PROJECT, DESIGN AND MANAGEMENT (PDM)
https://www.mlsjournals.com/Project-Design-Management
ISSN: 2683-1597

(2026) Project, Design and Management 8(1), -. doi.org/10.35992/pdm.v8i1.4547

IMPLEMENTACIÓN DEL REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN ENTIDADES FINANCIERAS SUPERVISADAS POR EL BANCO CENTRAL DE LA REPÚBLICA DOMINICANA

Implementation of the Cybersecurity and Information Security Regulation in Financial Institutions Supervised by the Central Bank of the Dominican Republic

Luis Rafael Villalona Mateo
Universidad Internacional Iberoamericana, República Dominicana
[luis.villalona@doctorado.unini.edu.mx] [https://orcid.org/0009-0009-8780-8160]
Ernesto Bautista Thompson
Universidad Internacional Iberoamericana, México
[ernesto.bautista@unini.edu.mx] [https://orcid.org/0000-0001-5219-6891]

Información del manuscrito:

Recibido/Received: 05/11/2025
Revisado/Reviewed: 02/06/2026
Aceptado/Accepted: 23/06/2026

Palabras clave:
Gestión de Proyectos; Seguridad Cibernética y de la Información; Ciberseguridad; Sector Financiero; Regulación Tecnológica.

RESUMEN

Esta investigación aborda, de manera rigurosa y crítica, la implementación del Reglamento de Seguridad Cibernética y de la Información en las entidades financieras supervisadas por el Banco Central de la República Dominicana, estableciendo un marco analítico que permite identificar, evaluar y proponer soluciones a las principales limitantes que afectan su cumplimiento. A través de un enfoque metodológico mixto, sustentado en datos empíricos y análisis correlacional, se evidencian brechas significativas en áreas como la cultura organizacional en ciberseguridad, la capacitación del talento humano, la modernización tecnológica, la coordinación interinstitucional y la claridad normativa. Los hallazgos revelan que, aunque existe un avance en la adopción del reglamento, persisten desafíos estructurales que requieren intervenciones estratégicas para garantizar una implementación efectiva y sostenible. Como resultado, esta investigación pretende generar productos científicos de alto valor práctico, tales como un manual de implementación, una metodología de evaluación y un análisis costo-beneficio, que permiten a las instituciones financieras tomar decisiones informadas y estratégicas. Estos aportes posicionan esta investigación como una herramienta de referencia para el fortalecimiento de la resiliencia digital, y como un punto de partida para futuras investigaciones que deseen profundizar en la gobernanza de la ciberseguridad, la eficacia regulatoria y la transformación digital en contextos similares. En consecuencia, esta obra se proyecta como una contribución sustantiva al desarrollo de políticas públicas, al diseño de marcos normativos más robustos y a la consolidación de una cultura de seguridad cibernética tanto a nivel nacional como internacional.

Keywords:
Project Management, Cybersecurity and Information Security, Cybersecurity, Financial Sector, Technological Regulation.

ABSTRACT

This research rigorously and critically addresses the implementation of the Cybersecurity and Information Security Regulation in financial institutions supervised by the Central Bank of the Dominican Republic, establishing an analytical framework to identify, evaluate, and propose solutions to the main limitations affecting its compliance. Through a mixed methodological approach, supported by empirical data and correlational analysis, significant gaps are revealed in areas such as organizational culture in cybersecurity, human talent training, technological modernization, interinstitutional coordination, and regulatory clarity. The findings show that although progress has been made in adopting the regulation, structural challenges persist that require strategic interventions to ensure effective and sustainable implementation. Consequently, the study seeks to produce scientifically rigorous deliverables with substantial practical relevance, such as an implementation manual, an evaluation methodology, and a cost-benefit analysis, enabling financial institutions to make informed and strategic decisions. These contributions position this research project as a reference tool for strengthening digital resilience and as a starting point for future research aiming to deepen governance in cybersecurity, regulatory effectiveness, and digital transformation in similar contexts. Consequently, this work is projected as a substantive contribution to the development of public policies, the design of more robust regulatory frameworks, and the consolidation of a sustainable digital security culture, both nationally and internationally.

Introducción

La transformación digital, impulsada por tecnologías como la inteligencia artificial, la computación en la nube y el Internet de las cosas (IoT), ha incrementado significativamente la exposición del sector financiero a riesgos cibernéticos complejos y persistentes. En este contexto, la literatura científica reciente ha abordado la ciberseguridad desde una perspectiva global, destacando su impacto en la estabilidad financiera y la necesidad de fortalecer los marcos regulatorios. Estudios del Fondo Monetario Internacional evidencian que los riesgos cibernéticos constituyen una amenaza sistémica creciente que requiere no solo regulación, sino también capacidades institucionales para su implementación efectiva (Gaidosch et al., 2026; Ravikumar, 2025). De igual manera, investigaciones del Banco de Pagos Internacionales señalan una evolución hacia enfoques regulatorios orientados a la resiliencia operativa, enfatizando la necesidad de mecanismos estructurados para la gestión del riesgo cibernético en las entidades financieras (Crisanto et al., 2023). En el ámbito regional, estudios del Banco Interamericano de Desarrollo y la Organización de los Estados Americanos evidencian que, aunque se han logrado avances normativos en América Latina, persisten brechas significativas en capacidades técnicas, cultura organizacional y coordinación interinstitucional, lo que limita la implementación efectiva de dichas regulaciones (BID & OEA, 2025; Banco Mundial, 2024). En República Dominicana, este proceso ha sido impulsado por políticas públicas como el programa República Digital, la expansión de la infraestructura de fibra óptica, y el desarrollo de zonas francas tecnológicas, lo que ha permitido una mayor conectividad, innovación y acceso a servicios digitales (Observatorio Nacional de Tecnologías de la Información y la Comunicación (ONTIC-RD, 2020).

En los últimos años, la República Dominicana ha experimentado un crecimiento significativo en su exposición a amenazas cibernéticas, en línea con las tendencias observadas a nivel global. Según datos de FortiGuard Labs, el país registró aproximadamente 5 mil millones de intentos de ciberataques en 2022, cifra que se redujo a cerca de 1,000 millones en 2023, lo que refleja una transición hacia ataques más sofisticados y dirigidos, en los que se prioriza la efectividad sobre el volumen (Fortinet, 2024). Asimismo, en el ámbito financiero, la Superintendencia de Bancos reportó pérdidas superiores a RD$1,677 millones asociadas a fraudes, especialmente vinculados al uso de tarjetas y canales digitales durante el año 2023 (Superintendencia de Bancos de la República Dominicana, 2024). Estos datos evidencian no solo la magnitud del riesgo cibernético en el contexto dominicano, sino también la creciente complejidad de las amenazas y su impacto directo en la estabilidad del sistema financiero, reforzando la necesidad de enfoques integrales que permitan fortalecer la resiliencia institucional frente a estos desafíos.

