Innovation in Open Finance and Cybersecurity Risk Management: A Systematic Literature Review

Sergio Espinoza Abanto[1]; Mateo Peralta Ginocchio[2]; Roxanna Ardiles Carvo[3]
[1]Facultad de Ciencias Empresariales, Carrera de Contabilidad y Finanzas, Universidad de Lima, Perú
20220899@aloe.ulima.edu.pe, 20221931@aloe.ulima.edu.pe, rardiles@ulima.edu.pe

Abstract- ***This paper proposes an integrated governance framework to drive the development of the open finance system in Peru and Latin America. Based on a systematic review of the available literature, structural gaps were identified that create friction between the innovation of new technologies and the cybersecurity risks that threaten the sector. The study evaluates five technological tools, such as authentication and access control, federated learning, or human behavior analytics, and how their effectiveness depends on a robust governance framework. The structural gaps identified (the fragmentation between technical and regulatory development, the underuse of human-centered models, the lack of security standards specific to DeFi, and the absence of international regulatory harmonization) are particularly evident in Peru and Latin America. To address this fragmentation, the research proposes a three-step governance framework that maximizes the potential of the region's emerging markets.***

Keywords- ***Open finance; cybersecurity; risk management; financial innovation; decentralized finance (DeFi)***

Innovación en Open Finance y gestión de riesgos de ciberseguridad: una revisión sistemática de la literatura

Resumen- ***El presente trabajo propone un marco de gobernanza integrada que impulse el desarrollo del sistema open finance en Perú y Latinoamérica. A partir de una revisión sistemática de la literatura disponible, se identificaron brechas estructurales que generan fricción entre la innovación de nuevas tecnologías y los riesgos de ciberseguridad que amenazan al sector. El estudio evalúa cinco herramientas tecnológicas como la autenticación y control de acceso, el aprendizaje federado o el análisis del comportamiento humano y cómo su eficacia depende de un marco de gobernanza sólido. Las brechas estructurales identificadas: la fragmentación entre el desarrollo técnico y el regulatorio, la subutilización de modelos centrados en el factor humano, la falta de estándares de seguridad específicos para DeFi y la ausencia de armonización regulatoria internacional, son especialmente evidentes en el Perú y América Latina. Para solucionar esta fragmentación, la investigación plantea un marco de gobernanza de tres pasos que maximice el potencial de los mercados emergentes de la región.***

Palabras clave ***- Open finance; ciberseguridad; gestión de riesgos; innovación financiera; finanzas descentralizadas (DeFi)***

I. INTRODUCCIÓN

La transformación digital viene siendo uno de los principales factores de cambio dentro de las industrias a nivel global. La adopción de tecnologías como la inteligencia artificial y las APIs ha permitido a las organizaciones del sector financiero (bancos, fintechs, entre otras) automatizar y facilitar la prestación de productos y servicios, donde la información sensible es compartida constantemente.

Debido a esta interconectividad es que se ha incrementado el riesgo de ataques cibernéticos en el sector. La filtración de datos, ataques a infraestructuras críticas, casos de ransomware, entre otros, representan amenazas reales que escalan en paralelo con el avance digital. Por ello, la gestión de riesgos de ciberseguridad es una prioridad estratégica para el sector financiero.

Los beneficios provenientes del intercambio de datos en el open finance conllevan riesgos relacionados con la ciberseguridad [1]. A pesar del rápido crecimiento en la ciberseguridad financiera, las soluciones propuestas carecen de un marco regulatorio integrado [2].

Este trabajo tiene como objetivo analizar la evidencia reciente sobre cómo las innovaciones asociadas al open finance transforman los riesgos de ciberseguridad y las estrategias utilizadas para su gestión, con el fin de proponer un marco de gobernanza integrada aplicable al contexto latinoamericano.

II. MARCO TEÓRICO

A. Open Finance

El open finance es una evolución del open banking que amplía el concepto de portabilidad y compartición de datos financieros a un rango extenso de servicios, abarcando seguros, pensiones, inversiones y créditos [3]. Su estructura se basa en APIs estandarizadas que hacen posible que terceros autorizados accedan a información financiera con el permiso del usuario, lo que da lugar a un ecosistema interoperable compuesto por diversos actores. Proveedores de servicios de datos, aseguradores, plataformas FinTech y bancos. Ésta crea valor al facilitar el acceso a servicios financieros personalizados y disminuir las fricciones operativas. Sin embargo, como se mencionó en la introducción, al ampliar la superficie de compartición de datos, amplía en gran medida los riesgos de ciberataques.

B. Innovación Tecnológica en Open Finance

Las finanzas descentralizadas (DeFi) representan uno de los desarrollos más innovadores del open finance, al proponer un sistema financiero entre pares construido sobre infraestructuras de cadena de bloques, que reduce la necesidad de intermediarios centralizados.

Existe un marco de vulnerabilidades DeFi organizado en tres capas: técnica y de código (fallos en contratos inteligentes), económica y de protocolo (MEV y manipulación de precios), e infraestructura y cross-chain (ataques en puentes y oráculos) [4]. Este enfoque analiza la seguridad de los protocolos DeFi de manera integral, considerando medidas antes de su lanzamiento, durante su operación y después de un incidente, y demuestra que los riesgos en los ecosistemas basados en blockchain son complejos y pueden surgir en múltiples niveles.

La tecnología blockchain ofrece propiedades únicas para la ciberseguridad financiera mediante su trazabilidad inalterable. La tecnología blockchain y las organizaciones autónomas descentralizadas (DAOs) representan un enfoque revolucionario para la ciberseguridad en el open finance, aunque se señala la necesidad de definiciones universales y marcos de gobernanza que regulen su aplicación [3].

