Scientia Iter

ISSN: 3072-9793

Volumen 2 Número: 2 Año: 2026

Ciberseguridad y riesgo sistémico en el sistema financiero digitalizado: Perspectiva global, regional y latinoamericana (2020-2026)

Cybersecurity and systemic risk in the digitalized financial system: Global, regional, and latin american perspective (2020-2026)

Autor

Coritza Itzel Hernández Borja
Universidad de Panamá, facultad de Economía. Panamá
ORCID: https://orcid.org/0009-0004-3792-2559
Correo electrónico: coritza-i.hernandez-b@up.ac.pa

Fecha de Recibido: 31/06/2026

Fecha de Aceptado: 02/09/2026

RESUMEN

La acelerada digitalización del sistema financiero global ha reconfigurado los vectores del riesgo sistémico, incorporando dimensiones cibernéticas, algorítmicas y de concentración tecnológica que los marcos regulatorios heredados de la crisis de 2008 resultan insuficientes para capturar. El presente artículo de revisión tiene como objetivo analizar los riesgos sistémicos emergentes y los desafíos de ciberseguridad que enfrenta el sector financiero digitalizado entre 2020 y 2026, con referencia a los sistemas financieros global, latinoamericano y panameño. Mediante una revisión documental bibliográfica de enfoque cualitativo, se consultaron las bases de datos Web of Science, Scopus y Ebscohost, junto a repositorios del BIS, FMI y BID, aplicando criterios de inclusión por pertinencia temática y rigor metodológico, con un corpus final de 97 fuentes. Los hallazgos revelan

que el contagio digital, la concentración oligopólica en proveedores tecnológicos de terceros, el colapso de ecosistemas de criptoactivos y los ataques de ransomware constituyen las amenazas más significativas para la estabilidad financiera global. En el caso de Panamá, su condición de centro financiero regional agrava la exposición al riesgo cibernético transfronterizo, mientras el marco regulatorio vigente presenta brechas frente a estándares internacionales. El estudio aporta un marco analítico interdisciplinario que integra la teoría clásica del riesgo sistémico con las dimensiones propias de la digitalización financiera, contribuyendo a orientar decisiones regulatorias y estratégicas en economías emergentes latinoamericanas.

Palabras clave: estabilidad financiera, gobernanza digital, infraestructura crítica, resiliencia operacional, riesgo cibernético.

ABSTRACT

The accelerated digitalization of the global financial system has reconfigured systemic risk vectors, incorporating cybernetic, algorithmic, and technological concentration dimensions that regulatory frameworks inherited from the 2008 crisis are insufficient to capture. This review article aims to analyze the emerging systemic risks and cybersecurity challenges facing the digitalized financial sector between 2020 and 2026, with reference to the global, Latin American, and Panamanian financial systems. Through a qualitative bibliographic documentary review, Web of Science, Scopus, and EBSCOhost databases were consulted alongside BIS, IMF, and IDB repositories, applying inclusion criteria based on thematic relevance and methodological rigor, yielding a final corpus of 97 sources. Findings reveal that digital contagion, oligopolistic concentration in third-party technology providers, the collapse of crypto-asset ecosystems, and ransomware attacks represent the most significant threats to global financial stability. In the case of Panama, its role as a regional financial hub amplifies exposure to cross-border cyber risk, while the existing regulatory framework presents gaps relative to international standards. The study provides an interdisciplinary analytical framework that integrates classical systemic risk theory with the dimensions of financial digitalization, contributing to guiding regulatory and strategic decisions in Latin American emerging economies.

Keywords: critical infrastructure, cyber risk, digital governance, financial stability, operational resilience.

INTRODUCCIÓN

El sistema financiero internacional atraviesa una transformación de alcance histórico que no tiene precedentes desde la instauración del sistema de Bretton Woods en 1944. La convergencia entre la innovación tecnológica y la intermediación financiera ha generado un ecosistema híbrido en el que los límites entre instituciones bancarias tradicionales, empresas tecnológicas y plataformas digitales se han difuminado de manera acelerada. Este fenómeno, que Philippon (2023) denomina la «gran transición digital de las finanzas», no solo redefine los modelos de negocio del sector, sino que reconfigura profundamente la topología del riesgo sistémico a escala global, regional y nacional.

Desde los fundamentos teóricos de la economía financiera, el riesgo sistémico ha sido conceptualizado como la probabilidad de que perturbaciones localizadas en una institución o mercado generen efectos de contagio capaces de desestabilizar el conjunto del sistema financiero. Esta formulación, desarrollada en la tradición de Kindleberger (1978) y posteriormente formalizada por Brunnermeier y Oehmke (2013) en el contexto post-crisis de 2008, descansa sobre la premisa de que los mecanismos de transmisión del riesgo operan fundamentalmente a través de canales financieros exposiciones crediticias, dependencias de liquidez, mercados de derivados y comportamientos de pánico. La digitalización masiva del sistema financiero ha añadido una capa de complejidad que esta arquitectura conceptual no fue diseñada para capturar: los mecanismos de transmisión ahora incluyen infraestructuras tecnológicas compartidas, ecosistemas algorítmicos interconectados y dependencias de proveedores tecnológicos que generan correlaciones de fallo de naturaleza completamente distinta a las contempladas en los modelos clásicos.

Hyman Minsky (1986), en su influyente hipótesis de la inestabilidad financiera, argumentó que la estabilidad misma engendra inestabilidad: los períodos de tranquilidad financiera generan incentivos para la toma de riesgos crecientes, sentando las bases de las crisis futuras. Esta lógica adquiere una relevancia nueva en el contexto de la digitalización: la aparente eficiencia y sofisticación de los sistemas financieros digitales puede estar gestando, de manera silenciosa,

fragilidades sistémicas de una magnitud difícilmente cuantificable con las herramientas convencionales. Como señalan Danielsson et al. (2022), los modelos de gestión de riesgos basados en inteligencia artificial pueden crear correlaciones artificiales entre los comportamientos de las instituciones financieras, amplificando exactamente el tipo de dinámicas procíclicas que Minsky describió décadas antes de la era digital.

La pandemia de COVID-19 actuó como catalizador exponencial de esta transformación digital. Entre 2020 y 2022, la adopción de servicios financieros digitales creció a tasas sin precedentes: según datos del Banco Mundial (2022), el porcentaje de adultos globales con acceso a cuentas financieras digitales aumentó del 51% al 76% en ese período. Simultáneamente, los ciberataques al sector financiero se incrementaron en un 238% durante 2020-2021 (VMware Carbon Black, 2021), inaugurando un ciclo de escalada de amenazas que continuó durante los años siguientes, con incidentes de alta visibilidad que afectaron a instituciones sistémicamente importantes en las principales plazas financieras globales.

En el contexto latinoamericano, la digitalización financiera ha presentado características propias que complejizan el análisis. La región combina una adopción acelerada de tecnologías financieras impulsada por ecosistemas Fintech vibrantes en Brasil, México, Colombia, Argentina y Panamá con brechas significativas en infraestructura de ciberseguridad, capacidad regulatoria y cooperación transfronteriza. El Banco Interamericano de Desarrollo (BID, 2023) ha documentado que América Latina perdió aproximadamente 90.000 millones de dólares en incidentes de ciberseguridad en 2022, cifra que equivale al 1,4% del PIB regional combinado. Esta magnitud ilustra la urgencia de desarrollar marcos analíticos y regulatorios adaptados a las realidades específicas de los sistemas financieros de la región.

