Development and Validation of a Cybersecurity Model for Ransomware Mitigation Based on NIST CSF 2.0: The Case Study of a Peruvian Micro-Small Enterprise

Lorenzo Biggi
Information Systems Engineering Department, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
u20201a714@upc.edu.pe

Jorge Rioja
Information Systems Engineering Department, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
u201710286@upc.edu.pe

Pedro Castaneda
Faculty of Systems Engineering and Electrical Mechanics, Universidad Nacional Toribio Rodriguez de Mendoza, Amazonas, Peru
pedro.castaneda@untrm.edu.pe

Juan Mansilla-Lopez
Information Systems Engineering Department, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
pcsijman@upc.edu.pe (corresponding author)

Alberto Daniel Garcia-Nunez
Universidad Pontificia Bolivariana, Medellin, Antioquia, Colombia
alberto.garcia@upb.edu.co

Received: 26 June 2025 | Revised: 23 August 2025 | Accepted: 2 September 2025

 DOI: https://doi.org/10.48084/etasr.12948

ABSTRACT

This study proposes a pragmatic cybersecurity model grounded in the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 to mitigate ransomware in Peruvian Micro and Small Enterprises (MSEs). Through a single-case study of a transportation-sector MSE and a case study methodology proposed in a previous study, the research advances in three stages: (1) cybersecurity posture diagnosis, (2) model design, and (3) expert validation. The model's five-phase structure, Organizational Profile Scope Definition, Critical Assets Identification, Risk Analysis, Cybersecurity Control Selection, and Action Plan Development, addresses MSEs' resource constraints while aligning with NIST CSF 2.0 functions. Expert evaluation yielded an average score of 3.74 out of 5 across nine assessment categories, with a Standard Deviation (SD) of 0.21, and with categories such as "Risk Assessment" and "Sustainability and Adaptability" achieving the highest given scores of 4 out of 5. This modular, cost-free approach bridges the framework adoption gap in resource-constrained enterprises and presents a feasible alternative to existing cybersecurity standards. Although validated through a single case, the proposed framework provides practical guidance for MSEs and establishes a foundation for future research across diverse sectors and geographic locations.

Keywords-cybersecurity; National Institute of Standards and Technology Cybersecurity Framework (NIST CSF); ransomware; risk management; Micro and Small Enterprises (MSEs)

I. INTRODUCTION

Micro and Small Enterprises (MSEs) represent 96.4% of all businesses in Peru and employ 45.8% of the national workforce [1], serving as critical drivers of economic activity. However, their accelerated digitalization, despite enhancing operational efficiency, has exposed them to escalating cyber threats, and especially ransomware attacks, which have emerged as a predominant risk. Globally, ransomware incidents in the transportation sector increased by 181% in 2023, affecting 12 million individuals [2], with cascading impacts on supply chains and public services. In Latin America, attacks like the 2022 Quito municipal disruption [3] highlighted significant systemic vulnerabilities.

Peruvian MSEs face heightened risks due to limited resources and low preparedness, with micro and small firms reporting substantially lower breach-readiness than large companies and often lacking specialized cybersecurity roles [4], while ransomware attacks are rising 15% year-on-year (33,788 incidents in 2023-2024) [5]. These attacks can completely halt an MSE's operations by encrypting critical assets, disrupting services, and incurring high direct and indirect costs. The average ransom payment is around $6,500 [6], but this rarely covers reputational damage, operational downtime, or recovery costs, while it is estimated that 60% of small businesses suffering severe cybersecurity breaches close within six months [7].

Despite this threat, many Peruvian MSEs lack a formally designated cybersecurity lead and, when assigned, responsibility often falls to non-specialist roles (e.g., infrastructure or general management), which results in ad-hoc protections [8]. Moreover, widely recognized frameworks such as ISO/IEC 27001 and COBIT 2019 are frequently perceived by SMEs as complex and resource-intensive, creating a practical framework adoption gap for smaller organizations [9]. This phenomenon has led to what various authors call the "framework adoption gap". Against this backdrop, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) has emerged for its modular, adaptable, and free-of-charge approach. Version 2.0, published in 2024, reinforces this orientation by explicitly including organizations of any size and operational context [10]. Research in [11] further confirmed the advantages of NIST CSF, especially compared to ISO/IEC 27001, while authors in [12] showed that NIST CSF outperforms ISO/IEC 27001 in adaptability and operational ease for budget-constrained MSEs. Similarly, authors in [13] confirm its scalable structure and flexibility through empirical models and expert evaluation. Table I presents a complete direct comparison of the main available frameworks, NIST CSF 2.0 (2024), ISO/IEC 27001:2022, COBIT 2019, and ISO/IEC 27032:2023, focusing on the crucial differences in costs, time, and implementation complexity. NIST CSF 2.0 stands out for the aforementioned advantages as well as being ideal for organizations without prior experience in security management [22]. In contrast, ISO/IEC 27001 requires a formal management system and external audits, with costs ranging between $5,000 and $15,000 [23]. COBIT 2019, geared toward Information Technology (IT) governance, demands organizational experience uncommon in MSEs [24], while ISO/IEC 27032:2023, although specialized in cybersecurity and specific threats like ransomware, lacks formal certification and requires high technical capabilities, limiting its effective adoption in microenterprises [25]. Thus, NIST CSF 2.0 emerges as the most balanced solution for Peruvian MSEs, enabling pragmatic and adaptable prioritization of critical controls [26-27].

In this context, this article proposes an adapted NIST CSF 2.0 model for mitigating ransomware risk, specifically tailored to MSEs. The study is based on a real case of a Peruvian transportation MSE, enabling contextualization of threats, limitations, and practical capabilities for framework implementation. The model identifies and prioritizes controls within NIST CSF functions, including Identify, Protect, Detect, Respond, Recover, and the new Govern function, with a focus on ransomware protection. To validate the relevance and applicability of the adaptation, we consulted the judgment of expert professionals with extensive cybersecurity experience. Although the full implementation of the model remains as future work, the validation results confirm its structural robustness and suitability for the MSE environment.

II. METHODOLOGY

The study followed the case study methodology in [28], structured in three phases: (1) baseline assessment of the organization's cybersecurity posture, (2) development of a NIST CSF 2.0-aligned risk management framework, and (3) rigorous validation via expert judgment. Data triangulation ensured reliability through document reviews (security policies, operational records), semi-structured interviews with key stakeholders (manager, IT assistant), and structured evaluations by two cybersecurity specialists.

A. Model Design Phases

The design of the cybersecurity model followed five structured phases, aligned with the core and implementation tiers of the NIST CSF 2.0: i) Organizational Profile Scope Definition, ii) Identification and Classification of Critical Assets, iii) Cybersecurity Risk Analysis, iv) Selection of Cybersecurity Controls, and v) Development of a Cybersecurity Action Plan. The overall structured workflow is illustrated in Figure 1.