En la literatura científica reciente, diversos estudios han analizado la implementación de regulaciones de ciberseguridad en el sector financiero. Kshetri (2021) señala que la adopción de marcos regulatorios fortalece la resiliencia institucional frente a amenazas digitales, aunque su efectividad depende de factores organizacionales y tecnológicos. De manera similar, Bouveret (2019), desde el Fondo Monetario Internacional, sostiene que las regulaciones en ciberseguridad son fundamentales para mitigar riesgos sistémicos, pero su implementación enfrenta brechas significativas, especialmente en economías emergentes. La complejidad técnica, organizacional y normativa exige metodologías que permitan traducir los requerimientos regulatorios en acciones concretas y medibles, es donde radica la importancia de desarrollar las

metodologías presentadas en esta investigación, ya que la ausencia de estos enfoques limita el cumplimiento normativo y la gestión adecuada del riesgo, por lo que el desarrollo de metodologías de implementación resulta clave para fortalecer la eficacia de los programas de seguridad en el sector financiero de la República Dominicana.

En América Latina, investigaciones de la Organización de los Estados Americanos (OEA, 2018) y del Banco Interamericano de Desarrollo (BID, 2020) evidencian que las instituciones financieras presentan niveles heterogéneos de madurez en ciberseguridad, destacándose debilidades en la capacitación del talento humano, la cultura organizacional y la resiliencia de infraestructuras críticas. Estos estudios coinciden en que la implementación normativa no garantiza, por sí sola, una protección efectiva.

En República Dominicana, los esfuerzos por crear un ciberespacio más seguro se remontan a la promulgación de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, publicada el 23 de abril de 2007 (Ministerio de Interior y Policía, 2007). Esta legislación marcó un hito al tipificar delitos informáticos y establecer mecanismos de cooperación nacional e internacional para su persecución.

En el ámbito regulatorio, la Junta Monetaria del Banco Central aprobó el Reglamento de Seguridad Cibernética y de la Información mediante la Segunda Resolución del 1 de noviembre de 2018, estableciendo lineamientos obligatorios para las entidades financieras en materia de protección tecnológica, gestión de riesgos y gobernanza de la seguridad digital (Banco Central de la República Dominicana, 2018). Asimismo, se han creado organismos especializados como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional y la Procuraduría Especializada en Crímenes y Delitos de Alta Tecnología (PEDATEC), encargados de la prevención, investigación y persecución de delitos informáticos, en coordinación con el Ministerio Público y organismos internacionales (Procuraduría General de la República, 2017). Si bien se han producido avances regulatorios significativos con la promulgación del Reglamento de Seguridad Cibernética y de la Información por parte del Banco Central de la República Dominicana en 2018, la evidencia empírica sobre su implementación efectiva en entidades financieras sigue siendo limitada.

A pesar del crecimiento de la literatura sobre seguridad cibernética y de la información, ciberseguridad y regulaciones en entidades financieras, existe una brecha importante en estudios empíricos que integren un enfoque metodológico mixto para analizar las condiciones reales de implementación normativa en contextos específicos como el sistema financiero dominicano. La mayoría de las investigaciones se han centrado en enfoques normativos o técnicos, sin abordar de manera integral las relaciones entre variables organizacionales, tecnológicas y regulatoria.

En coherencia con esta limitación presentada, la revisión de la literatura científica y técnica, tanto a nivel nacional como regional, evidencia una disponibilidad limitada de estudios empíricos que aborden de forma específica la implementación de metodologías y herramientas como las propuestas en esta investigación. En este sentido, el presente estudio aporta un enfoque novedoso que contribuye al desarrollo del conocimiento en el ámbito de la ciberseguridad aplicada al sector financiero. La originalidad del estudio se fundamenta en la incorporación de un enfoque metodológico aplicado y empírico para analizar la implementación del reglamento en el sistema financiero dominicano, desde una perspectiva integral no evidenciada en estudios previos.

Este artículo se inscribe en esa línea de investigación aplicada, así mismo el presente estudio, en donde se está proponiendo una metodología adaptada al contexto dominicano, trata de que las organizaciones en donde se implemente el Programa de Seguridad Cibernética y de la Información cumplan con la regulación, regulación que exige

una respuesta técnica y organizativa robusta. La propuesta metodológica se fundamenta en un enfoque mixto, que permitirá contrastar los hallazgos con las investigaciones previas y aportar evidencia sobre la viabilidad de aplicar modelos de gestión por proyectos en la implementación de programas de seguridad cibernética y de la información en el sector financiero de la República Dominicana.

Los resultados obtenidos en esta investigación evidencian que, si bien existe un marco normativo robusto impulsado por el Banco Central de la República Dominicana, así mismo su correcta implementación presenta desafíos muy significativos para la mayoría de las entidades financieras, especialmente aquellas con limitaciones técnicas, presupuestarias o de personal especializado. Del mismo modo, se identificó que el cumplimiento formal o total del reglamento de ciberseguridad no siempre garantiza una protección efectiva contra la evolución de las amenazas del día a día, ni con las amenazas avanzadas, lo que plantea, entre otras cosas que se verán en el desarrollo de este estudio, la necesidad de discutir los mecanismos de evaluación y seguimiento institucional, como también las leyes y regulaciones en seguridad cibernética y de la información del Estado Dominicano.

Este estudio se propone analizar de manera rigurosa las condiciones que obstaculizan la aplicación efectiva del reglamento, partiendo de una perspectiva crítica y multidimensional. Para ello, se han formulado hipótesis generales, que orientan a la investigación, estas son:

1. La insuficiencia de capacidades técnicas especializadas en el personal del área de seguridad cibernética y de la información, limita significativamente la efectividad de la implementación de políticas de seguridad de la información.
2. La ausencia de un marco jurídico robusto, con sanciones claras y mecanismos de supervisión efectivos, reduce la capacidad de cumplimiento normativo en las entidades del sector financiero.
3. El bajo nivel de resiliencia en infraestructuras críticas, especialmente en entidades medianas y pequeñas, incrementa la vulnerabilidad frente a incidentes cibernéticos.
4. Las restricciones presupuestarias dificultan la adopción de tecnologías avanzadas, afectando negativamente la madurez en ciberseguridad institucional.
5. La resistencia al cambio organizacional constituye una barrera estructural para la implementación efectiva de nuevas políticas y procedimientos en materia de seguridad de la información.