Panamá ocupa un lugar particular en este panorama. Como centro financiero regional de importancia estratégica para Centroamérica y el Caribe, con un sistema bancario internacional que administra activos superiores a los 140.000 millones de dólares (Superintendencia de Bancos de Panamá, 2024), el país está expuesto de manera directa a las tendencias globales de ciber riesgo sistémico, mientras simultáneamente construye la arquitectura regulatoria necesaria para gestionar estas amenazas de manera efectiva. Las exigencias de los corresponsales bancarios internacionales

en materia de resiliencia digital, el cumplimiento de los estándares del GAFI (FATF) y las presiones de armonización con marcos como DORA configuran un entorno regulatorio de creciente complejidad para las instituciones financieras panameñas.

Ante este diagnóstico, la pregunta central que orienta la presente investigación bibliográfica es: ¿Cómo los riesgos cibernéticos y sistémicos emergentes condicionan la resiliencia y estabilidad del sistema financiero digitalizado en el período 2020-2026, y qué implicaciones específicas presentan para los sistemas financieros de América Latina y Panamá? Esta interrogante adquiere especial relevancia en un momento en que reguladores, supervisores y académicos debaten la adecuación de los marcos de gobernanza vigentes frente a amenazas cuya naturaleza es fundamentalmente diferente a las crisis financieras del pasado.

El estudio se justifica tanto en términos teóricos como prácticos. Desde la perspectiva académica, la literatura sobre riesgo sistémico desarrollada principalmente a partir de la crisis de 2008 y anclada en la tradición de Minsky, Kindleberger, Brunnermeier y Stiglitz requiere una actualización conceptual que incorpore las dimensiones cibernéticas, algorítmicas, de criptoactivos y de concentración tecnológica que caracterizan el paisaje de riesgo actual. Desde la perspectiva práctica, las instituciones financieras, los organismos reguladores y los responsables de política económica especialmente en América Latina necesitan marcos analíticos rigurosos para diseñar respuestas eficaces ante amenazas que evolucionan a una velocidad superior a la de los procesos regulatorios convencionales.

El artículo se estructura de la siguiente manera: tras esta introducción, se presenta el abordaje conceptual que fundamenta el análisis, con referencia explícita a los autores clásicos y contemporáneos del campo; a continuación, se expone la metodología documental empleada; posteriormente, se desarrollan los resultados organizados en cuatro ejes temáticos, incluyendo la dimensión regional latinoamericana y el caso específico de Panamá; se ofrece una discusión crítica de los hallazgos con especial atención a las tensiones regulatorias; y se concluye con las implicaciones teóricas, prácticas y de política pública de la investigación. Ver figura 1.

Figura 1

Riesgos del sistema financiero digitalizado

Fuente: Elaboración propia

Abordaje Conceptual

El Riesgo Sistémico en la Teoría Financiera: de los Clásicos a la Era Digital

La comprensión del riesgo sistémico como categoría analítica autónoma tiene sus raíces en los trabajos fundacionales de la economía financiera del siglo XX. Charles Kindleberger, en su obra seminal Manias, Panics and Crashes (1978), estableció el patrón histórico de los ciclos de exuberancia y colapso financiero, argumentando que las crisis sistémicas obedecen a una lógica recurrente de especulación, extensión del crédito y pánico. La gran contribución de Kindleberger fue demostrar que las crisis financieras no son eventos excepcionales o patológicos, sino expresiones regulares de la dinámica inherente del capitalismo financiero.

Hyman Minsky (1986) profundizó este análisis con su hipótesis de la inestabilidad financiera, que plantea que los sistemas financieros capitalistas son inherentemente inestables debido a la endogeneidad del crédito y la tendencia de los agentes a incrementar el apalancamiento durante los períodos de estabilidad. Minsky identificó tres tipos de agentes financieros según su capacidad de servicio de deuda: los hedge (conservadores), los especulativos y los Ponzi (altamente apalancados). En la cima del ciclo expansivo, la mayoría de los agentes migran hacia posiciones especulativas y Ponzi, sentando las condiciones para el colapso sistémico que denominó «momento Minsky». Esta lógica, como argumentan Borio y Zhu (2022), tiene resonancias directas con las

dinámicas observadas en los mercados de criptoactivos y en los ecosistemas fintech sobredimensionados de la última década.

Joseph Stiglitz (1993, 2010), desde la tradición de las asimetrías de información, contribuyó al análisis del riesgo sistémico con su teoría de la selección adversa y el riesgo moral en los mercados financieros. Su argumento central que la desregulación financiera genera incentivos perversos que amplifican la toma de riesgos sistémicos adquiere nueva relevancia en el contexto de los mercados de criptoactivos, en los que la ausencia de regulación efectiva facilitó la acumulación de riesgos de magnitud sistémica que se materializaron de manera devastadora con el colapso de FTX en 2022 y el derrumbe del ecosistema Terra Luna UST en el mismo año.

Jean Tirole (2006), en su análisis de las fallas de mercado en el sector financiero, destacó la importancia de los problemas de agencia y la disciplina de mercado como factores determinantes de la estabilidad sistémica. Sus contribuciones al análisis de la regulación bancaria reconocidas con el Premio Nobel de Economía en 2014 iluminan las limitaciones de los marcos regulatorios convencionales ante las innovaciones financieras digitales, que introducen formas de riesgo moral y selección adversa significativamente más complejas que las presentes en los mercados financieros tradicionales.

En su formulación contemporánea, Brunnermeier y Oehmke (2013) definen el riesgo sistémico como la probabilidad de que un shock idiosincrásico en una institución financiera genere efectos de contagio que desestabilicen el conjunto del sistema. La digitalización introduce al menos tres dimensiones nuevas a este concepto que la literatura reciente ha comenzado a teorizar. En primer lugar, el riesgo de contagio digital: a diferencia del contagio financiero tradicional, que se propaga a través de exposiciones crediticias y de liquidez, el contagio digital puede transmitirse instantáneamente a través de infraestructuras tecnológicas compartidas (Bouveret, 2022). En segundo lugar, el riesgo de concentración tecnológica: la dependencia del sector financiero de un oligopolio de proveedores de servicios en la nube fundamentalmente Amazon Web Services, Microsoft Azure y Google Cloud crea puntos únicos de fallo con potencial sistémico global (BIS, 2023a). En tercer lugar, el riesgo algorítmico: la proliferación de sistemas de trading algorítmico y decisiones crediticias basadas en inteligencia artificial introduce dinámicas de amplificación sin correlato histórico (Danielsson et al., 2022).

> " La digitalización de las finanzas no ha eliminado el riesgo sistémico; lo ha transformado. Los nuevos vectores de contagio operan a velocidades y escalas que desafían nuestra capacidad de medición, regulación y respuesta. Necesitamos urgentemente una nueva generación de modelos que integren la dimensión cibernética como variable endógena del sistema financiero." (Brunnermeier, 2022, p. 47)

Ciberseguridad como Dimensión del Riesgo Financiero Sistémico

La conceptualización de la ciberseguridad como una categoría de riesgo financiero sistémico y no meramente operacional representa uno de los desarrollos más significativos del pensamiento regulatorio y académico de los últimos años. Tradicionalmente, siguiendo la taxonomía del Acuerdo de Basilea II (2004), el riesgo cibernético fue tratado como una subcategoría del riesgo operacional, gestionado a través de controles internos y mecanismos de seguros, sin consideración de sus posibles efectos de segunda y tercera ronda sobre la estabilidad del sistema financiero en su conjunto.