1) Organizational Profile Scope Definition

The initial phase A delineates the organizational boundaries of the analyzed MSE. The methodological objective is to ensure internal validity by specifying which processes, assets, and organizational dimensions are included, while the operational goal focuses on collecting structural information such as size, sector, main functions, personnel, critical assets, and technological processes essential to operations.

Triangulation of sources was employed through semi-structured interviews with the MSE general manager, document review (policies, organizational charts, operational records), and direct observation of operational processes and technological resources. Additionally, a traceable chain of evidence is established: each statement about the organizational context is supported by identifiable and auditable sources,

enabling other researchers to verify the empirical design's logic.

The phase concludes with the development of a technical document titled Organizational Profile Scope, which systematizes key elements of the business context, cybersecurity objectives, model exclusions, and assets to be analyzed. As summarized in Table II, this profile integrates relevant operational information, such as mission, vision, organizational structure, internal and external risk factors, and stakeholder expectations.

TABLE I. RELATED WORKS SUMMARY

Study	Central Theme	Key Contribution	Method / Validation	Relevance to the Proposed Model
[11]	Comparative analysis of cybersecurity assessment frameworks for SMEs.	Compares NIST CSF, CSRM-SME, CSEM, and ASMAS frameworks, highlighting their strengths and limitations.	Systematic review and comparison of four frameworks using defined criteria.	Assists in selecting the most suitable model for SMEs, providing criteria to strengthen cybersecurity; supports the selection of controls in the ransomware mitigation model.
[12]	CSF for SMEs in Peru based on ISO 27001 and NIST CSF.	Proposes an integrated framework combining ISO/IEC 27001 and NIST CSF controls applied to Peruvian SMEs.	Proposal design aligned with ISO/IEC 27001 and PDCA methodology.	Reinforces the choice of NIST CSF as a viable and context-adapted approach for the Peruvian setting.
[13]	Cybersecurity maturity evaluation aligned with NIST CSF.	Proposes a security maturity assessment framework based on NIST CSF, tailored for SME environments.	Surveys applied to experts and organizations, quantitative validation.	Demonstrates NIST CSF's applicability in small organizations; expert validation reinforces its suitability as a foundation for a ransomware mitigation model in microenterprises.
[14]	Early ransomware detection model using mutual information feature selection.	Presents a proactive detection algorithm identifying ransomware activity before full encryption.	Development of a computational model and experimental testing with ransomware datasets.	Offers a preventive ransomware detection strategy, complementary to the mitigation model; showcases data mining techniques useful for anticipating attacks in microenterprises.
[15]	Feature selection with redundancy coefficient for early ransomware detection.	Introduces a weighting factor in variable selection to enhance ransomware detection.	Development of a computational technique and validation with early detection simulations.	Highlights advanced pre-encryption ransomware detection methodologies, suggesting approaches that can be incorporated into the model for microenterprises to improve threat detection.
[16]	Incremental mutual information selection technique for early ransomware detection.	Designs a progressive method for feature selection to identify ransomware before massive encryption.	Development of an innovative algorithm and validation through ransomware data simulations.	Provides practical solutions for proactive ransomware detection in low-computational environments.
[17]	Cybersecurity strategies for critical railway systems.	Proposes a comprehensive strategy based on NIST CSF and IEC 62443 to protect railway infrastructure, including robust authentication and real-time monitoring.	Strategic proposal applied to railway infrastructure with technical review of standards.	Demonstrates NIST CSF's applicability in critical sectors like transportation, reinforcing its value as an adaptable framework in complex logistical environments.
[18]	Analysis of the maritime cybersecurity landscape based on NIST CSF v2.0.	Evaluates the maritime sector's maturity against NIST CSF v2.0, emphasizing the new 'Govern' pillar for improving cyber governance.	Systematic literature review using PRISMA methodology focused on NIST CSF functions.	Illustrates how to apply and evaluate NIST CSF in a critical industry; serves as a case for understanding the adaptability of the cybersecurity (and by extension mitigation) model in new domains.
[19]	Cybersecurity landscape in Supply Chain 4.0.	Reviews security challenges and solutions in digitized supply chain environments.	Literature review focused on cybersecurity and emerging technologies in logistical settings.	Provides context for threats in technological supply networks; highlights controls and challenges that may parallel those in SME suppliers or distributors in the mitigation model.
[20]	Cybersecurity governance and policies for SMEs in Industry 5.0.	Compares security policies between Saudi Arabia and the UK, recommending best practices for SMEs.	Comparative study (documentary and/or interviews with experts from both countries).	Informs how to adapt cybersecurity policies to national contexts in SMEs; guides the incorporation of robust governance frameworks in the ransomware mitigation model.
[21]	Specialized cybersecurity risk assessment framework for SMEs.	Introduces a specific framework and tool for managing cybersecurity risks in SMEs.	Conceptual proposal based on literature review.	Reinforces the use of expert evaluation as a key validation method for the proposed model.

2) Identification and Classification of Critical Assets

The second phase B, begins with an exhaustive identification of assets, considering resources such as computing equipment, information systems, applications, email accounts, cloud services, databases, and human assets (e.g., key personnel or critical suppliers). Each asset is described and categorized by its nature (hardware, software, information, human resources, external services). Two semi-structured interviews with the general manager and administrative assistant provided supporting artifacts, including a Visio process-flow diagram of the Quotation Attention process and the company's asset inventory spreadsheet. Asset identification is validated by triangulation of sources, as existing company records were reviewed, interviews were conducted with management and operational staff to identify undocumented elements, and direct observation of infrastructure was performed.

Each asset was then assessed under the Confidentiality, Integrity, and Availability (CIA) triad. Confidentiality evaluated how sensitive the asset's information is, integrity measured the impact of unauthorized modification, and availability assessed the effect of business operational unavailability. As shown in Table III, each dimension is scored on a 1-to-5 scale, and the sum determines the final criticality level according to predefined ranges (Table IV).

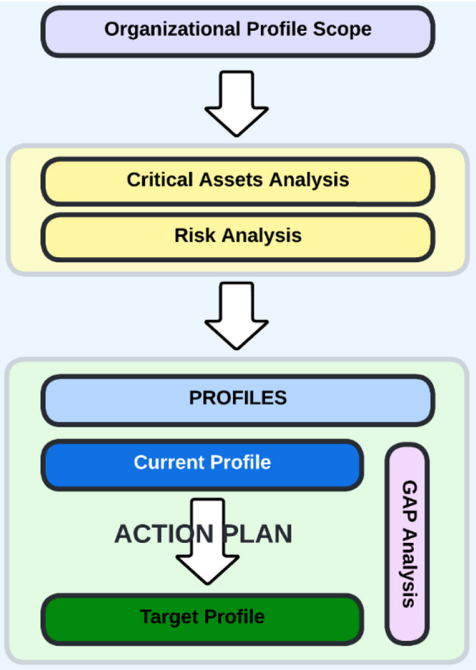

Fig. 1. Phased structure of the proposed cybersecurity model.

