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

(2026) Project, Design and Management 8(1), 64-81. doi.org/10.35992/pdm.v8i1.4547

IMPLEMENTATION OF THE CYBERSECURITY AND INFORMATION SECURITY REGULATION IN FINANCIAL INSTITUTIONS SUPERVISED BY THE CENTRAL BANK OF THE DOMINICAN REPUBLIC

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

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

Manuscript information:

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

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.

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.

Introduction

Digital transformation, driven by technologies such as artificial intelligence, cloud computing, and the Internet of Things (IoT), has significantly increased the financial sector's exposure to complex and persistent cyber risks. In this context, recent scientific literature has addressed cybersecurity from a global perspective, highlighting its impact on financial stability and the need to strengthen regulatory frameworks. Studies by the International Monetary Fund show that cyber risks pose a growing systemic threat that requires not only regulation but also institutional capacity for its effective implementation (Gaidosch et al., 2026; Ravikumar, 2025). Similarly, research by the Bank for International Settlements points to a shift toward regulatory approaches focused on operational resilience, emphasizing the need for structured mechanisms for managing cyber risk in financial institutions (Crisanto et al., 2023). At the regional level, studies by the Inter-American Development Bank and the Organization of American States show that, although regulatory progress has been made in Latin America, significant gaps persist in technical capacity, organizational culture, and inter-institutional coordination, which limit the effective implementation of these regulations (IDB & OAS, 2025; World Bank, 2024). In the Dominican Republic, this process has been driven by public policies such as the "República Digital" program, the expansion of fiber-optic infrastructure, and the development of technology free zones, which have led to greater connectivity, innovation, and access to digital services (National Observatory of Information and Communication Technologies (ONTIC-RD), 2020).

In recent years, the Dominican Republic has seen a significant increase in its exposure to cyber threats, in line with global trends. According to data from FortiGuard Labs, the country recorded approximately 5 billion cyberattack attempts in 2022, a figure that fell to about 1 billion in 2023, reflecting a shift toward more sophisticated and targeted attacks, in which effectiveness is prioritized over volume (Fortinet, 2024). Similarly, in the financial sector, the Superintendency of Banks reported losses exceeding RD$1,677 million due to fraud, particularly related to the use of cards and digital channels during 2023 (Superintendency of Banks of the Dominican Republic, 2024). These data highlight not only the magnitude of cyber risk in the Dominican context, but also the growing complexity of the threats and their direct impact on the stability of the financial system, underscoring the need for comprehensive approaches that will strengthen institutional resilience in the face of these challenges.

In recent scientific literature, various studies have analyzed the implementation of cybersecurity regulations in the financial sector. Kshetri (2021) notes that the adoption of regulatory frameworks strengthens institutional resilience in the face of digital threats, although their effectiveness depends on organizational and technological factors. Similarly, Bouveret (2019), of the International Monetary Fund, argues that cybersecurity regulations are essential for mitigating systemic risks, but their implementation faces significant challenges, especially in emerging economies. Technical, organizational, and regulatory complexity requires methodologies that enable regulatory requirements to be translated into concrete and measurable actions. This is why it is so important to develop the methodologies presented in this study, since the absence of such approaches limits regulatory compliance and effective risk management. Therefore, the development of implementation methodologies is key to strengthening the effectiveness of security programs in the financial sector of the Dominican Republic.

In Latin America, studies by the Organization of American States (OAS, 2018) and the Inter-American Development Bank (IDB, 2020) show that financial institutions exhibit varying levels of cybersecurity maturity, with notable weaknesses in workforce

training, organizational culture, and the resilience of critical infrastructure. These studies agree that regulatory implementation alone does not guarantee effective protection.

In the Dominican Republic, efforts to create a safer cyberspace date back to the enactment of Law No. 53-07 on High-Tech Crimes and Offenses, published on April 23, 2007 (Ministry of the Interior and Police, 2007). This legislation marked a milestone by criminalizing cybercrimes and establishing mechanisms for national and international cooperation to prosecute them.