Los países con mejores regulaciones y prácticas de ciberseguridad suelen tener ecosistemas de financiamiento digital más desarrollados y preparados para enfrentar ciberataques [5]. Además, la adopción de leyes de ciberseguridad puede incentivar a las empresas a invertir más en la investigación y desarrollo, favoreciendo la innovación. Por ello, la regulación y la innovación no deben verse como objetivos opuestos, sino como elementos que pueden fortalecerse mutuamente [6].

C. *Ciberseguridad y Gestión de Riesgos de Ciberseguridad*

Proteger la información altamente sensible que se maneja en el open finance es indispensable para que el sector genere confianza en los usuarios. Los ciberataques ponen en riesgo la seguridad financiera de estos, y también la reputación de las entidades financieras y prestadoras de servicios. De ahí la necesidad de que la gestión de riesgos se rija por un marco regulatorio.

El estudio del uso de inteligencia artificial para resolver problemas de ciberseguridad ha aumentado [2]. Sin embargo, existe una brecha entre el aspecto técnico de su uso y la regulación y gobernanza de datos.

Los riesgos de ciberseguridad, además de provenir de forma externa a las entidades financieras que participan del open finance, se originan internamente. Conocidas como amenazas internas, estas representan riesgos producto de individuos con acceso a información confidencial. Aunque las tecnologías de detección y prevención han alcanzado un alto nivel de desarrollo, la evidencia indica que los factores humanos siguen siendo un aspecto ignorado [7].

III. METODOLOGÍA

La investigación adoptó un enfoque cualitativo y empleó la revisión sistemática de la literatura como técnica para recopilar, analizar y sintetizar rigurosamente los estudios académicos sobre la relación entre la innovación en open finance y la gestión de los riesgos de ciberseguridad. Asimismo, se aplicó la declaración PRISMA 2020 como estándar metodológico para garantizar la transparencia y replicabilidad del proceso de identificación y selección de los estudios.

A. *Definición del tema, pregunta de investigación y palabras clave*

En esta etapa se definió el tema central de la investigación: Ciberseguridad e Innovación: Caso Open Finance. La pregunta orientadora es: ¿De qué forma la innovación en Open Finance influye en la gestión de riesgos de ciberseguridad frente a los constantes ciberataques? A partir de las variables identificadas, se definieron las palabras clave y la ecuación de búsqueda que se presentan en la Tabla 1.

TABLA 1
VARIABLES Y PALABRAS CLAVE DE BÚSQUEDA

Variable	Palabras clave
Open Finance	“open finance”, “open banking”
Gestión de Riesgos	“risk management”, “financial risk”
Ciberseguridad	“cybersecurity”, “information security”
Innovación Financiera	“financial innovation”, “fintech”

La ecuación de búsqueda empleada fue: (“open finance” OR “open banking”) AND (“risk management” OR “financial risk”) AND (“cybersecurity” OR “information security”) AND (“financial innovation” OR “fintech”)

B. *Búsqueda de Artículos*

La búsqueda se realizó en dos bases de datos: Scopus y Web of Science (WoS). Los resultados se presentan en la Tabla 2.

TABLA 2
ARTÍCULOS POR BASE DE DATOS

Base de datos	Artículos encontrados
Scopus	73
Web of Science	26
Total	99

C. *Eliminación de Artículos Duplicados*

Del total de 99 artículos identificados, se procedió a la revisión de duplicados mediante la comparación sistemática de títulos, autores y resúmenes. Tras este proceso, no se identificaron artículos duplicados entre Scopus y Web of Science, manteniéndose el total de 99 artículos para la siguiente fase de filtrado.

D. *Filtro por Título y Resumen: Criterios de Inclusión y Exclusión*

Se aplicaron criterios de inclusión y exclusión sobre los 99 artículos identificados mediante la lectura del título y el resumen de cada artículo, tal como se detalla en la Tabla 3.

TABLA 3
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

N°	Criterios de inclusión	Criterios de exclusión
1	Documento completo disponible	Disponibilidad parcial del documento
2	Publicaciones abiertas al público en general	Acceso restringido
3	Publicaciones de los últimos 7 años (2020-2026)	Período de publicación mayor a 7 años
4	Idioma: español o inglés	Idioma diferente al español o inglés
5	Estudios relacionados con el tema a investigar	Estudios fuera del contexto financiero o tecnológico

Asimismo, también se aplicaron criterios de calidad sobre los artículos identificados, tal como se detalla en la Tabla 4.

TABLA 4
CRITERIOS DE CALIDAD

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

E. *Lectura completa y selección final*

De los 70 documentos excluidos, 54 no contaban con acceso abierto o no pudieron recuperarse mediante los repositorios institucionales disponibles. De este grupo, 33 guardaban relación con la investigación, pero fueron excluidos debido a la imposibilidad de acceder al texto completo. Los 21 documentos restantes presentaban ambas limitaciones: falta de acceso y ausencia en relación directa con el objetivo de estudio. Asimismo, 11 documentos fueron excluidos exclusivamente por falta de pertinencia temática y 5 por haber sido publicados antes de 2020.

F. Extracción de los Datos y Síntesis

Este proceso permitió identificar tendencias temáticas, metodologías predominantes, convergencias, divergencias y vacíos en la literatura existente. Estos hallazgos orientan la agenda de investigación futura en la intersección entre open finance y ciberseguridad.

IV. RESULTADOS

A. Análisis de la Literatura

Los 29 estudios incluidos fueron recuperados de las bases de datos Scopus y Web of Science y se publicaron entre 2020 y 2026. Bajo este enfoque, de las 29 fuentes, el 27% son artículos cuantitativos, 23% son artículos cualitativos, 13% son revisiones sistemáticas de la literatura y el 37% restante, otras categorías de artículos.