TABLE II. ORGANIZATIONAL PROFILE SCOPE

Element	Description
Mission and Vision	Focus on safe, sustainable, and customer-tailored transportation solutions.
Organizational Structure	Manager, IT and Cybersecurity Assistant, Administrative Assistant, and Operational Assistant.
Critical Assets Involved	Website, quotation system, email, laptops, WordPress hosting.
Model Scope	Quotation Attention Process.
Exclusions	Physical security, third-party networks, and human resources not related to IT.

TABLE III. CRITERIA FOR EVALUATING ASSET CRITICALITY WITHIN CIA TRIAD

Dimension	Value	Description of Impact
Confidentiality	1-5	From "Not relevant" to "Catastrophic harm, fraud, or critical loss".
Integrity	1-5	From "Not relevant" to "Must be accurate and reliable at least 95.5%".
Availability	1-5	From "Not relevant" to "Must be accessible at least 95.5% of the time".

Each criticality level was documented in a structured manner, ensuring complete traceability: CIA criterion scores were stored, and the final criticality level was determined based on these values. Additionally, each asset was accompanied by supplementary information such as its functional category (e.g., system, service, infrastructure), assigned responsible party within the organization, information classification (confidential, public), specific location (local, cloud, external provider), and lifecycle status, providing precise operational context. This approach ensured a clear chain of evidence, allowing third parties to audit the classification process and understand the decisions made. Finally, an organized inventory was consolidated, synthesizing key assets requiring priority protection against ransomware. As summarized in Table V, the most critical assets are highlighted, clearly identified by their unique code, name, and assigned criticality level.

TABLE IV. CRITICALITY LEVELS ASSIGNED TO ASSETS ACCORDING TO ESTABLISHED RANGES

Score Range	Criticality Level	Description of Impact
13-15	Very High	Critical impact, affects processes by 95%, significant loss.
10-12	High	High impact, affects processes by 75%, possible minor losses.
7-9	Medium	Moderate impact, affects processes by 50%, no significant loss.
4-6	Low	Minor impact, affects processes by 10%, no significant loss.
1-3	Very Low	Insignificant impact, practically no effect.

TABLE V. SUMMARY OF IDENTIFIED CRITICAL ASSETS

Code	Asset Name	Criticality
AS-01	Email	Very High
AS-02	Website	High
AS-03	WordPress CMS	High
AS-04	Cloud Storage	Very High
AS-05	Laptops	High
AS-06	Router	High
AS-08	Manager	Very High
AS-11	Excel	Medium
AS-14	Quotation	Low

3) Cybersecurity Risk Analysis

In the third phase C, a ransomware-focused risk analysis is conducted on the critical assets. The methodological objective is to systematically link relevant threats and vulnerabilities to determine the most significant ransomware attack scenarios, while the operational aim involves creating a detailed cybersecurity risk matrix identifying possible ransomware scenarios for each critical asset, along with assessments of their likelihood and organizational repercussions.

The identification of threats, vulnerabilities, and risk scenarios was grounded in official international reference sources, such as NIST, Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Federal Trade Commission (FTC), and the Cyber Readiness Institute (CRI). Key threats include phishing emails, malware downloads, outdated Content Management System (CMS) vulnerabilities, credential theft in cloud services, and network intrusions exploiting weak configurations. Table VI summarizes these threats along with their main characteristics, attack vectors, and related assets.

Additionally, internal vulnerabilities or operational security gaps that could be exploited were cataloged, including lack of anti-spam/antimalware filters in email, absence of updated antivirus on laptops, use of weak passwords or lack of two-factor authentication, unpatched or obsolete systems (e.g., outdated WordPress plugins on the website), inappropriate cloud or network security configurations (open ports, unencrypted sensitive data), and lack of formal backup or incident response procedures. Table VII summarizes the

internal vulnerabilities detected in the company, classified by their code, technical description, and direct linkage to the analyzed assets.

TABLE VI. KEY THREATS AND COMPROMISED ASSETS

Code	Threat	Main Attack Vector	Compromised Assets
TH-01	Phishing	Malicious emails	AS-01, AS-08, AS-09, AS-14
TH-02	CMS Breach	Outdated WordPress plugins	AS-02, AS-03
TH-04	Credential Theft	Brute force or lack of Multi-factor Authentication (MFA)	AS-04
TH-06	Data Exfiltration	Simultaneous encryption and extraction	AS-01, AS-11, AS-14

TABLE VII. CATALOG OF CRITICAL ASSET VULNERABILITIES

Code	Detected Vulnerability	Main Cause	Affected Assets
VL-01	Lack of email filters.	Absence of antiphishing/antimalware.	AS-01, AS-14
VL-02	Weak security configurations.	No multifactor authentication or encryption.	AS-04, AS-14
VL-04	Outdated CMS plugins.	Lack of maintenance.	AS-02, AS-03
VL-05	Insufficient network security.	Deficient access control lists.	AS-06

Each combination of a threat and vulnerability for an asset defined a specific risk scenario (e.g., ransomware infiltration via phishing due to inadequate email filtering, or malware propagation in the internal network due to an outdated router). Risk identification was supported by triangulating multiple information sources, combining internal assessments with external information such as current ransomware campaign reports and expert security guidelines. Interviews with local cybersecurity specialists and company technical staff were also conducted to validate scenario plausibility.

For each identified risk, likelihood (P) and impact (I) were estimated qualitatively on a 1-5 scale adapted from ISO/IEC 27005:2022 and operationalized for an MSE context. Likelihood (P) reflects the plausibility of occurrence given exposure and control strength, and impact (I) captures business consequences in terms of service interruption, financial loss, reputational damage, and legal or regulatory exposure. Where relevant, we cross-checked the plausibility of attack paths against MITRE ATT&CK techniques frequently observed in ransomware campaigns (e.g., T1566 Phishing, T1190 Exploit Public-Facing Application, T1486 Data Encrypted for Impact). The assignments were supported by collected evidence such as historical incidents, asset attractiveness, exposure level, and the criticality established in phase B, considering the firm's size and sector, ensuring each assessment was transparent and auditable.

Thus, the development of a ransomware-specific risk matrix was enabled, tailored to the company's operational environment. Each risk was characterized by: (a) the affected asset, (b) the identified threat (c) the associated vulnerability, (d) a unique code for risk traceability, (e) a narrative description detailing how the incident would materialize and its direct consequences, and (f) the semi-quantitative evaluation of probability and impact, combined to determine the risk level by multiplying the estimated likelihood of occurrence by the potential severity of its consequences. This structure is summarized in Table VIII, presenting a condensed version of the main identified risk scenarios.