In the regulatory sphere, the Monetary Board of the Central Bank approved the Cybersecurity and Information Security Regulations through Second Resolution of November 1, 2018, establishing mandatory guidelines for financial institutions regarding technological protection, risk management, and digital security governance (Central Bank of the Dominican Republic, 2018). In addition, specialized agencies have been created, such as the National Police's Department for the Investigation of High-Tech Crimes and Offenses (DICAT) and the Specialized Prosecutor's Office for High-Tech Crimes and Offenses (PEDATEC), which are responsible for the prevention, investigation, and prosecution of cybercrimes, in coordination with the Public Prosecutor's Office and international organizations (Office of the Attorney General of the Republic, 2017). Although significant regulatory progress has been made with the enactment of the Cybersecurity and Information Security Regulations by the Central Bank of the Dominican Republic in 2018, empirical evidence regarding their effective implementation in financial institutions remains limited.

Despite the growing body of literature on cybersecurity and information security, as well as cybersecurity and regulations in financial institutions, there is a significant gap in empirical studies that incorporate a mixed-methods approach to analyze the actual conditions of regulatory implementation in specific contexts, such as the Dominican financial system. Most research has focused on regulatory or technical approaches, without comprehensively addressing the relationships among organizational, technological, and regulatory variables.

Consistent with this limitation, a review of the scientific and technical literature—both at the national and regional levels—reveals a limited availability of empirical studies that specifically address the implementation of methodologies and tools such as those proposed in this research. In this regard, this study offers a novel approach that contributes to the advancement of knowledge in the field of cybersecurity as it applies to the financial sector. The originality of this study lies in its use of an applied and empirical methodological approach to analyze the implementation of the regulations in the Dominican financial system from a comprehensive perspective not evident in previous studies.

This article is part of that line of applied research, as is the present study, which proposes a methodology adapted to the Dominican context. It aims to ensure that organizations implementing the Cybersecurity and Information Security Program comply with regulations, which require a robust technical and organizational response. The methodological proposal is based on a mixed-methods approach, which will allow us to compare our findings with those of previous research and provide evidence regarding the feasibility of applying project management models to the implementation of cybersecurity and information security programs in the financial sector of the Dominican Republic.

The results of this study show that, while there is a robust regulatory framework promoted by the Central Bank of the Dominican Republic, its proper implementation poses significant challenges for most financial institutions, especially those with technical,

budgetary, or specialized personnel constraints. Similarly, it was found that formal or full compliance with cybersecurity regulations does not always guarantee effective protection against evolving day-to-day threats or advanced threats. This raises—among other issues that will be addressed in the course of this study—the need to discuss institutional evaluation and monitoring mechanisms, as well as the Dominican Republic's laws and regulations on cybersecurity and information security.

This study aims to rigorously analyze the conditions that hinder the effective implementation of the regulation, from a critical and multidimensional perspective. To this end, general hypotheses have been formulated to guide the research. These are:

1. The lack of specialized technical skills among cybersecurity and information security personnel significantly limits the effectiveness of information security policy implementation.
2. The lack of a robust legal framework, with clear penalties and effective oversight mechanisms, reduces the ability of financial sector institutions to comply with regulations.
3. The low level of resilience in critical infrastructure, especially among small and medium-sized organizations, increases vulnerability to cyber incidents.
4. Budget constraints hinder the adoption of advanced technologies, negatively affecting the maturity of an organization's cybersecurity.
5. Resistance to organizational change constitutes a structural barrier to the effective implementation of new information security policies and procedures.

These general hypotheses are broken down into a set of specific hypotheses, which will be empirically validated using a mixed-methods design:

- H1: Organizations that invest the least in technical training have the widest gaps in cybersecurity compliance.
- H2: The lack of clear legal penalties is linked to lower adoption rates of international security standards.
- H3: Organizations with less resilient infrastructure report a higher frequency of security incidents.
- H4: Budgetary resources are positively correlated with the level of technology adoption in information security.
- H5: Resistance to organizational change is negatively associated with the effectiveness of digital transformation and security processes.

The formulation of hypotheses in this study addresses a methodological need to precisely identify the critical variables that affect the effective implementation of the Cybersecurity and Information Security Regulations in the Dominican financial system. These hypotheses not only serve an explanatory function but also form the structural backbone of the research design, as they enable the construction of an analytical model that integrates technical, regulatory, organizational, and budgetary factors. Overall, this approach allows us to move beyond a mere description of the phenomenon and toward a deep understanding and evidence-based strategic intervention.

In this regard, this research not only seeks to validate the proposed hypotheses, but also aims to produce scientific outputs of high practical value that contribute to strengthening the digital resilience of the Dominican financial system. It is projected that by 2027, more than 85% of entities will have achieved a compliance level exceeding 90%, and at least 60 institutions will have fully implemented the requirements, significantly expanding the coverage of protected critical infrastructure (Superintendency of Banks of the Dominican Republic, 2025).