Estas hipótesis generales se desagregan en un conjunto de hipótesis específicas, que serán validadas empíricamente mediante un diseño metodológico mixto:

- H1: Las entidades con menor inversión en capacitación técnica presentan mayores brechas de cumplimiento en seguridad cibernética.
- H2: La inexistencia de sanciones legales claras se correlaciona con una menor adopción de estándares internacionales de seguridad.
- H3: Las organizaciones con infraestructuras menos resilientes reportan mayor frecuencia de incidentes de seguridad.
- H4: La disponibilidad presupuestaria está positivamente relacionada con el nivel de implementación tecnológica en seguridad de la información.
- H5: La resistencia al cambio organizacional se asocia negativamente con la efectividad de los procesos de transformación digital y seguridad.

La formulación de hipótesis en este estudio responde a una necesidad metodológica de delimitar con precisión las variables críticas que inciden en la implementación efectiva del Reglamento de Seguridad Cibernética y de la Información en el sistema financiero dominicano. Estas hipótesis no solo cumplen una función explicativa, sino que constituyen el eje estructurante del diseño investigativo, al permitir la construcción de un modelo analítico que articula factores técnicos, normativos, organizacionales y presupuestarios. En conjunto, este enfoque permite trascender la mera descripción del fenómeno, avanzando hacia una comprensión profunda y una intervención estratégica basada en evidencia.

En este sentido, esta investigación no solo busca validar las hipótesis planteadas, sino también se pretende generar productos científicos de alto valor práctico que contribuyan al fortalecimiento de la resiliencia digital del sistema financiero dominicano. Se proyecta que para el año 2027, más del 85% de las entidades habrán alcanzado un nivel de cumplimiento superior al 90%, y al menos 60 instituciones lograrán una implementación completa, ampliando significativamente la cobertura de infraestructura crítica protegida (Superintendencia de Bancos de la República Dominicana, 2025).

La estructura del documento se organiza en capítulos que abordan el marco teórico, la metodología, el análisis de resultados, la discusión crítica y las conclusiones, complementados por anexos técnicos que detallan los productos derivados de la investigación. Esta obra se posiciona como una contribución sustantiva al desarrollo de políticas públicas, al diseño de marcos normativos más eficaces y a la consolidación de una cultura de seguridad digital sostenible, tanto a nivel nacional como internacional.

Método

Enfoque metodológico

El presente estudio se fundamenta en un enfoque metodológico mixto, el cual combina técnicas cuantitativas y cualitativas con el propósito de obtener una visión integral del fenómeno analizado. Este enfoque permite abordar simultáneamente la medición objetiva de variables y la interpretación contextual de los procesos organizacionales, facilitando una comprensión más completa de la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero dominicano. La integración de ambos enfoques responde a la necesidad de analizar no solo el nivel de cumplimiento normativo, sino también los factores estructurales que condicionan dicho proceso.

El enfoque cuantitativo se orienta a la recolección y análisis de datos medibles relacionados con variables clave como el cumplimiento normativo, la inversión tecnológica y la capacitación del talento humano, permitiendo identificar patrones y relaciones mediante técnicas estadísticas. Por su parte, el enfoque cualitativo permite profundizar en las percepciones, experiencias y dinámicas organizacionales de los actores involucrados, aportando una comprensión contextual del fenómeno que no puede ser captada únicamente a través de datos numéricos. Esta complementariedad metodológica fortalece la capacidad explicativa del estudio.

La adopción de un enfoque mixto se sustenta en la literatura metodológica, que establece que la combinación de datos cuantitativos y cualitativos permite una mayor validez y profundidad en la investigación, al integrar distintos tipos de evidencia en el análisis del problema (Creswell & Plano Clark, 2018). Asimismo, este enfoque facilita la triangulación de la información, entendida como el uso de múltiples fuentes y métodos para corroborar hallazgos, lo cual contribuye a mejorar la credibilidad y consistencia de

los resultados (Hernández Sampieri et al., 2014). En este sentido, el enfoque metodológico adoptado permite no solo describir el estado de la implementación del reglamento, sino también explicar las relaciones entre las variables que influyen en su efectividad en el contexto dominicano.

Diseño de investigación

La investigación adopta un diseño no experimental, con enfoque transeccional y descriptivo, estructurado en dos fases secuenciales. En la primera fase, de carácter cuantitativo, se aplican metodologías que permiten recolectar datos en un único momento temporal, sin manipular variables, con el objetivo de identificar patrones, relaciones y antecedentes normativos y técnicos sobre la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero dominicano. Las metodologías cuantitativas son fundamentales en investigaciones científicas orientadas a la transferencia de conocimiento, ya que permiten proporcionar datos precisos y confiables. Según Alan Bryman, el uso de métodos estadísticos en la investigación social facilita el análisis de grandes volúmenes de datos, la identificación de patrones y la formulación de relaciones entre variables, lo que contribuye a la robustez de los hallazgos empíricos (Bryman, 2016, pp. 147–148).

La segunda fase, de naturaleza cualitativa, se desarrolla mediante un diseño descriptivo basado en estudios de caso, seleccionados por criterios de relevancia institucional y nivel de madurez en ciberseguridad. Esta fase permite profundizar en las experiencias de los actores involucrados, mediante entrevistas semiestructuradas, encuestas abiertas y ejercicios interpretativos, que aportan una comprensión contextualizada del fenómeno. La investigación cualitativa permite captar las experiencias en su contexto natural, facilitando una comprensión profunda y detallada de los fenómenos estudiados. Luego de consultar diferentes fuentes se pudo concluir que este enfoque es esencial para explorar significados, interpretaciones y dinámicas sociales que no pueden ser captadas mediante métodos cuantitativos, lo que lo convierte en una herramienta valiosa para estudios exploratorios y descriptivos.

Fases del estudio

La presente investigación se estructura en un modelo secuencial de dos fases, con el objetivo de abordar el fenómeno de la implementación del Reglamento de Seguridad Cibernética y de la Información desde una perspectiva integral. Estas fases se articulan metodológicamente para garantizar la coherencia entre los objetivos, el enfoque mixto adoptado y las técnicas de recolección y análisis de datos.

La primera fase corresponde a un enfoque cuantitativo, desarrollado mediante una investigación no experimental con diseño transeccional. Este tipo de investigación permite observar fenómenos en su contexto natural sin manipular variables, y recolectar datos en un único momento temporal (Hernández Sampieri et al., 2014, p. 151). En esta etapa se aplican estudios exploratorios y documentales, orientados a identificar patrones, relaciones y antecedentes normativos y técnicos sobre la implementación del reglamento en el sector financiero dominicano. Además, se emplean métodos estadísticos que permiten analizar grandes cantidades de datos y establecer relaciones entre variables, lo cual es fundamental en investigaciones orientadas a la transferencia de conocimiento (Bryman, 2016, pp. 149-150).