TABLE VIII. SUMMARY OF RANSOMWARE RISK SCENARIOS

Code	Risk	Asset	P	I	Risk Level
R-001	Ransomware via phishing	Email	5	5	25
R-003	Exploitation of outdated CMS	Website / WordPress	4	4	20
R-004	Personal data leakage	Website / WordPress	3	5	15
R-005	Unauthorized access to stored data	Enterprise cloud	3	5	15
R-006	Exfiltration of confidential information	Enterprise cloud	3	4	12

4) Selection of Cybersecurity Controls

In the fourth phase D, a structured selection of cybersecurity controls is conducted, with the methodological objective of aligning detected vulnerabilities and threats with concrete measures to mitigate ransomware risk. This phase constitutes the prescriptive core of the proposed model, defining the security capabilities required to transition from the organization's current cybersecurity posture to a more mature and resilient target state.

The process begins with a filtered selection of NIST CSF 2.0 categories and subcategories, considering only those relevant to the model's functional scope (e.g., processes and critical assets associated with the "Quotation Attention" function). To guide this selection, the NIST IR 8374 in [26] is used as a reference, offering specialized guidance for prevention, response, and recovery practices against ransomware, focusing the evaluation on the most relevant domains.

Figure 2 illustrates how the proposed model visually maps the alignment of NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover) with their respective categories and subcategories. The figure uses a hierarchical flowchart to illustrate how each function, such as Govern (GV.OC, GV.RM, GV.RR) and Protect (PR.AA, PR.AT, PR.DS), links to specific subcategories (e.g., GV.OC-02, PR.AA-01), highlighting the tailored selection process for ransomware mitigation in a transportation MSE. Once the relevant subcategories are identified, a structured questionnaire is developed to assess their implementation level within the organization, based on predefined maturity criteria. This technical instrument was administered through guided interviews with the manager and key staff members. Table IX presents examples of the questionnaire items aligned with each CSF function.

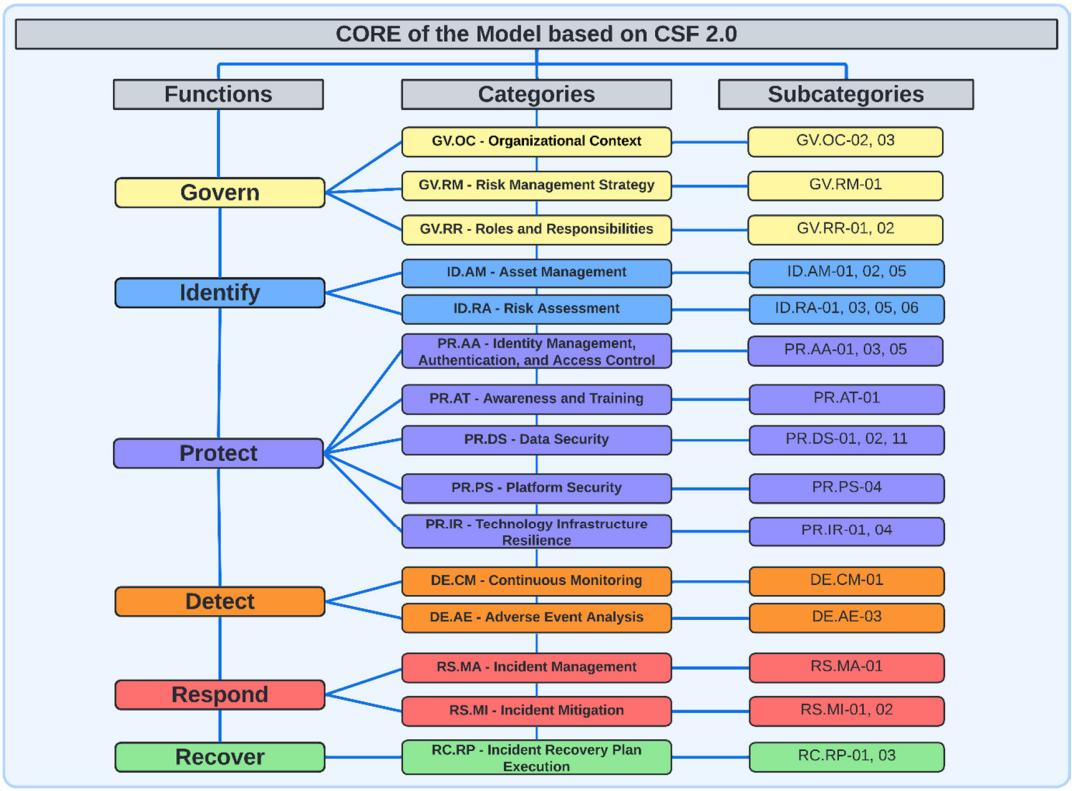

Fig. 2. Core of the proposed model based on NIST CSF 2.0 subcategories.

TABLE IX. EXCERPT OF STRUCTURED QUESTIONNAIRE

Function	Example Questionnaire Question
Govern	How does the company identify and manage the cybersecurity needs of employees and customers?
Identify	How does the company prioritize assets based on their importance or criticality to operations?
Protect	What measures does the company use to ensure authorized access, e.g., MFA?
Detect	How does the company monitor its networks to detect security issues?
Respond	What actions does the company take to contain and resolve security issues?
Recover	What steps does the company follow to restore operations after an incident?

The responses were used to establish the Current Profile, representing the organization's existing cybersecurity posture. Concurrently, a Target Profile was defined, setting the desired maturity level for each subcategory according to the organization's strategic priorities and the critical risks identified in phase C.

The difference between the Profiles forms the basis for the gap analysis that underpins improvement planning. Following NIST CSF guidance, both profiles are integrated into a single Organizational Profile, which documents the selected results, their current and desired levels, and associated risk considerations, serving as the central axis for prioritizing future mitigation actions. Table X presents a summary of this profile for the "Govern" function, illustrating how the model is operationalized in practical terms: it includes categories (C) and their respective subcategories (SC), current level (CL), target level (TL), gap (G), and priority (P).

TABLE X. CYBERSECURITY ORGANIZATIONAL PROFILE: SUMMARY OF THE "GOVERN" FUNCTION

C	SC	CL	TL	G	P
GV.OC: Organizational Context.	GV.OC-02	1	3	2	Medium
	GV.OC-03	2	3	1	Low
GV.RM: Risk Management.	GV.RM-01	1	3	2	Medium
GV.RR: Roles and Responsibilities.	GV.RR-01	2	3	1	Low
	GV.RR-02	2	3	1	Low

For each evaluated subcategory, specific controls from the NIST SP 800-53 Rev. 5 catalog are selected to address identified gaps. This mapping between CSF subcategories and SP 800-53 controls is built under a traceability and technical justification approach, considering variables such as operational feasibility, implementation complexity, estimated cost, and effectiveness against the risk. The control selection is consolidated in a structured table comprising four key components: (i) the evaluated subcategory, (ii) observed current practices in the organization, (iii) recommended controls, and (iv) candidate improvements. Table XI presents a representative summary of this analysis.