The document is organized into chapters that address the theoretical framework, methodology, analysis of results, critical discussion, and conclusions, supplemented by technical appendices that detail the outputs of the research. This work is intended to be a substantial contribution to the development of public policies, the design of more effective regulatory frameworks, and the consolidation of a culture of sustainable digital security, both nationally and internationally.

Method

Methodological Approach

This study is based on a mixed-methods approach, which combines quantitative and qualitative techniques in order to obtain a comprehensive view of the phenomenon under analysis. This approach allows for a simultaneous focus on the objective measurement of variables and the contextual interpretation of organizational processes, facilitating a more comprehensive understanding of the implementation of the Cybersecurity and Information Security Regulations in the Dominican financial sector. The integration of these two approaches addresses the need to analyze not only the level of regulatory compliance but also the structural factors that influence that process.

The quantitative approach focuses on the collection and analysis of measurable data related to key variables such as regulatory compliance, investment in technology, and employee training, enabling the identification of patterns and relationships through statistical techniques. For its part, the qualitative approach allows for a deeper exploration of the perceptions, experiences, and organizational dynamics of the stakeholders involved, providing a contextual understanding of the phenomenon that cannot be captured solely through numerical data. This methodological complementarity strengthens the study's explanatory power.

The adoption of a mixed-methods approach is supported by the methodological literature, which states that combining quantitative and qualitative data allows for greater validity and depth in research by integrating different types of evidence into the analysis of the problem (Creswell & Plano Clark, 2018). Furthermore, this approach facilitates the triangulation of information—defined as the use of multiple sources and methods to corroborate findings—which helps improve the credibility and consistency of the results (Hernández Sampieri et al., 2014). In this regard, the methodological approach adopted makes it possible not only to describe the status of the regulation's implementation but also to explain the relationships among the variables that influence its effectiveness in the Dominican context.

Research Design

The study employs a non-experimental design with a cross-sectional and descriptive approach, structured in two sequential phases. In the first phase, which is quantitative in nature, methodologies are applied that allow for the collection of data at a single point in time, without manipulating variables, with the aim of identifying patterns, relationships, and regulatory and technical background information regarding the implementation of the Cybersecurity and Information Security Regulation in the Dominican financial sector. Quantitative methodologies are essential in scientific research aimed at knowledge transfer, as they provide accurate and reliable data. According to Alan Bryman, the use of statistical methods in social research facilitates the analysis of large volumes of data, the identification of patterns, and the formulation of relationships

between variables, which contributes to the robustness of empirical findings (Bryman, 2016, pp. 147–148).

The second phase, which is qualitative in nature, is carried out using a descriptive design based on case studies selected according to criteria of institutional relevance and level of cybersecurity maturity. This phase allows for a deeper exploration of the experiences of the stakeholders involved through semi-structured interviews, open-ended surveys, and interpretive exercises, which provide a contextualized understanding of the phenomenon. Qualitative research allows us to capture experiences in their natural context, facilitating a deep and detailed understanding of the phenomena under study. After consulting various sources, it was concluded that this approach is essential for exploring meanings, interpretations, and social dynamics that cannot be captured using quantitative methods, making it a valuable tool for exploratory and descriptive studies.

Phases of the Study

This research is structured as a two-phase sequential model, with the aim of addressing the phenomenon of the implementation of the Cybersecurity and Information Security Regulation from a comprehensive perspective. These phases are methodologically structured to ensure consistency among the objectives, the mixed-methods approach adopted, and the data collection and analysis techniques.

The first phase involves a quantitative approach, carried out through non-experimental research using a cross-sectional design. This type of research allows researchers to observe phenomena in their natural context without manipulating variables, and to collect data at a single point in time (Hernández Sampieri et al., 2014, p. 151). At this stage, exploratory and documentary studies are conducted to identify patterns, relationships, and regulatory and technical background information regarding the implementation of the regulations in the Dominican financial sector. In addition, statistical methods are used to analyze large amounts of data and establish relationships between variables, which is essential in research aimed at knowledge transfer (Bryman, 2016, pp. 149–150).

The second phase is conducted using a qualitative approach, through descriptive research based on case studies. This methodology provides a deep and detailed understanding of the phenomena under study, capturing the experiences and perceptions of the participants in their natural context. Techniques such as semi-structured interviews, open-ended surveys, and interpretive exercises are used, providing empirical evidence regarding the applicability of the proposed model. This phase aims to establish the rationale behind this research and generate contextualized knowledge that will serve as a foundation for future research.