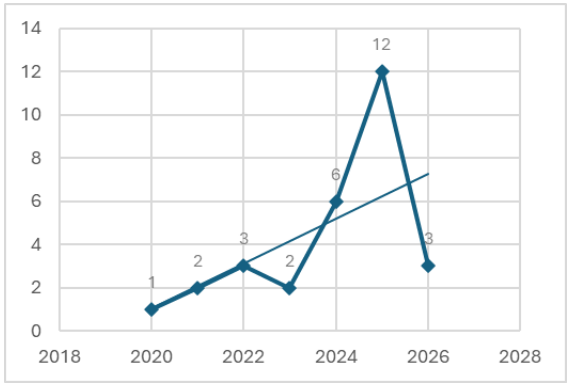


Fig 1: Publicaciones por año

Además, se aprecia una gran variedad de áreas de investigación relacionadas al Open Finance y la Ciberseguridad, destacando en igual medida con un 17% las áreas de Ciberseguridad bancaria (Cat. A), Ciberseguridad en Fintech (Cat. C), DeFi/Blockchain (Cat. D), y Detección de Fraude/Amenazas Internas (Cat. E).

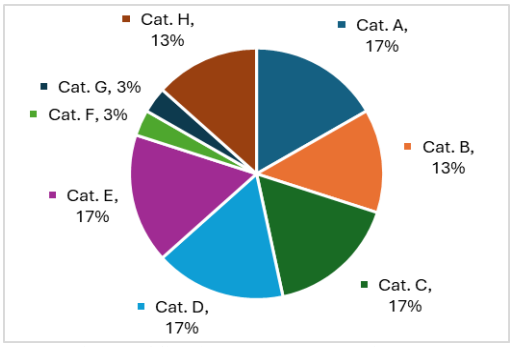


Fig 2: Publicaciones por área temática

En cuanto al país de origen de las publicaciones, la Figura 3 muestra que hay una mayor concentración de estudios provenientes de Estados Unidos y el Reino Unido, compartiendo la mayor participación, con un 13,33% de las publicaciones cada uno, mientras que los demás países presentan porcentajes menores.

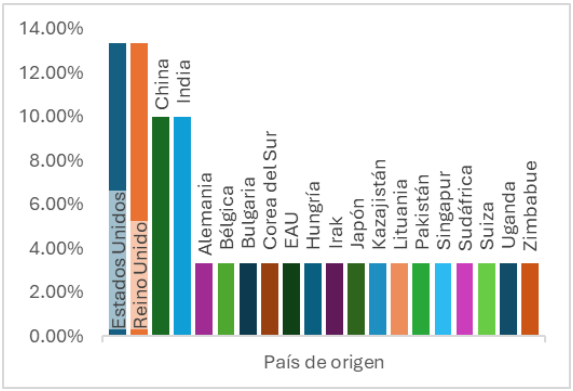


Fig 3: Publicaciones según país de origen

B. El Ecosistema del Open Finance y su Superficie de Ataque

El open finance configura un ecosistema de múltiples capas donde el valor económico se genera precisamente mediante la apertura e interoperabilidad de los datos financieros. Esta misma apertura define una superficie de ataque de complejidad sin precedentes. Las APIs permiten el uso compartido de los datos entre las instituciones financieras y los usuarios; si estas son vulneradas pueden exponer información sensible de millones de usuarios y desencadenar fallos en cascada en todo el sector [4].

Dentro del marco del open finance se encuentran las finanzas descentralizadas, que buscan eliminar por completo a los intermediarios en el intercambio de datos. Por ello, son consideradas la expresión más radical de este modelo. El valor total bloqueado en sistemas DeFi escaló aproximadamente de 700 millones de dólares a cerca de 150 mil millones en dos años [8].

Las DeFi funcionan a través de la blockchain junto a los contratos inteligentes, los que permiten las transacciones entre usuarios. Sin embargo, estos no están libres de errores ni de

ataques de seguridad. Una vez desplegados, los errores de código no pueden corregirse y las pérdidas derivadas de ataques son en su mayoría irrecuperables, habiendo alcanzado los 6.450 millones de dólares [9].

La gran variedad de actores en el sector financiero amplía adicionalmente la superficie de ataque. Un banco con mayores recursos puede desarrollar una mejor infraestructura de ciberseguridad que una empresa FinTech, exponiendo el problema del eslabón más débil. Un ataque exitoso a cualquiera de los cinco bancos más activos en mercados de financiamiento mayorista generaría derrames significativos hacia otras instituciones [10].

La innovación en ciberseguridad también se ve limitada. Las empresas con más exposición a ataques cibernéticos prefieren dejar de invertir en el desarrollo de nuevos productos en vista de un entorno propenso a ataques [11]. Además, el hecho de que el sector financiero dependa de plataformas de empresas extranjeras genera otro tipo de riesgos de seguridad nacional [12].

C. Amenazas Predominantes en Entornos de Open Finance

Desde 2018 el sector financiero se ha convertido en uno de los sectores más atractivos para atacantes alrededor del mundo. La pandemia de COVID-19 reveló que el 80% de las instituciones reportaron incidentes de ciberseguridad en los primeros meses, registrando un 238% de incremento en ataques [13]. Las amenazas dentro del open finance se dividen en técnicas, operacionales y sistemáticas.

En el ámbito de las amenazas técnicas, los ataques a contratos inteligentes constituyen uno de los vectores más críticos del ecosistema DeFi. El 40% de los estudios especializados se concentra en ataques de manipulación de oráculos, seguido de un 33.33% enfocado en manipulación de precios y flash loans [9]. Los ataques de flash loans explotan la posibilidad de tomar prestadas grandes cantidades de criptodivisas dentro de una única transacción sin colateral para manipular precios o drenar liquidez de protocolos antes de que los mecanismos de detección puedan actuar. Los ataques de valor máximo extraíble (MEV) permiten a mineros u operadores de nodos extraer valor económico a expensas de los usuarios mediante la reordenación de transacciones [3]. Las vulnerabilidades en APIs, infraestructuras en la nube y blockchain representan, asimismo, los vectores más explotados en el sector FinTech en general [14].