The consolidated result of this phase is the Cybersecurity Organizational Profile, which integrates both the current and target states for each critical subcategory, along with a documented list of selected SP 800-53 controls.

TABLE XI. REPRESENTATIVE SUMMARY OF CONTROL SELECTION

Subcategory	Current Practices	Candidate Controls
GV.OC-02: Understanding of stakeholders and their expectations.	No formal mechanisms exist to capture the security needs of stakeholders. Periodic meetings are not held, nor are specific expectations documented.	PM-9 PM-18 SR-5
GV.OC-03: Legal and regulatory requirements.	While general security regulations are complied with, there are no specific processes or formal documentation to support such compliance.	AC-1 AT-1 AU-1
GV.RM-01: Risk management objectives.	There is no clear strategy for managing cyber risks. Objectives are neither defined nor validated with stakeholders.	PM-9 RA-7

5) Development of a Cybersecurity Action Plan

In the final phase E of the model, a detailed action plan is developed to address the gaps identified between the Current and Target Cybersecurity Profiles, completing the methodological proposal. This phase represents the transition from diagnosis to action, translating gap analysis findings into strategic, prioritized, and organizationally feasible initiatives.

To support this transition, a gap analysis was applied based on a formula that precisely quantifies the maturity level achieved per NIST CSF 2.0 category (4). This approach evaluates each subcategory with a score from 1 to 4, based on its implementation level (1 = Partial, 2 = Risk-Informed, 3 = Repeatable, 4 = Adaptive), and calculates the percentage of the current level relative to the target level:

$$P_{Cat} = \frac{\sum_{i=1}^{n} N_i}{4 \cdot n} \cdot 100\% \quad (4)$$

where P_{Cat} is the percentage obtained for the evaluated category (representing current achievement, target, or identified gap), N_i is the level assigned to each evaluated subcategory within the category (values from 1 to 4), n is the total number of subcategories evaluated in the category, and the value 4 represents the maximum possible level per the NIST CSF 2.0 maturity scale.

This quantitative analysis provides a clear visualization of critical areas and enables prioritization of gaps based on their urgency. Thus, it establishes an objective basis for planning specific and phased interventions, considering the resource constraints typical of MSEs. Figure 3 presents a summary of the applied gap analysis, showing the percentage of current compliance, target, and existing gap per NIST CSF 2.0 function.

Based on these results, a structured action plan is designed, converting each prioritized gap into concrete and executable actions. These actions are linked to NIST SP 800-53 Rev. 5 controls, selected based on their technical relevance, estimated cost, ease of implementation, and effectiveness against the corresponding risk. For instance, to address a critical gap in the subcategory "PR.AA-03: Users, services, and hardware are authenticated," the immediate implementation of MFA is proposed, clearly defining responsible parties, timelines, required resources, and success criteria.

Function	Category	Current %	Target %	GAP %
Govern (GV)	Organizational Context (GV.OC)	37.5%	75.0%	37.5%
	Risk Management Strategy (GV.RM)	25.0%	75.0%	50.0%
	Roles, Responsibilities, and Authorities (GV.RR)	50.0%	75.0%	25.0%
	Summary Function GV	**37.5%**	**75.0%**	**37.5%**
IDENTIFY (ID)	Asset Management (ID.AM)	25.0%	75.0%	50.0%
	Risk Assessment (ID.RA)	25.0%	75.0%	50.0%
	Summary Function ID	**25.0%**	**75.0%**	**50.0%**
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)	25.0%	75.0%	50.0%
	Awareness and Training (PR.AT)	25.0%	75.0%	50.0%
	Data Security (PR.DS)	25.0%	75.0%	50.0%
	Platform Security (PR.PS)	25.0%	75.0%	50.0%
	Technology Infrastructure Resilience (PR.IR)	25.0%	75.0%	50.0%
	Summary Function PR	**25.0%**	**75.0%**	**50.0%**
DETECT (DE)	Continuous Monitoring (DE.CM)	25.0%	75.0%	50.0%
	Adverse Event Analysis (DE.AE)	25.0%	75.0%	50.0%
	Summary Function DE	**25.0%**	**75.0%**	**50.0%**
RESPOND (RS)	Incident Management (RS.MA)	25.0%	75.0%	50.0%
	Incident Mitigation (RS.MI)	25.0%	75.0%	50.0%
	Summary Function RS	**25.0%**	**75.0%**	**50.0%**
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)	37.5%	75.0%	37.5%
	Summary Function RC	**37.5%**	**75.0%**	**37.5%**

Fig. 3. Gap analysis summary across the selected categories.

Each initiative in the plan is detailed through a precise set of components ensuring traceability and effective execution:

- NIST CSF 2.0 category involved.
- Related risk and its description.
- Identified risk level (scale of 1 to 25).
- Action required to mitigate the gap.
- Action type (preventive, detective, or corrective).
- Specific NIST SP 800-53 control associated.
- Priority level (high, medium, or low).
- Responsible party for execution.
- Identified risk owner.
- Tools required for implementation.
- Verifiable success indicators.
- Periodic review frequency (quarterly, annual, etc.).

The plan's design also considers differentiated solutions based on required effort. Low-cost actions, such as phishing recognition training, are scheduled for immediate execution, whereas initiatives requiring technological investment or external consultancy are planned incrementally, subject to budget availability.

To ensure the plan's feasibility and validity, a triangulation of sources was conducted, including: (1) results from structured interviews with key staff, (2) review of internal process

documentation, and (3) expert validation with cybersecurity professionals. This process ensured that the proposed actions are not only technically sound but also realistic. Table XII presents a representative summary of the proposed action plan.

Upon completion of this phase, the model evolves from risk identification to strategic mitigation, delivering a verifiable and actionable roadmap aligned with international standards. This roadmap ensures that all actions are evidence-based, prioritized, and sustainable, effectively enhancing the cyber-resilience of the organization and its ability to withstand and recover from ransomware and related cybersecurity threats.

