UNIVERSIDAD DE PIURA

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

Ciberseguridad e intermediación financiera

Trabajo de Suficiencia Profesional para optar el Título de Economista

Jessica Mariella Casariego Palomino

Revisor:
Mgtr. Harry Omar Patrón Torres

Piura, abril de 2025

Declaración Jurada de Originalidad del Trabajo Final

Yo, Jessica Mariella Casariego Palomino, egresada del **Programa Académico** de Economía de la Facultad de Ciencias Económicas y Empresariales de la Universidad de Piura, identificado(a) con **DNI**: 73131453, declaro que:

Soy autora del trabajo final titulado:
"**Ciberseguridad e intermediación financiera**"
El mismo que presento bajo la modalidad de **Trabajo de suficiencia profesional** para optar el Título profesional de Economista.

El texto de mi trabajo final es original y no vulnera los derechos de terceros o, de ser el caso, derechos de los coautores, incluidos los derechos de propiedad intelectual, datos personales, entre otros. En tal sentido, el texto de mi trabajo final no ha sido plagiado total ni parcialmente, para lo cual, he respetado las normas internacionales de citas y referencias de las fuentes consultadas. Asimismo, el texto del trabajo final que presento no ha sido publicado ni presentado antes en cualquier medio electrónico o físico; y que la investigación, los resultados, datos, conclusiones y demás información presentada que atribuyo a mi autoría son veraces.

En caso de detectarse el incumplimiento de lo declarado asumo frente a terceros, la Universidad de Piura y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

La revisión del trabajo estuvo a cargo de los siguientes docentes de la Universidad de Piura:

- Mgtr. Harry Omar Patrón Torres, identificado con DNI: 07251849

Declaro (declaramos) que:
Luego de haber empleado el software de coincidencia Turnitin, revisado las fuentes de información señaladas por el autor, y en razón de mi (nuestra) experiencia como investigador(es), declaro (declaramos) que las ideas expuestas en el trabajo final alcanzan las condiciones de calidad, integridad y originalidad acorde a los objetivos institucionales y estándares en materia de investigación. Finalmente, no asumo (asumimos) responsabilidad por la posible vulneración de derechos de autor en el trabajo final referido, pues tal responsabilidad es exclusiva del autor.

Fecha: *30/04/2025*.

…… ……

Firma del autor[1] *Firma del revisor*[1]

[1] Firma idéntica al DNI. No se admite digital, salvo certificado.

Dedicatoria

Con inmensa gratitud, consagro este esfuerzo a Dios, cuya guía ilumina mi camino y me otorga fortaleza frente a los desafíos. Expreso un sincero agradecimiento a mis padres, cuya entrega desinteresada y apoyo continuo han sido pilares en mi crecimiento tanto académico como personal. Sus valores y enseñanzas han sido clave en mi desarrollo integral.

Agradecimientos

Manifiesto mi profundo agradecimiento al Mgtr. Luis Bendezú por su invaluable asesoramiento en la revisión y evaluación de esta investigación. Extiendo mi gratitud a los docentes universitarios, quienes contribuyeron significativamente a mi formación académica al compartir su experiencia y conocimiento. De manera especial, agradezco al profesor Mgtr. Harry Patrón por sus orientaciones y recomendaciones, que aportaron notablemente a este trabajo. Asimismo, expreso un reconocimiento sincero a mi familia y amigos, cuyo respaldo constante y motivación fueron fundamentales para lograr este objetivo.

Resumen

Este trabajo de suficiencia profesional desarrolla un análisis crítico del artículo "Cyber-attacks and banking intermediation" de Boungou (2023), complementado con la experiencia profesional de la autora en Monnet Payment Solutions. La investigación examina el impacto de los ciberataques en la intermediación bancaria, evaluando sus efectos sobre la captación de depósitos, la estructura temporal de préstamos y el desempeño financiero de las instituciones. El análisis revela que los ciberataques afectan negativamente la intermediación bancaria a través de múltiples canales, aunque se identifican limitaciones metodológicas importantes en la medición del riesgo cibernético. El estudio evalúa la aplicabilidad de estos hallazgos al contexto peruano, considerando las características distintivas del mercado financiero local, como su alta concentración bancaria y la creciente presencia de *fintech*. Se propone una agenda de investigación que incluye el desarrollo de una base de datos comprehensiva de incidentes cibernéticos, el análisis de interconexiones en el sistema financiero peruano y la evaluación de diferentes arquitecturas regulatorias. Las recomendaciones de política enfatizan la necesidad de un enfoque integral que combine medidas micro y macro prudenciales, sugiriendo la creación de un comité de estabilidad cibernética que coordine la respuesta del sector financiero ante estas amenazas emergentes. La experiencia profesional de la autora en una empresa *fintech* enriquece el análisis al proporcionar una perspectiva práctica sobre los desafíos de la seguridad operacional en el sector financiero digital.

Tabla de contenido

Introducción

El presente trabajo de suficiencia profesional tiene como objetivo analizar el impacto de los ciberataques en la intermediación bancaria, mediante un análisis crítico del artículo "*Cyber-attacks and banking intermediation*" de Boungou (2023) y la experiencia profesional de la autora en Monnet Payment Solutions. Este estudio resulta particularmente relevante en un contexto donde las instituciones financieras enfrentan amenazas cibernéticas crecientes, con el sector bancario experimentando hasta 300 veces más incidentes que otros sectores de la economía.

En el primer capítulo se exponen las características organizacionales de Monnet Payment Solutions y las funciones desempeñadas en el área de Control de Gestión. Se detallan los conocimientos adquiridos durante la carrera de Economía que fueron aplicados directamente en las labores de conciliación y análisis financiero, evidenciando la conexión entre la formación universitaria y el desempeño profesional en el campo *fintech*. La experiencia en la empresa ha permitido observar de primera mano los desafíos que enfrentan las instituciones financieras en materia de seguridad operacional y gestión de riesgos tecnológicos.

En el segundo capítulo se desarrolla propiamente el análisis crítico del artículo de Boungou (2023), examinando cómo los ciberataques afectan diferentes dimensiones de la intermediación bancaria. Se evalúa la solidez metodológica del estudio, que utiliza datos de 2,144 bancos estadounidenses durante el período 2011-2019, y se analizan sus hallazgos sobre el impacto en la captación de depósitos, la estructura temporal de préstamos y el desempeño bancario. El análisis se complementa con una revisión de literatura reciente sobre riesgos cibernéticos en el sector financiero, identificando brechas en la investigación actual y proponiendo líneas futuras de estudio.

Particular atención se presta a la aplicabilidad de estos hallazgos al contexto peruano, considerando las características distintivas del mercado financiero local como su alta concentración bancaria, la creciente presencia de *fintech* y las brechas en inclusión financiera digital. Se desarrollan recomendaciones de política específicas para fortalecer la resiliencia del sistema financiero peruano ante amenazas cibernéticas, enfatizando la necesidad de un enfoque integral que combine medidas micro y macro prudenciales.

Finalmente, en la sección de Conclusiones se sintetiza los principales hallazgos del análisis y se proponen sugerencias concretas para mejorar la gestión de riesgos cibernéticos en el sector financiero peruano. Este trabajo busca contribuir a la comprensión de cómo los ciberataques afectan la intermediación financiera y proponer medidas específicas para fortalecer la resiliencia del sistema bancario ante estas amenazas emergentes.