Las amenazas internas constituyen uno de los riesgos más sistemáticamente subestimados. Son responsables del 35% de las filtraciones de datos; los actores internos maliciosos generan daños 20 veces mayores que los externos, con un costo promedio de 4.5 millones de dólares por incidente [15]. Personas con acceso restringido como empleados internos, desarrolladores de APIs de terceros y operadores de plataformas FinTech pueden convertirse en autores de estos ataques. La exfiltración de datos, el abuso de privilegios, la ingeniería social y la explotación de vulnerabilidades en la nube son las formas en las que se pueden presentar [7].

En cuanto a las amenazas sistemáticas, la adopción masiva de contratos inteligentes sin estándares de seguridad adecuados podría replicar los factores que contribuyeron a la crisis financiera global de 2008: opacidad, complejidad y velocidad de contagio [16]. El auge del crédito BigTech añade otra dimensión: la expansión de sus límites comerciales puede crear desviaciones sistemáticas que reducen la capacidad de los modelos de control de riesgo para identificar correctamente a los clientes de la larga cola, elevando el riesgo de incumplimiento crediticio y abriendo vectores de ataque orientados a manipular los datos de entrenamiento de dichos modelos [17].

D. Marco Regulatorio y Gobernanza de la Ciberseguridad en Open Finance

Los países con mejores regulaciones y prácticas de ciberseguridad suelen tener ecosistemas de financiamiento digital más desarrollados y preparados para enfrentar ciberataques [5]. Este desarrollo se ve impulsado por la implementación de leyes de ciberseguridad que pueden incentivar a las empresas a invertir más en investigación y desarrollo [6]. Un marco regulatorio robusto y bien diseñado, por tanto, no frena la innovación; la orienta y la hace más sostenible.

Los sandboxes regulatorios emergen como uno de los mecanismos institucionales más innovadores para gestionar la tensión entre innovación y regulación en el FinTech. Los sandboxes fomentan la innovación financiera, facilitan marcos regulatorios efectivos y crean entornos de aprendizaje colaborativo entre reguladores e innovadores, aunque resultan más efectivos en países con ecosistemas FinTech consolidados [18]. Un estudio comparativo entre el Reino Unido, Singapur y Hungría muestra que los sandboxes aceleran el desarrollo de productos, mejoran el acceso a financiamiento y fortalecen la colaboración entre reguladores y empresas, aunque su impacto varía principalmente según el contexto institucional [19].

El caso de la banca suiza es referente de cómo la claridad regulatoria impulsa la innovación segura. La Ley DLT suiza, al proveer una base legal clara para aplicaciones basadas en blockchain, ha posicionado al país como pionero en la adopción de activos digitales, con bancos que combinan la tokenización y la custodia segura dentro de un marco jurídico establecido [20]. La regulación puede actuar como habilitador de innovación responsable cuando está diseñada con participación del sector y con un horizonte tecnológico claro.

En el plano de la gobernanza interna, tratar la ciberseguridad como una cuestión técnica delegada a equipos de TI resulta insuficiente ante la naturaleza estratégica de las amenazas actuales. Las organizaciones que la reconocen como prioridad estratégica de primer nivel la integran en la planificación corporativa y en los mecanismos de decisión ejecutiva, así desarrollan una resiliencia significativamente mayor y pueden encontrar en ello una fuente de ventaja competitiva [21]. Por ejemplo, en mercados emergentes, la brecha de gobernanza se refleja en que el 20% de las instituciones financieras aún no han adoptado marcos

específicos de cibercriminalidad a pesar de la disponibilidad de herramientas estandarizadas [22].

E. Herramientas Tecnológicas para la Gestión de Riesgos de Ciberseguridad

Las herramientas tecnológicas disponibles para la gestión de riesgos de ciberseguridad en el open finance se clasifican en autenticación y control de acceso, detección de fraude basada en IA y machine learning, aprendizaje federado con preservación de privacidad, análisis del comportamiento del usuario y mecanismos criptográficos avanzados.

En cuanto al control de acceso, la autenticación multifactor (MFA) sigue siendo una de las medidas preventivas más efectivas para prevenir accesos no autorizados en entornos FinTech [14]. Por otro lado, la arquitectura Zero Trust, que asume que ningún usuario o sistema es inherentemente confiable incluso dentro del perímetro organizacional, se presenta como uno de los marcos preventivos más adecuados para el sector bancario en el contexto de amenazas internas, complementada por tecnologías UEBA (User and Entity Behavior Analytics) y sistemas de detección de anomalías [7].

La detección de fraude mediante IA ha alcanzado resultados notables. La combinación de modelos de conjunto interpretable (Random Forest y XGBoost) con técnicas de IA explicable (SHAP y LIME) logra una precisión del 89.09% y un AUC de 0.9997 en la detección de fraude en tarjetas de crédito, y se destaca que la interpretabilidad de los modelos, no solo su precisión, es un factor crítico para mantener la confianza de las instituciones y cumplir con los requisitos regulatorios [23]. Un sistema basado en redes neuronales gráficas con aprendizaje por refuerzo (RL-GNN) mejora en un 15.7% la capacidad discriminativa y reduce en un 33% los falsos positivos frente a modelos base, con una latencia de inferencia de 42 milisegundos por lote, lo que lo hace viable para entornos transaccionales de alto volumen [24].

