisión sistemática evidenciaron que la regulación del uso de inteligencia artificial en la ciberseguridad del sector financiero se encuentra en una fase de consolidación fragmentada. Los estudios analizados no mostraron un único marco normativo global, sino una combinación de estándares de seguridad de la información, leyes de protección de datos, normas de cumplimiento financiero, políticas de gobernanza tecnológica y propuestas emergentes de regulación algorítmica.

Esta configuración permitió identificar cuatro ejes principales: los marcos de ciberseguridad y gobernanza institucional; las normas de privacidad y protección de datos; los mecanismos técnicos aplicables a banca móvil; y las brechas regulatorias derivadas de la desigual madurez normativa entre jurisdicciones.

En primer lugar, los resultados mostraron que los marcos tradicionales de seguridad de la información siguen siendo la base de la ciberseguridad bancaria. Instrumentos como ISO 27002, ISO 27014, COBIT, FFIEC, NIST Cybersecurity Framework e ISO/IEC 27001 fueron identificados como referencias recurrentes para evaluar controles, auditoría, gestión de riesgos, supervisión directiva y madurez institucional. Este resultado coincide con Al Batayneh et al., (2021), quienes sostuvieron que los marcos de gobernanza de seguridad pueden utilizarse para evaluar la preparación institucional de los bancos antes de incorporar tecnologías avanzadas.

Asimismo, converge con Nadella et al., (2025), quienes indicaron que los estándares clásicos mantienen relevancia, pero deben complementarse con técnicas de IA generativa, privacidad diferencial, cifrado y detección adaptativa de anomalías. Esta convergencia sugiere que la regulación bancaria no está siendo sustituida por la IA, sino reconfigurada por ella. Sin embargo, la diferencia principal radica en que los marcos tradicionales fueron diseñados para riesgos relativamente estructurados, mientras que los sistemas de IA operan sobre patrones dinámicos, datos masivos y amenazas adaptativas. Por ello, su aplicación directa a banca móvil resulta limitada si no se incorporan exigencias sobre explicabilidad, monitoreo continuo, trazabilidad algorítmica y supervisión humana.

ISSN: 2665-0398

En segundo lugar, la revisión identificó que las normas de protección de datos constituyen el principal puente regulatorio entre IA, ciberseguridad financiera y banca móvil. Marcos como GDPR, CCPA, PSD2, PIPL, DPDPA, LGPD y GLBA fueron recurrentes en la literatura por su relación con privacidad, consentimiento, seguridad de datos, autenticación fuerte y responsabilidad institucional.

Este hallazgo coincide con Kumari (2026), quien señaló que la protección de datos en sistemas financieros digitales exige integrar regulación, ciberseguridad, blockchain, cifrado, IA y responsabilidad del usuario. También se relaciona con Ullah et al., (2024), quienes destacaron que la banca global enfrenta riesgos de phishing, ransomware, amenazas internas e incumplimiento regulatorio, por lo que requiere políticas de seguridad robustas, cooperación internacional y tecnologías avanzadas.

No obstante, el presente estudio permite precisar que la banca móvil incrementa la complejidad regulatoria porque concentra datos financieros, biométricos, conductuales, geográficos y transaccionales en dispositivos personales. En consecuencia, la regulación de datos no debería limitarse a la protección formal de la información, sino incluir controles sobre el ciclo de vida del dato, el uso de modelos predictivos, la minimización de datos y la intervención de terceros tecnológicos.

En tercer lugar, se observó que la aplicabilidad específica de los marcos regulatorios a plataformas de banca móvil continúa siendo parcial. Los estudios revisados mostraron una fuerte orientación técnica hacia autenticación multifactor, biometría, OAuth 2.0, FIDO2, detección de fraude, ciberdefensa multicanal, protección frente a DDoS, sistemas IDS/IPS y monitoreo conductual. Ilyasov (2025) sostuvo que la integración de MFA en aplicaciones móviles mejora la seguridad y la usabilidad cuando se apoya en servicios cloud, biometría y autenticación adaptativa.