Capítulo 1. Informe de experiencia profesional

1.1 Experiencia profesional en Monnet Payment Solutions

1.1.1 *Descripción de la empresa*

Monnet Payment Solutions emerge como una innovadora empresa *fintech* que nació en mayo de 2020, en pleno contexto de la pandemia global, cuando las transacciones digitales experimentaron un crecimiento sin precedentes. La empresa fue fundada por Eduardo Luna y Franco Zurita, dos visionarios empresarios que identificaron una oportunidad significativa en el mercado de pagos digitales, específicamente en el segmento de *payouts* o dispersiones de dinero.

La compañía se distingue en el mercado latinoamericano por ofrecer una solución integral que combina servicios de *payins* (recaudo) y *payouts* (dispersión) en una única plataforma. Esta propuesta de valor única permite a las empresas gestionar eficientemente tanto el cobro a sus clientes como el pago a sus proveedores, sin necesidad de establecer presencia física en cada país donde operan. Este enfoque ha demostrado ser particularmente valioso para empresas de diversos sectores, desde aplicaciones de transporte hasta comercio electrónico.

Desde sus inicios, Monnet Payment Solutions adoptó una visión regional, iniciando operaciones simultáneamente en Perú, Chile y Ecuador. Esta estrategia de expansión internacional rápida ha sido fundamental para su crecimiento, permitiéndole alcanzar una presencia significativa en ocho países de Latinoamérica, incluyendo México, Colombia, Guatemala y Honduras. La empresa ha demostrado un crecimiento exponencial en sus operaciones, procesando más de mil millones de dólares en transacciones durante 2023, lo que representa un incremento del doble respecto al año anterior.

La misión de Monnet Payment Solutions se centra en ofrecer la solución más completa para cobros y pagos por internet, facilitando la inclusión financiera y digital en toda Latinoamérica. Su visión apunta a consolidarse como la mayor pasarela de pagos de la región, con presencia en la mayoría de los países latinoamericanos. Estos objetivos ambiciosos están respaldados por un equipo de más de 180 profesionales altamente calificados que operan bajo un modelo de trabajo principalmente remoto, reflejando la naturaleza innovadora y adaptable de la empresa.

El éxito de Monnet Payment Solutions se evidencia en diversos reconocimientos obtenidos, incluyendo su listado entre las 100 mejores startups peruanas según Forbes en 2022 y 2023, su participación en el programa de aceleramiento ScaleUp de Endeavor, y sus nominaciones a premios internacionales de innovación en pagos. La empresa ha mantenido un enfoque en la rentabilidad desde sus inicios, alcanzando el punto de equilibrio en sus primeros seis meses de operación y manteniendo un crecimiento sostenido desde entonces.

La estructura organizacional de la empresa refleja su compromiso con la innovación y la excelencia operativa. Cuenta con diversos departamentos especializados, incluyendo tecnología,

operaciones, finanzas y control de gestión, cada uno contribuyendo de manera específica al objetivo común de proporcionar soluciones de pago eficientes y seguras. La inversión continua en capital humano y desarrollo tecnológico constituye un pilar fundamental de su estrategia de crecimiento.

De cara al futuro, Monnet Payment Solutions mantiene ambiciosos planes de expansión, incluyendo su próxima entrada al mercado brasileño en el segundo semestre de 2024, lo que representa un paso estratégico significativo para consolidar su presencia en la región. Además, la empresa está explorando nuevas oportunidades en el sector de remesas, aprovechando su infraestructura tecnológica y su capacidad para realizar transferencias inmediatas.

1.1.2 *Descripción general de la experiencia profesional*

La trayectoria profesional de la autora en Monnet Payment Solutions inició en marzo de 2023, incorporándose como Agente de Conciliación Payout, un rol que le permitió familiarizarse con los procesos fundamentales de la empresa y sentar las bases para su posterior desarrollo profesional. Su desempeño y capacidad de adaptación la llevaron a ascender al cargo de Analista Jr. de Control de Gestión Payout en mayo de 2024, posición que ocupa actualmente.

Durante su etapa como Agente de Conciliación Payout, la autora asumió responsabilidades críticas en el monitoreo y control de los saldos diarios del balance de Payouts entre clientes y bancos en múltiples países, incluyendo Chile, Argentina y Ecuador. Esta labor requería la elaboración de informes de conciliación detallados que garantizaban la precisión y transparencia de las operaciones financieras internacionales. Un aspecto destacado de su gestión fue la implementación de protocolos de alerta para la detección temprana de incidentes en el sistema y errores operativos, lo que contribuyó significativamente a la eficiencia y seguridad de las operaciones.

En este rol inicial, la autora desarrolló una comprensión profunda de los procesos de validación de los análisis de cuentas en los estados financieros, una competencia que resultaría fundamental para su posterior promoción. Su capacidad para mantener un control preciso sobre las operaciones internacionales y su habilidad para identificar y resolver discrepancias de manera eficiente fueron factores clave que la distinguieron en su desempeño.

El ascenso al cargo de Analista Jr. de Control de Gestión Payout representó una expansión significativa de sus responsabilidades y alcance profesional. En esta posición, la autora asumió un rol más estratégico en el análisis y control de los avances de las conciliaciones en todos los países donde opera la empresa. Sus funciones se ampliaron para incluir la automatización de tareas, controles y procesos, así como la realización de cuadraturas de Back Office versus Contabilidad en múltiples jurisdicciones.

Una de las contribuciones más significativas en su rol actual ha sido la implementación de un sistema mejorado para la elaboración de estados de cuenta y saldos al cierre de los comercios. Este sistema ha optimizado la precisión y eficiencia en el proceso de *reporting* financiero, proporcionando

una visión más clara y actualizada de la situación financiera de los clientes. La autora ha demostrado una particular aptitud para la identificación y resolución de discrepancias en las conciliaciones internacionales, lo que ha contribuido a mantener la integridad de las operaciones financieras de la empresa.

La evolución profesional de la autora en Monnet Payment Solutions refleja una progresión natural desde funciones operativas hacia responsabilidades más analíticas y estratégicas. Su capacidad para adaptarse a un entorno *fintech* en rápida evolución y su compromiso con la mejora continua de los procesos han sido fundamentales en su desarrollo profesional. La experiencia adquirida en la gestión de operaciones financieras internacionales y en la implementación de mejoras en los procesos de control ha contribuido significativamente a su crecimiento profesional y al éxito operativo de la empresa.

Antes de su incorporación a Monnet Payment Solutions, la autora acumuló experiencia valiosa en diversos sectores, lo que le proporcionó una base sólida para su actual rol. Su paso por el ICPNA como Asistente de Procesos Logísticos entre mayo de 2022 y enero de 2023 le permitió desarrollar habilidades en el análisis de pagos y la identificación de oportunidades de mejora en los procesos operativos. Durante este período, se destacó por su capacidad para elaborar reportes efectivos para la jefatura y por su habilidad para atender consultas y solicitudes de manera ágil y eficiente.

Previamente, su experiencia en COMDATA GROUP SAC como Asesora de Ventas para Pacífico Seguros le permitió desarrollar habilidades significativas en la gestión de relaciones con clientes y en el logro de objetivos comerciales. Durante su tiempo en esta posición, superó consistentemente las metas de ventas establecidas, logrando vender 60 seguros mensuales cuando el promedio por ejecutivo era de 45, lo que demostró su capacidad para el logro de resultados excepcionales.

Su trayectoria profesional incluye también una experiencia enriquecedora en Buró Group SAC como Ejecutiva de Ventas para Financiera Crediscotia, donde se enfocó en la planificación e implementación de mejoras en los procesos de venta. Esta experiencia le proporcionó una comprensión valiosa del sector financiero y desarrolló sus habilidades en la captación y retención de clientes mediante una comunicación eficiente.