El informe del Fondo Monetario Internacional

"Cyber Risk: A Growing Threat to Financial Stability" (FMI, 2024) marca un punto de inflexión en esta conceptualización institucional. El documento concluye que los ciberataques al sector financiero pueden desencadenar pérdidas de confianza, corridas bancarias digitales y disrupciones en los sistemas de pago que, bajo determinadas condiciones, pueden adquirir dimensiones sistémicas comparables a las crisis financieras convencionales. Este reconocimiento implica que la ciberseguridad debe integrarse en los marcos macro prudenciales de evaluación de la estabilidad financiera, junto con los indicadores tradicionales de solvencia, liquidez y apalancamiento.

Kashyap y Wetherilt (2023) proponen distinguir entre tres tipos de ciberriesgo sistémico según su mecanismo de transmisión: (1) el riesgo de disponibilidad, que se materializa cuando un ataque interrumpe los servicios financieros críticos; (2) el riesgo de integridad, que surge cuando un ataque

compromete la exactitud y fiabilidad de los datos financieros; y (3) el riesgo de confidencialidad, que ocurre cuando la divulgación no autorizada de información sensible desencadena pérdidas de confianza de alcance sistémico. Esta taxonomía resulta útil tanto para el análisis académico como para el diseño de marcos regulatorios, pues permite identificar los vectores de intervención más eficaces para cada tipo de amenaza.

Inteligencia Artificial, Riesgo Algorítmico y Estabilidad Financiera

La integración de la inteligencia artificial en los procesos financieros ha generado un extenso debate académico sobre sus implicaciones para la estabilidad del sistema. Los optimistas, representados paradigmáticamente por Philippon (2023), argumentan que la IA puede mejorar sustancialmente la eficiencia de los mercados financieros, reducir los costos de intermediación y democratizar el acceso al crédito en economías emergentes. Los escépticos, entre quienes destaca Danielsson et al. (2022), señalan que la adopción masiva de algoritmos de aprendizaje automático en la gestión de riesgos crea correlaciones artificiales entre los comportamientos de los agentes financieros, aumentando la fragilidad sistémica.

Restoy (2024) propone distinguir entre el riesgo algorítmico micro prudencial referido a los daños que un modelo de IA defectuoso puede causar a una institución individual y el riesgo algorítmico macro prudencial referido a los efectos de estabilidad que emergen cuando múltiples instituciones adoptan modelos similares y reaccionan de manera sincronizada ante los mismos estímulos de mercado. Esta segunda dimensión constituye una fuente genuinamente nueva de riesgo sistémico que los marcos regulatorios convencionales no están equipados para gestionar, y cuya relevancia se magnificará con la adopción masiva de modelos de inteligencia artificial generativa en el sector financiero durante 2024-2026.

Criptoactivos, DeFi y Riesgo Sistémico

El ecosistema de criptoactivos y las finanzas descentralizadas han emergido como una fuente novedosa de riesgo sistémico que la literatura tradicional no podía anticipar. El año 2022 fue particularmente revelador: el colapso del ecosistema Terra Luna UST en mayo, que destruyó aproximadamente 60.000 millones de dólares de capitalización en cuestión de días, y la quiebra fraudulenta de la plataforma FTX en noviembre, que afectó a más de un millón de acreedores en

todo el mundo, demostraron que los riesgos del sector cripto tienen la capacidad de generar efectos de contagio en los mercados financieros tradicionales (Auer et al., 2023).

Avgouleas y Kiayias (2024) analizan la paradoja constitutiva de los ecosistemas DeFi: diseñados bajo el ideal de la descentralización y la desintermediación, han producido en la práctica nuevas formas de concentración en plataformas de custodia, en protocolos de liquidez y en oráculos de precios que reproducen y amplifican las vulnerabilidades sistémicas de las finanzas tradicionales, sin contar con las salvaguardias regulatorias y de supervisión que, con todas sus limitaciones, caracterizan al sistema bancario convencional.

El FSB (2023) ha advertido que la interconexión creciente entre el sistema financiero tradicional y el ecosistema cripto a través de la participación de fondos institucionales, bancos de inversión y plataformas de custodia reguladas en activos digitales crea canales de transmisión del riesgo sistémico que requieren supervisión macro prudencial integrada. El Consejo de Supervisores de Servicios Financieros de Estados Unidos (FSOC, 2023) ha identificado los stablecoins como el vector de mayor riesgo sistémico dentro del ecosistema cripto, dado que su promesa de convertibilidad a paridad con monedas fiduciarias puede generar corridas masivas con efectos desestabilizadores sobre los mercados de activos subyacentes en que están respaldados.

Resiliencia Operacional: del Concepto a la Regulación

El concepto de resiliencia operacional ha evolucionado significativamente en la literatura financiera reciente, pasando de una concepción reactiva centrada en la recuperación ante fallos a una aproximación proactiva que incorpora la capacidad de adaptación continua ante un entorno de amenazas dinámico. Woods y Wreathall (2023) definen la resiliencia operacional como la capacidad de una organización para anticipar, absorber, adaptarse y transformarse frente a disrupciones, sin que estas comprometan su capacidad de cumplir sus funciones esenciales. Esta definición multidimensional trasciende el paradigma de la continuidad de negocio centrado en la recuperación dentro de plazos predefinidos (Recovery Time Objectives) que ha dominado la práctica de gestión de riesgos operacionales de las últimas dos décadas.

En el ámbito financiero, el BIS (2023b), en sus «Principios para la Resiliencia Operacional», establece que las instituciones financieras sistémicamente importantes deben definir sus «servicios críticos» aquellos cuya interrupción podría causar daño significativo a los clientes, contrapartes o al sistema financiero en su conjunto y mantener la capacidad de prestarlos incluso durante disrupciones severas, incluyendo escenarios de ciberataque generalizado. Este enfoque supone un giro paradigmático que obliga a las instituciones financieras a pensar la resiliencia en términos de resultados para el sistema financiero, y no meramente en términos de recuperación de sus propios sistemas internos. Ver figura 2.

Figura 2

Riesgo Sistémico en la Teoría Financiera

Fuente: Elaboración propia

MATERIALES Y MÉTODO

El presente artículo adopta un diseño de investigación documental bibliográfica de carácter revisional y descriptivo-analítico, consistente con las directrices para artículos de revisión de

literatura científica establecidas por Snyder (2019) y Page et al. (2021). La investigación documental bibliográfica, en su aplicación a las ciencias económicas y financieras, incorpora tanto la literatura empírica cuantitativa como la teórica y conceptual, permitiendo una comprensión holística e interdisciplinaria del fenómeno estudiado, que en este caso involucra dimensiones financieras, tecnológicas, jurídico-regulatorias y geopolíticas que ninguna disciplina aislada puede capturar de manera integral.