La segunda fase se desarrolla bajo un enfoque cualitativo, mediante una investigación descriptiva basada en estudios de caso. Esta metodología permite una comprensión profunda y detallada de los fenómenos estudiados, captando las

experiencias y percepciones de los actores involucrados en su contexto natural. Se emplean técnicas como entrevistas semiestructuradas, encuestas abiertas y ejercicios interpretativos, que aportan evidencia empírica sobre la aplicabilidad del modelo propuesto. Esta fase busca fundamentar las razones que dieron origen a esta investigación y generar conocimiento contextualizado que sirva de base para futuras investigaciones.

Ambas fases se complementan en un diseño secuencial, fortaleciendo la validez interna del estudio y asegurando que los métodos empleados respondan adecuadamente a las preguntas de investigación planteadas. Aunque esta investigación no pretende establecer conclusiones absolutas sobre el fenómeno estudiado, sí busca realizar un primer acercamiento riguroso que contribuya al desarrollo académico y práctico del campo de la ciberseguridad financiera.

Técnica de recolección de datos

Este estudio se compone de dos fases metodológicas, cada una con técnicas de recolección de datos específicas que responden a los objetivos planteados en el estudio. En la fase cuantitativa, se emplean técnicas de recolección documental y análisis de registros institucionales, orientadas a identificar patrones normativos, niveles de cumplimiento y variables relacionadas con la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero dominicano. Estas fuentes secundarias permiten obtener datos objetivos y verificables, facilitando el análisis estadístico y la comparación entre entidades.

Las encuestas fueron diseñadas para captar información relevante sobre el grado de implementación del reglamento, los desafíos enfrentados, las estrategias adoptadas y la percepción institucional sobre su efectividad. El instrumento principal utilizado fue un cuestionario estructurado compuesto por ítems tipo Likert, diseñado para medir variables claves asociadas a la implementación del Reglamento de Seguridad Cibernética y de la Información. Se aplicaron de manera directa y confidencial, garantizando el anonimato de los participantes y el resguardo de los datos sensibles compartidos. Esta medida fue esencial para fomentar la participación voluntaria y honesta de los encuestados, quienes accedieron a colaborar bajo el compromiso de que los resultados serían utilizados exclusivamente con fines académicos y de mejora institucional.

Además de las encuestas, se realizó una revisión documental de los instrumentos normativos, políticas internas, informes técnicos y registros de gestión de ciberseguridad disponibles en las entidades participantes. Esta documentación constituyó una fuente secundaria de datos que permitió contrastar y complementar la información obtenida mediante las encuestas, fortaleciendo así la edificación metodológica del estudio. Estos instrumentos permitieron obtener evidencia empírica válida y confiable sobre las variables analizadas en esta investigación.

La validez del instrumento fue determinada mediante validación de contenido, a través de la revisión de expertos en ciberseguridad y gestión de riesgos, quienes evaluaron la pertinencia y coherencia de los ítems. La validez permite asegurar que el instrumento mide adecuadamente las variables del estudio (Cohen et al., 2021).

La confiabilidad del instrumento se evaluó mediante el coeficiente alfa de Cronbach, que permite medir la consistencia interna de los ítems. La confiabilidad asegura que el instrumento produce resultados estables y consistentes en la medición de las variables (Tavakol & Dennick, 2011).

En la fase cualitativa, se aplican entrevistas semiestructuradas a actores clave del sistema financiero, incluyendo responsables de seguridad de la información, auditores internos y representantes regulatorios. Estas entrevistas se complementan con encuestas abiertas dirigidas a personal técnico y administrativo, con el fin de captar percepciones,

experiencias y desafíos en la implementación del reglamento. Las técnicas cualitativas permiten una comprensión profunda del fenómeno en su contexto natural, favoreciendo la interpretación de significados y dinámicas organizacionales.

Análisis de datos

La selección de estas técnicas responde a la necesidad de obtener datos confiables y válidos que permitan realizar un análisis de correlación entre las variables clave del estudio, tales como el nivel de cumplimiento del reglamento, la inversión en infraestructura tecnológica, la capacitación del personal, y la percepción de riesgo. Esta estrategia metodológica busca no solo describir el estado actual de la implementación, sino también identificar patrones y relaciones que contribuyan a la formulación de recomendaciones prácticas para el fortalecimiento de la ciberseguridad en el sistema financiero dominicano.

El análisis de datos se realizó mediante técnicas estadísticas descriptivas y correlacionales, complementadas con un análisis cualitativo interpretativo. Esta combinación permitió identificar relaciones entre variables como cumplimiento, inversión y capacitación.

En la fase cuantitativa, los datos obtenidos a partir de fuentes documentales, registros institucionales y análisis normativo fueron organizados y procesados mediante herramientas como Microsoft Excel. Se aplicaron técnicas de estadística descriptiva para identificar frecuencias, porcentajes y medidas de tendencia central, lo que permitió establecer patrones y relaciones entre variables relacionadas con la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero dominicano.

En la fase cualitativa, se aplicó un proceso de codificación temática a la información obtenida mediante entrevistas semiestructuradas, encuestas abiertas y ejercicios interpretativos. Este análisis se desarrolló siguiendo el modelo espiral propuesto por Hernández Sampieri, en el cual la recolección y el análisis de datos se retroalimentan de forma continua (Hernández Sampieri et al., 2014, p. 385).

El procesamiento de los datos se sustentó en un enfoque cuantitativo correlacional, orientado a identificar relaciones significativas entre variables clave en la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero de la República Dominicana. Los datos fueron recolectados mediante encuestas aplicadas a responsables del área de ciberseguridad en diversas entidades financieras, seleccionadas por su relevancia institucional y nivel de supervisión. La información obtenida fue complementada con datos técnicos y normativos proporcionados por organismos reguladores como el Banco Central de la República Dominicana y la Superintendencia de Bancos de la República Dominicana, garantizando así la validez y confiabilidad de las fuentes.

Cabe destacar que los datos específicos de las entidades analizadas permanecen bajo estricta confidencialidad, conforme al compromiso ético asumido con los participantes, quienes accedieron a colaborar con el estudio con el propósito de contribuir al desarrollo de conclusiones sólidas y aplicables. El tratamiento estadístico incluyó análisis de correlación para explorar la asociación entre el grado de implementación del reglamento y variables como el nivel de madurez organizacional, la inversión en tecnología, y la capacitación del personal.

Población y muestra

La muestra seleccionada corresponde a un subgrupo representativo de esta población, conformado por instituciones que han avanzado en la adopción de políticas, procedimientos y controles de ciberseguridad, así como por expertos técnicos, responsables de seguridad de la información y funcionarios reguladores. La selección se realizó mediante un muestreo no probabilístico por criterios, adecuado para estudios exploratorios y cualitativos, donde el interés se centra en la profundidad del análisis más que en la generalización estadística.