Un aspecto destacable en la trayectoria profesional de la autora es su capacidad para aplicar el conocimiento adquirido en cada posición para mejorar su desempeño en roles posteriores. Su experiencia en ventas y servicio al cliente ha enriquecido su comprensión de las necesidades del usuario final, mientras que su experiencia en procesos logísticos ha fortalecido su capacidad para optimizar operaciones y mejorar la eficiencia de los procesos.

1.1.3 *Fundamentación y análisis de la contribución de la formación académica*

La formación académica de la autora como Bachiller en Economía por la Universidad de Piura ha sido fundamental en su desarrollo profesional, proporcionándole una base sólida de conocimientos

y habilidades que han resultado esenciales en su rol actual en Monnet Payment Solutions. Esta formación universitaria, complementada con estudios especializados posteriores, ha contribuido significativamente a su capacidad para enfrentar los desafíos en el sector *fintech* y financiero.

La educación en Economía ha dotado a la autora de una comprensión profunda de los principios económicos y financieros que rigen el mercado. Esta base teórica ha sido particularmente valiosa en su rol actual, donde el análisis de datos financieros y la comprensión de las dinámicas del mercado son cruciales para la toma de decisiones efectivas. Su capacidad para interpretar tendencias económicas y comprender el impacto de variables macroeconómicas en las operaciones de la empresa ha sido fundamental para su contribución al éxito de Monnet Payment Solutions.

Un componente crucial de su formación ha sido el Diplomado en Metodologías Ágiles para la Innovación cursado en ZEGEL IPAE entre octubre de 2021 y marzo de 2022. Este programa le proporcionó conocimientos especializados en áreas clave como liderazgo para la innovación, *design thinking*, *lean startup*, y la implementación de metodologías Scrum y Kanban. Estas herramientas han sido particularmente valiosas en el entorno dinámico de una empresa *fintech*, donde la agilidad y la innovación son fundamentales para el éxito operativo.

La formación técnica de la autora se fortaleció significativamente con el XIII Curso de Excel Empresarial en la Universidad de Piura, completado entre marzo y abril de 2023. Este curso especializado fortaleció sus habilidades en el manejo de datos, automatización de procesos y elaboración de reportes, competencias que aplica diariamente en su rol como Analista Jr. de Control de Gestión. La capacidad para manipular y analizar grandes volúmenes de datos de manera eficiente ha sido crucial para la optimización de procesos y la toma de decisiones basada en evidencia.

La combinación de su formación académica en economía con las certificaciones técnicas posteriores ha creado una base sólida para su desarrollo profesional en el sector *fintech*. Sus conocimientos en economía le permiten comprender las implicaciones más amplias de las transacciones financieras, mientras que su formación técnica le proporciona las herramientas necesarias para implementar soluciones prácticas y eficientes.

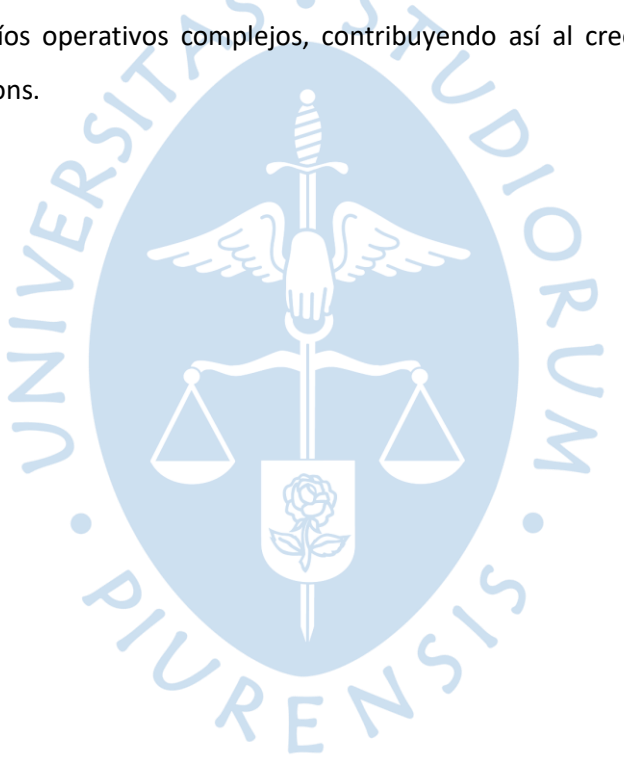
Un aspecto particularmente relevante de su formación ha sido el desarrollo de habilidades analíticas y de resolución de problemas. La formación en economía enfatiza el pensamiento crítico y el análisis sistemático, habilidades que la autora aplica constantemente en su trabajo diario. Su capacidad para identificar patrones, analizar datos complejos y proponer soluciones efectivas se deriva directamente de esta base académica sólida.

Las competencias desarrolladas durante su formación académica, incluyendo el trabajo en equipo, la comunicación asertiva y la capacidad analítica, han sido fundamentales en su progreso profesional. Estas habilidades blandas, combinadas con sus conocimientos técnicos, le han permitido destacar en roles que requieren tanto experiencia técnica como habilidades interpersonales efectivas.

El dominio del idioma inglés a nivel intermedio, adquirido durante su formación, ha sido un activo valioso en su rol actual, facilitando la comunicación efectiva en un entorno empresarial internacional. Esta competencia lingüística le permite participar efectivamente en proyectos multinacionales y colaborar con equipos diversos dentro de la organización.

La formación continua ha sido una constante en la trayectoria profesional de la autora, reflejando su compromiso con el aprendizaje permanente y la mejora continua. Su participación en programas de capacitación y certificaciones demuestra una comprensión clara de la importancia de mantenerse actualizada en un sector tan dinámico como el *fintech*.

La aplicación práctica de su formación académica se evidencia en su capacidad para implementar mejoras significativas en los procesos de control y gestión. Su comprensión de los principios económicos, combinada con sus habilidades técnicas, le ha permitido desarrollar soluciones innovadoras para desafíos operativos complejos, contribuyendo así al crecimiento y eficiencia de Monnet Payment Solutions.



Capítulo 2. Ciberseguridad e intermediación financiera

Los ciberataques se han convertido en una de las principales amenazas para la estabilidad del sistema financiero global, especialmente para el sector bancario que experimenta hasta 300 veces más incidentes que otros sectores (Boungou, 2023). La creciente digitalización de los servicios financieros, acelerada por la pandemia, ha expandido la superficie de ataque y creado nuevas vulnerabilidades que los atacantes buscan explotar (Jin et al., 2023). En este contexto, resulta fundamental comprender cómo los ciberataques afectan la intermediación bancaria, ya que las instituciones financieras cumplen un rol crítico en la asignación de recursos y la estabilidad económica. Investigaciones recientes señalan que estos ataques pueden generar pérdidas sustanciales, erosionar la confianza de los depositantes y comprometer la capacidad de los bancos para cumplir su función de intermediación (Gatzert y Schubert, 2022). El trabajo de investigación "*Cyber-attacks and banking intermediation*" elaborado por Boungou (2023) contribuye significativamente a esta discusión al proporcionar evidencia empírica sobre los mecanismos específicos a través de los cuales los ciberataques impactan en la captación de depósitos y el otorgamiento de créditos en el sistema bancario estadounidense.