El aprendizaje federado con preservación de privacidad constituye una de las herramientas más innovadoras para el ecosistema open finance. Su implementación entre cinco bancos japoneses permitió construir modelos de detección de transacciones fraudulentas más precisos que los entrenados con datos de una sola institución, sin haber comprometido la privacidad de la información transaccional ni infringir la normativa de protección de datos [25]. Esta tecnología permite un intercambio blindado de información mas no de los datos crudos entre instituciones, y garantiza que la información personal se mantenga segura sin violar las leyes de privacidad. Así, viabiliza la cooperación entre instituciones para identificar y gestionar riesgos.

La gran variedad de amenazas dentro del sector requiere que las instituciones formulen estrategias defensivas que combinen soluciones tecnológicas con un marco integral [26]. Para garantizar el cumplimiento regulatorio, las plataformas colaborativas FinTech demandan una formación especializada y de alianzas estratégicas para una gestión efectiva de riesgos [27].

F. Brechas y Desafíos Pendientes en la Interacción Open Finance - Ciberseguridad

La fragmentación en la investigación académica en temas de ciberseguridad financiera, la gobernanza de datos y la regulación es la primera brecha identificada. A lo largo de 25 años los avances técnicos y regulatorios han evolucionado, pero de manera independiente [2]. Los responsables de la toma de decisiones en las instituciones financieras carecen de guías integradas que conecten las herramientas disponibles con los marcos regulatorios.

Una segunda brecha crítica es la subutilización de los modelos centrados en el comportamiento humano. Las amenazas internas son responsables de una gran parte de los incidentes y generan daños desproporcionados. Sin embargo, los modelos de aprendizaje profundo y NLP aplicados al análisis del comportamiento humano permanecen subutilizados en la mayor parte de las instituciones financieras [15]. Dentro del open finance, la diversidad de actores con acceso privilegiado es mucho mayor que en los sistemas financieros cerrados tradicionales, lo cual agrava la amenaza [7].

La desconexión entre el ritmo de innovación tecnológica en DeFi y el desarrollo de marcos de seguridad adecuados es otra brecha. Todavía no existe una solución definitiva para la prevención de ataques MEV, rug pulls y front-running [3], [9]. Sin un proceso de gobernanza complejo, cualquier vulnerabilidad dentro del blockchain es prácticamente imposible de corregir.

El intercambio de información entre instituciones financieras supera las fronteras dentro del open finance, por lo que es crítico pensar en cómo gestionar los riesgos en un entorno global antes que regional [12]. La exposición a los riesgos cibernéticos sin marcos regulatorios sólidos aumenta a medida que los sistemas financieros se adaptan a un entorno digital [28].

Por último, persiste una brecha estratégica a nivel organizacional. Las empresas con mayor exposición al riesgo cibernético acortan sus ciclos de patentamiento y ven reducida la rentabilidad de sus inversiones en I+D [11], generando un círculo vicioso que frena la capacidad innovadora. La ciberseguridad como bien público en el sistema bancario enfrenta además la tendencia al free-riding, que induce una subinversión colectiva y hace que la ciberseguridad óptima a nivel social difiera del equilibrio privado, justificando la intervención regulatoria como mecanismo corrector [10]. La integración acelerada de blockchain e inteligencia artificial amplía simultáneamente las capacidades y los riesgos del ecosistema open finance [29].

V. DISCUSIÓN DE RESULTADOS

A. Open Finance e Innovación: Oportunidad y Riesgo Simultáneos

El crecimiento del ecosistema open finance ha demostrado que la innovación financiera y la exposición al riesgo son dos caras de la misma moneda. Las propiedades que hacen atractivo al ecosistema descentralizado, apertura, composabilidad, acceso sin permisos, transparencia, son exactamente las mismas que generan superficies de ataque complejas y, en muchos casos, irreversibles. Por ejemplo, las pérdidas acumuladas en el ecosistema DeFi relacionadas con ataques a contratos inteligentes son producto de un sistema que impide corregir errores una vez desplegados.

La exposición al riesgo cibernético distorsiona la estrategia de innovación corporativa. La intención de innovar es frenada por la inseguridad que enfrentan las organizaciones al momento de planificar invertir en I+D y esto a largo plazo compromete la competitividad entre instituciones.

Por ello el sector financiero debe replantear el modelo de desarrollo tecnológico. Frenar la innovación no es la respuesta adecuada; al contrario, los países con marcos regulatorios más robustos son también los que logran mayor avance tecnológico.

B. Regulación y Gobernanza: Avances Desiguales en un Ecosistema Global

El sector exige un marco de armonización internacional. Al no existir fronteras en cuanto a dónde se puede compartir la información, los mecanismos de respuesta a incidentes deberían tener un enfoque global.

Los ecosistemas financieros digitales más seguros están directamente relacionados con marcos de gobernanza de ciberseguridad sólidos. El caso de la banca suiza demuestra que la regulación puede funcionar como habilitador estratégico cuando se construye con participación del sector y con un horizonte tecnológico claro, a diferencia de los mercados emergentes, donde existen debilidades institucionales que bloquean avances.

La ciberseguridad debe ser vista como activo estratégico. Integrar la gestión de riesgos cibernéticos en la planificación ejecutiva y en la toma de decisiones corporativas demuestra una capacidad de respuesta superior, contrastando con los modelos tradicionales donde la ciberseguridad es con frecuencia responsabilidad del equipo técnico, sin una conexión real con la agenda estratégica.

C. Herramientas Tecnológicas: Potencial Probado y Límites Pendientes

La autenticación multifactor, la arquitectura Zero Trust, los modelos de detección de fraude basados en IA y el aprendizaje federado con preservación de privacidad son las herramientas con mayor grado de efectividad dentro del sector. Las restricciones regulatorias y organizacionales, sin embargo, generan fricción al momento de implementarlas.