TABLE XII. EXTRACT OF THE ACTION PLAN

Category	Related Risk	Proposed Action	Controls
Identity Management, Authentication and Access Control (PR.AA)	R-001: Ransomware via phishing. R-002: Exfiltration of confidential data. R-008: Credentials theft and unauthorized access.	Implement centralized identity management and MFA, with periodic access audits and user training on secure credential practices.	AC-1, IA-2, IA-5
Continuous Monitoring (DE.CM)	R-001: Ransomware through phishing.	Implement continuous monitoring with risk-based adjustments and alerts for unauthorized access and network anomalies.	AU-6, CA-7
Awareness and Training (PR.AT)	R-001: Ransomware via phishing. R-009: Infection by malware. R-022: Theft of credentials or unauthorized access to accounts.	Deploy interactive cybersecurity training with phishing simulations and periodic assessments on ransomware and credential hygiene.	AT-2, AT-3
Incident Mitigation (RS.MI)	R-001: Ransomware via phishing. R-011: Unauthorized access and propagation of malware in the network. R-007: Unauthorized access and propagation of malware in the network.	Develop and test an Incident Response Plan (IRP) with trained staff and periodic drills for ransomware scenarios.	IR-4, IR-6
Asset Management (ID.AM)	R-003: Exploitation of vulnerabilities in plugins or outdated themes. R-006: Loss of confidentiality of information. R-009: Infection by malware.	Establish and maintain a centralized asset inventory, updated quarterly and prioritized by business criticality.	CM-8, PM-5

B. Validation Process

To evaluate the content validity and practical applicability of the proposed model, an additional structured expert judgment process was implemented. Specifically, two cybersecurity professionals were invited to review the proposed model. Their backgrounds span critical infrastructure protection, cyber risk assessment, and the implementation of international frameworks across diverse organizational contexts, including MSEs and critical sectors such as energy and industrial control systems. Experts were selected based on three criteria: (1) more than 15 years of professional experience, (2) direct involvement in applying CSFs in MSEs and critical sectors, and (3) availability and willingness to participate. Each expert independently reviewed the model using the structured validation form, after which clarifications and feedback were exchanged to resolve ambiguities and improve the model. Two key documents were prepared to support the evaluation:

- Descriptive Model Document: A comprehensive explanation of the proposed model, detailing each phase and its expected outcomes.
- Validation Form: A structured evaluation tool containing nine items for assessment, accompanied by specific evaluation criteria and instructions for the experts.

The experts evaluated each item using a Likert scale (1-5), where 1 represents "Very Low" and 5 represents "Very High". Table XIII summarizes the criteria considered, focusing on the clarity, relevance, and coherence of each model component. Table XIV details the specific items evaluated by the experts to assess the comprehensiveness and applicability of the proposed cybersecurity risk management model.

TABLE XIII. EVALUATION CRITERIA FOR THE VALIDATION PROCESS

Criteria	Description
Clarity	Evaluate whether the item is well written and presented in a comprehensible manner.
Relevance	Measure the importance and relevance of the item in relation to the objectives of the model.
Coherence	Assess whether the item is consistent with the rest of the model and properly integrated.

The performance of the proposed cybersecurity model was evaluated using the following validation metrics:

$$G_s = \frac{\sum_{i=1}^{9} I_S}{9} \quad (1)$$

$$I_s = \frac{\sum_{k=1}^{n} S_k}{\mathrm{n}} \quad (2)$$

$$\sigma = \sqrt{\frac{\sum_{k=1}^{9} (S_k - G_s)^2}{9}} \quad (3)$$

where (1) calculates the overall average score G_s, where I_s represents the average score for each of the nine items evaluated. This metric must be greater than or equal to 3.5 to indicate above-average quality. Equation (2) computes the average score of each item, where S_k indicates the score for that item, and n is the number of evaluators. This metric must be greater than or equal to 3.0, chosen as the minimum acceptable score, aligning with the scale's moderate rating, ensuring no critical component falls below a baseline of adequacy. Equation (3) determines the Standard Deviation (SD) σ of the results. This last metric must be less than or equal to 0.5, a stringent requirement that ensures evaluator consensus and reliability in a small-sample validation process.

TABLE XIV. ITEMS EVALUATED IN THE VALIDATION PROCESS

No.	Item	Description
1	Profile Definition	The model adequately establishes the scope of the organizational profile, clearly identifying the processes, roles, and responsibilities of the MSE.
2	Identification and Classification of Critical Assets	The company's critical assets were cataloged clearly and systematically, reflecting their importance in terms of CIA.
3	Analysis of Threats and Vulnerabilities	Threats and vulnerabilities associated with critical assets were properly analyzed and documented, with a specific focus on ransomware attacks.
4	Risk Assessment	The risk analysis properly identifies the risks to which the assets are exposed, considering both likelihood and impact.
5	Selection of Cybersecurity Controls	The created organizational profile is appropriate for the company, selecting specific and suitable controls for ransomware protection.
6	Determination of Maturity Levels	The organizational profile clearly establishes the current and target cybersecurity maturity levels across the six NIST CSF 2.0 functions.
7	Organizational Profile Gap Analysis	The gap analysis was conducted thoroughly, clearly identifying deficiencies across the six functions of the NIST CSF 2.0.
8	Action Plan	The action plan defines appropriate actions to close risk gaps and elevate the company to the established Tier 3 in the target profile.
9	Sustainability and Adaptability	The proposed model is sustainable and adaptable, allowing the company to effectively respond to future cyber threats.

III. VALIDATION RESULTS

The outcomes of the expert judgment process are presented in Table XV and Figure 4, depicting the average evaluation scores across all assessed items. The results demonstrate consistent performance across all evaluated items, with scores ranging from 3.3 to 4.0, and an overall average of 3.74/5 (SD = 0.21). In addition, all predefined success criteria were satisfied:

- Average score ≥ 3.5,
- Individual item scores ≥ 3.0, and
- Strong evaluator consensus (SD ≤ 0.5).

The highest ratings in "Risk Assessment" and "Sustainability and Adaptability" (both 4.0), indicate that experts perceived the model particularly effective in identifying and managing ransomware-related risks while maintaining feasibility for MSE environments. Comparatively, "Organizational Profile Gap Analysis" (3.3) and "Identification and Classification of Critical Assets" (3.5) received slightly lower ratings, suggesting there is room for improvement regarding documentation and traceability.

Post-validation refinements, guided by the experts' feedback, strengthened weaker areas, such as "Identification and Classification of Critical Assets" (3.5→4.0) and "Determination of Maturity Levels" (3.7→4.2), while the "Organizational Profile Gap Analysis" (3.3→3.8) improved through clearer vulnerability descriptions and regulatory compliance integration.