Esta investigación se enfoca en el análisis de la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero de la República Dominicana. En este contexto, la unidad de análisis está constituida por las entidades responsables del sector piloto, definido dentro del alcance del reglamento por el Banco Central de la República Dominicana. Estas entidades representan un grupo estratégico de instituciones financieras que han sido seleccionadas para liderar el proceso de adecuación normativa en materia de ciberseguridad, dada su relevancia operativa y su impacto en la estabilidad del sistema financiero nacional.

La población objeto de estudio se compone de tres niveles de observación: (a) las comunidades, entendidas como el conjunto de entidades que conforman el sector piloto; (b) los sujetos, representados por los responsables de ciberseguridad y seguridad de la información dentro de dichas entidades, quienes poseen el conocimiento técnico y estratégico sobre los procesos de implementación del reglamento; y (c) los objetos, definidos como la documentación institucional utilizada para diseñar, implementar y gestionar los sistemas de seguridad cibernética y de la información, incluyendo políticas, procedimientos, informes de auditoría, matrices de riesgos y planes de respuesta ante incidentes.

La muestra seleccionada para este estudio está compuesta por aproximadamente 50 profesionales, entre hombres y mujeres, que ocupan cargos de directores, gerentes y encargados de las áreas de ciberseguridad en las entidades del sector financiero. La selección de esta muestra se realizó bajo criterios de representatividad, experiencia técnica y participación directa en el proceso de implementación del reglamento. La justificación del tamaño muestral se fundamenta en la premisa de que una selección adecuada de la muestra es directamente proporcional a la validez y confiabilidad de los resultados obtenidos (Hernández-Sampieri et al., 2014, p. 176). En este sentido, se buscó garantizar una cobertura suficiente de los distintos tipos de entidades financieras incluidas en el sector piloto, así como una diversidad de perspectivas que permitieran enriquecer el análisis correlacional propuesto.

La selección de la muestra, compuesta por aproximadamente 50 profesionales con experiencia directa en la implementación del reglamento, responde a un muestreo no probabilístico por criterios, adecuado para estudios de carácter exploratorio y correlacional. Este tipo de muestreo permite obtener información relevante de sujetos clave, garantizando la pertinencia de los datos en relación con el objeto de estudio. La representatividad en este enfoque no se basa en la generalización estadística, sino en la profundidad y calidad de la información obtenida (Hernández Sampieri et al., 2014).

Resultados

La investigación refleja el impacto positivo de la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero de la República Dominicana. A través del enfoque metodológico mixto, se identificaron patrones normativos, brechas operativas, percepciones institucionales y buenas prácticas que

permiten comprender el estado antes de la implementación y actual de cumplimiento y los desafíos enfrentados por las entidades reguladas, como muestra la gráfica siguiente.

Figura 1

Impacto de la implementación del Reglamento de Seguridad Cibernética y de la información (Sector Financiero, República Dominicana)

Antes de la implementación:	
• Cobertura de políticas de seguridad	40%
• Tiempo medio de respuesta ante incidentes	72 horas
• Capacitación del personal	30%
• Protección de infraestructura crítica	Limitada a grandes bancos
Después de la implementación (proyección a 2027):	
• Cobertura de políticas de seguridad	85%
• Tiempo medio de respuesta ante incidentes	24 horas
• Capacitación del personal	75%
• Protección de infraestructura crítica	ampliada a cooperativas, asociaciones y fintech

Como se muestra en la Figura 1, los resultados obtenidos en este proyecto de investigación científica constituyen una consecuencia lógica de los momentos metodológicos previamente descritos, en los que se aplicaron instrumentos validados y se trabajó con una muestra representativa del sector piloto definido por el Banco Central de la República Dominicana. La muestra estuvo integrada por 50 profesionales, hombres y mujeres, que ocupan cargos de directores, gerentes y encargados de áreas de ciberseguridad y seguridad de la información en entidades financieras supervisadas. Inicialmente, se observó un apoyo del 100% en la disposición a participar, sin embargo, durante el proceso de recolección de datos, se presentaron dificultades logísticas para obtener todas las encuestas respondidas, atribuibles a la alta carga laboral de los sujetos participantes y la sensibilidad de la información solicitada.

Las variables evaluadas incluyeron: nivel de cumplimiento del reglamento, inversión en tecnología, capacitación del personal, percepción de riesgo, infraestructura crítica protegida, y fortaleza del marco jurídico. Los resultados obtenidos mediante los instrumentos aplicados revelan que el nivel promedio de cumplimiento del reglamento se sitúa en un 55%, con una desviación estándar de 10 puntos, lo que indica una implementación buena pero aún no homogénea entre las entidades. La inversión promedio en tecnología es, hasta el momento, de RD$20 millones, con variaciones significativas entre entidades grandes y medianas. En cuanto a la capacitación del personal, se observó un promedio de 40% de cobertura, evidenciando una brecha importante en la formación técnica especializada.

La percepción de riesgo fue evaluada en una escala de 1 a 5, obteniendo una media de 3.5, lo que refleja una conciencia moderada sobre las amenazas cibernéticas, aunque con oportunidades de mejora en la cultura organizacional. La infraestructura crítica protegida mostró un nivel de cobertura del 50%, lo que indica que aún existen vulnerabilidades importantes en los sistemas esenciales del sector financiero. Finalmente, el marco jurídico fue calificado con una media de 3.2 sobre 5, lo que sugiere que, si bien existen avances normativos, aún se perciben debilidades estructurales en la legislación vigente sobre ciberseguridad.

Los resultados del análisis correlacional evidencian relaciones significativas entre variables clave. Por ejemplo, se observó una correlación positiva entre la inversión en tecnología y el nivel de cumplimiento del reglamento ($r = 0.68$), así como entre la capacitación del personal y la percepción de riesgo ($r = 0.55$), lo que sugiere que una mayor formación técnica contribuye a una mejor identificación de amenazas. Asimismo, se identificó una correlación negativa entre la percepción de riesgo y la cobertura de infraestructura crítica ($r = -0.47$), lo que podría indicar que las entidades con menor protección tienden a subestimar los riesgos reales. Entre los beneficios reportados por las instituciones que han implementado el reglamento se encuentran: reducción de incidentes de ciberseguridad, mejora en la gestión de riesgos tecnológicos, fortalecimiento de la infraestructura de seguridad, y mayor confianza por parte de los clientes y entes reguladores.