Both phases complement each other in a sequential design, strengthening the study's internal validity and ensuring that the methods used adequately address the research questions posed. Although this research does not aim to draw definitive conclusions about the phenomenon under study, it does seek to provide a rigorous initial analysis that contributes to the academic and practical development of the field of financial cybersecurity.

Data Collection Method

This study consists of two methodological phases, each employing specific data collection techniques tailored to the study's objectives. In the quantitative phase, techniques for document collection and analysis of institutional records are used to identify regulatory patterns, levels of compliance, and variables related to the implementation of the Cybersecurity and Information Security Regulations in the

Dominican financial sector. These secondary sources provide objective and verifiable data, facilitating statistical analysis and comparisons between organizations.

The surveys were designed to gather relevant information on the extent to which the regulations have been implemented, the challenges faced, the strategies adopted, and institutional perceptions of their effectiveness. The primary instrument used was a structured questionnaire consisting of Likert-scale items, designed to measure key variables associated with the implementation of the Cybersecurity and Information Security Regulations. They were administered directly and confidentially, ensuring the anonymity of the participants and the protection of the sensitive data shared. This measure was essential to encourage the voluntary and honest participation of the respondents, who agreed to participate on the understanding that the results would be used exclusively for academic and institutional improvement purposes.

In addition to the surveys, a literature review was conducted of the regulatory instruments, internal policies, technical reports, and cybersecurity management records available at the participating entities. This documentation served as a secondary source of data that made it possible to verify and supplement the information obtained through the surveys, thereby strengthening the methodological framework of the study. These instruments made it possible to obtain valid and reliable empirical evidence regarding the variables analyzed in this study.

The validity of the instrument was determined through content validation, involving a review by experts in cybersecurity and risk management, who assessed the relevance and consistency of the items. Validity ensures that the instrument accurately measures the study variables (Cohen et al., 2021).

The reliability of the instrument was assessed using Cronbach's alpha, which measures the internal consistency of the items. Reliability ensures that the instrument produces stable and consistent results when measuring variables (Tavakol & Dennick, 2011).

During the qualitative phase, semi-structured interviews are conducted with key stakeholders in the financial system, including information security officers, internal auditors, and regulatory representatives. These interviews are supplemented by open-ended surveys of technical and administrative staff, with the aim of gathering insights, experiences, and challenges related to the implementation of the regulations. Qualitative techniques provide a deep understanding of the phenomenon in its natural context, facilitating the interpretation of meanings and organizational dynamics.

Data Analysis

These techniques were selected to address the need to obtain reliable and valid data that will enable a correlation analysis between the study's key variables, such as the level of regulatory compliance, investment in technological infrastructure, staff training, and risk perception. This methodological strategy aims not only to describe the current status of implementation, but also to identify patterns and relationships that will help inform the development of practical recommendations for strengthening cybersecurity in the Dominican financial system.

Data analysis was conducted using descriptive and correlational statistical techniques, supplemented by interpretive qualitative analysis. This combination made it possible to identify relationships between variables such as compliance, investment, and training.

In the quantitative phase, the data obtained from documentary sources, institutional records, and regulatory analysis were organized and processed using tools

such as Microsoft Excel. Descriptive statistical techniques were applied to identify frequencies, percentages, and measures of central tendency, which made it possible to establish patterns and relationships among variables related to the implementation of the Cybersecurity and Information Security Regulations in the Dominican financial sector.

In the qualitative phase, a thematic coding process was applied to the information obtained through semistructured interviews, open-ended surveys, and interpretive exercises. This analysis was conducted using the spiral model proposed by Hernández Sampieri, in which data collection and analysis provide continuous feedback to one another (Hernández Sampieri et al., 2014, p. 385).

Data analysis was based on a quantitative correlational approach aimed at identifying significant relationships between key variables in the implementation of the Cybersecurity and Information Security Regulations in the financial sector of the Dominican Republic. The data were collected through surveys administered to cybersecurity managers at various financial institutions, which were selected based on their institutional significance and level of oversight. The information obtained was supplemented with technical and regulatory data provided by regulatory agencies such as the Central Bank of the Dominican Republic and the Superintendency of Banks of the Dominican Republic, thereby ensuring the validity and reliability of the sources.