El aprendizaje federado resuelve uno de los dilemas más persistentes del open finance: detectar amenazas entre instituciones sin comprometer la confidencialidad de los datos de los clientes ni infringir la regulación de protección de datos. Esta tecnología permite que los modelos se entrenen de manera conjunta sin centralizar la información. Esto la convierte en una de las herramientas con mayor potencial de impacto sistémico en el ecosistema del open finance.

La evolución tecnológica a la vez convierte a los ataques cibernéticos en amenazas mucho más complejas. El uso de inteligencia artificial permite automatizar el phishing y evadir los sistemas de detección.

No solo basta con desarrollar mejores tecnologías; cuando las herramientas son integradas en marcos de gobernanza sólidos y son respaldadas por una cultura organizacional de seguridad, demuestran ser más eficaces en todos los niveles.

D. Brechas, Fragmentación y Agenda Pendiente

La principal brecha que se identificó es la falta de conexión entre un enfoque técnico y uno de gobernanza de ciberseguridad financiera. Los estudios técnicos abordan principalmente la prevención y detección, mientras que los de gobernanza operan con marcos y audiencias distintos. Esto se evidencia dentro de las organizaciones, donde los equipos de ciberseguridad junto con las áreas de innovación operan sin una comunicación ni marcos compartidos que se necesitan.

Por otro lado, el factor humano sigue siendo subestimado. Si bien existen diversas herramientas para la prevención y detección, estas no son utilizadas en una gran parte de las organizaciones. Esto se materializa en un riesgo económico y reputacional mucho más grande frente a las amenazas externas.

Resulta indispensable la generación de evidencia empírica en contextos de mercados emergentes y de América Latina, donde la digitalización financiera avanza aceleradamente, pero la investigación en ciberseguridad del open finance permanece incipiente.

VI. PROPUESTA DE VALOR

Tras revisar la literatura, se observa que todavía no existe una conexión entre un marco regulatorio y la gestión de riesgos de ciberseguridad en el open finance. La ausencia de evidencia regional sobre ciberseguridad para Perú y Latinoamérica ahonda más esta problemática, puesto que representan mercados con potencial de alta digitalización en el sector financiero.

El alineamiento técnico-regulatorio propone un primer paso en la gestión de riesgos de ciberseguridad en el contexto latinoamericano. Este funciona como un filtro obligatorio para todos los productos o servicios nuevos que, en caso de que cumplan con todas las medidas de seguridad, al mismo tiempo se ajusten a las leyes y regulaciones del país [2], [5].

El marco establece además evaluar las amenazas internas a través de un trabajo colaborativo entre las áreas de ciberseguridad, cumplimiento y recursos humanos mediante la incorporación de modelos de análisis del comportamiento humano [7], [15].

El tercer componente exigido plantea un mecanismo de coordinación regulatoria regional en el que la

Superintendencia de Banca, Seguros y AFP y sus contrapartes en otros países de Latinoamérica compartan estándares mínimos de ciberseguridad y protocolos de respuesta para el open finance, apoyándose en sandboxes regulatorios que permitan probar soluciones bajo supervisión conjunta [12], [18], [19].

De este modo el marco regulatorio busca que estos tres componentes trabajen de manera conjunta, de modo que la innovación en open finance y la gestión de riesgos de ciberseguridad se desarrollen bajo un mismo punto de decisión. Estos tres componentes se resumen en la Fig. 4.

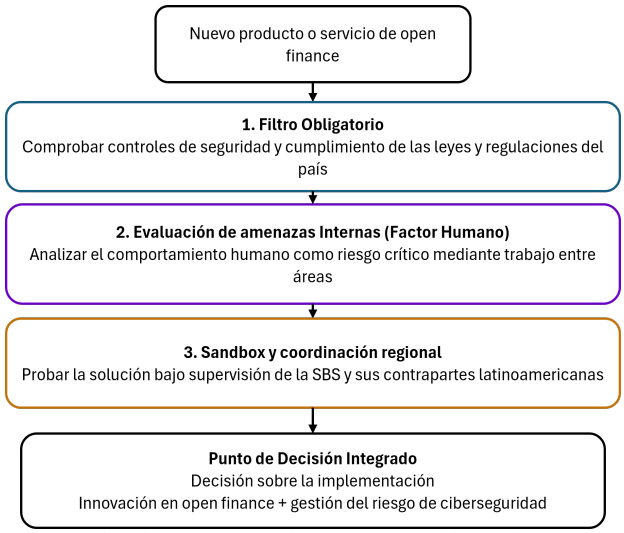


Fig 4:Marco de gobernanza integrada propuesto para el open finance en Perú y Latinoamérica

VII. CONCLUSIONES

La innovación en open finance y la gestión de riesgos de ciberseguridad no operan como fuerzas opuestas, sino como dimensiones que se condicionan mutuamente. El avance tecnológico amplía al mismo tiempo el valor generado para el ecosistema y la superficie expuesta a los ataques. Por tanto, frenar la innovación no reduce el riesgo cibernético; por el contrario, los ecosistemas con marcos regulatorios y de gobernanza más sólidos son también los que alcanzan mayor dinamismo innovador.

Las principales tendencias de innovación tecnológica en el ecosistema de open finance giran en torno a la apertura de datos mediante APIs estandarizadas, el desarrollo de las finanzas descentralizadas sobre infraestructuras blockchain, la aplicación de contratos inteligentes y organizaciones autónomas descentralizadas, y la incorporación de inteligencia artificial y aprendizaje automático para la detección de fraude. A ello se suma uno de los desarrollos más prometedores para el sector, el aprendizaje federado con preservación de privacidad, que permite a distintas instituciones colaborar en la detección de amenazas sin centralizar datos sensibles.