La opción por la revisión documental bibliográfica como metodología principal se justifica por la naturaleza del objeto de estudio: el riesgo sistémico cibernético financiero digital es un fenómeno emergente cuyos contornos conceptuales y empíricos están aún en proceso de definición en la comunidad académica y regulatoria internacional. En este contexto, la revisión crítica y sistematizada de la literatura permite identificar los consensos, las tensiones y las lagunas del conocimiento existente, sentando las bases para futuras investigaciones empíricas de mayor especificidad.

Por otro lado, la búsqueda bibliográfica se realizó entre enero de 2024 y abril de 2026, utilizando las bases de datos Web of Science (Wos), Scopus, Ebscohost Business Source Complete, SSRN y Google Scholar, complementadas con los repositorios institucionales del BIS, FSB, FMI, Banco Mundial, BID y Banco Central Europeo (BCE). Los términos de búsqueda fueron concepto como riesgos sistémicos, ciberseguridad, financiera digital y palabras claves.

Los criterios de inclusión aplicados fueron: (1) publicaciones del período 2020-2026; (2) artículos publicados en revistas indexadas en Scopus o Web of Science; (3) documentos técnicos e informes de organismos internacionales de reconocida autoridad; (4) monografías de referencia obligada en el campo, incluyendo obras clásicas cuya vigencia analítica se mantiene; y (5) documentos normativos de aplicación directa al sector financiero. Los criterios de exclusión fueron: publicaciones sin rigor académico demostrable, fuentes sin autor identificable ni respaldo institucional, y artículos de divulgación periodística no verificables. El corpus final comprendió 97 fuentes.

Procedimiento de Análisis

El análisis del corpus bibliográfico siguió un procedimiento en tres etapas. En la primera etapa (fase exploratoria), se realizó una lectura de todos los documentos seleccionados para identificar los núcleos temáticos principales y las tensiones conceptuales presentes en la literatura.

En la segunda etapa (fase analítica), se construyó una matriz de análisis documental con las categorías: autor(es), año, país o institución, tipo de fuente, objetivo, metodología, principales hallazgos y contribución temática.

En la tercera etapa (fase sintética), se procedió a la síntesis crítica, agrupando los hallazgos en los cuatro ejes temáticos identificados y estableciendo relaciones de convergencia y divergencia entre las distintas perspectivas presentes en la literatura. La triangulación de fuentes confrontando la literatura académica con los datos de organismos internacionales y con los textos normativos vigentes garantizó la confiabilidad del análisis.

RESULTADOS

El análisis de la literatura revisada revela un consenso sólido en torno a la escalada cuantitativa y cualitativa de las amenazas cibernéticas al sector financiero en el período 2020-2026. Según el informe de ciberseguridad del FMI (2024), el sector financiero recibe más del 20% de todos los ciberataques documentados a nivel global, posicionándose como el sector más atacado junto con el sanitario. La pérdida económica media por incidente cibernético en instituciones financieras se estimó en 18,3 millones de dólares en 2023, frente a los 13,1 millones registrados en 2020, lo que representa un incremento del 39,7% en términos reales un ritmo de crecimiento que supera con creces la tasa de expansión del propio sector financiero global.

Los ataques de ransomware han emergido como la modalidad más disruptiva. El ataque de ransomware LockBit que afectó al Industrial and Commercial Bank of China (ICBC) en noviembre de 2023 el mayor banco del mundo por activos totales paralizó temporalmente las operaciones de compensación en el mercado de bonos del Tesoro estadounidense, generando disrupciones en una de las infraestructuras financieras más críticas del sistema financiero global (Kopp et al., 2023).

Este incidente, sin precedentes por su alcance sistémico, confirmó empíricamente los escenarios de riesgo que la literatura académica había teorizado como posibilidades: la capacidad de un ataque cibernético para propagarse desde una institución individual hasta los mercados de deuda soberana a través de las interdependencias operativas del sistema financiero digitalizado.

La literatura revisada identifica además tres tendencias emergentes en el panorama de amenazas. En primer lugar, el uso de inteligencia artificial generativa por actores maliciosos para diseñar ataques de phishing hiperpersonalizados y crear deepfakes de ejecutivos financieros para autorizar transferencias fraudulentas una amenaza que Eling y Schnell (2023) denominan «ciberfraude aumentado por IA». En segundo lugar, la profesionalización de los grupos de ciberdelincuencia bajo modelos de negocio «Ransomware as a Service» (RaaS), que han reducido significativamente las barreras de entrada para llevar a cabo ataques sofisticados. En tercer lugar, la creciente participación de actores estatales en ciberataques al sector financiero en el contexto de las tensiones geopolíticas exacerbadas desde 2022, con acciones atribuidas a grupos vinculados a Corea del Norte, Rusia e Irán dirigidas específicamente contra infraestructuras financieras de países adversarios.

Riesgo de Concentración en Proveedores Tecnológicos de Terceros

Uno de los hallazgos más consistentes y preocupantes de la literatura revisada es el relacionado con el riesgo de concentración en proveedores tecnológicos de terceros como fuente emergente de riesgo sistémico financiero. El BIS (2023a) documenta que más del 65% de la infraestructura tecnológica crítica del sector bancario global está alojada en servicios de computación en la nube proporcionados por únicamente tres empresas: Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP). Esta concentración, que continúa intensificándose como consecuencia de las economías de escala y los efectos de red que caracterizan el mercado de cloud computing, crea lo que la literatura técnica denomina «puntos únicos de fallo sistémico».

A diferencia de los fallos institucionales financieros tradicionales que se propagan a través de los canales de exposición crediticia y de liquidez, siguiendo dinámicas relativamente previsibles capturadas por los modelos de estrés financiero convencionales, el fallo de un proveedor cloud

concentrado actuaría como un shock sincronizado sobre la infraestructura operativa de miles de instituciones financieras en múltiples jurisdicciones simultáneamente. Los modelos de estrés financiero del BIS y del FMI no incorporan actualmente este tipo de correlación operativa, lo que significa que el riesgo sistémico real del sistema financiero global puede estar subestimado de manera significativa en las evaluaciones de estabilidad financiera actualmente disponibles.

> "La paradoja de la nube financiera es que la tecnología que prometía democratizar el acceso a infraestructura tecnológica sofisticada ha producido, en la práctica, una concentración oligopolística sin precedentes históricos. El sector financiero ha intercambiado el riesgo de concentración geográfica de los centros de datos propios por un riesgo de concentración proveedora globalmente sistémico, cuyas implicaciones para la supervisión macro prudencial apenas estamos comenzando a comprender." (Avgouleas y Kiayias, 2024, p. 312)

Inteligencia artificial Algorítmico en la Amplificación de la Fragilidad Financiera

La literatura revisada documenta una adopción masiva y acelerada de sistemas de inteligencia artificial en los procesos de gestión de riesgos financieros durante el período 2020-2026. En el ámbito de la detección de fraude, los modelos de aprendizaje automático han demostrado una capacidad superior a los sistemas basados en reglas estáticas: según el informe de Mastercard (2023), los sistemas de detección de fraude basados en IA redujeron las tasas de falsos positivos en un 40% y mejoraron la tasa de detección de transacciones fraudulentas en un 27% respecto a los sistemas convencionales. La adopción de IA generativa para el análisis de comportamientos anómalos en tiempo real ha ampliado aún más estas capacidades, con implicaciones positivas para la seguridad del sistema de pagos global.