En el presente capítulo se desarrolla un análisis crítico del trabajo de Boungou (2023). El análisis aborda múltiples dimensiones que permiten una evaluación integral del estudio, considerando su relevancia en el contexto actual donde las instituciones financieras enfrentan crecientes amenazas cibernéticas (Cele y Kwenda, 2024; Elsayed et al., 2024; Gatzert y Schubert, 2022; Jin et al., 2023). Se examinan los antecedentes de investigación relacionados con los riesgos cibernéticos en el sector bancario y su impacto en la estabilidad financiera, evaluando su pertinencia y suficiencia para sustentar el problema de investigación. Se analiza el marco teórico propuesto por el autor, incluyendo los canales a través de los cuales los ciberataques afectan la captación de depósitos, el otorgamiento de créditos y el desempeño bancario, así como el papel que juegan las características específicas de las instituciones financieras en su vulnerabilidad ante estas amenazas.

La evaluación contempla un análisis detallado de la metodología empleada, considerando la idoneidad del diseño de investigación, la robustez de las técnicas econométricas utilizadas y la validez de los resultados obtenidos. Se presta especial atención a la estrategia empírica, evaluando sus ventajas y limitaciones frente a aproximaciones metodológicas previas. El análisis metodológico también aborda la pertinencia de los supuestos subyacentes, las pruebas de robustez realizadas y las posibles fuentes de sesgo que podrían afectar la validez de las conclusiones del estudio. Se examina la solidez del enfoque econométrico empleado para estimar el impacto de los ciberataques sobre la intermediación bancaria, así como la relevancia de las variables de control incluidas en el modelo y la construcción del indicador de riesgo cibernético utilizado para la investigación.

El análisis incluye una evaluación crítica de los resultados y sus implicaciones, determinando su contribución a la literatura sobre riesgos cibernéticos en el sector financiero. Se examinan los

hallazgos sobre el efecto de los ciberataques según las características bancarias y la dinámica de su impacto en diferentes dimensiones de la intermediación financiera. Se identifican las principales limitaciones conceptuales y metodológicas del trabajo, como los posibles sesgos en la medición del riesgo cibernético, los factores no observables que podrían afectar los resultados, y la posibilidad de generalizar los hallazgos a otros contextos institucionales o períodos temporales. A partir de esta revisión crítica, se propone una agenda de investigación que aborde las brechas identificadas y expanda el conocimiento sobre los mecanismos que vinculan los ciberataques con la estabilidad del sistema financiero. Asimismo, se desarrolla una discusión sobre la aplicabilidad de los hallazgos al contexto peruano y se plantean recomendaciones de política fundamentadas en la evidencia analizada, considerando aspectos como el riesgo sistémico, la interconexión bancaria y la efectividad de las medidas de ciberseguridad.

2.1 Antecedentes de la investigación

La investigación de Boungou (2023) desarrolla sus antecedentes a partir del Informe de Verizon, que identifica al sector bancario como el más afectado por incidentes con pérdidas de datos durante la década previa (Verizon, 2017). El autor complementa esta evidencia inicial con estudios de Kopp et al. (2017), Lagarde (2018) y Eisenbach et al. (2022), quienes señalan la particular vulnerabilidad de los bancos ante ciberataques debido a su rol como intermediarios financieros. Para dimensionar la magnitud del problema, el trabajo cita datos del Boston Consulting Group (2019) que indican que las instituciones financieras pueden sufrir hasta 300 veces más ciberataques anuales que empresas de otros sectores.

Los antecedentes presentados incluyen referencias al Fondo Monetario Internacional (2018) y Jamilov et al. (2021) sobre cómo el incremento en ciberataques podría deteriorar la provisión de servicios financieros y la confianza en el sistema bancario. El autor refuerza estos argumentos citando estimaciones de Verizon (2016) y Lagarde (2018) sobre pérdidas potenciales de cientos de miles de millones de dólares anuales. Como evidencia específica, presenta el caso del banco FIB de Bulgaria que en 2014 experimentó una corrida de depósitos del 10% tras ser víctima de correos electrónicos fraudulentos.

La revisión de antecedentes realizada por Boungou (2023) presenta varias limitaciones significativas. En primer lugar, aunque menciona estudios relevantes, no profundiza en sus metodologías ni hallazgos específicos, lo que impide comprender cabalmente la contribución incremental de su investigación. Por ejemplo, al citar trabajos como Kopp et al. (2017) y Eisenbach et al. (2022), el autor podría haber detallado qué aspectos específicos de la relación entre ciberataques e intermediación bancaria quedaron sin explorar en estas investigaciones previas.

La segunda limitación importante radica en la falta de un análisis crítico de la literatura existente. El autor se limita a presentar los antecedentes de manera descriptiva, sin cuestionar la

solidez metodológica de los estudios citados ni discutir posibles contradicciones entre sus hallazgos. Esta ausencia de evaluación crítica es particularmente notable en el uso de estimaciones sobre pérdidas financieras, donde no se discuten las metodologías empleadas para calcular estas cifras ni sus potenciales sesgos.

Un tercer aspecto cuestionable es la excesiva dependencia en reportes institucionales y declaraciones de autoridades financieras, en lugar de investigaciones académicas revisadas por pares. Si bien las referencias al Informe Verizon y al Boston Consulting Group proporcionan contexto valioso, la ausencia de una revisión más exhaustiva de la literatura académica debilita la fundamentación teórica del estudio. Esta limitada presencia de trabajos académicos podría explicarse por varios factores. Por un lado, la naturaleza confidencial de los incidentes cibernéticos en el sector financiero dificulta la construcción de bases de datos comprehensivas para análisis empíricos (Jin et al., 2023). Adicionalmente, la rápida evolución de las amenazas cibernéticas genera un rezago entre la ocurrencia de nuevos tipos de ataques y la publicación de investigaciones que los analicen (Chen et al., 2024). Las instituciones financieras también muestran resistencia a compartir información detallada sobre incidentes de seguridad por temor a impactos reputacionales o responsabilidades legales, como señalan Gatzert y Schubert (2022) en su análisis del sector bancario estadounidense. A esto se suma la complejidad metodológica de aislar el efecto causal de los ciberataques en el desempeño bancario, dado que estos incidentes frecuentemente coinciden con otros shocks que afectan a las instituciones financieras (Elsayed et al., 2024).

Un cuarto aspecto cuestionable es la ausencia de estudios sobre ciberataques en el sector financiero latinoamericano. Esta brecha en la literatura resulta relevante considerando las características distintivas de los mercados financieros de la región, como su alta concentración bancaria, menor desarrollo tecnológico y marcos regulatorios heterogéneos. La escasez de investigaciones sobre América Latina limita la comprensión de cómo los riesgos cibernéticos afectan a sistemas financieros con menor profundidad y mayor presencia de instituciones no bancarias. Estudios recientes como el de Cele y Kwenda (2024) sugieren que las economías emergentes pueden ser particularmente vulnerables a amenazas cibernéticas debido a sus brechas en infraestructura digital y capacidades técnicas. En el contexto latinoamericano, donde la digitalización financiera se ha acelerado significativamente, esta carencia de evidencia empírica dificulta el desarrollo de políticas efectivas para fortalecer la resiliencia del sector bancario ante ciberataques.

Finalmente, los antecedentes presentados muestran un sesgo hacia evidencia que respalda la hipótesis del autor sobre el impacto negativo de los ciberataques, sin considerar posibles argumentos contrarios o factores mitigantes. Por ejemplo, no se discuten estudios que hayan encontrado efectos limitados o nulos de los ciberataques en la intermediación bancaria, ni se exploran investigaciones sobre la efectividad de las medidas de ciberseguridad implementadas por los bancos. Esta selectividad

en la presentación de antecedentes podría llevar a una sobrestimación de la vulnerabilidad del sector bancario ante amenazas cibernéticas.