De manera complementaria, Asmar & Tuqan (2024) indicaron que la banca digital requiere modelos de machine learning, cifrado y monitoreo continuo para enfrentar phishing, ransomware, fraude y amenazas internas. Asimismo, Dasari & Kaluri (2024) demostraron que los modelos jerárquicos de machine learning pueden fortalecer la clasificación de ataques DDoS, lo cual resulta crítico para la disponibilidad de plataformas financieras móviles. Estos hallazgos coinciden en reconocer que la banca móvil requiere controles técnicos específicos; sin embargo, divergen en el tratamiento regulatorio de dichos controles.

Mientras la literatura técnica se concentró en precisión, rendimiento o capacidad de detección, la literatura jurídica abordó con menor profundidad la auditoría de modelos, la explicabilidad, la responsabilidad por falsos positivos y la gobernanza

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

de proveedores. Esta diferencia revela una brecha entre innovación técnica y madurez regulatoria.

En cuarto lugar, los resultados mostraron que la implementación de IA en ciberseguridad bancaria móvil plantea desafíos éticos relevantes. Los problemas más recurrentes fueron privacidad, explicabilidad, sesgo algorítmico, transparencia, rendición de cuentas, calidad de datos, exclusión digital y dependencia de infraestructura tecnológica.

Alrafi & Mishra (2024) señalaron que la IA mejora la detección de fraude y la gestión de amenazas, pero requiere proteger los datos del consumidor y asegurar decisiones algorítmicas responsables. De forma similar, Alnaabi & Al Mahruqi (2026) identificaron barreras asociadas con ambigüedad regulatoria, infraestructura heredada, escasez de capacidades y gobernanza ética. Estos resultados convergen con Matlala (2026), quien sostuvo que la IA generativa puede transformar los servicios financieros africanos mediante chatbots, personalización y eficiencia operativa, aunque también puede ampliar riesgos de ciberseguridad, sesgo, baja calidad de datos y exclusión.

La contribución de la presente revisión consiste en contextualizar estos desafíos en la banca móvil, donde las decisiones automatizadas se ejecutan en tiempo real, con alto volumen de datos sensibles y bajo una interacción directa con usuarios que no siempre comprenden el funcionamiento de los sistemas inteligentes.

En quinto lugar, la revisión permitió identificar brechas regulatorias entre jurisdicciones. Alazzam et al., (2026) mostraron diferencias de madurez normativa entre Emiratos Árabes Unidos y Jordania respecto a IA, IoT y ciberseguridad financiera. Mota Makore (2024) sostuvo que Sudáfrica requiere un marco regulatorio específico para IA que permita promover inclusión financiera sin descuidar responsabilidad, ciberseguridad y protección frente a riesgos algorítmicos.

Por su parte, Bui (2026) propuso para Vietnam un marco de evaluación de riesgos que transforma obligaciones legales sobre ciberseguridad, AML/CFT, datos y banca digital en controles auditables. Estos estudios coinciden en que la regulación de IA en finanzas depende de la capacidad institucional y del nivel de desarrollo normativo de cada país.

Sin embargo, divergen en su énfasis: algunos priorizan inclusión financiera, otros cumplimientos técnicos y otra madurez legal comparada. Esta diversidad confirma que la gobernanza global de IA en ciberseguridad financiera aún carece de armonización suficiente, especialmente cuando se analiza su aplicación a servicios móviles transfronterizos.

En sexto lugar, las brechas regulatorias no solo aparecieron entre países, sino también entre sectores financieros. Leelavathi et al., (2024) evidenciaron diferencias entre la banca tradicional y

ISSN: 2665-0398

las plataformas de criptomonedas en materia de amenazas, prevención, detección y respuesta. Sujadmiko et al. (2025) mostraron que la banca offshore, el secreto bancario y la recuperación de activos presentan retos adicionales para la trazabilidad digital, aun cuando herramientas como IA, machine learning y blockchain analytics pueden apoyar la detección de flujos ilícitos.

Estos resultados convergen con Nefla & Jellouli (2025), quienes identificaron que las tecnologías emergentes en finanzas generan oportunidades para eficiencia e inclusión, pero también riesgos de ciberseguridad, sesgo algorítmico, fragmentación regulatoria y sostenibilidad. En este punto, la banca móvil se configura como un espacio híbrido: opera dentro del sistema financiero regulado, pero comparte riesgos con fintech, plataformas digitales, servicios cloud, APIs abiertas y ecosistemas descentralizados.

Otro hallazgo relevante fue el desfase entre la velocidad de avance de los modelos técnicos de IA y la capacidad regulatoria para auditarlos. Maashi et al., (2023) y Udayakumar et al., (2023) propusieron modelos avanzados de deep learning para detección de fraude financiero, con altos niveles de rendimiento predictivo. No obstante, estos estudios abordaron de manera limitada aspectos como explicabilidad, sesgo, responsabilidad, protección de datos y supervisión ex post.

Este resultado coincide con Fahimifar & Momenzadeh (2025), quienes identificaron una transición temática desde la seguridad de la información tradicional hacia IA, machine learning, fintech, aprendizaje federado y detección inteligente de fraude. La implicancia central es que la regulación debe avanzar desde el cumplimiento documental hacia una gobernanza algorítmica verificable, capaz de auditar datos, modelos, decisiones automatizadas, proveedores tecnológicos y resultados operativos.

En términos generales, los resultados permitieron responder al objetivo de la revisión al identificar y clasificar los marcos regulatorios existentes en cuatro categorías: marcos de ciberseguridad y seguridad de la información; normas de protección de datos y privacidad; marcos de gobernanza, cumplimiento y ética de IA; y enfoques sectoriales vinculados con banca digital, fintech, banca móvil y servicios financieros transfronterizos. La principal contribución analítica radica en demostrar que la aplicabilidad de estos marcos a banca móvil no es automática.

Las plataformas móviles requieren una regulación más específica debido a su dependencia de autenticación biométrica, procesamiento en tiempo real, modelos de detección de fraude, datos conductuales, infraestructura cloud, proveedores externos y canales multiactor. Por ello, una gobernanza adecuada de IA en banca móvil debe

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

integrar seguridad técnica, protección de datos, supervisión algorítmica, control humano, transparencia, gestión de terceros y cooperación internacional.

La primera limitación se relaciona con la delimitación documental. La revisión se centró en artículos científicos indexados y disponibles a texto completo, por lo que pudo excluir guías regulatorias, circulares supervisoras, estándares técnicos, documentos de bancos centrales e informes institucionales no indexados. Esta restricción puede limitar la comprensión de regulaciones recientes que todavía no han sido suficientemente tratadas en la literatura académica.

La segunda limitación corresponde a la heterogeneidad metodológica de los estudios incluidos. La muestra integró estudios jurídicos, revisiones sistemáticas, análisis bibliométricos, propuestas conceptuales y modelos técnicos experimentales. Esta diversidad enriqueció la interpretación, pero impidió una comparación homogénea sobre efectividad regulatoria o impacto empírico de los marcos identificados.

La tercera limitación se vincula con la especificidad de la banca móvil. Aunque varios estudios abordaron banca digital, fintech, e-banking o servicios financieros móviles, no todos analizaron directamente aplicaciones de banca móvil. Por ello, algunas inferencias se realizaron a partir de evidencia relacionada con autenticación móvil, fraude digital, cloud computing, biometría y servicios financieros digitales.

La cuarta limitación deriva del carácter cambiante del objeto de estudio. La regulación de IA, ciberseguridad y banca móvil evoluciona rápidamente; en consecuencia, algunos hallazgos podrían modificarse con la aprobación de nuevas normas, estándares técnicos o políticas de supervisión financiera. Esta condición exige interpretar los resultados como una síntesis actualizada, pero no definitiva.

La quinta limitación se asocia con la desigual representación geográfica. La literatura disponible mostró mayor presencia de estudios sobre Europa, Estados Unidos, Asia y algunas economías africanas, mientras que América Latina tuvo menor visibilidad. Esto puede afectar la generalización de los hallazgos hacia contextos regulatorios menos representados.

Futuras investigaciones deberían desarrollar comparaciones empíricas entre jurisdicciones para evaluar cómo los marcos de IA, ciberseguridad y protección de datos se implementan realmente en plataformas de banca móvil. Estos estudios podrían analizar diferencias entre modelos regulatorios de la Unión Europea, Estados Unidos, Reino Unido, Sudáfrica, Vietnam, Emiratos Árabes Unidos, Jordania y países latinoamericanos.

También se recomienda diseñar modelos de madurez regulatoria para IA en ciberseguridad

ISSN: 2665-0398

bancaria móvil. Estos modelos deberían incluir dimensiones como explicabilidad, protección de datos biométricos, auditoría de modelos, supervisión humana, seguridad de APIs, resiliencia operativa, gestión de proveedores cloud, mitigación de sesgos y respuesta ante incidentes.

Asimismo, futuros estudios deberían incorporar literatura gris regulatoria, incluyendo documentos de bancos centrales, organismos supervisores, autoridades de protección de datos, agencias de ciberseguridad y organismos internacionales. Esta ampliación permitiría contrastar la evidencia académica con la práctica normativa y supervisora.

Otra línea prioritaria consiste en realizar estudios empíricos con bancos, fintech, proveedores tecnológicos y reguladores para evaluar cómo se aplican en la práctica los controles sobre IA defensiva, autenticación adaptativa, detección automatizada de fraude, biometría y monitoreo conductual. Este enfoque permitiría medir no solo la existencia formal de los marcos, sino también su efectividad operativa.

Finalmente, se recomienda profundizar en riesgos emergentes vinculados con IA generativa, aprendizaje federado, modelos adversariales, blockchain analytics, AIoT y datos sintéticos en banca móvil. Estas tecnologías pueden fortalecer la detección de amenazas y la protección de datos, pero también introducen nuevos riesgos sobre manipulación de modelos, exposición de información sensible, decisiones automatizadas erróneas y responsabilidad institucional. Por ello, la agenda futura debería avanzar hacia una gobernanza integrada, adaptativa y transfronteriza de la IA aplicada a la ciberseguridad financiera móvil.

Conclusiones

Los resultados de la revisión permitieron evidenciar que la regulación del uso de inteligencia artificial en la ciberseguridad del sector financiero se encuentra estructurada en torno a marcos heterogéneos, integrados por estándares de seguridad de la información, normas de protección de datos, políticas de cumplimiento financiero, enfoques de gobernanza algorítmica y lineamientos éticos emergentes. Entre los hallazgos más relevantes se identificó que instrumentos como ISO/IEC 27001, ISO 27002, ISO 27014, COBIT, NIST Cybersecurity Framework, GDPR, CCPA, PSD2, GLBA y otros marcos nacionales constituyen referencias centrales para la gestión de riesgos, protección de datos, autenticación, auditoría y cumplimiento.

Sin embargo, también se constató que estos marcos no fueron diseñados específicamente para regular sistemas de IA aplicados a plataformas de banca móvil, por lo que su aplicabilidad requiere complementarse con criterios de explicabilidad, trazabilidad algorítmica, supervisión humana,

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

gestión de terceros tecnológicos, protección biométrica y monitoreo continuo.

En relación con el objetivo de investigación, el estudio permitió identificar y clasificar los marcos regulatorios existentes a nivel global que abordan la IA en la ciberseguridad financiera en cuatro grandes categorías: marcos de seguridad de la información y ciberseguridad; normas de privacidad y protección de datos; esquemas de gobernanza, cumplimiento y ética de IA; y enfoques sectoriales aplicables a banca digital, fintech y servicios financieros móviles.

Esta clasificación permitió establecer que la banca móvil representa un entorno regulatorio particularmente complejo, debido a que combina procesamiento de datos financieros, biometría, geolocalización, autenticación adaptativa, infraestructura cloud, modelos predictivos de fraude y servicios digitales de alta disponibilidad. En consecuencia, la regulación aplicable a estas plataformas no puede limitarse a estándares generales de ciberseguridad, sino que requiere una gobernanza integrada que articule seguridad técnica, protección de derechos, control algorítmico y resiliencia operativa.

El presente trabajo se desarrolló como un artículo de revisión sistemática, basado en la identificación, selección, análisis y síntesis de literatura científica relevante sobre inteligencia artificial, ciberseguridad financiera, regulación y banca móvil. La adopción de este enfoque permitió organizar la evidencia disponible de manera estructurada, comparar estudios jurídicos, técnicos y de gobernanza, y reconocer patrones comunes, brechas regulatorias y desafíos éticos asociados con la implementación de IA en servicios financieros digitales.

En ese sentido, la revisión sistemática resultó adecuada para responder al objetivo planteado, debido a que permitió integrar evidencia dispersa y clasificar los aportes de la literatura según su relación con marcos regulatorios, aplicabilidad móvil, desafíos éticos y brechas jurisdiccionales.

Como reflexión final, los hallazgos sugieren que la gobernanza de la IA en la ciberseguridad bancaria móvil debe avanzar hacia modelos regulatorios más adaptativos, interoperables y transfronterizos. La rápida evolución de tecnologías como IA generativa, aprendizaje federado, AIoT, blockchain analytics, autenticación biométrica y detección automatizada de fraude exige superar enfoques normativos fragmentados.

Futuras investigaciones deberían profundizar en estudios comparativos entre jurisdicciones, evaluar empíricamente la implementación de estos marcos en bancos y fintech, e incorporar literatura gris proveniente de bancos centrales, autoridades de protección de datos y organismos supervisores.

Asimismo, resulta necesario desarrollar modelos de madurez regulatoria que permitan medir

ISSN: 2665-0398

la capacidad de las instituciones financieras para auditar modelos de IA, proteger datos sensibles, mitigar sesgos, garantizar explicabilidad y responder eficazmente a amenazas cibernéticas emergentes en plataformas de banca móvil.

Referencias

Al Batayneh, A. A., Qasaimeh, M., & Al-Qassas, R. S. (2021). A scoring system for information security governance framework using deep learning algorithms: A case study on the banking sector. *Journal of Data and Information Quality, 13*(2), Article 9. Documento en línea. Disponible https://doi.org/10.1145/3418172

Alazzam, F. A. F., Gharaibeh, Z. I. Y., Jarah, B. A. F., AlJabali, A. M. A., & Al-Zaqeba, M. A. A. (2026). Legal and cybersecurity challenges of integrating artificial intelligence and the internet of things in financial institutions in the United Arab Emirates and Jordan. *International Journal of Data and Network Science, 10*, 265–272. Documento en línea. Disponible https://doi.org/10.5267/j.ijdns.2025.9.021

Al-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and Systems, 55*(2), 302–330. Documento en línea. Disponible https://doi.org/10.1080/01969722.2022.2112539

Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. *Iraqi Journal for Computer Science and Mathematics, 5*(3). Documento en línea. Disponible https://doi.org/10.52866/ijcsm.2024.05.03.004

Alnaabi, A. A. H., & Al Mahruqi, A. A. H. (2026). Artificial intelligence methods for enhancing cybersecurity in Oman: A comprehensive review. *Journal of Cloud Computing, 15*, Article 48. Documento en línea. Disponible https://doi.org/10.1186/s13677-026-00860-2

Alrafi, H. S., & Mishra, S. (2024). The impact of AI-based cyber security on the banking and financial sectors. *Journal of Cybersecurity and Information Management, 14*(1), 8–19. Documento en línea. Disponible https://doi.org/10.54216/JCIM.140101

Asmar, M., & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon, 10*, Article e37571. Documento en línea. Disponible https://doi.org/10.1016/j.heliyon.2024.e37571

Aysan, A. F., Ciftler, B. S., & Unal, I. M. (2024). Predictive power of random forests in analyzing risk management in Islamic banking. *Journal of Risk and Financial Management, 17*(3), Article 104. Documento en línea. Disponible https://doi.org/10.3390/jrfm17030104

Bui, L. V. (2026). Legal and regulatory challenges in addressing high-tech crimes in the banking sector: Developing a cybersecurity risk assessment framework for Vietnam. *Journal of Banking Regulation, 27*, Article 4. Documento en línea. Disponible https://doi.org/10.1057/s41261-025-00302-0

Chitimira, H., & Ncube, P. (2021). The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks. *Potchefstroom Electronic Law Journal, 24*, 1–33. Documento en línea. Disponible https://doi.org/10.17159/1727-3781/2021/v24i0a10742

Dasari, S., & Kaluri, R. (2024). An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. *IEEE Access, 12*, 10834–10845. Documento en línea. Disponible https://doi.org/10.1109/ACCESS.2024.3352281

Eskandarany, A. (2024). Adoption of artificial intelligence and machine learning in banking systems: A qualitative survey of board of

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 7, Número: 14, Año: 2026 (Enero 2026 - Junio 2026)

directors. *Frontiers in Artificial Intelligence, 7*, Article 1440051. Documento en línea. Disponible https://doi.org/10.3389/frai.2024.1440051

Fahimifar, S., & Momenzadeh, A. (2025). From information security to artificial intelligence: A scientometrics analysis of research trends in cybersecurity within the banking industry. *Journal Research Scientometrics, 11*(2), 299–326. Documento en línea. Disponible https://doi.org/10.22070/rsci.2025.20186.1790

Faraji, M. R., Shikder, F., Hasan, M. H., Islam, M. M., & Akter, U. K. (2024). Examining the role of artificial intelligence in cyber security (CS): A systematic review for preventing prospective solutions in financial transactions. *International Journal of Religion, 5*(10), 4766–4782. Documento en línea. Disponible https://doi.org/10.61707/7rfyma13

Garad, A., Riyadh, H. A., Al-Ansi, A. M., & Beshr, B. A. H. (2024). Unlocking financial innovation through strategic investments in information management: A systematic review. *Discover Sustainability, 5*, Article 381. Documento en línea. Disponible https://doi.org/10.1007/s43621-024-00542-6

Gaviyau, W., & Godi, J. (2025). Banking sector transformation: Disruptions, challenges and opportunities. *FinTech, 4*, Article 48. Documento en línea. Disponible https://doi.org/10.3390/fintech4030048

Ilyasov, R. (2025). Integrating cloud-based multi-factor authentication (MFA) systems into mobile applications. *Scientific Work International Scientific Journal, 19*(5), 334–337. Documento en línea. Disponible https://doi.org/10.36719/2663-4619/115/334-337

Kamuangu, P. (2025). Exploring the convergence of cybersecurity, fintech and artificial general intelligence: Innovations and implications. *Abhigyan*. Documento en línea. Disponible https://doi.org/10.1177/09702385251379163

Kumari, A. (2026). Personal data protection in the age of digital financial systems. *Electronic Government, 22*(2), 220–240.

Leelavathi, K., Samal, A., Thirulogasundaram, V. P., Vaishnavi, V. S., Malashree, S., & Muthukrishnan, B. (2024). Cybersecurity practices in cryptocurrency and traditional banking: An analysis of evolving threats and AI solutions. *Nanotechnology Perceptions, 20*(S5), 768–776.

Maashi, M., Alabduallah, B., & Kouki, F. (2023). Sustainable financial fraud detection using Garra Rufa fish optimization algorithm with ensemble deep learning. *Sustainability, 15*(18), Article 13301. Documento en línea. Disponible https://doi.org/10.3390/su151813301

Manta, L. F., Manta, A. G., & Gherțescu, C. (2025). Decoding digital synergies: How mechatronic systems and artificial intelligence shape banking performance through quantile-driven method of moments. *Applied Sciences, 15*(10), Article 5282. Documento en línea. Disponible https://doi.org/10.3390/app15105282

Matlala, N. P. (2026). Generative artificial intelligence transformation in African financial institutions: An evaluation of the benefits and risks. *Development Southern Africa, 43*(1), 149–163. Documento en línea. Disponible https://doi.org/10.1080/0376835X.2026.2632039

Mota Makore, S. T. (2024). Regulating artificial intelligence to advance financial inclusion in South Africa. *Potchefstroom Electronic Law Journal, 27*, 1–35. Documento en línea. Disponible https://doi.org/10.17159/1727-3781/2024/v27i0a17488

Nadella, G. S., Addula, S. R., Yadulla, A. R., Sajja, G. S., Meesala, M., Maturi, M. H., Meduri, K., & Gonaygunta, H. (2025). Generative AI-enhanced cybersecurity framework for enterprise data privacy management. *Computers, 14*(2), Article 55. Documento en línea. Disponible https://doi.org/10.3390/computers14020055

ISSN: 2665-0398

Nefla, D., & Jellouli, S. (2025). Emerging technologies in finance: Challenges for a sustainable finance. *Cogent Business & Management, 12*(1), Article 2495191. Documento en línea. Disponible https://doi.org/10.1080/23311975.2025.2495191

Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. *Computer Science & IT Research Journal, 5*(4), 903–925. Documento en línea. Disponible https://doi.org/10.51594/csitrj.v5i4.1049

Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data privacy laws and their impact on financial technology companies: A review. *Computer Science & IT Research Journal, 5*(3), 628–650. Documento en línea. Disponible https://doi.org/10.51594/csitrj.v5i3.911

Parveen, R., Alnwissari, M., & Amuda, Y. J. (2025). The adoption of artificial intelligence, machine learning, financial technology (FinTech) and automation in banking sector. *Scientific Culture, 11*(4), 1292–1306. Documento en línea. Disponible https://doi.org/10.5281/zenodo.18171179

Rodríguez-Barboza, J. R., Carreño-Flores, O. D., Davila-Zamora, L. M., Jalixto-Erazo, H. M., Oré de los Santos, M. A., Cruces-Torres, O. J., Ruiz-Villavicencio, R. E., & Villegas-Rivas, D. (2024). Posthumanist technologies in business: AI and cloud computing for global optimization and ethical challenges. *Advance Sustainable Science, Engineering and Technology, 6*(4), Article 02404021. Documento en línea. Disponible https://doi.org/10.26877/asset.v6i4.1064

Sayari, K., Firdouse, M. K. J., & Al Abri, F. (2025). Artificial intelligence and machine learning adoption in the financial sector: A holistic review. *IAES International Journal of Artificial Intelligence, 14*(1), 19–31. Documento en línea. Disponible https://doi.org/10.11591/ijai.v14.i1.pp19-31

Shahzadi, A., Ishaq, K., Nawaz, N. A., Rosdi, F., & Khan, F. A. (2025). Unveiling personalized and gamification-based cybersecurity risks within financial institutions. *PeerJ Computer Science, 11*, Article e2598. Documento en línea. Disponible https://doi.org/10.7717/peerj-cs.2598

Sujadmiko, B., Meutia, I. F., Zainal, A. G., & Yulianti, D. (2025). Technology, cyber and international offshore banks: Financial services for asset recovery of Indonesian convicts. *European Journal of Privacy Law & Technologies, 1*. Documento en línea. Disponible https://doi.org/10.57230/EJPLT251BSIFMAGZDY

Sung, S.-F., Ju, I.-L., & Chen, Y.-C. (2026). Examining the effect of earnings management, performance management, and corporate social performance on Artificial Intelligence of Things system construction. *Sensors and Materials, 38*(4), 1899–1908. Documento en línea. Disponible https://doi.org/10.18494/SAM6146

Udayakumar, R., Joshi, A., Boomiga, S. S., & Sugumar, R. (2023). Deep Fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. *Journal of Internet Services and Information Security, 13*(4), 138–157. Documento en línea. Disponible https://doi.org/10.58346/JISIS.2023.I4.010

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The integration of artificial intelligence in cybersecurity measures for sustainable finance platforms: An analysis. *Computer Science & IT Research Journal, 5*(6), 1221–1246. Documento en línea. Disponible https://doi.org/10.51594/csitrj.v5i6.1195

Ullah, M. W., Alam, M. T., Sultana, T., Rahman, M. M., Faraji, M. R., & Ahmed, M. F. (2024). A systematic review on information security policies in the USA banking system and global banking: Risks, rewards, and future trends.

Edelweiss Applied Science and Technology, 8(6), 8437–8453. Documento en línea. Disponible https://doi.org/10.55214/25768484.v8i6.3816

Vdovichena, O., Krymska, A., Koroliuk, Y., Shymko, A., & Vdovichen, A. (2025). The role of artificial intelligence technologies in rebuilding the post-war economy and ensuring cyber security: An example from Ukraine. *Salud, Ciencia y Tecnología – Serie de Conferencias, 4*, Article 642. Documento en línea. Disponible https://doi.org/10.56294/sctconf2025642

Vučinić, M., & Luburić, R. (2022). Fintech, risk-based thinking and cyber risk. *Journal of Central Banking Theory and Practice, 11*(2), 27–53. Documento en línea. Disponible https://doi.org/10.2478/jcbtp-2022-0012

Waliullah, Md., George, M. J., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *AJATES, 1*(1), 226–257. Documento en línea. Disponible https://doi.org/10.63125/fh49gz18