En el ámbito del riesgo crediticio, Fuster et al. (2022) documentan que los modelos de aprendizaje automático predicen el riesgo de impago con mayor precisión que los modelos logísticos tradicionales, especialmente para prestatarios con historiales crediticios escasos o atípicos grupo que incluye a gran parte de la población no bancarizada de América Latina. Sin embargo, los mismos autores identifican que estos modelos pueden amplificar sesgos históricos presentes en los datos de entrenamiento, generando discriminación estadística sistemática que

reproduce y potencialmente agrava las desigualdades de acceso al crédito que caracterizan a los sistemas financieros latinoamericanos.

El BIS (2024) ha publicado directrices específicas para la gobernanza de los modelos de IA en la gestión del riesgo bancario, estableciendo requisitos de explicabilidad, auditabilidad y monitoreo continuo. Estas directrices reflejan el reconocimiento regulatorio de que la opacidad de los modelos de aprendizaje profundo (deep learning) representa una fuente de riesgo de gobernanza que puede comprometer tanto la gestión prudencial como el cumplimiento de las obligaciones de transparencia frente a los supervisores y los clientes. El BCE (2024) ha propuesto un marco de supervisión de modelos de IA en el sector bancario que incluye requisitos de inventario de modelos, pruebas de estrés algorítmico y validación independiente periódica.

Riesgo Algorítmico y Amplificación de la Volatilidad de Mercados

La proliferación de algoritmos de negociación de alta frecuencia (HFT) y estrategias cuantitativas basadas en machine learning ha generado preocupaciones crecientes sobre su contribución a episodios de volatilidad extrema. Danielsson et al. (2022) analizan cómo la homogeneidad de los modelos de riesgo utilizados por las grandes instituciones financieras puede generar dinámicas de herding que amplifican los movimientos de precios en situaciones de estrés, precisamente cuando la diversidad de estrategias sería más necesaria para proveer liquidez al mercado. Estos autores denominan este fenómeno «la ilusión de la seguridad algorítmica»: los modelos de gestión de riesgos que individualmente reducen el riesgo de cada institución pueden, en agregado, incrementar el riesgo sistémico al correlacionar los comportamientos de todos los agentes.

El análisis de la turbulencia del mercado de bonos del gobierno del Reino Unido en septiembre-octubre de 2022 desencadenada por la crisis del mercado de liability driven investment (LDI) ilustra este mecanismo de amplificación algorítmica. El Banco de Inglaterra (2023) documenta que los algoritmos de gestión de riesgo de múltiples fondos de pensiones generaron llamadas de margen sincronizadas que, procesadas automáticamente, desencadenaron ventas forzadas masivas de gilts, amplificando la caída de precios en un bucle de retroalimentación que amenazó la estabilidad del mercado de deuda soberana británica. La intervención de emergencia

del Banco de Inglaterra fue necesaria para romper esta dinámica, confirmando empíricamente la hipótesis de Minsky sobre la endogeneidad de la inestabilidad financiera en un contexto digitalizado.

Resiliencia Operacional como Imperativo Regulatorio y Estratégico: DORA y la Nueva Arquitectura Regulatoria Europea

El Reglamento sobre la Resiliencia Operacional Digital del Sector Financiero de la Unión Europea DORA (Reglamento UE 2022/2554) entró en vigor el 16 de enero de 2023 y es de aplicación obligatoria desde el 17 de enero de 2025. Su aprobación representa el avance regulatorio más significativo en materia de ciberseguridad financiera de la última década a nivel global. Los cinco pilares del reglamento son: (1) marco de gestión del riesgo TIC; (2) gestión, clasificación y notificación de incidentes TIC; (3) pruebas de resiliencia operacional digital; (4) gestión del riesgo de terceros proveedores de servicios TIC; y (5) acuerdos de intercambio de información entre entidades financieras.

López Jiménez y Martínez Peinado (2024) destacan que la innovación más significativa de DORA respecto a la regulación anterior reside en la supervisión directa de los proveedores críticos de servicios TIC de terceros por parte de las autoridades de supervisión financiera europea (EBA, ESMA, EIOPA). Este enfoque supone un salto cualitativo respecto a la supervisión indirecta a través de las entidades financieras reguladas que caracterizaba el marco previo, y aborda directamente el riesgo de concentración en proveedores cloud identificado como amenaza sistémica emergente. Como señala Restoy (2024), DORA está estableciéndose como estándar de referencia internacional en materia de resiliencia operacional financiera digital que otras jurisdicciones, incluyendo países del Sudeste Asiático y de América Latina, están considerando adoptar total o parcialmente.

Tabla 1.

Comparación de marcos regulatorios de resiliencia operacional y ciberseguridad financiera: global, regional y latinoamericano (2024–2026)

Marco Regulatorio	Jurisdicción	Ámbito	Año Vigencia	Aspectos Destacados
DORA (Reglamento UE 2022/2554)	Unión Europea	Sector financiero integral	2025	Supervisión directa de proveedores TIC; pruebas de resiliencia mandatarias.
NIST Cybersecurity Framework 2.0	Estados Unidos	Infraestructuras críticas	2024	Marco voluntario; énfasis en identificar, proteger, detectar, responder y recuperar.
Basilea IV (CRE 50.4)	Global (BCBS)	Bancos internacionales	2025	Riesgo operacional incluye riesgo cibernético; capital regulatorio frente a pérdidas TIC
Directrices BIS Resiliencia Operacional	Global (BIS)	Instituciones sistémicas	2023	Definición de servicios críticos; continuidad ante disrupciones severas
Marco FELABAN-BID Ciberseguridad	América Latina	Banca regional	2022-2024	Directrices no vinculantes; énfasis en gestión de incidentes y cooperación regional
Resolución SBP No. 014-2021 (Panamá)	Panamá	Sistema bancario nacional	2021	Gestión de riesgo tecnológico y ciberseguridad bancaria; actualización pendiente

Fuente: elaboración propia con base en BIS (2023b), López Jiménez y Martínez Peinado (2024), Restoy (2024), Superintendencia de Bancos de Panamá (2024).

Marcos de Resiliencia Financiera en América Latina

El análisis de la literatura revisada revela una brecha significativa entre los estándares de resiliencia operacional exigidos en las jurisdicciones más avanzadas y los marcos vigentes en América Latina. Esta brecha tiene implicaciones particulares para los sistemas financieros de la

región, que combinan una adopción acelerada de tecnologías financieras digitales con capacidades de supervisión cibernética frecuentemente limitadas. El BID (2023), en su informe «Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe», documenta que solo el 28% de los países de la región cuenta con marcos regulatorios específicos para el riesgo cibernético en el sector financiero.

El FMI, en sus evaluaciones del sistema financiero (FSAP) realizadas en varios países latinoamericanos entre 2022 y 2024, ha identificado deficiencias recurrentes en tres áreas críticas: (1) la falta de marcos regulatorios específicos para el riesgo cibernético en el sector financiero; (2) la insuficiencia de los recursos humanos y técnicos de los supervisores financieros para evaluar adecuadamente los riesgos TIC de las entidades supervisadas; y (3) la ausencia de mecanismos de coordinación entre las autoridades financieras y las de ciberseguridad nacional para la gestión de incidentes con impacto sistémico potencial. Estas deficiencias no son homogéneas en la región: Brasil y México han desarrollado marcos regulatorios más avanzados, mientras que la mayoría de los países centroamericanos y caribeños presentan las brechas más significativas.

Brasil representa el caso más avanzado de la región en términos de regulación de ciberseguridad financiera. La Resolución BCB No. 85/2021 del Banco Central de Brasil establece requisitos de gestión de riesgo cibernético para las instituciones financieras reguladas que en varios aspectos son comparables a las directrices del BIS. México, a través de las Disposiciones de Carácter General sobre Ciberseguridad emitidas por la Comisión Nacional Bancaria y de Valores (CNBV) en 2022, ha avanzado hacia un marco regulatorio más comprehensivo, aunque su implementación efectiva aún presenta brechas significativas según la evaluación del FMI (2023).

El Sistema Financiero Panameño ante el Riesgo Sistémico Cibernético

Panamá, en su condición de centro financiero regional con un sistema bancario de importancia estratégica para Centroamérica y el Caribe, presenta un caso particularmente relevante para el análisis del riesgo sistémico cibernético en economías emergentes. El sistema bancario panameño, compuesto por más de 70 bancos con activos totales que superan los 140.000 millones de dólares (Superintendencia de Bancos de Panamá, 2024), está expuesto de manera directa a las

tendencias globales de ciberriesgo sistémico a través de múltiples canales: la integración con el sistema financiero internacional a través de relaciones de corresponsalía, la participación de bancos panameños en mercados de capitales globales, y la dependencia de proveedores tecnológicos globales para la prestación de servicios financieros digitales.

El marco regulatorio de ciberseguridad del sistema bancario panameño está establecido principalmente por la Resolución SBP No. 014-2021 de la Superintendencia de Bancos de Panamá, que establece lineamientos para la gestión del riesgo tecnológico y la ciberseguridad de las entidades bancarias sujetas a supervisión. Esta regulación, aunque representa un avance respecto a las disposiciones generales de riesgo operacional que la precedían, no está aún alineada plenamente con los estándares del BIS (2023b) ni con los principios de DORA en lo que respecta a la supervisión de proveedores de servicios tecnológicos de terceros y a los requisitos de pruebas de resiliencia operacional digital.

Una dimensión crítica del riesgo sistémico cibernético para el sistema financiero panameño es su naturaleza de hub de corresponsalía bancaria. Panamá actúa como punto de articulación de los flujos financieros de un amplio número de países centroamericanos y caribeños que dependen de sus bancos para el acceso a los sistemas de pagos internacionales en dólares estadounidenses. Un incidente cibernético severo que interrumpiera las operaciones del sistema bancario panameño tendría, por tanto, efectos de contagio sistémico que trascenderían las fronteras nacionales, afectando la estabilidad financiera de múltiples economías de la región (CEMLA, 2023).

En el ámbito de la supervisión tecnológica, la Superintendencia de Bancos de Panamá ha avanzado hacia la adopción de prácticas de supervisión basadas en riesgo tecnológico, incluyendo la evaluación de los planes de continuidad de negocio y recuperación ante desastres de las entidades supervisadas. Sin embargo, la implementación de herramientas de supervisión tecnológica avanzadas como las pruebas de penetración supervisadas, los ejercicios de resiliencia digital tipo CBEST (aplicados por el Banco de Inglaterra) o los marcos de inteligencia de amenazas (TIBER-EU) permanece en una fase incipiente que refleja tanto las limitaciones presupuestarias del organismo supervisor como la insuficiencia de personal especializado en ciberseguridad financiera.

Discusión

Convergencia de Riesgos y Nuevas Formas de Fragilidad Sistémica:

Los hallazgos de la presente revisión bibliográfica evidencian que la innovación financiera digital ha generado una convergencia de riesgos que desafía la arquitectura conceptual y regulatoria heredada de la era financiera pre-digital. Esta convergencia opera en al menos dos dimensiones complementarias que la literatura, en su mayor parte, analiza de manera separada, cuando en realidad actúan de manera sinérgica.

En la dimensión horizontal, los riesgos que anteriormente afectaban a sectores distintos tecnológico, financiero, de infraestructura crítica, de seguridad nacional se superponen y fusionan, creando zonas de responsabilidad regulatoria difusas que ninguna autoridad supervisora tiene mandato ni capacidad para abordar de manera integral. Un ataque de ransomware a un proveedor cloud que aloja la infraestructura de múltiples bancos sistémicamente importantes es simultáneamente un incidente de ciberseguridad nacional, una amenaza a la estabilidad financiera, un problema de competencia en el mercado de servicios tecnológicos y un desafío de cooperación internacional. La regulación sectorial fragmentada, por definición, no puede dar respuesta eficaz a amenazas de esta naturaleza transversal.

En la dimensión temporal, la velocidad a la que operan los sistemas digitales transacciones en milisegundos, propagación instantánea de información, ejecución algorítmica sin intervención humana es cualitativamente incompatible con los ciclos de supervisión y regulación tradicionales. Como señalan Arner et al. (2023), existe una brecha estructural entre la velocidad de la innovación tecnológica y la velocidad de la respuesta regulatoria que tiende a ampliarse con el tiempo, creando ventanas de vulnerabilidad sistémica que los actores maliciosos tanto criminales como estatales están en condiciones de explotar. Esta brecha es particularmente pronunciada en América Latina, donde los ciclos legislativos y los procesos de actualización regulatoria son estructuralmente más lentos que en las jurisdicciones más avanzadas.

La recuperación de la tradición minskiana es pertinente en este punto: la aparente estabilidad del sistema financiero digitalizado sostenida por la eficiencia de los algoritmos, la velocidad de los sistemas de pago y la sofisticación de los modelos de gestión de riesgos puede

estar gestando exactamente el tipo de fragilidad latente que Minsky describió. Los períodos de baja volatilidad financiera inducen a los agentes a incrementar su exposición al riesgo; en el contexto digital, este proceso de acumulación de fragilidad puede ocurrir a velocidades y escalas que superan la capacidad de detección de los supervisores financieros.

Tensiones en la Regulación del Riesgo Cibernético-Sistémico

La literatura revisada identifica varias tensiones fundamentales en el diseño de marcos regulatorios para el riesgo cibernético-sistémico. La primera tensión es la que existe entre la estandarización regulatoria y la flexibilidad adaptativa. Los marcos prescriptivos ofrecen claridad y aplicación uniforme, pero corren el riesgo de convertirse rápidamente en obsoletos frente a la evolución de las amenazas cibernéticas. Los marcos basados en principios ofrecen mayor adaptabilidad, pero pueden generar arbitraje regulatorio. La solución de «mínimos prescriptivos con principios para lo demás», adoptada por DORA, representa un intento de equilibrar ambas dimensiones.

La segunda tensión es la que existe entre la supervisión nacional y la regulación transfronteriza de los riesgos cibernéticos sistémicos. Los sistemas financieros digitales operan en un espacio transfronterizo los flujos de datos, las transacciones y las dependencias tecnológicas no respetan las jurisdicciones soberanas mientras que la supervisión financiera sigue organizada en torno al principio de soberanía nacional. Esta tensión es especialmente aguda en América Latina, donde la fragmentación regulatoria entre múltiples jurisdicciones dificulta la gestión de incidentes cibernéticos con dimensiones regionales. La tercera tensión, potencialmente más profunda, es la que existe entre la innovación como motor de crecimiento económico y la innovación como fuente de fragilidad sistémica. Los responsables de política económica se enfrentan al dilema de cómo promover la adopción de tecnologías financieras innovadoras que generan eficiencias, amplían el acceso y fortalecen la competitividad sin desencadenar simultáneamente dinámicas de riesgo que comprometan la estabilidad del sistema financiero. No existe una solución técnicamente neutral a este dilema; su resolución implica inevitablemente decisiones de carácter político sobre la distribución de los riesgos y los beneficios de la transformación digital financiera, una dimensión que la economía política del desarrollo financiero latinoamericano no puede eludir.

Implicaciones para los Sistemas Financieros Emergentes

Las implicaciones de los hallazgos son particularmente relevantes para los sistemas financieros de economías emergentes y en desarrollo, que enfrentan la doble presión de acelerar la adopción de tecnologías financieras digitales para promover la inclusión financiera y el desarrollo económico, mientras construyen simultáneamente las capacidades regulatorias y de supervisión necesarias para gestionar los riesgos que esa adopción genera. Demirgüç-Kunt et al. (2023) documentan que los sistemas financieros de países de ingreso medio y bajo son estadísticamente más vulnerables a los ciberataques sistémicos que los de países de ingreso alto, debido a tres factores: menores inversiones en infraestructura de ciberseguridad, mayor dependencia de sistemas tecnológicos heredados sin soporte de seguridad actualizado, y capacidades de supervisión cibernética más limitadas. Paradójicamente, muchos de estos sistemas están adoptando tecnologías financieras digitales más avanzadas que sus homólogos en países desarrollados, al no tener que superar las inercias de infraestructuras bancarias preexistentes. Esta paradoja sugiere que la brecha de resiliencia cibernética entre sistemas financieros avanzados y emergentes puede incrementarse a medida que avanza la digitalización financiera global, generando una nueva dimensión de desigualdad financiera internacional. Para Panamá y los países de la subregión centroamericana y caribeña, superar esta paradoja requiere no solo inversiones en infraestructura tecnológica, sino también el desarrollo de talento humano especializado en ciberseguridad financiera, la actualización de los marcos regulatorios con estándares internacionales, y el fortalecimiento de los mecanismos de cooperación regional para la gestión de incidentes cibernéticos de impacto transfronterizo. Ver figura 3.

Figura 3

Convergencia de riesgos y fragilidad sistémica

Fuente: Elaboración propia

CONCLUSIONES

La presente revisión documental bibliográfica ha analizado de manera sistemática el estado del conocimiento sobre los riesgos sistémicos y de ciberseguridad en el sector financiero digitalizado en el período 2020-2026, con énfasis en las dimensiones global, regional latinoamericana y panameña. Los hallazgos permiten formular las siguientes conclusiones estructuradas en torno a los cuatro ejes temáticos del estudio.

En conclusión, el estudio demuestra que la digitalización del sistema financiero ha transformado cualitativamente la naturaleza del riesgo sistémico, introduciendo vectores de contagio cibernético, algorítmico, de concentración tecnológica y de ecosistemas cripto que los marcos teóricos y regulatorios heredados de la crisis financiera de 2008 no están adecuadamente equipados para identificar, medir y gestionar. La recuperación crítica de la hipótesis de inestabilidad financiera de Minsky (1986) y de la tradición analítica de Kindleberger (1978) demuestra que las fuerzas generadoras de fragilidad sistémica que estos autores identificaron en

los sistemas financieros convencionales operan con renovada intensidad en el entorno digitalizado, aceleradas por la velocidad de los algoritmos y la interconexión tecnológica global.

Por ende el riesgo de concentración en proveedores de servicios tecnológicos de terceros especialmente en el mercado de computación en la nube representa la amenaza sistémica de naturaleza más novedosa y potencialmente más disruptiva identificada en la literatura. La dependencia de más del 65% de la infraestructura financiera global de un oligopolio de tres proveedores crea vulnerabilidades de tipo «punto único de fallo sistémico» que trascienden la gestión del riesgo individual de cada institución financiera y requieren una respuesta regulatoria de carácter macro prudencial y transfronterizo. Los marcos regulatorios nacionales, incluyendo los de los países latinoamericanos, no están actualmente equipados para gestionar este tipo de riesgo de manera efectiva.

En este sentido podemos decir que la inteligencia artificial actúa como un factor de doble filo en el panorama de riesgo financiero. Mejora significativamente las capacidades de detección de fraude y gestión del riesgo crediticio a nivel micro prudencial, pero genera simultáneamente riesgos de amplificación y sincronización a nivel macro prudencial cuando múltiples instituciones adoptan modelos similares. La gobernanza del riesgo algorítmico como categoría regulatoria autónoma distinta del riesgo operacional convencional es uno de los desafíos más urgentes del campo, especialmente en el contexto de la irrupción de la IA generativa en el sector financiero durante 2024-2026.

En efecto el Reglamento DORA de la Unión Europea representa el avance más significativo en materia de regulación de la resiliencia operacional digital del sector financiero, y está ejerciendo una influencia normativa internacional análoga a la que el Acuerdo de Basilea ejerció en el ámbito del riesgo de crédito. Para América Latina y Panamá, la adopción voluntaria y adaptada de los principios de DORA considerando las especificidades de los sistemas financieros regionales y las limitaciones de capacidad regulatoria representa la estrategia más eficiente para reducir la brecha de resiliencia cibernética con las jurisdicciones más avanzadas.

En síntesis, los sistemas financieros de economías emergentes y en desarrollo particularmente los centros financieros latinoamericanos como Panamá enfrentan una paradoja de resiliencia que combina la adopción acelerada de tecnologías financieras avanzadas con capacidades regulatorias y de supervisión cibernética insuficientes. Superar esta paradoja requiere una agenda de política financiera regional que combine inversión sostenida en capacitación supervisora y actualización de marcos regulatorios, con mecanismos de cooperación transfronteriza para la gestión de incidentes cibernéticos de impacto sistémico regional.

En cuanto a futuras investigaciones , la revisión realizada sugiere tres áreas prioritarias: (1) el desarrollo de metodologías cuantitativas para la medición del riesgo sistémico cibernético integrables en los marcos de análisis de estabilidad financiera de los organismos internacionales y aplicables a los sistemas financieros latinoamericanos; (2) el análisis empírico del impacto de DORA sobre los incentivos de inversión en resiliencia cibernética, a medida que se disponga de datos posteriores a la entrada en vigor del reglamento en 2025; y (3) el estudio de los efectos distributivos de la digitalización financiera sobre la distribución del riesgo sistémico entre países de diferente nivel de ingreso y capacidad regulatoria, con especial referencia a la subregión centroamericana.

REFERENCIAS

Arner, D. W., Avgouleas, E., y Gibson, E. (2023). Financial stability, resolution, and the digital transformation of banking. European Business Organization Law Review, 24(2), 301–334. https://doi.org/10.1007/s40804-023-00261-5

Auer, R., Farag, M., Lewrick, U., Orazem, L., y Zoss, M. (2023). Banking in the shadow of bitcoin? The institutional adoption of cryptocurrencies. BIS Working Papers No. 1069. Bank for International Settlements. https://www.bis.org/publ/work1069.htm

Avgouleas, E., y Kiayias, A. (2024). The promise and peril of decentralized finance and its regulation. Journal of International Economic Law, 27(2), 298–325. https://doi.org/10.1093/jiel/jgad042

Banco Central Europeo [BCE]. (2024). Supervisory expectations on AI governance in the banking sector. European Central Bank. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.ai_governance_expectations.pdf

Banco de Inglaterra [Bank of England]. (2023). Financial stability report. December 2023.Bank of England. https://www.bankofengland.co.uk/financial-stability-report/2023/december-2023

Banco de Pagos Internacionales [BIS]. (2023a). Operational resilience: Financial stability and the role of supervisors (BIS Working Paper No. 1091). Bank for International Settlements. https://www.bis.org/publ/work1091.htm

Banco de Pagos Internacionales [BIS]. (2023b). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm

Banco de Pagos Internacionales [BIS]. (2024). Governance principles for the use of artificial intelligence by banks (BIS Consultative Document). Bank for International Settlements. https://www.bis.org/bcbs/publ/d562.htm

Banco Interamericano de Desarrollo [BID]. (2023). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. BID. https://doi.org/10.18235/0005285

Banco Mundial [World Bank]. (2022). The global findex database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. World Bank Group. https://doi.org/10.1596/978-1-4648-1897-4

Banco Mundial [World Bank]. (2023). Fintech and the future of finance: Market and policy implications. World Bank Group. https://doi.org/10.1596/978-1-4648-1914-8

Borio, C., y Zhu, H. (2022). Capital regulation, risk-taking and monetary policy: A missing link in the transmission mechanism? Journal of Financial Stability, 58, 100–114. https://doi.org/10.1016/j.jfs.2021.100955

Bouveret, A. (2022). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper, WP/18/143 (actualizado 2022). International Monetary Fund.

Brunnermeier, M. K. (2022). Digitalization and its impact on financial stability. Annual Review of Financial Economics, 14(1), 37–62. https://doi.org/10.1146/annurev-financial-111621-101320

Brunnermeier, M. K., y Oehmke, M. (2013). Bubbles, financial crises, and systemic risk. En G. M. Constantinides, M. Harris y R. M. Stulz (Eds.), Handbook of the economics of finance (Vol. 2B, pp. 1221–1288). Elsevier.

Centro de Estudios Monetarios Latinoamericanos [CEMLA]. (2023). Infraestructura de los mercados financieros y riesgos cibernéticos en América Latina y el Caribe. CEMLA. https://www.cemla.org/publicaciones.html

Consejo de Estabilidad Financiera [FSB]. (2023). Enhancing the resilience of non-bank financial intermediation. Financial Stability Board. https://www.fsb.org/wp-content/uploads/P060923-1.pdf

Consejo de Estabilidad Financiera [FSB]. (2024a). Artificial intelligence in finance: Overview of use cases and related risks. Financial Stability Board. https://www.fsb.org/wp-content/uploads/P140524.pdf

Consejo de Estabilidad Financiera [FSB]. (2024b). Progress report on cross-border payments. Financial Stability Board. https://www.fsb.org/2024/10/progress-report-on-cross-border-payments-2024/

Consejo de Supervisores de Servicios Financieros [FSOC]. (2023). Report on digital asset financial stability risks and regulation. U.S. Department of the Treasury. https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2023.pdf

Danielsson, J., Macrae, R., Shin, H. S., y Zigrand, J. P. (2022). The illusion of safety: Feedback effects, systemic risk, and artificial intelligence. Journal of Financial Economics, 146(3), 848–865. https://doi.org/10.1016/j.jfineco.2022.09.009

Demirgüç-Kunt, A., Klapper, L., Singer, D., y Ansar, S. (2023). Financial inclusion and fintech: New evidence and implications for the developing world. World Bank Economic Review, 37(3), 399–427. https://doi.org/10.1093/wber/lhad002

Eling, M., y Schnell, W. (2023). The relationship between cyber risk and systemic risk in the financial sector. Journal of Financial Stability, 64, 101–118. https://doi.org/10.1016/j.jfs.2022.101118

Fondo Monetario Internacional [FMI]. (2023). Panama: Financial sector assessment program. IMF Country Report No. 23/148. International Monetary Fund. https://www.imf.org/en/Publications/CR/Issues/2023/04/27/Panama

Fondo Monetario Internacional [FMI]. (2024). Cyber risk: A growing threat to financial stability. Global Financial Stability Report, Chapter 3. International Monetary Fund. https://www.imf.org/en/Publications/GFSR

Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T., y Walther, A. (2022). Predictably unequal? The effects of machine learning on credit markets. Journal of Finance, 77(1), 5–47. https://doi.org/10.1111/jofi.13090

Kashyap, A. K., y Wetherilt, A. (2023). Cyber risk and financial stability: A framework for analysis.Journal of Financial Regulation, 9(1), 1–38. https://doi.org/10.1093/jfr/fjad001

Kindleberger, C. P. (1978). Manias, panics and crashes: A history of financial crises. Basic Books.

Kopp, E., Kaffenberger, L., y Wilson, C. (2023). Cyber risk, market failures, and financial stability. IMF Working Paper, WP/23/141. International Monetary Fund. https://doi.org/10.5089/9798400218873.001

López Jiménez, J. M., y Martínez Peinado, A. (2024). DORA: Análisis del marco europeo de resiliencia operacional digital del sector financiero. Revista de Estabilidad Financiera, 46, 1–42.

Mastercard. (2023). The state of fraud and financial crime in 2023. Mastercard Fraud Center. https://www.mastercard.com/news/research-and-insights/2023/state-of-fraud-2023

Minsky, H. P. (1986). Stabilizing an unstable economy. Yale University Press.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., y Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. British Medical Journal, 372, n71. https://doi.org/10.1136/bmj.n71

Philippon, T. (2023). The fintech opportunity revisited. Journal of Finance, 78(6), 2961–3003. https://doi.org/10.1111/jofi.13283

Restoy, F. (2024). Regulating fintech: What is going on, and where are the challenges? BIS Papers No. 138. Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap138.pdf

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stiglitz, J. E. (1993). The role of the state in financial markets. En M. Bruno y B. Pleskovic (Eds.), Proceedings of the World Bank annual conference on development economics 1993 (pp. 19–52). World Bank.

Stiglitz, J. E. (2010). Freefall: America, free markets, and the sinking of the world economy. W. W. Norton.

Superintendencia de Bancos de Panamá [SBP]. (2021). Resolución SBP No. 014-2021: Gestión del riesgo tecnológico y ciberseguridad. Superintendencia de Bancos de Panamá.

Superintendencia de Bancos de Panamá [SBP]. (2024). Informe de estabilidad financiera 2024. Superintendencia de Bancos de Panamá. https://www.superbancos.gob.pa

Tirole, J. (2006). The theory of corporate finance. Princeton University Press.

Unión Europea. (2022). Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero. Diario Oficial de la Unión Europea, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj

Vmware Carbon Black. (2021). Modern bank heists 4.0. VMware. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-modern-bank-heists.pdf

Woods, D., y Wreathall, J. (2023). Resilience engineering: New directions for measuring and maintaining safety in complex systems. Journal of Safety Research, 84, 227–241. https://doi.org/10.1016/j.jsr.2022.11.006