2.2 Marco teórico

El marco teórico desarrollado por Boungou (2023) se estructura en torno a cuatro canales principales a través de los cuales los ciberataques podrían afectar la intermediación bancaria. El primer canal propuesto es la reducción en el volumen de depósitos captados, argumentando que los incidentes cibernéticos pueden erosionar la confianza de los depositantes y provocar retiros de fondos. El segundo canal es la consecuente disminución en el volumen de préstamos, especialmente los de largo plazo, debido a la menor disponibilidad de recursos. El tercer canal se relaciona con el deterioro en el desempeño bancario como resultado directo de los ataques, mientras que el cuarto canal sugiere una reducción en la capacidad de los bancos para constituir provisiones por pérdidas crediticias.

El autor vincula estos canales teóricos con la literatura sobre incertidumbre y comportamiento bancario, citando a Berger et al. (2022) para argumentar que incluso los bancos que mantienen niveles adecuados de depósitos podrían acumular liquidez de manera preventiva ante la incertidumbre generada por los ciberataques. Este comportamiento precautorio, según el marco teórico, podría llevar a una reducción en la rentabilidad bancaria, como sugieren Lagarde (2018) y Dang y Nguyen (2022). El autor utiliza estos elementos para construir su hipótesis central sobre cómo la intermediación bancaria podría verse comprometida ante el aumento de los ciberataques.

Una limitación fundamental del marco teórico es la ausencia de un modelo formal que especifique las relaciones entre las variables de interés. El autor se limita a describir verbalmente los canales de transmisión propuestos, sin desarrollar un marco analítico que permita derivar predicciones específicas y comprobables. Esta carencia es particularmente notable dado que existe literatura sobre modelización del comportamiento bancario que podría haberse adaptado para incorporar el impacto de los ciberataques. Por ejemplo, el modelo seminal de Diamond y Dybvig (1983) sobre corridas bancarias podría extenderse para incorporar shocks de confianza generados por ciberataques. De manera similar, los modelos de gestión de activos y pasivos bancarios, como los que fundamentan el trabajo de Berger et al. (2022) sobre acumulación preventiva de liquidez ante la incertidumbre, podrían modificarse para examinar cómo la amenaza de ciberataques altera las decisiones de composición de cartera. El marco analítico de Eisenbach et al. (2022) sobre riesgos operacionales también ofrece una base que podría expandirse para modelar formalmente los canales de transmisión propuestos.

El marco teórico también muestra debilidades en la especificación de los mecanismos causales. Por ejemplo, al discutir el primer canal relacionado con la reducción de depósitos, el autor no elabora suficientemente sobre los factores que determinarían la magnitud de la respuesta de los depositantes ante un ciberataque. No se consideran elementos importantes cuyo rol ha sido documentado en la literatura previa. Por ejemplo, no se incorpora el efecto de los seguros de depósitos en la estabilidad

bancaria, un mecanismo que Diamond y Dybvig (1983) demostraron crucial para prevenir corridas bancarias. Tampoco se considera la efectividad de la comunicación bancaria durante crisis, que según Iyer et al. (2020) resulta fundamental para mantener la confianza de los inversionistas tras ciberataques. Adicionalmente, se omite la posible heterogeneidad en la respuesta de diferentes tipos de depositantes, un aspecto que Tosun (2021) encontró significativo al analizar la reacción del mercado ante violaciones de seguridad corporativa.

Otra crítica relevante es la falta de consideración de posibles efectos no lineales o umbrales en las relaciones propuestas. El marco teórico asume implícitamente que los efectos de los ciberataques son uniformes y proporcionales a su magnitud, sin contemplar la posibilidad de que existan niveles críticos a partir de los cuales los impactos se amplifiquen o que la respuesta del sistema bancario varíe según el tipo o la severidad del ataque.

El autor también omite discutir potenciales efectos de retroalimentación entre los canales propuestos. Por ejemplo, no se analiza el mecanismo de retroalimentación donde una reducción en la capacidad de constituir provisiones, documentada por Jin et al. (2023) como consecuencia de los ciberataques, podría deteriorar los indicadores de solidez bancaria. Este deterioro, según Iyer et al. (2020), típicamente conduce a una pérdida de confianza de los depositantes, lo que a su vez genera mayores retiros de fondos y presiona aún más la capacidad del banco para mantener provisiones adecuadas, creando así un círculo vicioso que amplifica el impacto inicial del ciberataque. Esta simplificación del marco teórico limita su capacidad para capturar la complejidad de las interacciones entre ciberataques e intermediación bancaria.

2.3 Metodología

Boungou (2023) desarrolla su análisis empírico utilizando datos de 2,144 bancos estadounidenses durante el período 2011-2019, lo que resulta en más de 16,000 observaciones a nivel banco-año. El autor justifica la selección de Estados Unidos como caso de estudio señalando que es uno de los países más expuestos a ciberataques según el reporte ITU (2017), con el sector bancario como el más vulnerable. La metodología se basa en un modelo de efectos fijos que relaciona diferentes medidas de intermediación bancaria con un indicador de riesgo cibernético. La especificación econométrica base es:

$$Banking_{i,t} = c + \alpha_1 Cyber\_attacks_t + \alpha_2 X_{i,t} + \alpha_3 Y_t + \theta_t + \lambda_i + \varepsilon_{i,t}$$

donde $Banking_{i,t}$ representa las variables de intermediación bancaria del banco i en el año t. Específicamente, se utilizan cinco medidas diferentes: (1) el ratio de depósitos de clientes sobre activos totales, que captura la capacidad del banco para atraer financiamiento minorista; (2) el volumen de préstamos con vencimiento menor a 3 meses sobre activos totales; (3) el volumen de préstamos con vencimiento entre 3 y 12 meses sobre activos totales; (4) el volumen de préstamos con vencimiento entre 1 y 5 años sobre activos totales; y (5) el volumen de préstamos con vencimiento mayor a 5 años

sobre activos totales. Estas últimas cuatro medidas permiten examinar cómo los ciberataques afectan la estructura temporal de la cartera crediticia del banco. $Cyber\_attacks_t$ es el indicador de riesgo cibernético desarrollado por Lhuissier y Tripier (2021), $X_{i,t}$ son controles específicos de los bancos, Y_t son variables macroeconómicas, mientras que θ_t y λ_i representan efectos fijos de tiempo y banco respectivamente.

La elección metodológica más cuestionable del estudio es la medida de ciberataques empleada. El autor utiliza un indicador basado en el número de tweets sobre riesgos cibernéticos, desarrollado por Lhuissier y Tripier (2021). Si bien esta medida tiene la ventaja de proporcionar datos de alta frecuencia, presenta limitaciones significativas. En primer lugar, el indicador basado en tweets presenta limitaciones fundamentales como proxy de los ciberataques reales. Al basarse en discusiones en redes sociales, el indicador puede estar sesgado por varios factores: la cobertura mediática selectiva que tiende a enfocarse en ataques de alto perfil mientras ignora incidentes menores pero potencialmente significativos; la posible manipulación estratégica de la narrativa en redes sociales por parte de actores interesados; y el sesgo de atención temporal donde ciertos eventos reciben una cobertura desproporcionada debido a factores contextuales como ciclos noticiosos o eventos políticos. Adicionalmente, como señalan Iyer et al. (2020), muchos ciberataques no se reportan públicamente o se revelan con retraso significativo por razones estratégicas o regulatorias, lo que implica que el volumen de discusión en redes sociales podría no correlacionarse adecuadamente con la incidencia real de ataques. Chen et al. (2024) también advierten que la naturaleza técnica de muchos incidentes cibernéticos puede resultar en una subrepresentación en las discusiones públicas, especialmente para ataques sofisticados que requieren conocimiento especializado para su comprensión.