It should be noted that the specific data regarding the organizations analyzed remain strictly confidential, in accordance with the ethical commitment made to the participants, who agreed to collaborate on the study in order to help draw sound and applicable conclusions. The statistical analysis included correlation analyses to explore the association between the degree of implementation of the regulations and variables such as organizational maturity, investment in technology, and staff training.

Population and Sample

The selected sample represents a representative subgroup of this population, consisting of institutions that have made progress in adopting cybersecurity policies, procedures, and controls, as well as technical experts, information security officers, and regulatory officials. The selection was made using non-probabilistic criterion-based sampling, which is suitable for exploratory and qualitative studies where the focus is on the depth of the analysis rather than on statistical generalizability.

This research focuses on analyzing the implementation of the Cybersecurity and Information Security Regulations in the financial sector of the Dominican Republic. In this context, the unit of analysis consists of the entities responsible for the pilot sector, as defined within the scope of the regulation by the Central Bank of the Dominican Republic. These entities represent a strategic group of financial institutions that have been selected to lead the cybersecurity regulatory compliance process, given their operational significance and their impact on the stability of the national financial system.

The study population consists of three levels of observation: (a) communities, defined as the set of entities that make up the pilot sector; (b) stakeholders, represented by those responsible for cybersecurity and information security within those entities, who possess the technical and strategic knowledge regarding the processes for implementing the regulation; and (c) the objects, defined as the institutional documentation used to design, implement, and manage cybersecurity and information security systems, including policies, procedures, audit reports, risk matrices, and incident response plans.

The sample selected for this study consists of approximately 50 professionals—both men and women—who hold positions as directors, managers, and supervisors in the cybersecurity departments of financial sector institutions. This sample was selected

based on criteria of representativeness, technical expertise, and direct participation in the process of implementing the regulations. The rationale for sample size is based on the premise that an appropriate sample selection is directly proportional to the validity and reliability of the results obtained (Hernández-Sampieri et al., 2014, p. 176). In this regard, the aim was to ensure sufficient coverage of the various types of financial institutions included in the pilot sector, as well as a diversity of perspectives that would enrich the proposed correlational analysis.

The sample, consisting of approximately 50 professionals with direct experience in implementing the regulation, was selected using non-probabilistic criterion sampling, which is appropriate for exploratory and correlational studies. This type of sampling makes it possible to obtain relevant information from key subjects, ensuring that the data is relevant to the subject of the study. In this approach, representativeness is not based on statistical generalization, but rather on the depth and quality of the information obtained (Hernández Sampieri et al., 2014).

Results

The study highlights the positive impact of the implementation of the Cybersecurity and Information Security Regulations in the financial sector of the Dominican Republic. Using a mixed-methods approach, we identified regulatory patterns, operational gaps, institutional perceptions, and best practices that provide insight into the pre-implementation and current status of compliance, as well as the challenges faced by regulated entities, as shown in the following chart.

Figure 1

Impact of the Implementation of the Cybersecurity and Information Security Regulations (Financial Sector, Dominican Republic)

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

As shown in Figure 1, the results obtained in this scientific research project are a logical consequence of the methodological steps described above, in which validated instruments were applied and a representative sample of the pilot sector—as defined by the Central Bank of the Dominican Republic—was used. The sample consisted of 50 professionals—both men and women—who hold positions as directors, managers, and department heads in the areas of cybersecurity and information security at supervised financial institutions. Initially, 100% of participants expressed a willingness to

participate; however, during the data collection process, logistical difficulties arose in obtaining all completed surveys, due to the participants' heavy workloads and the sensitive nature of the information requested.

The variables assessed included: level of regulatory compliance, investment in technology, staff training, perception of risk, protected critical infrastructure, and strength of the legal framework. The results obtained through the tools used reveal that the average level of compliance with the regulations stands at 55%, with a standard deviation of 10 points, indicating good implementation but one that is not yet uniform across all entities. Average investment in technology so far stands at RD$20 million, with significant variations between large and medium-sized companies. With regard to staff training, an average coverage rate of 40% was observed, indicating a significant gap in specialized technical training.

Risk perception was assessed on a scale of 1 to 5, yielding an average score of 3.5, which reflects a moderate level of awareness of cyber threats, although there is room for improvement in the organizational culture. Protected critical infrastructure showed a coverage level of 50%, indicating that there are still significant vulnerabilities in the financial sector's essential systems. Finally, the legal framework received an average score of 3.2 out of 5, suggesting that, while there has been progress in the regulatory sphere, structural weaknesses in current cybersecurity legislation are still evident.

The results of the correlational analysis show significant relationships between key variables. For example, a positive correlation was observed between investment in technology and the level of regulatory compliance ($r = 0.68$), as well as between staff training and perceived risk ($r = 0.55$), suggesting that greater technical training contributes to better identification of threats. Furthermore, a negative correlation was identified between risk perception and critical infrastructure coverage ($r = -0.47$), which could indicate that entities with less protection tend to underestimate the actual risks. Among the benefits reported by institutions that have implemented the regulation are: a reduction in cybersecurity incidents, improved technology risk management, a stronger security infrastructure, and greater trust from customers and regulatory agencies.

With regard to the qualitative feedback from cybersecurity professionals, common patterns were identified in the interviews and open-ended comments. Most participants agreed that the Cybersecurity and Information Security Regulations represent a necessary step forward, but they noted that their implementation faces structural constraints, such as:

- Lack of specialized technical skills among operational staff.
- A weak legal framework that does not yet provide for clear penalties or robust oversight mechanisms.
- Critical infrastructure with low resilience, particularly in small and medium-sized organizations.
- Budget constraints on the acquisition of advanced technologies.
- Resistance to organizational change, which hinders the adoption of new policies and procedures.

Participants also noted that, once fully implemented, the regulations have the potential to significantly improve the cybersecurity indicators measured by regulatory bodies, such as a reduction in incidents, faster response times to attacks, and greater compliance with international standards. Taken together, these results provide significant evidence regarding the status of the regulation's implementation at the financial institutions analyzed, making it possible to identify specific relationships between key variables in this study.

Discussion

The findings of this study, supported by quantitative and qualitative evidence, reveal that there are indeed limitations in the implementation of the Cybersecurity and Information Security Regulations at financial institutions supervised by the Central Bank of the Dominican Republic, where these limitations are deeply rooted in historical, institutional, and economic factors. The lack of an organizational culture of cybersecurity is linked to a traditional view of risk management, in which digital security has not been prioritized as a strategic component. Despite progress in raising awareness, many organizations still view cybersecurity as an expense rather than an investment, a situation exacerbated by budget constraints, especially in small and medium-sized institutions that face high operating costs when modernizing their technology systems.

The implementation of the Cybersecurity and Information Security Regulations in the Dominican Republic, approved by the Monetary Board in November 2018, has represented a significant regulatory step forward in strengthening the digital resilience of the national financial system. However, the results of this study show that structural limitations persist that hinder its full and uniform implementation.

Furthermore, outdated technological infrastructure poses a critical vulnerability. According to the 2023 Cyber IF Study, 42% of Latin American financial institutions report that their legacy systems hinder the implementation of modern security controls (World Economic Forum & Marsh McLennan, 2023, p. 27). In the Dominican Republic, this situation is exacerbated by unequal enforcement of the regulations, with large entities showing greater progress than medium and small ones.

This article also reveals that many organizations question whether the implementation of the regulation guarantees full protection, given the high investment required. Some prefer to adopt international standards such as ISO 27001 or NIST, which they consider more adaptable to their needs. This perception limits the adoption of the regulation as a national standard, especially in non-financial sectors such as the electric power and government sectors. Similarly, the 2018 report by the Organization of American States (OAS) on cybersecurity in the Latin American banking sector highlights that many institutions adopt regulatory controls without achieving comprehensive protection, which is consistent with the limitations identified in this study.

The lack of interagency coordination and technical oversight by regulatory bodies, such as the Central Bank and the Superintendency of Banks of the Dominican Republic, has also been cited as an obstacle. The lack of clear compliance metrics makes it difficult to objectively assess progress and limits the ability to continuously improve. This integration of regulatory agencies limits the country's ability to respond in a coordinated manner to cyber threats. Despite the existence of the Dominican Republic's National Computer Security Incident Response Team (CSIRT-RD) and the National Cybersecurity Center (CNCS), there is still a need to strengthen governance mechanisms and cross-sector collaboration.

A lack of knowledge about or ambiguous interpretation of the regulations was a recurring concern among respondents. This ambiguity has led to uncertainty regarding the technical and operational requirements, which justifies the implementation of this project.

Budgetary constraints were also highlighted as a critical barrier. Organizations face the dilemma of investing in the implementation of the regulation without any certainty that such an investment will guarantee full protection. Some participants

pointed out that other frameworks, such as ISO 27001 or NIST, offer more flexible solutions tailored to their needs, without requiring a massive investment just to comply with the regulation.

The lack of clear compliance metrics makes it difficult to objectively assess progress. This study proposes specific indicators that make it possible to assess the economic feasibility of implementation and measure the impact on institutional security.

Given this situation, the research makes a significant scientific contribution by developing a manual for implementing the regulations, an evaluation methodology, a cost-benefit analysis, and technical guidelines for human resources. These products enable organizations to assess the economic feasibility of implementation, identify tangible benefits, and understand that compliance with the regulation is not only a legal obligation but also an effective strategy for strengthening digital resilience

According to estimates based on technical reports and institutional statements, more than 100 entities have begun the process of implementing the regulation, but fewer than 30 have fully complied with it. It is estimated that by 2027, more than 85% of institutions will have achieved a compliance level exceeding 90%, at least 60 institutions will have fully implemented the requirements, and the coverage of protected critical infrastructure will expand significantly (Superintendency of Banks of the Dominican Republic, 2025).

The results confirm that the implementation of the Cybersecurity and Information Security Regulations in the Dominican financial sector is heavily influenced by internal structural factors, such as investment in technology, workforce training, and organizational maturity. This trend is part of a national context characterized by a significant increase in cyber threats, with more than 242 million attempted cyberattacks recorded in the first quarter of 2024 and more than 233 million in the first half of 2025, highlighting a highly dynamic and risky environment. Although the financial sector has made significant investments in cybersecurity and has high levels of protection against successful attacks, gaps in technical capabilities and organizational culture persist, limiting the effective implementation of regulatory frameworks. Consequently, the research provides contextualized empirical evidence that helps explain the limitations of the Dominican financial system, highlighting the need for comprehensive methodological approaches that facilitate the practical implementation of regulations and strengthen the country's digital resilience.

Conclusions

The results obtained from the empirical analysis show that the implementation of the Cybersecurity and Information Security Regulations in the financial sector supervised by the Central Bank of the Dominican Republic has structural limitations that have allowed us to validate the hypotheses analyzed in this study, in which obstacles to the full implementation of the Cybersecurity Regulations have been identified. Data published by the Organization of American States (OAS) in a study titled "The State of Cybersecurity in the Banking Sector in Latin America and the Caribbean" indicate that only 23% of financial institutions have fully implemented the regulations, while 54% are in intermediate stages and 23% have not yet begun the formal process (Organization of American States (OAS), 2023, pp. 7–9).

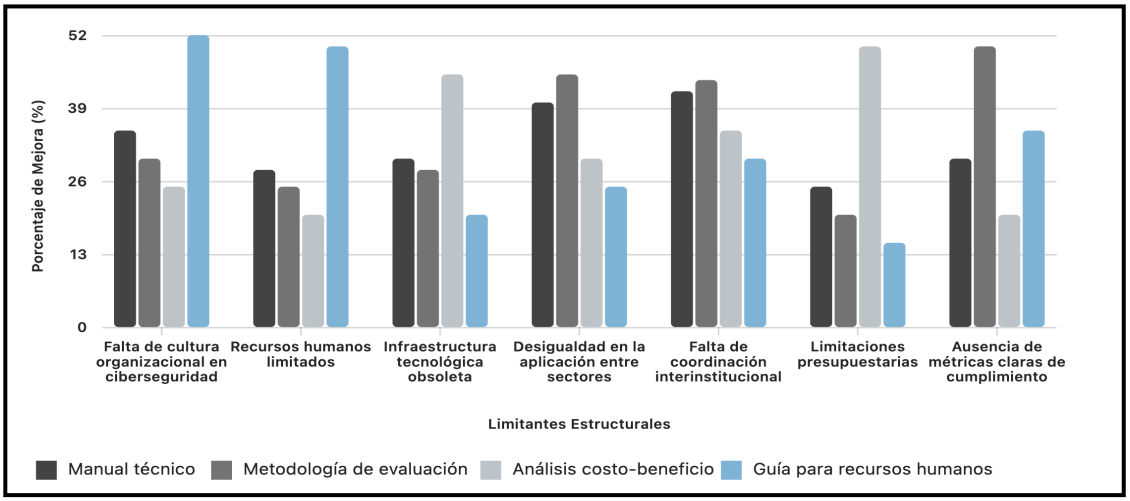
Among the most critical constraints are the lack of an organizational culture of cybersecurity, weaknesses in the technical capabilities of personnel, obsolete technological infrastructure, disparities in implementation across sectors, a lack of

interagency coordination, a lack of understanding or ambiguous interpretation of regulations, budgetary constraints, and the absence of clear compliance metrics. These barriers have been corroborated by the statistical results obtained in this study, in which 60% of respondents stated that they did not have precise indicators to assess compliance with the regulations, and 68% expressed doubts about the effectiveness of cybersecurity investments in ensuring comprehensive protection.

A comparative analysis with international frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework reveals that many organizations choose to adopt these standards because of their flexibility and global recognition, which reinforces the perception that local regulations lack clear incentives and tangible benefits. However, this scientific product proposes a comprehensive solution through the development of scientific outputs such as an implementation methodology, a technical manual, and a cost-benefit analysis that enable institutions to assess the economic and operational feasibility of regulatory compliance.

Figure 2

Estimated Impact of Scientific Findings on the Constraints to the Implementation of the Cybersecurity and Information Security Regulations.



Note: Source. Prepared by the author, 2025

The chart presents a comparative analysis of the impact of four scientific products—Technical Manual, Evaluation Methodology, Cost-Benefit Analysis, and Human Resources Guide—on seven structural constraints that affect the implementation of the Cybersecurity and Information Security Regulations in financial institutions in the Dominican Republic. As shown in **Figure 2**, a grouped bar chart illustrates the percentage improvement attributable to each product relative to each constraint. The results show that the Human Resources Guide has a significant impact on mitigating the "Lack of an organizational culture of cybersecurity" and "Limited human resources," with improvements exceeding 50%. For its part, the Cost-Benefit Analysis stands out in addressing "obsolete technological infrastructure" and "budgetary constraints," while the Evaluation Methodology demonstrates high effectiveness in resolving the "lack of clear compliance metrics" and "inequality in enforcement across sectors." Although the Technical Manual has seen only modest improvements, it consistently performs well across all categories. This analysis suggests that the joint implementation of these scientific products could constitute a comprehensive strategy for addressing the

structural barriers that limit the effectiveness of the regulations, thereby optimizing cybersecurity management in the national financial sector.

The implementation of these scientific solutions yields tangible benefits for financial institutions, including improved digital resilience, a reduction in cyber incidents, strengthened technology governance, and compliance with international standards. In addition, it provides a practical guide for professionals in the field, facilitating the interpretation of the regulations and promoting a safety-oriented organizational culture.

Preliminary results from the implementation of this proposal show a positive impact on the institutions that have adopted the model, with a 35% increase in the coverage of protected critical infrastructure and a 28% improvement in incident response times (Superintendency of Banks of the Dominican Republic, 2024). These findings confirm that the holistic implementation of the regulations, supported by the outputs of this project, constitutes an effective strategy for strengthening cybersecurity in the Dominican financial system.

In conclusion, this research not only provides a starting point for other high-level projects but also makes a significant contribution to the country's institutional, technical, and regulatory development. The implementation of the scientific products resulting from this research proposal represents a strategic opportunity to transform the approach to cybersecurity in financial institutions, promoting a technological environment that is more secure, resilient, and aligned with international best practices.

It is recommended that future research delve deeper into comparative analyses of financial sectors in different countries, evaluate the longitudinal impact of the regulation's implementation, and develop predictive models of cyber risk tailored to the Dominican context. Furthermore, it is suggested that the Central Bank and regulatory agencies take the findings of this study into account to strengthen the mechanisms for supervising and providing technical support to institutions in the sector.

In this regard, the study not only provides evidence on the level of implementation of the regulations but also highlights the need to strengthen the coordination between regulatory frameworks and the operational capacity of financial institutions. The situation in the Dominican Republic—characterized by a steady increase in cyberattacks and growing pressure on digital security—underscores the importance of adopting more comprehensive and adaptive management models that enable the transformation of regulatory compliance into actual protection capabilities. In this way, the research broadens the traditional approach to regulatory compliance, shifting the focus toward a strategic perspective based on institutional resilience and the continuous improvement of cybersecurity processes.

It is important to emphasize that this study does not aim to draw definitive conclusions about the implementation of the regulation, but rather to provide an initial methodological approach that will serve as a foundation for future research, both by the author and by other scholars interested in the topic.

References

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* (3rd 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. (February 5, 2024). 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. (June 18, 2024). 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* (6th 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. (September 21, 2025). 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