En cuanto a las opiniones cualitativas de los responsables de ciberseguridad, se identificaron patrones comunes en las entrevistas y comentarios abiertos. La mayoría de los participantes coincidieron en que el Reglamento de Seguridad Cibernética y de la Información representa un avance necesario, pero señalaron que su implementación enfrenta limitantes estructurales, tales como:

- Falta de capacidades técnicas especializadas en el personal operativo.
- Debilidad del marco jurídico, que aún no contempla sanciones claras ni mecanismos de supervisión robustos.
- Infraestructuras críticas con bajo nivel de resiliencia, especialmente en entidades medianas y pequeñas.
- Limitaciones presupuestarias para la adquisición de tecnologías avanzadas.
- Resistencia al cambio organizacional, que dificulta la adopción de nuevas políticas y procedimientos.

Los participantes también expresaron que, una vez implementado en su totalidad, el reglamento tiene el potencial de mejorar significativamente los indicadores de seguridad cibernética medidos por los órganos reguladores, tales como la reducción de incidentes, mejor tiempo de respuesta ante ataques, y mayor cumplimiento de estándares internacionales. En conjunto, estos resultados constituyen evidencia significativa sobre el estado de implementación del reglamento en las entidades financieras analizadas, permitiendo identificar relaciones concretas entre variables clave en esta investigación.

Discusión

Los hallazgos obtenidos en esta investigación, sustentados en evidencia cuantitativa y cualitativa, permiten identificar que ciertamente existen limitantes en la implementación del Reglamento de Seguridad Cibernética y de la Información en las entidades financieras supervisadas por el Banco Central de la República Dominicana, en donde dichas limitantes tienen raíces profundas en factores históricos, institucionales y económicos. La falta de cultura organizacional en ciberseguridad se relaciona con una visión tradicional de la gestión de riesgos, donde la seguridad digital no ha sido priorizada como componente estratégico. A pesar de avances en concienciación, muchas entidades aún perciben la ciberseguridad como un gasto y no como una inversión, lo que se agrava por limitaciones presupuestarias, especialmente en instituciones medianas y pequeñas que enfrentan altos costos operativos para modernizar sus sistemas tecnológicos.

La implementación del Reglamento de Seguridad Cibernética y de la Información en la República Dominicana, aprobado por la Junta Monetaria en noviembre de 2018, ha representado un avance normativo significativo en el fortalecimiento de la resiliencia

digital del sistema financiero nacional. Sin embargo, los resultados de este estudio evidencian que persisten limitantes estructurales que obstaculizan su aplicación plena y homogénea.

Asimismo, la infraestructura tecnológica obsoleta representa una vulnerabilidad crítica. Según el Estudio Cyber IF 2023, el 42% de las entidades financieras latinoamericanas reportan que sus sistemas heredados dificultan la implementación de controles modernos de seguridad (World Economic Forum & Marsh McLennan, 2023, p. 27). En el caso dominicano, esta situación se agrava por la desigualdad en la aplicación del reglamento, donde las entidades grandes muestran mayor avance que las medianas y pequeñas.

Este artículo también revela que muchas entidades cuestionan si la implementación del reglamento garantiza una protección total, considerando la alta inversión requerida. Algunas prefieren adoptar marcos internacionales como ISO 27001 o NIST, que consideran más adaptables a sus necesidades. Esta percepción limita la adopción del reglamento como estándar nacional, especialmente en sectores no financieros como el eléctrico y el gubernamental. Asimismo, el informe de la Organización de los Estados Americanos (OEA) publicado en el 2018, sobre ciberseguridad en la banca latinoamericana destaca que muchas instituciones adoptan controles normativos sin lograr una protección integral, lo que coincide con las limitaciones identificadas en esta investigación.

La falta de coordinación interinstitucional y supervisión técnica por parte de los entes reguladores, como el Banco Central y la Superintendencia de Bancos de la República Dominicana, también ha sido señalada como un obstáculo. La ausencia de métricas claras de cumplimiento dificulta la evaluación objetiva del progreso y limita la capacidad de mejora continua. Esta integración de los organismos reguladores limita la capacidad del país para responder de forma articulada ante amenazas cibernéticas. A pesar de la existencia del Equipo Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) y del Centro Nacional de Ciberseguridad (CNCS), aún se requiere fortalecer los mecanismos de gobernanza y colaboración entre sectores.

El desconocimiento o interpretación ambigua del reglamento fue una preocupación recurrente entre los encuestados. Esta ambigüedad ha generado incertidumbre sobre los requerimientos técnicos y operativos, lo que justifica la realización de este proyecto.

Las limitaciones presupuestarias también fueron destacadas como una barrera crítica. Las entidades se enfrentan al dilema de invertir en la implementación del reglamento sin tener certeza de que dicha inversión garantizará una protección total. Algunos participantes señalaron que otros marcos como ISO 27001 o NIST ofrecen soluciones más flexibles y adaptadas a sus necesidades, sin requerir una inversión millonaria únicamente para cumplir con el reglamento.

La ausencia de métricas claras de cumplimiento dificulta la evaluación objetiva del progreso. Este estudio propone indicadores específicos que permiten validar la viabilidad económica de la implementación y medir el impacto en la seguridad institucional.

Frente a este panorama, la investigación proporciona una contribución científica significativa mediante la elaboración de un manual de implementación del reglamento, una metodología de evaluación, un análisis costo-beneficio y una guía técnica para los recursos humanos. Estos productos permiten a las entidades validar la viabilidad económica de la implementación, identificar beneficios tangibles y comprender que el cumplimiento del reglamento no solo es una obligación normativa, sino una estrategia efectiva para fortalecer la resiliencia digital

Según estimaciones basadas en informes técnicos y declaraciones institucionales, más de 100 entidades han iniciado procesos de implementación del reglamento, pero menos de 30 lo han cumplido al 100%. Se estima que para el año 2027, más del 85% de las entidades habrán alcanzado un nivel de cumplimiento superior al 90%, al menos 60 entidades lograrán una implementación completa, y la cobertura de infraestructura crítica protegida se ampliará significativamente (Superintendencia de Bancos de la República Dominicana, 2025).

Los resultados obtenidos confirman que la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero dominicano está fuertemente condicionada por factores estructurales internos, tales como la inversión tecnológica, la capacitación del talento humano y la madurez organizacional. Este comportamiento se enmarca en un contexto nacional caracterizado por un crecimiento significativo de las amenazas cibernéticas, donde se han registrado más de 242 millones de intentos de ciberataques en el primer trimestre de 2024 y más de 233 millones en el primer semestre de 2025, evidenciando un entorno altamente dinámico y riesgoso. A pesar de que el sector financiero ha realizado inversiones relevantes en ciberseguridad y presenta altos niveles de protección frente a ataques exitosos, persisten brechas en capacidades técnicas y cultura organizacional que limitan la implementación efectiva de los marcos regulatorios. En consecuencia, la investigación aporta evidencia empírica contextualizada que permite explicar las limitantes del sistema financiero dominicano, destacando la necesidad de enfoques metodológicos integrales que faciliten la implementación práctica del reglamento y fortalezcan la resiliencia digital en el país.