El aumento en la frecuencia de los ciberataques ha modificado de forma directa los protocolos de gestión de riesgos del sector financiero. Este crecimiento sostenido desde 2018 obligó a las instituciones a abandonar esquemas de control periódico y a adoptar mecanismos de monitoreo continuo como la autenticación multifactor y arquitecturas Zero Trust. Sin embargo, esto conlleva un costo adicional; las organizaciones con mayor exposición cibernética acortan sus ciclos de patentamiento y reducen la rentabilidad de sus inversiones en investigación y desarrollo, de modo que la frecuencia de los ataques endurece los protocolos defensivos y también condiciona la capacidad innovadora de las instituciones afectadas.

Dentro de las estrategias de ciberseguridad más efectivas para cubrir los riesgos identificados destacan la autenticación multifactor y la arquitectura Zero Trust para el control de accesos, los modelos de detección de fraude basados en inteligencia artificial explicable para el análisis transaccional, el aprendizaje federado con preservación de privacidad para la cooperación entre instituciones, y los sandboxes regulatorios como espacio institucional para experimentar de forma segura.

Aún con estos avances técnicos, existe una fragmentación entre el desarrollo técnico y regulatorio de la ciberseguridad financiera, lo que se refleja en la ausencia de un marco de regulación internacional. Los modelos de análisis del comportamiento humano son subutilizados, a pesar de que las amenazas internas generen daños más grandes que las externas. Se evidencia un desfase en el ritmo de innovación en DeFi y el desarrollo de estándares de seguridad para riesgos como los ataques MEV o los puentes cross-chain.

La relación entre innovación y ciberseguridad en el open finance funciona mejor cuando se aborda de manera integral, combinando herramientas tecnológicas con gobernanza, regulación armonizada y una cultura organizacional que reconozca al factor humano como parte central de la gestión del riesgo.

VIII. RECOMENDACIONES

Se recomienda a las organizaciones del sector financiero desarrollar marcos de ciberseguridad adaptados a un entorno cada día más interconectado y automatizado en lugar de los tradicionales. Estos deben incluir tecnologías como la autenticación multifactor, la arquitectura Zero Trust y los modelos de detección de fraude basados en inteligencia artificial dentro de una misma estrategia de gobernanza. La ciberseguridad debe ser una prioridad estratégica gestionada desde la alta dirección y no una función exclusiva de un equipo meramente técnico.

Se debe tener en cuenta la integración de estándares internacionales de ciberseguridad aplicables al open finance, ya que las regulaciones y mecanismos de respuesta continúan siendo, en su mayoría, nacionales. Fortalecer los sandboxes regulatorios puede llegar a facilitar este cambio sin ponerle un freno al desarrollo de nuevos productos y servicios.

Para atender las amenazas internas, las organizaciones deberían invertir en modelos de análisis del comportamiento humano que actualmente son subutilizados en todo el sector.

Resulta imperativo generar evidencia empírica sobre la ciberseguridad del open finance en el contexto latinoamericano, dada la escasez de estudios regionales identificada en este trabajo. Las futuras investigaciones deben enfocarse en medir de manera cuantitativa el impacto de los sandboxes regulatorios sobre la reducción efectiva del riesgo cibernético, así como avanzar en el diseño de estándares de seguridad específicos para el ecosistema DeFi que atiendan riesgos como los ataques MEV, la seguridad de los puentes cross-chain y la gobernanza descentralizada de protocolos.

IX. Limitaciones

La búsqueda de fuentes para este trabajo se limitó a Scopus y Web of Science, excluyendo 54 documentos sin acceso completo. La literatura proviene mayoritariamente de fuera de Latinoamérica, con mayor cantidad de investigaciones concentradas en Estados Unidos y el Reino Unido. Finalmente, el marco propuesto es conceptual, no tiene validación empírica.

Referencias

[1] A. Kay, C. Hutcherson, C. Keene, X. Zhang, y M. G. Terwilliger, "How financial institutions address cybersecurity threats: A critical analysis", Issues in Information Systems, vol. 22, núm. 1, pp. 63–74, 2021, doi: 10.48009/1_iis_2021_63-74

[2] J. Sopko y L. Šafár, "Cybersecurity and financial systems: a global perspective on research fragmentation and innovation gaps", SN Business and Economics, vol. 6, núm. 4, art. 90, 2026, doi: 10.1007/s43546-026-01105-9

[3] J. Lee y V.-M. Khan, "Developing cybersecurity in open banking and open finance: the application of blockchain technology and decentralised autonomous organisations," en A Research Agenda for Financial Law and Regulation, pp. 113–137, Edward Elgar Publishing, 2025.

[4] S. Jiang, W. You, S. Xuan, y J. Shen, "Decentralized finance security: A survey of attacks, defenses, and open challenges", High-Confidence Computing, vol. 6, núm. 2, art. 100383, 2026, doi: 10.1016/j.hcc.2026.100383

[5] S. Cheng, J. Li, L. Luo, y Y. Zhu, "Cybersecurity governance and digital finance: Evidence from sovereign states", Finance Research Letters, vol. 65, jul. 2024, doi: 10.1016/j.frl.2024.105503

[6] H. H. Nong, Y. Lin, y Q. Zhang, "Cybersecurity policy and corporate R&D investment", Finance Research Letters, vol. 75, abr. 2025, doi: 10.1016/j.frl.2025.106785

[7] S. Huy, S. Ang, M. Ho, y V. Balasubramaniam, "Insider Threats in Banking Sector: Detection, Prevention, and Mitigation", Journal of Cyber Security and Risk Auditing, vol. 2025, núm. 4, pp. 257–265, 2025, doi: 10.63180/jcsra.thestap.2025.4.5

[8] S. Werner, A. Klages-Mundt, D. Perez, D. Harz, L. Gudgeon, y W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," en Proc. 4th ACM Conference on Advances in Financial Technologies (AFT 2022), pp. 30–46, 2023, doi: 10.1145/3558535.3559780

[9] C. M. Kareem y A. C. Shakir, "A Systematic Review of Security Innovations in Decentralized Finance (DeFi) Using Blockchain Technology", Informatica, vol. 49, núm. 33, pp. 253–274, 2025, doi: 10.31449/inf.v49i33.7990

[10] K. Anand, C. Duley, y P. Gai, "Cybersecurity and financial stability," Deutsche Bundesbank Discussion Paper, núm. 08/2022, 2022, ISBN 978-3-95729-876-8.