Esta limitación es particularmente relevante cuando se compara con metodologías alternativas disponibles. Por ejemplo, estudios como Tosun (2021), Chen et al. (2024), Jin et al. (2023) e Iyer et al. (2020) han utilizado datos de la Privacy Rights Clearinghouse[1], que proporciona información verificable sobre incidentes cibernéticos específicos, incluyendo detalles sobre la naturaleza del ataque y el número de registros afectados. Esta base de datos permite una identificación más precisa de los eventos y su magnitud, lo que resulta crucial para estimar sus efectos económicos.

La especificación econométrica también presenta algunas debilidades. Aunque el autor incluye efectos fijos de banco y tiempo, así como controles específicos de banco y variables macroeconómicas, no aborda adecuadamente posibles problemas de endogeneidad. Por ejemplo, un sistema deficiente de control interno podría aumentar la vulnerabilidad a ciberataques y simultáneamente afectar los volúmenes de intermediación bancaria a través de múltiples canales. Las deficiencias en los sistemas de control podrían generar retrasos en el procesamiento de transacciones o errores en la verificación

[1] Disponible en https://privacyrights.org/data-breaches

de identidad de clientes, llevando a una reducción en el volumen de depósitos captados, como sugieren Jin et al. (2023) en su análisis de incidentes operativos en bancos. Asimismo, estas deficiencias podrían resultar en evaluaciones crediticias menos precisas que reduzcan el volumen de préstamos otorgados, un efecto documentado por Berger et al. (2022) en su estudio sobre riesgo operacional en holdings bancarios estadounidenses. En este contexto, la estimación del efecto de los ciberataques sobre la intermediación bancaria podría estar sesgada si no se controla adecuadamente por la calidad de los sistemas de control interno.

Este problema de endogeneidad podría abordarse mediante varias estrategias metodológicas. Una aproximación sería utilizar variables instrumentales basadas en ciberataques a bancos geográficamente cercanos, pero no directamente conectados con la institución analizada. Alternativamente, se podría emplear un diseño de diferencias en diferencias aprovechando la variación exógena en la exposición a ciberataques generada por la implementación escalonada de regulaciones de ciberseguridad. Una tercera estrategia sería utilizar el método de emparejamiento por puntaje de propensión para comparar instituciones con características similares pero diferente exposición a ciberataques. Sin embargo, la efectividad del método de emparejamiento por puntaje de propensión dependería crucialmente del número de bancos que han experimentado ciberataques en la muestra. Como señalan Jin et al. (2023), la baja frecuencia de ciberataques reportados públicamente podría resultar en un grupo de tratamiento demasiado pequeño para realizar emparejamientos significativos. Este desafío se magnifica cuando se consideran tipos específicos de ataques o períodos temporales limitados, como lo evidencian Iyer et al. (2020) en su análisis de violaciones de datos bancarios. Adicionalmente, la heterogeneidad en la severidad y naturaleza de los ciberataques podría complicar la identificación de pares comparables, un problema metodológico destacado por Chen et al. (2024) en su estudio sobre brechas de seguridad corporativa.

Otra limitación metodológica es la falta de pruebas de robustez más exhaustivas. Si bien el autor realiza algunas verificaciones utilizando medidas alternativas de financiamiento bancario y diferentes tipos de ciberataques, no explora suficientemente la sensibilidad de sus resultados a diferentes especificaciones econométricas o métodos de estimación. Por ejemplo, no se consideran potenciales efectos rezagados de los ciberataques ni se exploran posibles no linealidades en las relaciones estudiadas.

La agregación temporal de los datos también merece atención crítica. El uso de datos anuales podría estar ocultando dinámicas importantes que operan en frecuencias más altas. Dado que los ciberataques son eventos discretos que pueden tener efectos inmediatos sobre el comportamiento de los depositantes, la elección de datos anuales limita significativamente la capacidad del estudio para capturar la dinámica temporal de estos impactos. Esta limitación es particularmente relevante considerando que los bancos estadounidenses reportan sus estados financieros trimestralmente a los

reguladores. El uso de datos trimestrales, disponibles a través de los reportes Call Reports, permitiría un análisis más granular de cómo los ciberataques afectan la intermediación bancaria, facilitando la identificación de efectos que podrían perderse en agregaciones anuales. Jin et al. (2023), por ejemplo, aprovechan la frecuencia trimestral para identificar cambios en las provisiones por pérdidas crediticias tras ciberataques, demostrando la importancia de una mayor granularidad temporal para comprender los mecanismos de ajuste bancario.

2.4 Resultados empíricos

Los hallazgos presentados por Boungou (2023) se organizan en torno a tres aspectos principales de la intermediación bancaria. En primer lugar, el autor encuentra que los ciberataques tienen un impacto negativo y significativo en la captación de depósitos de clientes. Los coeficientes estimados oscilan entre -0.23 y -0.55, siendo significativos al nivel del 5%. Estos resultados se mantienen robustos a diferentes especificaciones del modelo, incluyendo la incorporación progresiva de controles específicos bancarios y variables macroeconómicas. En términos económicos, los coeficientes sugieren que un aumento en los ciberataques está asociado con una reducción sustancial en el ratio de depósitos sobre activos totales.

El segundo conjunto de resultados se refiere al impacto en la estructura de vencimientos de los préstamos bancarios. El autor documenta que los bancos ajustan sus carteras crediticias en respuesta a los ciberataques, aumentando los préstamos de muy corto plazo (menos de 3 meses) y corto plazo (3-12 meses), mientras reducen significativamente los préstamos de largo plazo (más de 5 años). Los coeficientes son estadísticamente significativos y económicamente relevantes, con un impacto positivo de 1.31 en préstamos muy cortos y un efecto negativo de -1.26 en préstamos largos.

El análisis de los resultados empíricos revela varias limitaciones importantes. En primer lugar, la significancia estadística de los coeficientes no necesariamente implica causalidad. Esta limitación se ve agravada por la ausencia de un modelo teórico formal que, como se discutió anteriormente, podría haber proporcionado una estructura analítica para identificar los vínculos causales entre ciberataques e intermediación bancaria. Por ejemplo, una extensión del modelo de Diamond y Dybvig (1983) podría haber especificado los mecanismos precisos a través de los cuales los ciberataques afectan las decisiones de los depositantes y las respuestas óptimas de los bancos. Sin este fundamento teórico, y aunque el autor controla por características bancarias y condiciones macroeconómicas, la naturaleza del diseño de investigación no permite descartar completamente la existencia de variables omitidas que podrían estar correlacionadas tanto con los ciberataques como con las decisiones bancarias.

Una segunda limitación se relaciona con la interpretación económica de los resultados. El autor no proporciona una discusión detallada sobre la magnitud relativa de los efectos encontrados en comparación con otros determinantes de la intermediación bancaria. Esta omisión dificulta evaluar la importancia práctica de los hallazgos en el contexto más amplio de la gestión bancaria. Además, no se

explora suficientemente la heterogeneidad de los efectos según características bancarias relevantes como el tamaño, la estructura de propiedad o el modelo de negocio.

Los resultados sobre el impacto en el desempeño bancario, medido a través del retorno sobre activos (ROA), también merecen un análisis crítico. El autor encuentra un efecto negativo y significativo de los ciberataques sobre la rentabilidad, con coeficientes que varían entre -0.45 y -0.23. Sin embargo, no se profundiza en los mecanismos específicos a través de los cuales los ciberataques afectan la rentabilidad. Por ejemplo, no se descompone el efecto entre cambios en los ingresos y en los costos operativos, lo que sería crucial para comprender mejor las implicaciones para la gestión bancaria.