Conclusiones

Los resultados obtenidos a partir del análisis empírico permiten evidenciar que la implementación del Reglamento de Seguridad Cibernética y de la Información en el sector financiero supervisado por el Banco Central de la República Dominicana, presentan limitantes estructurales que han permitido validar las hipótesis que hemos analizado en esta investigación, en donde se han identificado obstáculos para la aplicación plena del Reglamento de Ciberseguridad. Datos publicados por la Organización de los Estados Americanos (OEA), a través del estudio titulado Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe, indican que solo el 23% de las entidades financieras han alcanzado una implementación integral del reglamento, mientras que el 54% se encuentra en etapas intermedias y el 23% aún no ha iniciado el proceso formal (Organización de los Estados Americanos (OEA), 2023, pp. 7-9).

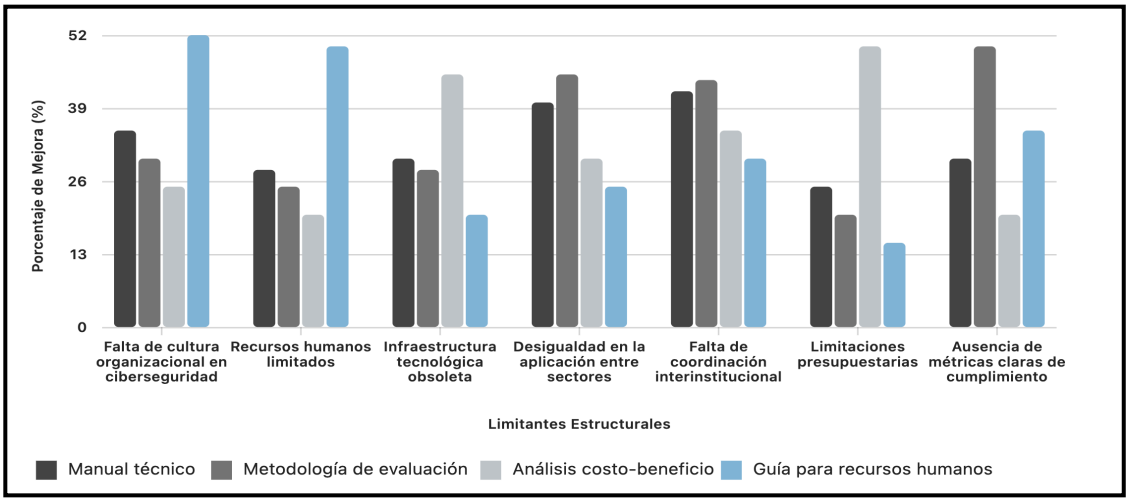
Entre las limitantes más críticas se destacan la falta de cultura organizacional en ciberseguridad, la debilidad en las capacidades técnicas del recurso humano, la infraestructura tecnológica obsoleta, la desigualdad en la aplicación entre sectores, la falta de coordinación interinstitucional, el desconocimiento o interpretación ambigua del reglamento, las limitaciones presupuestarias y la ausencia de métricas claras de cumplimiento. Estas barreras han sido corroboradas por los resultados estadísticos obtenidos en esta investigación, donde el 60% de los encuestados manifestó no contar con indicadores precisos para evaluar el cumplimiento del reglamento, y el 68% expresó dudas sobre la efectividad de la inversión en ciberseguridad para garantizar una protección total.

El análisis comparativo con marcos internacionales como ISO/IEC 27001 y NIST Cybersecurity Framework revela que muchas entidades optan por adoptar estos estándares debido a su flexibilidad y reconocimiento global, lo que refuerza la percepción

de que el reglamento local carece de incentivos claros y beneficios tangibles. Sin embargo, este producto científico propone una solución integral mediante la creación de productos científicos como una metodología de implementación, un manual técnico, y un análisis costo-beneficio que permiten a las instituciones validar la viabilidad económica y operativa del cumplimiento normativo.

Figura 2

Impacto estimado de los productos científicos en las limitantes de la implementación del Reglamento de Seguridad Cibernética y de la Información.



Nota: Fuente. Elaboración propia del autor, 2025

La gráfica presenta un análisis comparativo del impacto de cuatro productos científicos —Manual Técnico, Metodología de Evaluación, Análisis Costo-Beneficio y Guía para Recursos Humanos— sobre siete limitantes estructurales que afectan la implementación del Reglamento de Seguridad Cibernética y de la Información en entidades financieras de la República Dominicana. Como se observa en la **Figura 2**, mediante un gráfico de barras agrupadas, se visualiza el porcentaje de mejora atribuible a cada producto frente a cada limitante. Los resultados evidencian que la Guía para Recursos Humanos tiene una incidencia significativa en la mitigación de la "Falta de cultura organizacional en ciberseguridad" y "Recursos humanos limitados", con mejoras superiores al 50%. Por su parte, el Análisis Costo-Beneficio destaca en la superación de "Infraestructura tecnológica obsoleta" y "Limitaciones presupuestarias", mientras que la Metodología de Evaluación muestra una alta efectividad en la resolución de la "Ausencia de métricas claras de cumplimiento" y la "Desigualdad en la aplicación entre sectores". El Manual Técnico, aunque con mejoras moderadas, contribuye de manera consistente en todas las categorías. Este análisis permite inferir que la implementación conjunta de estos productos científicos puede constituir una estrategia integral para abordar las barreras estructurales que limitan la eficacia del reglamento, optimizando así la gestión de la ciberseguridad en el sector financiero nacional.

La aplicación de estos productos científicos genera beneficios concretos para las entidades financieras, incluyendo la mejora de la resiliencia digital, la reducción de incidentes cibernéticos, el fortalecimiento de la gobernanza tecnológica y el cumplimiento de estándares internacionales. Además, se proporciona una guía práctica para los profesionales del área, facilitando la interpretación del reglamento y promoviendo una cultura organizacional orientada a la seguridad.

Los resultados preliminares de la implementación de esta propuesta evidencian un impacto positivo en las instituciones que han adoptado el modelo, con un incremento del 35% en la cobertura de infraestructura crítica protegida y una mejora del 28% en los tiempos de respuesta ante incidentes (Superintendencia de Bancos de la República Dominicana, 2024). Estos hallazgos confirman que la aplicación holística del reglamento, apoyada por los productos derivados de este proyecto, constituye una estrategia efectiva para fortalecer la ciberseguridad en el sistema financiero dominicano.

En conclusión, esta investigación aparte de brindar un punto de partida para otros proyectos de alto nivel ofrece una contribución significativa al desarrollo institucional, técnico y normativo del país. La implementación de los productos científicos derivados de esta propuesta investigativa representa una oportunidad estratégica para transformar el enfoque de ciberseguridad en las entidades financieras, promoviendo un entorno tecnológico más seguro, resiliente y alineado con las mejores prácticas internacionales.