TABLE XV. AVERAGE EXPERT EVALUATION SCORE PER ITEM

No.	Item	Average Score
1	Profile Definition	3.7
2	Identification and Classification of Critical Assets	3.5
3	Analysis of Threats and Vulnerabilities	3.8
4	Risk Assessment	4.0
5	Selection of Cybersecurity Controls	3.8
6	Determination of Maturity Levels	3.7
7	Organizational Profile Gap Analysis	3.3
8	Action Plan	3.8
9	Sustainability and Adaptability	4.0

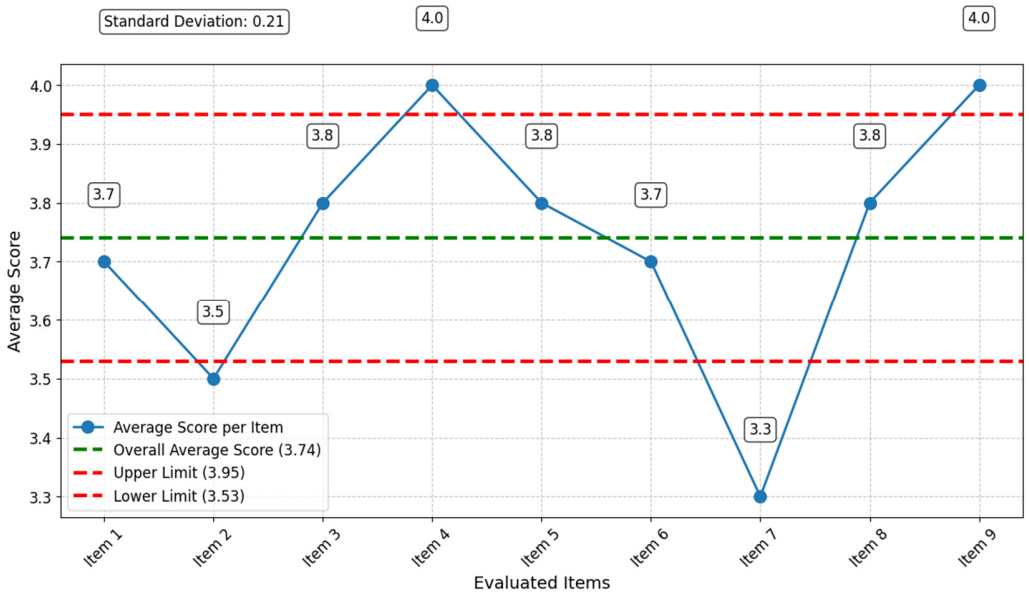

Fig. 4. Average expert evaluation score of each item.

IV. DISCUSSION

The proposed model's phased structure enables MSEs to implement cybersecurity measures incrementally, prioritizing critical areas such as email security (R-001: Phishing via malicious emails) without requiring substantial upfront investment. This design aligns with the suggestion of authors in [11], who emphasized simplicity and scalability in SME CSFs. Additionally, the model extends prior work by incorporating ransomware-specific controls, for example, MFA for cloud access, and contextualizing them within a Peruvian transportation-sector case study. In contrast to approaches such as in [14-16], which emphasize early ransomware detection using advanced computational infrastructure, this work focuses on preventive and organizationally actionable controls, including asset inventory management and phishing awareness training. These features make the model both cost-effective and feasible for smaller organizations with limited technical capacity. Similarly, while sector-specific adaptations of NIST CSF 2.0 in [17-18] illustrate its flexibility, this study uniquely contributes by integrating sustainability and adaptability, validated with a 4.0 expert score, into the MSE cybersecurity context.

Nevertheless, certain limitations must be acknowledged. While the single-case study provides in-depth insights tailored to a Peruvian transportation MSE, its generalizability is limited to other industries or regions. Future work could expand validation through multi-case studies across diverse sectors (e.g., manufacturing, finance) and a wider geographical context to enhance broader applicability. Furthermore, the validation was conducted with only two experts, limiting statistical robustness.

V. CONCLUSION

By addressing the cybersecurity maturity gap in resource-limited environments, this study contributes both theoretically and practically to the field of cybersecurity management for Micro and Small Enterprises (MSEs). Theoretically, it demonstrates how international frameworks like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 can be localized for MSEs without compromising methodological rigor. Practically, it introduces a phased, ransomware-focused roadmap for cybersecurity enhancement, validated through expert assessment and grounded in a real-world Peruvian transportation-sector case study. The results show that even with limited technical and financial resources, MSEs can meaningfully advance their cybersecurity posture by adopting structured frameworks supported by incremental implementation strategies.

Future research should build upon this foundation in multiple directions. The development of automated monitoring tools could support compliance tracking and reduce the manual burden on small firms. Penetration testing would provide technical validation to complement the expert-based evaluation, while expanding the model to additional sectors such as manufacturing or finance, along with longitudinal studies of sustained resilience gains, would enhance its external validity. Finally, policy-focused studies could explore financial incentives and regulatory frameworks that promote adoption among MSEs. In sum, this study provides a scalable and context-aware template for enhancing cybersecurity resilience in emerging economies, bridging the gap between global best practices and local feasibility.

ACKNOWLEDGMENT

The authors express their gratitude to the Dirección de Investigación of the Universidad Peruana de Ciencias Aplicadas (UPC) for the support provided for this research work through the UPC-EXPOST-2025-2 incentive.

REFERENCES

[1] COMEXPERU, "Micro and Small Enterprises in Peru: Results in 2022," 2022. [Online]. Available: https://www.comexperu.org.pe/upload/articles/reportes/reporte-mypes-2022.pdf.

[2] S. Bowcut. "Digital safeguards: Navigating cybersecurity in transportation." Cybersecurityguide, Apr. 2025. [Online]. Available: https://cybersecurityguide.org/industries/transportation.

[3] C. Tornaghi. "The Dramatic Cyberattack That Put Latin America on Alert." Americas Quarterly, Jul. 2023. [Online]. Available: https://www.americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert.

[4] J. L. Del Campo. "Mypes in our country do not take cybersecurity into account: why this is a big mistake and how to remedy it." El Comercio, Feb. 2025. [Online]. Available: https://elcomercio.pe/tecnologia/ciberseguridad/las-mypes-en-nuestro-pais-no-toman-en-cuenta-la-ciberseguridad-por-que-esto-es-un-gran-error-y-como-remediarlo-intecnia-corp-bitdefender-ataques-informaticos-ciberdelincuentes-empresas-noticia.

[5] P. Valdivia. "Peru stands as a focus of cyber attacks in Latin America." El Comercio, Aug. 2024. [Online]. Available: https://elcomercio.pe/tecnologia/ciberseguridad/peru-se-alza-como-un-foco-de-ataques-ciberneticos-en-latinoamerica-malwere-phishing-ransomware-noticia.

[6] Economy Magazine. "SMEs in Peru register nearly 10 million cyber attack attempts." Revista Economia, Jun. 2024. [Online]. Available: https://www.revistaeconomia.com/pymes-de-peru-registran-cerca-de-10-millones-de-intentos-de-ciberataque.

[7] Verizon Business. "Small Business Cyber Security and Data Breaches." Verizon. [Online]. Available: https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches.

