Sombreado 1: **Riesgo cibernético en las infraestructuras financieras: entorno actual, riesgos y avances recientes**

1. Introducción

Este sombreado da continuidad a los análisis presentados en los *Reportes de Infraestructura Financiera e Instrumentos de Pago* (RIFI), en los que se abordó el riesgo cibernético como una amenaza creciente para la estabilidad financiera. Primero, desde un enfoque conceptual y normativo[1], y luego, a través de simulaciones de su materialización[2].

Para este año, el análisis se enfoca en caracterizar el entorno actual del riesgo cibernético en el sistema financiero, con especial atención en su impacto potencial sobre las IMF. Se presentan eventos relevantes ocurridos a nivel internacional, se revisan los avances normativos en materia de ciberresiliencia y se documentan las acciones implementadas por las autoridades y las IMF en Colombia. En particular, se destacan los esfuerzos del Banco de la República (Banrep) en el fortalecimiento de la resiliencia del CUD, a partir de las recomendaciones formuladas en el ejercicio de simulación del RIFI 2024. El objetivo es contribuir a una comprensión integral del ciberriesgo, articulando elementos conceptuales, regulatorios y operativos que permitan seguir reforzando la resiliencia del sistema financiero colombiano.

2. Panorama global del ciberriesgo

El sector financiero está especialmente expuesto a ciberataques debido al gran volumen de datos y transacciones sensibles que gestiona, lo que lo convierte en un objetivo prioritario para los ciberdelincuentes. Entre 2004 y 2023 se registraron más de 20.000 ciberataques contra este sector a nivel mundial, con pérdidas acumuladas cercanas a los USD 12 billones (Natalucci *et al.*, 2024), equivalentes a casi una quinta parte del total registrado en todas las industrias[3].

La rápida adopción de nuevas tecnologías ha creado brechas que son aprovechadas por delincuentes cada vez más sofisticados (World Economic Forum, 2025). En 2023 los ataques de denegación de servicio distribuido (DDoS, por su sigla en inglés) alcanzaron niveles récord en frecuencia y complejidad, siendo el sector financiero el principal objetivo a nivel mundial (FS-ISAC, 2024). Ese mismo año, los ataques de *ransomware* aumentaron un 64 % en esta industria (Mahendru, 2023).

---

1 El RIFI de 2023 introdujo un marco de ciberresiliencia para las IMF basado en los Principios aplicables a las Infraestructuras del Mercado Financiero (PFMI, por su sigla en inglés; CPMI e Iosco, 2012) y la Guía de Ciberresiliencia (CPMI e Iosco, 2016), resaltando su importancia en la estabilidad financiera y advirtiendo sobre vulnerabilidades ante riesgos cibernéticos. Además, presentó una taxonomía de ciberriesgo, resaltó iniciativas internacionales y locales, y urgió a reforzar capacidades regulatorias y operativas, fomentar la cooperación público-privada y explorar mecanismos para garantizar la continuidad del sistema financiero.

2 El recuadro de 2024 evaluó el ciberriesgo en el CUD, sistema de pagos de alto valor en Colombia, mediante simulaciones de ataques, basados en la taxonomía de Kaffenberger y Kopp (2019).

3 Los bancos en particular han sido los más afectados. JPMorgan Chase, por ejemplo, informó en enero de 2024 que sufre 45 billones de incidentes cibernéticos al día, gasta USD 15 billones en tecnología al año y emplea a 62.000 ingenieros, la mayoría especializados en ciberseguridad (Walker, 2024).

En el caso de las IMF, eventos recientes en sistemas de pagos de alto valor (SPAV) han puesto en evidencia el impacto potencial de un ciberataque sobre la estabilidad financiera, dada su función crítica en el sistema financiero y en la ejecución de la política monetaria. Algunos ejemplos relevantes incluyen:

- Lesoto (2023): un ciberataque a su banco central comprometió cinco servidores y obligó a desconectar temporalmente sus sistemas. Se suspendieron las transferencias electrónicas interbancarias y los bancos locales operaron manualmente.
- México (2018): varios participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) fueron atacados mediante la generación de órdenes de transferencia ilegítimas en sus sistemas internos, provocando pérdidas con cargo a sus propios recursos. El Banco de México activó esquemas de contingencia y ordenó operar a través de canales alternos (COAS).

Si bien en algunos casos los ataques no se dirigieron directamente a las IMF, su dependencia a múltiples proveedores (tecnológicos, bancarios, públicos y privados) ha permitido que incidentes en sistemas interconectados generen pérdidas en los SPAV. Uno de los métodos más frecuentes en los ciberataques fue la transmisión de órdenes de pago fraudulentas a través de Swift[4], mediante el acceso no autorizado a credenciales de participantes legítimos:

- Chile (2018): un ciberataque al Banco de Chile resultó en el robo de aproximadamente USD 10 millones mediante transferencias fraudulentas a través de Swift. Los atacantes utilizaron un *malware* destructivo que afectó más de 9.000 computadores y 500 servidores. El banco suspendió temporalmente operaciones en cuatrocientas sucursales como medida de contención.
- Bangladés (2016): su banco central fue víctima de un ataque que derivó en la sustracción de USD 81 millones tras el envío de solicitudes de transferencia fraudulentas al Banco de la Reserva Federal de Nueva York. Los atacantes intentaron transferir casi USD 1 billón, pero la mayoría de las operaciones fueron bloqueadas. Los fondos robados fueron canalizados a Filipinas y blanqueados a través de casinos.

3. Entorno regulatorio y avances en ciberresiliencia de las IMF colombianas

La creciente exposición del sistema financiero a amenazas cibernéticas ha impulsado el desarrollo global de estándares técnicos y marcos regulatorios orientados a fortalecer la resiliencia operativa de las IMF.

Entre los principales referentes se encuentran los Principios para Infraestructuras del Mercado Financiero (PFMI) y la Guía de Ciberresiliencia (CPMI-Iosco, 2012 y 2016), complementados con los Principios de Resiliencia Operativa (BCBS), las directrices sobre tercerización (Iosco, 2021) y los marcos sobre gestión de terceros y notificación de incidentes (FSB). Estos lineamientos han ampliado el enfoque regulatorio, al incorporar aspectos de gobernanza, supervisión de proveedores y preparación ante disrupciones.

A nivel regional, sobresalen el Marco de Ciberseguridad NIST (Estados Unidos) y la Ley de Resiliencia Operativa Digital (DORA, en la Unión Europea), que han reforzado la supervisión sobre proveedores tecnológicos críticos.

En Colombia las autoridades han tomado como referencia estos marcos para fortalecer la gestión del ciberriesgo. Se han definido requerimientos mínimos, adoptado lineamientos para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI),

4 Red global de mensajería financiera que permite la comunicación estandarizada entre bancos, IMF y empresas en más de doscientos países.

han introducido la Taxonomía Única de Incidentes Cibernéticos (TUIC) y reforzado los esquemas de reporte. El Banrep, con el objetivo de monitorear de forma estructurada el riesgo operativo, desarrolló el indicador de riesgo cibernético (IRC) y estableció protocolos específicos para monitorear el riesgo operativo en sistemas críticos.

En este contexto, las IMF locales han adoptado medidas sustantivas para reforzar su ciberresiliencia:

La Cámara de Riesgo Central de Contraparte (CRCC) fortaleció su enfoque en ciberseguridad desde 2018 mediante un SGSI alineado con estándares internacionales y respaldado por una política institucional. En 2024 mantuvo la operación de un Centro de Operaciones de Seguridad (SOC), encargado del monitoreo en tiempo real y la correlación de eventos para la detección de incidentes. La entidad también ejecutó pruebas de continuidad, evaluaciones externas de seguridad y acciones de concienciación, contribuyendo al fortalecimiento de la cultura organizacional en ciberseguridad.

El Depósito Central de Valores (DCV) incorporó mejoras de ciberseguridad y control operativo con la entrada en operación de su nuevo sistema en abril de 2024. El acceso se realiza a través del entorno seguro Sebra, con autenticación y gestión de identidades centralizada y perfiles personalizados, controlados por cada entidad participante. Se aplica el principio de doble revisión para operaciones sensibles y se registra toda la actividad de los usuarios. Se mantuvieron los lineamientos del SGSI institucional, se realizaron simulacros de crisis cibernética y se implementaron mecanismos automáticos para la gestión de cuentas inactivas, la selección de títulos y la liquidación en tiempo real, fortaleciendo la resiliencia operativa.

El Depósito Centralizado de Valores (Deceval) durante 2024 mantuvo su SGSI con énfasis en la mejora continua y la protección de la confidencialidad, integridad y disponibilidad de la información. En el marco de la integración regional, actualizó políticas internas, fortaleció protocolos de atención a incidentes cibernéticos y gestionó vulnerabilidades de forma preventiva. Su infraestructura tecnológica se consolidó bajo una arquitectura interoperable basada en principios *cloud-agnostic*[5]. Además, ejecutó campañas de sensibilización, ejercicios de *phishing*, y mantuvo activos sus procesos de monitoreo y respuesta, integrando capacidades con el grupo empresarial para mejorar la resiliencia tecnológica y operativa.

En la siguiente sección se destacan los avances implementados en el CUD durante 2024, los cuales responden a las recomendaciones formuladas en el RIFI del año anterior.

4. Avances en ciberresiliencia por parte del CUD

A partir del ejercicio de simulación incluido en el RIFI 2024, y de las oportunidades de mejora identificadas, el Banrep avanzó en la implementación de medidas para continuar robusteciendo la resiliencia del CUD.

El ejercicio simuló ataques tipo *ransomware* contra entidades sistémicamente importantes (ESI) y proveedores de telecomunicaciones. Los resultados muestran que los incumplimientos pueden alcanzar hasta el 54 % del valor total de pagos, y reducirse a cerca del 40 % si las entidades adoptan una reacción activa, es decir, si reintentan los pagos fallidos utilizando la liquidez recibida. En el caso de un ataque al principal proveedor de conectividad, los pagos no liquidados pueden llegar al 70 % (65 % con reacción activa), afectando a más de la mitad de las entidades activas en ambos escenarios.

Con base en estos resultados, se formularon recomendaciones orientadas a fortalecer la preparación institucional mediante simulacros, fomentar la cooperación internacional y

5 Se refiere a una arquitectura tecnológica diseñada para ser compatible con múltiples proveedores de servicios en la nube, lo que permite mayor flexibilidad, portabilidad de aplicaciones y reducción de riesgos por dependencia de un único proveedor (*vendor lock-in*).

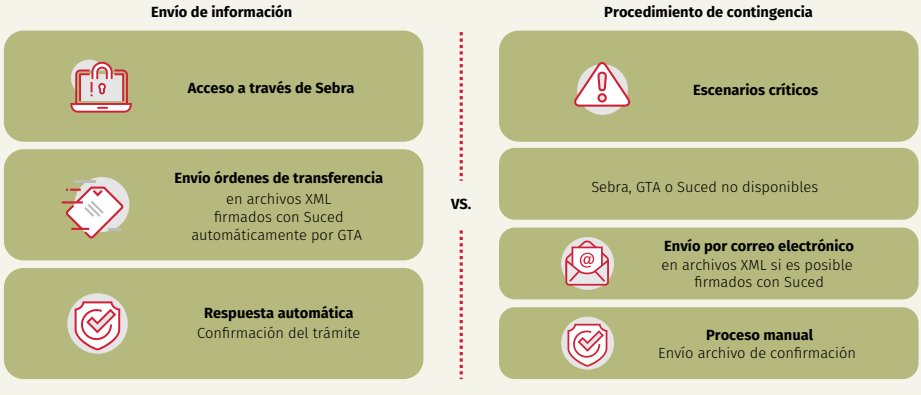
promover el uso de inteligencia artificial generativa para la detección temprana de amenazas, la automatización de respuestas y la reducción del error humano. En el caso del CUD, se resaltó, además, la importancia de contar con canales de conexión alternos, dedicados e independientes, que aseguren la continuidad operativa ante fallas del canal principal y permitan el envío oportuno de información crítica mientras se restablece la conexión.

Acorde con estos lineamientos, y como parte del enfoque coordinado entre autoridades financieras, los resultados del ejercicio fueron presentados en el Comité de Coordinación para el Seguimiento al Sistema Financiero (CCSSF) y compartidos con las demás entidades que integran la red de seguridad financiera. Esta instancia de coordinación interinstitucional permitió socializar los aprendizajes del ejercicio, promover una visión común sobre los riesgos operativos y reforzar la preparación conjunta ante amenazas cibernéticas de alto impacto.

En este contexto, primero se describe el funcionamiento del canal de contingencia previsto para la transmisión de instrucciones en caso de fallas en los canales principales del CUD, y luego se detallan las medidas implementadas por el Banrep, en concordancia con las recomendaciones incluidas en el recuadro del RIFI 2024.

El Diagrama S1.1 ilustra el procedimiento de envío de información en condiciones normales y bajo contingencia. Las entidades acceden al CUD mediante Sebra, la plataforma segura del Banrep, y transmiten órdenes de transferencia en archivos XML (formato estandarizado para intercambio de datos), firmados digitalmente con Suced, el sistema de certificación electrónica del Banrep. La transmisión se realiza a través de la gestión de transferencia de archivos (GTA), módulo diseñado para el envío seguro de archivos. El sistema confirma automáticamente el trámite. Este canal es seguro, eficiente y ampliamente utilizado en la operación habitual.

Diagrama S1.1
Comparación con el procedimiento de contingencia



Fuente: Banco de la República.

En caso de indisponibilidad de los canales principales (Sebra, GTA o Suced), las entidades activan la contingencia enviando los archivos XML por correo electrónico desde cuentas autorizadas. Preferiblemente deben estar firmados con Suced. El Banrep procesa las instrucciones manualmente y remite una confirmación.

Este canal de contingencia cuenta con respaldo normativo (Circular CEOS DSP 158 de diciembre de 2023) y está documentado en el *Manual de Contingencia del CUD*. Permite mantener la continuidad del sistema, incluso ante fallas generalizadas en Sebra, servicios web o Suced con lineamientos detallados para su activación frente a incidentes tecnológicos o cibernéticos.

Complementando este canal de contingencia previsto en la normativa vigente, el Banrep implementó diversas acciones durante el año, entre las cuales se destacan:

- Fortalecimiento de la preparación operativa de entidades con rol sistémico: se implementó un plan de acompañamiento a entidades participantes del CUD que no utilizaban habitualmente el canal alternativo. Como parte de este plan, se realizaron prácticas reales en ambiente de producción, con el propósito de verificar su capacidad de respuesta ante la eventualidad de una falla en los canales principales.
- Fortalecimiento del marco institucional de respuesta ante ciberincidentes: en diciembre de 2024, el Banrep expidió la Circular Reglamentaria Interna DG-T, DGRP-463, que establece un plan de gestión de desastres para escenarios de ciberseguridad de alto impacto. Esta circular reconoce al CUD como un sistema crítico e incorpora protocolos de respuesta, recuperación y reanudación del servicio, apoyados en una estructura de gobierno para incidentes que integra las áreas operativas, tecnológicas y de gestión de riesgos del Banrep.

Estas acciones complementan el canal de contingencia previsto en la normativa vigente y responden a las recomendaciones formuladas en el RIFI 2024. En conjunto, contribuyen al fortalecimiento de la ciberresiliencia del CUD y a la continuidad de los servicios de pagos de alto valor ante posibles eventos disruptivos, en línea con los estándares técnicos y normativos adoptados por el Banrep.

5. Conclusiones

El riesgo cibernético continúa consolidándose como una de las principales amenazas para la estabilidad del sistema financiero, debido a la creciente sofisticación de los ataques, la interconexión de los servicios y la criticidad de las IMF. La evidencia internacional demuestra que incluso incidentes localizados pueden tener efectos sistémicos cuando involucran componentes críticos como los SPAV.

En respuesta, el marco normativo internacional ha evolucionado hacia la estandarización de principios de ciberresiliencia, el fortalecimiento de la cooperación entre autoridades y la exigencia de planes efectivos de recuperación. En Colombia, las autoridades han avanzado en la incorporación de estos lineamientos: la SFC ha liderado el desarrollo de un marco regulatorio integral para la gestión del ciberriesgo, mientras que el Banrep y los administradores de IMF han implementado medidas orientadas a fortalecer sus respectivas infraestructuras.

Entre las acciones de las IMF locales se encuentran la operación de centros de monitoreo, la realización de pruebas de continuidad operativa, la implementación de sistemas seguros de acceso y la actualización de protocolos internos. Estas iniciativas reflejan una convergencia con buenas prácticas internacionales y un esfuerzo sostenido por mejorar su preparación ante ciberamenazas.

Asimismo, se destaca el avance del Banrep en el fortalecimiento de la resiliencia del CUD, demostrando la capacidad institucional para traducir en acciones concretas los aprendizajes derivados del seguimiento a las IMF que realiza el mismo Banrep a través de su función de seguimiento a la infraestructura financiera, en particular de los ejercicios de simulación. Estas acciones han contribuido a reforzar la continuidad operativa del sistema y a mejorar su capacidad de respuesta ante incidentes.

No obstante, la naturaleza dinámica del ciberriesgo exige una mejora continua. En este sentido, se han identificado líneas de trabajo adicionales orientadas a fortalecer la capacidad de anticipación del sistema, entre ellas, el desarrollo de ejercicios de simulación más realistas que incorporen funciones de aprendizaje y reacción por parte de los agentes, así como la modelación de agentes heterogéneos en los ejercicios de choque a la liquidez intradía en el CUD. Estos enfoques permitirán una evaluación más precisa de los efectos de un incidente y una mejor preparación frente a escenarios complejos.

Los avances presentados reafirman la importancia de consolidar una visión integral del ciberriesgo, articulando su comprensión conceptual con la medición y la gestión activa,

y traduciéndolo en mejoras continuas en la gobernanza, la supervisión y la cooperación interinstitucional. La resiliencia cibernética no solo es un imperativo técnico, sino un componente esencial para la confianza y estabilidad del sistema financiero colombiano.

Referencias

Achieving Greater Convergence in Cyber Incident Reporting: Progress Report to the G20. https://www.fsb.org/2023/04/achieving-greater-convergence-in-cyber-incident-reporting/

Adelmann, F.; Elliott, J. A.; Ergen, I.; Gaidosch, T.; Jenkinson, N.; Khiaonarong, T.; Morozova, A.; Schwarz, N.; Wilson, C. (2020). "Cyber Risk and Financial Stability: It's a Small World after All", Staff Discussion Note, núm. 2020/007, International Monetary Fund, https://doi.org/10.5089/9781513512297.006

Adrian, T.; Ferreira, C. (2024). "Cyber Risk: A Growing Concern for Macrofinancial Stability", en *Global Financial Stability Report: The Last Mile – Financial Vulnerabilities and Risks* (capítulo 3), Fondo Monetario Internacional, abril https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3.ashxfsb.org

Autoridad Europea de Seguros y Pensiones de Jubilación (s. f.). Digital Operational Resilience Act (DORA), disponible en: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Banco de la República (2021). Circular Externa Operativa y de Servicios DSP-158: Sistema de Cuentas de Depósito (CUD), 29 de octubre, disponible en: https://www.banrep.gov.co/sites/default/files/reglamentacion/archivos/ceos%20dso-158_OCT_29_2021.pdf

Banco de la República (2021). *Manual de Contingencia del Sistema de Cuentas de Depósito* (CUD), disponible en: https://www.banrep.gov.co/es/sistemas-pago/cud/plan-contingencia

Basel Committee on Banking Supervision (2021). "Principles for the Sound Management of Operational Risk (revised version)", Bank for International Settlements, marzo, disponible en: https://www.bis.org/bcbs/publ/d515.htm

Basel Committee on Banking Supervision (2021). "Principles for Operational Resilience", Bank for International Settlements, marzo, disponible en: https://www.bis.org/bcbs/publ/d516.htm

Comité de Pagos e Infraestructuras del Mercado; la Organización Internacional de Comisiones de Valores [CPMI e Iosco] (2012). "Principios aplicables a las infraestructuras de los mercados financieros" Banco de Pagos Internacionales (BIS), disponible en: https://www.bis.org/cpmi/publ/d101_es.pdf

Comité de Pagos e Infraestructuras del Mercado; Organización Internacional de Comisiones de Valores [CPMI e Iosco] (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*, Banco de Pagos Internacionales (BIS), disponible en: https://www.bis.org/cpmi/publ/d146.pdf

Comité de Pagos e Infraestructuras del Mercado, Organización Internacional de Comisiones de Valores [CPMI e Iosco] (2022). "Evaluación de implementación de la PFMI: evaluación de nivel 3 sobre la ciberresiliencia de las infraestructuras de los mercados financieros", noviembre, disponible en: https://www.bis.org/cpmi/publ/d212.pdffsb.org

Escobar-Villarraga, M. (2023). "Indicador de riesgo cibernético", en *Reporte de Estabilidad Financiera*, primer semestre de 2023 (Recuadro 2), junio, Banco de la República, disponible en: https://repositorio.banrep.gov.co/bitstream/handle/20.500.12134/10638/recuadro-2-reporte-estabilidad-financiera-primer-semestre-2023.pdf

Federal Financial Institutions Examination Council (2017). "Cybersecurity Assessment Tool", mayo, disponible en: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Feingold, S.; Wood, J. (2024). "Global Financial Stability at Risk Due to Cyber Threats, IMF Warns. Here's What to Know", World Economic Forum, mayo, disponible en: https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

Financial Services Information Sharing and Analysis Center (2024). "DDoS: Here to Stay", marzo, disponible en: https://www.fsisac.com/hubfs/Knowledge/DDoS/FSISAC_DDoS-HereToStay.pdf

Financial Stability Board (2023). *Cyber Lexicon: Updated in 2023*, abril, disponible en: https://www.fsb.org/2023/04/cyber-lexicon-updated-in-2023/fsb.org

Financial Stability Board (2023). Enhancing Third-Party Risk Management and Oversight: A Toolkit For Financial Institutions and Financial Authorities", diciembre, disponible en: https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/

G7 Cyber Expert Group (2016). "G7 Fundamental Elements of Cybersecurity for the Financial Sector", European Central Bank, octubre, disponible en:. https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

G7 Cyber Expert Group (2017). "G7 Fundamental Elements for Effective Assessment of Cybersecurity in The Financial Sector", European Central Bank, octubre, disponible en: https://www.ecb.europa.eu/paym/pol/shared/pdf/October_2017-G7-fundamental-elements-for-effective-assessment-of-cybersecurity-in-the-financial-sector.en.pdf

Kaffenberger, L.; Kopp, E. (2019). "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment", Carnegie Endowment for International Peace, disponible en: https://carnegieendowment.org/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf

Khausela, T. (2024). "CBL Speaks on Cyber Attack", *Lesotho Times*, 13 de febrero, disponible en: https://lestimes.com/cbl-speaks-on-cyber-attack/

Kopp, E.; Kaffenberger, L.; Wilson, C. (2017). "Cyber Risk, Market Failures, and Financial Stability", IMF Working Paper, núm. 17/185, International Monetary Fund, diciembre, disponible en: https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104

Mahendru, P. (2023). "The State of Ransomware in Financial Services 2023", *Sophos News*, julio, disponible en: https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/

Natalucci, F.; Qureshi, M. S.; Suntheim, F. (2024). "Rising Cyber Threats Pose Serious Concerns for Financial Stability", IMF Blog, abril, disponible en: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

National Institute of Standards and Technology (2024). "Framework for Improving Critical Infrastructure Cybersecurity, version 2.0", U.S. Department of Commerce, disponible en: https://doi.org/10.6028/NIST.CSWP.29

Organización Internacional de Comisiones de Valores (2021). "Principios sobre tercerización: informe final", octubre, disponible en: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdfiosco.org

Ravikumar, R. (2025). "Strengthening Cybersecurity: Lessons from the Cybersecurity Survey", Technical Notes and Manuals núm. 2025, 006 (2025), International Monetary Fund, disponible en: https://doi.org/10.5089/9798400296864.005

Superintendencia Financiera de Colombia (2018). Circular Externa 007 de 2018: Requerimientos mínimos para la gestión del riesgo de ciberseguridad, 5 de junio, disponible en: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1031741

Superintendencia Financiera de Colombia (2020). Guía de conceptos del Formato 408: Métricas e indicadores de seguridad de la información y ciberseguridad, disponible en: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1060320

Superintendencia Financiera de Colombia (2020). Circular Externa 033 de 2020: Instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos (TUIC), el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol (TLP), noviembre, disponible en: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1049276

Walker, O. (2024). "JPMorgan Suffers Wave of Cyber Attacks as Fraudsters Get 'More Devious'", *Financial Times*, 17 de enero, disponible en: https://www.ft.com/content/cd287352-cb3b-48d8-a85b-668713b80962

World Bank (2021a). "A Snapshot: Payment Systems Worldwide: Summary Outcomes of the Sixth Global Payment Systems Survey", World Bank Group, disponible en: http://documents.worldbank.org/curated/en/099011624132054588

World Bank (2021b). "Cyber Risks in Fast Payment Systems and Implications for National Payments System Oversight (Focus Note)", disponible en: https://fastpayments.worldbank.org/sites/default/files/2021-10/Oversight_Final_0.pdf

World Bank (2025). "Cyber Risks In Fast Payment Systems (Focus Note)", febrero, disponible en: https://fastpayments.worldbank.org/sites/default/files/2025-02/Cybersecurity%20Focus%20Note_Feb%2019_Final.pdf

World Economic Forum (2025). *Global Cybersecurity Outlook, 2025*, disponible en: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdfreports.weforum.org