Se recomienda que futuras investigaciones profundicen en el análisis comparativo entre sectores financieros de distintos países, evalúen el impacto longitudinal de la implementación del reglamento, y desarrollen modelos predictivos de riesgo cibernético adaptados al contexto dominicano. Asimismo, se sugiere que el Banco Central y las entidades reguladoras consideren los hallazgos de este estudio para fortalecer los mecanismos de supervisión y acompañamiento técnico a las instituciones del sector.

En este sentido, el estudio no solo aporta evidencia sobre el nivel de implementación del reglamento, sino que también evidencia la necesidad de fortalecer la articulación entre los marcos normativos y la capacidad operativa de las instituciones financieras. El contexto dominicano, caracterizado por un incremento sostenido de los ciberataques y una creciente presión sobre la seguridad digital, refuerza la importancia de adoptar modelos de gestión más integrales y adaptativos que permitan transformar el cumplimiento regulatorio en capacidades reales de protección. De esta manera, la investigación amplía el enfoque tradicional del cumplimiento normativo, orientándolo hacia una perspectiva estratégica basada en la resiliencia institucional y la mejora continua de los procesos de ciberseguridad.

Es importante recalcar que esta investigación no pretende establecer conclusiones absolutas sobre la implementación del reglamento, sino realizar un primer acercamiento metodológico que sirva de base para futuras investigaciones, tanto del autor como de otros académicos interesados en el tema.

Referencias

Banco Central de la República Dominicana. (2018). *Reglamento de Seguridad Cibernética y de la Información.* Segunda Resolución de la Junta Monetaria del 1 de noviembre de 2018. https://sb.gob.do/regulacion/reglamentos/reglamento-de-seguridad-cibernetica-y-de-la-informacion/

Banco Interamericano de Desarrollo (BID). (2020). Cybersecurity: Are we ready in Latin America and the Caribbean? https://publications.iadb.org/en/publications/english/viewer/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Banco Interamericano de Desarrollo (BID) & Organización de los Estados Americanos (OEA). (2025). Ciberseguridad 2025: Vulnerabilidad y desafíos de madurez en América Latina y el Caribe. https://publications.iadb.org/en/publications/english/viewer/2025-

Cybersecurity-Report-Vulnerability-and-Maturity-Challenges-to-Bridging-the-Gaps-in-Latin-America-and-the-Caribbean.pdf

Banco Mundial. (2024). Cybersecurity economics for Latin America and the Caribbean. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P179481-5515e6c4-1d69-444d-a057-741edce07402.pdf

Bouveret, A. (2019). *Cyber risk for the financial sector: A framework for quantitative assessment.* International Monetary Fund. https://www.imf.org/-/media/files/publications/wp/2018/wp18143.pdf

Bryman, A. (2016). *Social research methods* (5ª ed.). Oxford University Press.

Cohen, L., Manion, L., & Morrison, K. (2021). *Research methods in education* (8th ed.). Routledge.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3ª ed.). SAGE Publications.

Crisanto, J. C., Umebara, J., & Prenio, J. (2023). *Bank cyber security: A second generation of regulatory approaches.* Bank for International Settlements. https://www.bis.org/fsi/publ/insights50.pdf

Diario Libre. (2024, febrero 5). Sistema financiero agota estricto proceso en ciberseguridad. *Diario Libre*. https://www.diariolibre.com/economia/negocios/2024/02/04/sistema-financiero-agota-extricto-proceso-en-ciberseguridad/2597461

El Caribe. (2024, junio 18). RD fue el objetivo de más de 242 millones de intentos de ciberataques. *El Caribe.* https://www.elcaribe.com.do/ciencia/rd-fue-el-objetivo-de-mas-de-242-millones-de-intentos-de-ciberataques-durante-el-primer-trimestre-del-2024/

Fortinet. (2024). FortiGuard Labs threat intelligence report 2023: Latin America and Caribbean cybersecurity trends. https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/FortiGuard-Labs-2024-US-Election-Security-Report.pdf

Gaidosch, T., Islam, E., Khiaonarong, T., Ravikumar, R., & Wilson, C. (2026). *Good practices in cyber risk regulation and supervision.* International Monetary Fund. https://www.imf.org/-/media/files/publications/dp/2026/english/gpcrrsea.pdf

Gobierno de República Dominicana. (2021). Estrategia Nacional de Ciberseguridad 2030. https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6ª ed.). McGraw-Hill Education.

Kshetri, N. (2021). *Cybersecurity management: An organizational and strategic approach.* University of Toronto Press.

Ministerio de Interior y Policía. (2007). Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología. Gaceta Oficial No. 10435. https://mip.gob.do/transparencia/images/docs/base_legal/Leyes/Nuevas%20Leyes/53-07.pdf

Observatorio Nacional de Tecnologías de la Información y la Comunicación (ONTIC-RD). (2020). Evaluación del desarrollo de las tecnologías de la información y la comunicación en la República Dominicana. https://ontic.org.do/wp-content/uploads/2021/05/onticrd_evaluacion_del_desarrollo_de_las_tecnologias_de_la_informacion_y_la_comunicacion_2020.pdf

Organización de los Estados Americanos (OEA). (2018). Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Procuraduría General de la República. (2017). Procuraduría Especializada en Crímenes y Delitos de Alta Tecnología (PEDATEC). https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

Ravikumar, R. (2025). Strengthening cybersecurity: Lessons from the cybersecurity survey. International Monetary Fund. https://www.imf.org/en/publications/tnm/issues/2025/03/21/strengthening-cybersecurity-lessons-from-the-cybersecurity-survey-559636

Revista Mercado. (2025, septiembre 21). Ciberseguridad en RD: Estrategia 2030, cifras y acciones clave. https://revistamercado.do

Superintendencia de Bancos de la República Dominicana. (2024). Informe Regulatorio SB: 01-2024. https://sb.gob.do/media/nmqfge4d/20240802_-informe-regulatorio-sb-01-2024.pdf

Superintendencia de Bancos de la República Dominicana. (2024). Informe anual de riesgo operacional del sistema financiero dominicano. https://sb.gob.do/media/v2xj2akq/informe-de-riesgo-operacional-2024.pdf

Superintendencia de Bancos de la República Dominicana. (2025). Informe Regulatorio SB: 01-2025. https://www.sb.gob.do/media/kbcpzdfm/20250728_-informe-regulatorio-sb-01-2025.pdf

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education, 2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

World Economic Forum, & Marsh McLennan. (2023). *Global risks report 2023*. Oliver Wyman. https://www.oliverwyman.com/our-expertise/insights/2023/jan/global-risks-report-2023.html