La robustez de los resultados también podría cuestionarse desde varias perspectivas. Aunque el autor realiza algunas pruebas utilizando medidas alternativas de financiamiento bancario y diferentes categorías de ciberataques, no explora suficientemente la sensibilidad de los hallazgos a cambios en la especificación del modelo o en la definición de las variables principales. Por ejemplo, no se considera la posibilidad de efectos no lineales o umbrales en el impacto de los ciberataques, ni se explora la existencia de efectos asimétricos según la dirección del cambio en el riesgo cibernético.

Una limitación adicional del análisis es el uso del mismo conjunto de variables de control para todas las variables dependientes analizadas, sin considerar que los determinantes de cada dimensión de la intermediación bancaria podrían ser distintos. La captación de depósitos muestra una fuerte sensibilidad a variables macroeconómicas y de competencia bancaria (Berger et al., 2022), mientras que la estructura temporal de los préstamos responde principalmente a factores específicos de la demanda crediticia y la gestión de riesgos (Jin et al., 2023). Diferentes aspectos de la intermediación bancaria requieren conjuntos distintos de variables de control para capturar adecuadamente sus determinantes (Chen et al., 2024). El modelo econométrico podría fortalecerse incorporando controles específicos para cada variable dependiente, siguiendo las prácticas metodológicas más recientes en el análisis de impactos de ciberataques en instituciones financieras.

2.5 Implicaciones de los resultados

Boungou (2023) concluye que los ciberataques tienen un impacto negativo significativo en la intermediación bancaria a través de diversos canales. El autor destaca que sus resultados proporcionan la primera evidencia empírica del impacto de los ciberataques en la intermediación bancaria, enfatizando tres hallazgos principales. Primero, los bancos recolectan menos depósitos en respuesta a los ciberataques. Segundo, esta reducción en depósitos lleva a los bancos a prestar menos a largo plazo. Tercero, estos impactos negativos en la intermediación bancaria afectan el desempeño de los bancos y su capacidad para constituir provisiones por pérdidas crediticias.

El autor sugiere dos líneas potenciales para investigación futura. La primera consiste en estudiar cómo los bancos ajustan sus balances, especialmente su estructura de activos y pasivos, en respuesta a los ciberataques. La segunda propone analizar si los ciberataques inducen un riesgo

sistémico, considerando la interconexión de los bancos estadounidenses con el resto del mundo. Estas sugerencias reconocen implícitamente algunas de las limitaciones del estudio actual y apuntan hacia áreas importantes que requieren mayor investigación.

Una evaluación crítica de las conclusiones revela varias debilidades importantes. Primero, aunque el autor afirma proporcionar la primera evidencia empírica sobre el impacto de los ciberataques en la intermediación bancaria, esta afirmación parece excesiva dado que estudios previos han explorado aspectos relacionados de la relación entre ciberataques y comportamiento bancario (Elsayed et al., 2024; Jin et al., 2023). La contribución del estudio radica más bien en su enfoque específico sobre los canales de intermediación y en su análisis sistemático de múltiples dimensiones del comportamiento bancario.

Las implicaciones de política derivadas del estudio también merecen un análisis crítico. Si bien el autor sugiere que los resultados deberían alentar a los formuladores de políticas y a los bancos a implementar herramientas para fortalecer la resiliencia ante ciberataques, no desarrolla recomendaciones específicas ni discute los potenciales *trade-offs* entre seguridad y eficiencia operativa. La ausencia de un análisis más detallado sobre las implicaciones regulatorias es particularmente notable dado el énfasis del estudio en el riesgo sistémico.

La agenda de investigación futura propuesta, aunque relevante, presenta algunas omisiones importantes. Por ejemplo, no se menciona la necesidad de desarrollar medidas más precisas de los ciberataques ni de explorar la heterogeneidad de sus efectos según diferentes tipos de ataques o características bancarias. Tampoco se discute la importancia de examinar la efectividad de diferentes estrategias de mitigación de riesgos cibernéticos o de analizar cómo la regulación bancaria podría adaptarse para abordar mejor estas amenazas emergentes.

Un aspecto particularmente débil de las conclusiones es la falta de discusión sobre las implicaciones de los resultados para la gestión de riesgos bancarios. El autor no elabora sobre cómo los bancos podrían incorporar el riesgo cibernético en sus marcos de gestión de riesgos existentes ni discute las implicaciones para la asignación de capital y la planificación de contingencia. Esta omisión es significativa dado que los resultados sugieren que los ciberataques tienen efectos importantes tanto en la estructura de financiamiento como en la asignación de crédito.

2.6 Agenda de investigación y aplicación al contexto peruano

La investigación futura sobre ciberataques y estabilidad financiera en Perú debería priorizar cuatro áreas clave de estudio. En primer lugar, resulta fundamental desarrollar una base de datos comprehensiva de incidentes cibernéticos en el sistema financiero peruano, inspirada en la Privacy Rights Clearinghouse (PRC) de Estados Unidos pero con un enfoque específico en el sector financiero. La PRC, que documenta violaciones de datos en todos los sectores de la economía estadounidense, ha permitido investigaciones como las de Tosun (2021) e Iyer et al. (2020) que analizan subconjuntos de

estos incidentes para estudiar impactos sectoriales específicos. En el caso peruano, aunque un enfoque multisectorial similar sería valioso, la prioridad inicial podría centrarse en el sector financiero dada su criticidad para la estabilidad económica. Esta base de datos permitiría analizar patrones específicos de vulnerabilidad en el contexto local y evaluar la efectividad de diferentes medidas de mitigación.

Este esfuerzo requeriría una colaboración interinstitucional entre la Autoridad Nacional de Protección de Datos Personales (ANPDP), la Superintendencia de Banca, Seguros y AFP (SBS) y las instituciones financieras. La ANPDP, que ya tiene el mandato legal de supervisar y proteger los datos personales en todos los sectores económicos, podría asumir un rol central en la recopilación y gestión de esta base de datos, aprovechando su experiencia en el manejo de información sensible y su autoridad regulatoria existente. Su labor se complementaría con la experticia técnica de la SBS en supervisión bancaria y la información proporcionada por las instituciones financieras. Este modelo de colaboración tripartita permitiría aprovechar las competencias existentes de cada institución mientras se fortalece la capacidad nacional de monitoreo y análisis de incidentes cibernéticos.

Un segundo aspecto prioritario es el análisis de la interconexión entre instituciones financieras peruanas y su rol en la transmisión de riesgos cibernéticos. La alta concentración del sistema bancario peruano, donde cuatro bancos controlan aproximadamente el 80% de los activos, sugiere que los efectos de contagio podrían ser particularmente relevantes. Este contagio podría manifestarse a través de múltiples canales: conexiones directas mediante el mercado interbancario, donde un ciberataque que comprometa la liquidez de un banco grande podría generar una cadena de incumplimientos; relaciones operativas compartidas, como el uso de los mismos proveedores de servicios tecnológicos o infraestructura de pagos, que podrían actuar como vectores de propagación de ataques; y efectos reputacionales, donde un incidente en un banco importante podría desencadenar una crisis de confianza que afecte a todo el sistema, similar al efecto documentado por Iyer et al. (2020) en su análisis de cómo los ciberataques impactan la valoración de bonos bancarios. Los investigadores deberían examinar cómo esta estructura de mercado influye en la propagación de impactos cibernéticos y en la resiliencia sistémica.

La tercera línea de investigación debería enfocarse en el rol de las *fintech* y el sistema financiero no bancario. El crecimiento acelerado del sector *fintech* en Perú introduce nuevos vectores de riesgo cibernético que podrían afectar la estabilidad del sistema financiero tradicional. Es necesario estudiar cómo la creciente interconexión entre entidades tradicionales y nuevos actores digitales modifica los patrones de vulnerabilidad y transmisión de riesgos cibernéticos.