[11] G. Lattanzio y Y. Ma, "Cybersecurity risk and corporate innovation", Journal of Corporate Finance, vol. 82, art. 102445, 2023, doi: 10.1016/j.jcorpfin.2023.102445

[12] D. Bassens y R. Hendrikse, "Asserting Europe's technological sovereignty amid American platform finance: Countering financial sector dependence on Big Tech?", Political Geography, vol. 97, art. 102648, 2022, doi: 10.1016/j.polgeo.2022.102648

[13] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, y J. Hur, "Cybersecurity threats in FinTech: A systematic review", Expert Systems With Applications, vol. 241, art. 122697, 2024, doi: 10.1016/j.eswa.2023.122697

[14] S. K. Jha, S. Verma, S. Gupta, K. K. Kumar, D. Kapila, y S. Mohapatra, "Cybersecurity in FinTech: Strategies for protecting digital finance from cyber threats and ensuring secure transactions", Journal of Discrete Mathematical Sciences & Cryptography, vol. 28, núm. 8, pp. 2977–2987, 2025, doi: 10.47974/JDMSC-2442

[15] F. R. Alzaabi y A. Mehmood, "A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods", IEEE Access, vol. 12, pp. 30907–30927, 2024, doi: 10.1109/ACCESS.2024.3369906

[16] R. E. Duran y P. Griffin, "Smart contracts: will Fintech be the catalyst for the next global financial crisis?", Journal of Financial Regulation and Compliance, vol. 29, núm. 1, pp. 104–122, 2021, doi: 10.1108/JFRC-09-2018-0122

[17] Z. Ji, X. Zhang, H. Liang, y Y. Lyu, "Technology Empowers Finance: Boundaries and Risks", Mathematics, vol. 12, núm. 21, art. 3394, 2024, doi: 10.3390/math12213394

[18] L. Gumbo y U. A. K. Chude-Okonkwo, "Regulatory sandbox as a frontier for innovation and sustainability: a systematic review", Cogent Business and Management, vol. 12, núm. 1, art. 2510555, 2025, doi: 10.1080/23311975.2025.2510555

[19] J. Kálmán, "The Role of Regulatory Sandboxes in FinTech Innovation: A Comparative Case Study of the UK, Singapore, and Hungary", FinTech, vol. 4, núm. 2, art. 26, 2025, doi: 10.3390/fintech4020026

[20] P. Schueffel y D. Stuessi, "Beyond Traditions: Swiss Banking's Journey into Digital Assets and Blockchain", FinTech, vol. 4, núm. 2, art. 18, 2025, doi: 10.3390/fintech4020018

[21] M. Hepfer y T. C. Powell, "Make Cybersecurity a Strategic Asset", MIT Sloan Management Review, vol. 62, núm. 1, pp. 40–46, 2020.

[22] V. Maphosa, "An overview of cybersecurity in Zimbabwe's financial services sector", F1000Research, vol. 12, art. 1251, 2024, doi: 10.12688/f1000research.132823.2

[23] S. Iqbal, K. M. Awan, S. Kamal, y Z. U. Rehman, "Interpretable Ensemble Learning Models for Credit Card Fraud Detection", Applied Sciences, vol. 15, núm. 22, art. 12073, 2025, doi: 10.3390/app152212073

[24] R. R. Devi, J. E. Raja, y Y. B. Chin, "Reinforcement learning with graph neural network (RL-GNN) fusion for real-time financial fraud detection: a context-aware community mining approach", Scientific Reports, vol. 15, núm. 1, art. 42953, 2025, doi: 10.1038/s41598-025-25200-3

[25] S. Kanamori et al., "Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks", Journal of Information Processing, vol. 30, pp. 789–795, 2022, doi: 10.2197/ipsjjip.30.789

[26] G. Ali, M. M. Mijwil, B. A. Buruga, y M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech", Iraqi Journal for Computer Science and Mathematics, vol. 5, núm. 3, pp. 45–91, 2024, doi: 10.52866/ijcsm.2024.05.03.004

[27] Farzana, R. Banu, A. Rahman, y I. Siddiq, "Frontiers in fintech risk management: A collaborative research platform for a secure future", Journal of Information & Optimization Sciences, vol. 46, núm. 8, pp. 2423–2433, 2025, doi: 10.47974/JIOS-2057

[28] K. F. Mauladi, I. M. L. M. Jaya, y M. A. Esquivias, "Exploring the Link between Cashless Society and Cybercrime in Indonesia", Journal of Telecommunications and the Digital Economy, vol. 10, núm. 3, pp. 58–76, 2022, doi: 10.18080/jtde.v10n3.533

[29] G. Dubauskas y M. Išoraitė, "Banking development peculiarities: blockchain, artificial intelligence (AI) and cybersecurity issues", Entrepreneurship and Sustainability Issues, vol. 12, núm. 3, pp. 61–72, 2025, doi: 10.9770/x7965543644