[8] E. I. Ahon, "Study on Cybersecurity in Senior Management," eBIZ, IALaw, Dec. 2024. Online]. Available: https://ebiz.pe/wp-content/uploads/2024/12/241231-Estudio-sobre-Ciberseguridad-en-la-Alta-Direccion-2024.pdf.

[9] European Union Agency for Cybersecurity., *Cybersecurity for SMEs: challenges and recommendations.* LU: Publications Office, 2021.

[10] NRI Secure Blog. "NIST CSF 2.0: What's New and Why It Matters." NRI Secure, Aug. 2025. [Online]. Available: https://www.nri-secure.com/blog/nist-csf-2.

[11] W. N. E. W. M. Ludin, M. Mohd, and W. F. Paizi@Fauzi, "Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 8, 2024, https://doi.org/10.14569/IJACSA.2024.0150878.

[12] M. L. Angelo Edú, G. P. Alexis, and W. P. Lenis, "Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls," in *2023 18th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, Portugal, Jun. 2023, pp. 1–7, https://doi.org/10.23919/CISTI58278.2023.10211874.

[13] L. Bernardo, S. Malta, and J. Magalhães, "An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF," *Electronics*, vol. 14, no. 7, Mar. 2025, Art. no. 1364, https://doi.org/10.3390/electronics14071364.

[14] T. M. H. Mohamed, B. A. S. Al-rimy, and S. A. Almalki, "A Ransomware Early Detection Model based on an Enhanced Joint Mutual Information Feature Selection Method," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15400–15407, Aug. 2024, https://doi.org/10.48084/etasr.7092.

[15] B. A. S. Al-rimy *et al.*, "Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection," *Future Generation Computer Systems*, vol. 115, pp. 641–658, Feb. 2021, https://doi.org/10.1016/j.future.2020.10.002.

[16] M. Gazzan and F. T. Sheldon, "An Incremental Mutual Information-Selection Technique for Early Ransomware Detection," *Information*, vol. 15, no. 4, Mar. 2024, Art. no. 194, https://doi.org/10.3390/info15040194.

[17] N. Ibadah, C. Benavente-Peces, and M.-O. Pahl, "Securing the Future of Railway Systems: A Comprehensive Cybersecurity Strategy for Critical On-Board and Track-Side Infrastructure," *Sensors*, vol. 24, no. 24, Dec. 2024, Art. no. 8218, https://doi.org/10.3390/s24248218.

[18] A. Dimakopoulou and K. Rantos, "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0," *Journal of Marine Science and Engineering*, vol. 12, no. 6, May 2024, Art. no. 919, https://doi.org/10.3390/jmse12060919.

[19] T. Sobb, B. Turnbull, and N. Moustafa, "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions," *Electronics*, vol. 9, no. 11, Nov. 2020, Art. no. 1864, https://doi.org/10.3390/electronics9111864.

[20] N. Rawindaran *et al.*, "Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom," *Digital*, vol. 3, no. 3, pp. 200–231, Aug. 2023, https://doi.org/10.3390/digital3030014.

[21] M. El-Hajj and Z. A. Mirza, "ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool," *Electronics*, vol. 13, no. 19, Oct. 2024, Art. no. 3910, https://doi.org/10.3390/electronics13193910.

[22] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, Feb. 2024. https://doi.org/10.6028/NIST.CSWP.29.

[23] Vanta. "NIST CSF vs. ISO 27001: What's the difference?." Vanta. [Online]. Available: https://www.vanta.com/collection/iso-27001/nist-csf-vs-iso-27001.

[24] G. Volders. "COBIT's Value for Small and Medium Enterprises." ISACA, Nov. 2021. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/cobits-value-for-small-and-medium-enterprises.

[25] A. English. "The Fundamentals of ISO/IEC 27032 – What You Need to Know." PECB Insights, Aug. 2023. [Online]. Available: https://insights.pecb.com/fundamentals-iso-iec-27032-what-you-need-know.

[26] W. C. Barker, W. Fisher, K. Scarfone, and M. Souppaya, "Ransomware risk management : a cybersecurity framework profile," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST IR 8374, Feb. 2022. https://doi.org/10.6028/NIST.IR.8374.

[27] Pivot Point Security. "ISO 27001 vs NIST Cybersecurity Framework: What's the Difference?." Pivot Point Security, Sept. 2024. [Online]. Available: https://www.pivotpointsecurity.com/difference-between-iso-27001-vs-nist-cybersecurity-framework.

[28] R. K. Yin, *Case study research and applications: design and methods*, Sixth edition. Los Angeles: SAGE, 2018.

AUTHORS PROFILE

Lorenzo Biggi is an Information Systems Engineer at the Peruvian University of Applied Sciences (UPC) in Lima, Peru. Passionate about cybersecurity and particularly enthusiastic about red teaming, actively exploring offensive security techniques to identify vulnerabilities and enhance system resilience (u20201a714@upc.edu.pe).

Jorge Rioja is an Information Systems Engineer at the Peruvian University of Applied Sciences in Lima, Peru. He is currently an Information Security intern at Alfin Banco, supporting cybersecurity operations and risk mitigation. He has participated in academic and professional projects involving frameworks such as NIST CSF 2.0 and ISO/IEC 27001. His professional interests include cybersecurity risk management and offensive security (u201710286@upc.edu.pe).

Pedro Castañeda is a RENACYT Researcher and holds a Ph.D. in Systems Engineering, a master's degree in management and information technology management from UNMSM, and a master's degree in Business Administration (MBA) from Universidad ESAN. He has completed doctoral studies in Public Policy and State Management at the Centro de Altos Estudios Nacionales (CAEN). He leads e-brokerage projects, software development and process improvement, using agile and traditional methodologies. He has the following certifications: Project Management Professional (PMP), Scrum Certified Developer (CSD), IBM Certified Professional in Rational Unified Process, and ORACLE Certifications. Areas of Interest: Artificial Intelligence, Software Productivity, Business Intelligence, Data Analytics, Machine Learning, Software Engineering. (Email: pedro.castaneda@untrm.edu.pe, ORCID: https://orcid.org/0000-0003-1865-1293).

Juan Mansilla-Lopez received a bachelor's degree in Systems Engineering from Universidad de Lima in 1997 and a master's degree in Finance from Universidad ESAN in 2011. Since 2022, he has been the coordinator of the Information Systems Engineering program at the Universidad Peruana de Ciencias Aplicadas. His research interests include artificial intelligence, Internet of Things, finance, and stock markets. (Email: pcsijman@upc.edu.pe, ORCID: https://orcid.org/0000-0003-0039-6044).

Alberto Daniel García-Núñez is a Ph.D. candidate in Technology and Innovation Management at Universidad Pontificia Bolivariana (UPB) and holds a Master's in Information Technology Management (ITESM). (Email: alberto.garcia@upb.edu.co, ORCID: https://orcid.org/0000-0002-9402-3785).