El cuarto aspecto por investigar es la efectividad de diferentes arquitecturas regulatorias para la gestión de riesgos cibernéticos. Se requieren estudios que evalúen el impacto de las regulaciones existentes y exploren diseños alternativos que consideren las particularidades del mercado financiero peruano, incluyendo su alto nivel de informalidad y las brechas en inclusión financiera.

Respecto a la aplicabilidad de los hallazgos de Boungou (2023) al contexto peruano, es necesario considerar varias características distintivas del mercado local. La menor profundidad del mercado financiero peruano y sus mayores niveles de concentración podrían amplificar el impacto de los ciberataques sobre la intermediación bancaria. Adicionalmente, la menor sofisticación tecnológica de algunos participantes del mercado y las brechas en educación financiera digital podrían exacerbar la vulnerabilidad del sistema.

Las recomendaciones de política para el contexto peruano deben articularse en tres niveles. A nivel micro prudencial, la SBS debería establecer requerimientos mínimos de inversión en ciberseguridad proporcionales al tamaño y complejidad de cada institución. Estas exigencias deberían complementarse con evaluaciones periódicas de vulnerabilidad y ejercicios de simulación de crisis cibernéticas.

A nivel macro prudencial, resulta crucial desarrollar un marco de monitoreo del riesgo sistémico que incorpore explícitamente la dimensión cibernética. Esto podría incluir la creación de un sistema de alerta temprana basado en indicadores de riesgo cibernético y la implementación de pruebas de estrés que consideren escenarios de ataques coordinados. El Banco Central de Reserva del Perú debería incorporar estos elementos en su evaluación regular de la estabilidad financiera.

Finalmente, a nivel de coordinación interinstitucional, se recomienda establecer un comité de estabilidad cibernética que integre a la SBS, el BCRP, el Ministerio de Economía y Finanzas, y representantes del sector privado. Este comité facilitaría el intercambio de información sobre amenazas cibernéticas, coordinaría respuestas ante incidentes mayores y promovería la adopción de estándares comunes de ciberseguridad en el sector financiero.

Conclusiones

El análisis crítico del trabajo de Boungou (2023) sobre el impacto de los ciberataques en la intermediación bancaria revela hallazgos significativos que contribuyen a nuestra comprensión de los riesgos emergentes en el sistema financiero. La evidencia empírica presentada demuestra que los ciberataques afectan negativamente múltiples dimensiones de la intermediación bancaria, desde la captación de depósitos hasta la estructura temporal de los préstamos y el desempeño financiero de las instituciones.

Sin embargo, el estudio presenta limitaciones metodológicas importantes que deben considerarse al interpretar sus resultados. La medición de ciberataques mediante un indicador basado en tweets, aunque innovadora, podría no capturar adecuadamente la magnitud y naturaleza de las amenazas cibernéticas reales. La ausencia de un modelo teórico formal y las potenciales preocupaciones de endogeneidad sugieren que los resultados deben interpretarse con cautela.

La aplicación de estos hallazgos al contexto peruano requiere considerar las características distintivas del mercado financiero local. La alta concentración bancaria, la creciente presencia de *fintech* y las brechas en inclusión financiera digital sugieren que los mecanismos de transmisión de los ciberataques podrían manifestarse de manera diferente en Perú. Esto resalta la necesidad de desarrollar investigación específica que considere estas particularidades del mercado local.

Las implicaciones de política derivadas del análisis sugieren la necesidad de un enfoque integral que combine medidas micro y macro prudenciales. La creación de una base de datos comprehensiva de incidentes cibernéticos, el fortalecimiento de los marcos regulatorios y la mejora en la coordinación interinstitucional emergen como prioridades clave para fortalecer la resiliencia del sistema financiero ante amenazas cibernéticas.

La agenda de investigación futura debe abordar las brechas identificadas en la literatura actual. Es crucial desarrollar medidas más precisas de riesgo cibernético, analizar los mecanismos de contagio en sistemas financieros concentrados y evaluar la efectividad de diferentes estrategias de mitigación. Particular atención merece el estudio de cómo la creciente digitalización del sector financiero modifica los patrones de vulnerabilidad y transmisión de riesgos cibernéticos.

Finalmente, la experiencia internacional sugiere que la gestión efectiva de los riesgos cibernéticos requiere un equilibrio delicado entre la innovación financiera y la seguridad operativa. El desafío para los reguladores y las instituciones financieras peruanas será desarrollar marcos de gestión de riesgos que promuevan la digitalización financiera mientras mantienen la estabilidad del sistema. La colaboración entre el sector público y privado, junto con el desarrollo de capacidades técnicas especializadas, será fundamental para enfrentar este reto emergente.

Referencias

Berger, A., Curti, F., Mihov, A., & Sedunov, J. (2022). Operational risk is more systemic than you think: Evidence from U.S. bank holding companies. *Journal of Banking and Finance*, 143, 106619.

Boston Consulting Group. (2019). Global Wealth 2019: Reigniting Radical Growth. BCG Editorial.

Boungou, W. (2023). Cyber-attacks and banking intermediation. *Economics Letters*, 233, 111354. https://doi.org/10.1016/j.econlet.2023.111354

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime, 32*(1), 31-48. https://doi.org/10.1108/JFC-10-2023-0263

Chen, W., Li, X., Wu, H., & Zhang, L. (2024). The impact of managerial myopia on cybersecurity: Evidence from data breaches. *Journal of Banking & Finance*, 166, 107254.

Dang, V., & Nguyen, H. (2022). Bank profitability under uncertainty. *The Quarterly Review of Economics and Finance*, 83, 119-134.

Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. *Journal of Political Economy, 91*(3), 401-419.

Eisenbach, T., Kovner, A., & Lee, M. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*, 145, 802-826.

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. *Future Business Journal, 10*(1), 115. https://doi.org/10.1186/s43093-024-00402-9

Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance, 89*(3), 725–763.

IMF. (2018). *Is Growth at Risk? Global Financial Stability Report, October*. https://www.imf.org/en/Publications/GFSR/Issues/2024/10/22/global-financial-stability-report-october-2024

ITU. (2017). *Global Cybersecurity Index (GCI) 2017*. International Communication Unit, ITU, July. https://www.unodc.org/e4j/data/_university_uni_/global_cybersecurity_index_gci_2017.html?lng=en

Iyer, S. R., Simkins, B. J., & Wang, H. (2020). Cyberattacks and impact on bond valuation. *Finance Research Letters*, 33, 101215.

Jamilov, R., Rey, H., & Tahoun, A. (2021). *The anatomy of cyber risk*. NBER Working paper, No. 28906.

Jin, J., Li, N., Liu, S., & Khalid Nainar, S. M. (2023). Cyber attacks, discretionary loan loss provisions, and banks' earnings management. *Finance Research Letters*, 54, 103705.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber Defense Must Be Global*. IMF Blog, October 26, 2017. https://www.imf.org/en/Blogs/Articles/2017/10/26/cyber-defense-must-be-global

Lagarde, C. (2018). *Estimating Cyber Risk for the Financial Sector*. IMF Blog, June 22, 2018. https://www.imf.org/en/Blogs/Articles/2018/06/22/blog-estimating-cyber-risk-for-the-financial-sector

Lhuissier, S., & Tripier, F. (2021). *Measuring cyber risk*. Banque de France Editorial.

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, 76, 101795.

Verizon. (2017). *Data Breach Investigations Report 2017*. Verizon Enterprise. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf