Enhancing Information Security in Technology Small and Medium-Sized Enterprises: A Metrics-Driven Model Based on ISO/IEC 27001:2022

Gabriel Quispe-Kobashikawa
Faculty of Information Systems Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
u20201a402@upc.edu.pe

Cesar Zuloaga-Estrada
Faculty of Information Systems Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
u201914170@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
Faculty of Information Systems Engineering, 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: 30 December 2025 | Revised: 9 February 2026 | Accepted: 14 February 2026

 DOI: https://doi.org/10.48084/etasr.17248

ABSTRACT

This paper designs and evaluates an Information Security Management System (ISMS) model tailored for technology-sector Small and Medium-sized Enterprises (SMEs) in Metropolitan Lima. The model integrates the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 standard with operational guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and incorporates decision-support frameworks such as Factor Analysis of Information Risk (FAIR) (for economic impact assessment) and Common Vulnerability Scoring System (CVSS) v3.1 (for vulnerability severity). Structured around the Plan–Do–Check–Act (PDCA) cycle, the model introduces three custom metrics—the Global Model Compliance Metric (GMCM), the Improvement Index per Evaluation Cycle (IIEC), and the Associated Residual Risk Index (ARRI)—to monitor maturity progression and residual risk levels. A six-month pre- and post-implementation evaluation in a single SME showed a 9-percentage-point increase in GMCM and a 22-percentage-point reduction in ARRI, reflecting an improved security control posture while acknowledging the constraints of short-term assessment. The paper presents the theoretical foundation for the proposed hybridization, details the ISO–NIST control mapping, formalizes the new metrics, and explains how FAIR and CVSS jointly inform prioritization. Finally, it discusses threats to validity and outlines a practical adoption roadmap for SMEs. The generalization of results remains tentative and calls for longitudinal replication across multiple organizations.

Keywords-cybersecurity; ISO 27001; SMEs; information security management; risk assessment; NIST; FAIR; PDCA; CVSS

I. INTRODUCTION

The COVID-19 pandemic and the global lockdown of 2020 triggered a sharp rise in cybercrime worldwide, a trend that has continued in subsequent years. This increase has been driven mainly by the widespread adoption of remote communication and collaboration tools, which expanded the attack surface of organizations [1]. Reports indicate a steady growth in cyber threats: detections of malicious files increased by 3% between 2022 and 2023 [2], more than 75% of incidents are associated with phishing and social engineering [3], and phishing cases rose by 442% between the first and second halves of 2024 [4].

In Peru, reports of cybercrime grew by 65% between 2019 and 2021, with around 70% of cases related to fraud and identity theft [5, 6]. At the regional level, Latin American organizations experience an average of 2,569 cybersecurity incidents per week—40% above the global average [7]. This situation is mainly attributed to limited investment in cybersecurity infrastructure and the low adoption of Information Security Management Systems (ISMSs).

Although various technological measures—such as Data Leakage Prevention (DLP) systems, User and Entity Behavior Analytics (UEBA), and advanced access controls—have been implemented, studies show that around 90% of successful phishing attacks stem from human error [8]. Therefore, an effective information security strategy must integrate technological, human, and organizational dimensions.

The persistent rise of cyber threats, together with the resource constraints typical of Small and Medium-sized Enterprises (SMEs), underscores the need for pragmatic and scalable security programs that adhere to international standards while remaining feasible to implement. SMEs, particularly in the technology sector, face recurring challenges such as phishing, credential compromise, and cloud misconfigurations, which are often intensified by limited budgets and personnel.

In response to this challenge, this paper proposes a hybrid ISMS model tailored to technology-sector SMEs in Metropolitan Lima. The model integrates International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 as the structural foundation, harmonizes selected controls with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 to enhance operational applicability, employs Factor Analysis of Information Risk (FAIR) to quantify the economic impact of risks, and uses Common Vulnerability Scoring System (CVSS) v3.1 to assess technical vulnerability severity. The model follows the Plan–Do–Check–Act (PDCA) cycle and introduces three monitoring metrics—the Global Model Compliance Metric (GMCM), the Improvement Index per Evaluation Cycle (IIEC), and the Associated Residual Risk Index (ARRI)—to measure maturity progression and residual risk.

A six-month case study conducted in a local SME showed a 9-percentage-point increase in GMCM and a 22-percentage-point reduction in ARRI, indicating an improved security posture. These results suggest that a hybrid approach can strengthen governance and control efficiency while maintaining feasibility in resource-limited environments. The proposal also outlines a practical adoption roadmap and a risk schedule that links common SME risks with corresponding ISO/NIST controls.

Unlike prior descriptive works on ISO/IEC 27001 adoption, this study integrates ISO, NIST, FAIR, and CVSS under a unified and role-specific framework, introduces measurable metrics for continuous improvement, and defines an ISO–NIST harmonization protocol adapted to the SME context. This contribution aims to provide a structured, evidence-based approach for strengthening information security management in technology-sector SMEs in Metropolitan Lima and, by extension, in similar organizations across Latin America.

To ground this proposal within the existing body of knowledge, the introduction draws on prior research on information security management and risk governance in SMEs. These studies identify key drivers of information loss, their organizational impact, and the constraints SMEs face when adopting international standards.

A. Internal and External Factors Affecting the Loss of Sensitive Information

The five articles analyzed offer a comprehensive view of the internal and external factors that influence the likelihood of incidents related to the loss of sensitive information in business environments. Authors in [9] and [10] highlight internal factors such as security awareness, staff training, and organizational leadership. Authors in [11] emphasize the importance of having adequate security policies and controls in place.

Complementarily, the research analyzed recognizes the impact of external variables, particularly the evolving regulatory framework and the increasing sophistication of cyber threats. However, each academic work addresses this issue from particular perspectives: the industrial process sector [12], the context of the COVID-19 pandemic [9], vulnerabilities to social engineering attacks [11], and privacy challenges in physical access control systems [13].

Authors in [14] show that during the COVID-19 pandemic, both exogenous factors (global disruption and government policies) and endogenous factors (organizational response capacity) led to a notable increase in companies' exposure to security breaches. The temporal analysis reveals a direct correlation between this period and the simultaneous increase in the frequency of incidents, their level of technical complexity, and the volume of compromised information. These results underscore the critical need to develop proactive strategies to anticipate and mitigate risks in crisis scenarios.

B. Cybersecurity Strategies and their Impact on Mitigating Information Leaks

The articles analyzed comprehensively address the cybersecurity models and methodologies applied to counteract information leaks in the business environment. In particular, studies [15] and [16] highlight the adoption of the ISO/IEC 27001 standard as a reference framework for information security management. This standard provides an organized

system of controls and procedures designed to safeguard critical data and reduce the risks associated with their leakage.

On the other hand, studies [17] and [18] analyze the implementation of cryptographic techniques and risk assessment methodologies as measures to prevent information leaks. Among these strategies, the use of advanced encryption algorithms and the systematic identification of vulnerabilities in corporate infrastructures stand out. Complementarily, research [19] and [20] addresses cyber-resilience approaches and layered security architectures, which aim to strengthen organizations' ability to detect, adapt, and respond to threats, thereby reducing the impact of potential breaches of confidential data.

Furthermore, authors in [21] propose a comprehensive framework for cyber risk management, highlighting the need to proactively identify, assess, and manage threats in organizational contexts. Along the same lines, studies [22] and [23] introduce methodologies based on multi-criteria decision techniques and specialized risk analysis models. These approaches facilitate the systematic assessment of threats, allowing actions to be prioritized, key vulnerabilities to be detected, and the distribution of resources to be optimized in order to strengthen IT security.

In the field of information leak prevention, various studies have adopted strategies that combine comprehensive policies, critical success factors, regulatory frameworks, and ethical components. Comparative analyses between industrial sectors and national regulations [24, 25] demonstrate the relevance of implementing robust policies, in addition to highlighting the fundamental role of government agencies in establishing standards and incentive mechanisms. The specialized literature [26-28] also reveals that incorporating ethical principles into decision-making processes can enhance organizational security culture, thereby reducing the likelihood of incidents and improving protection against information leaks.

C. Effects of Information Loss Incidents on Organizational Performance and Positioning

The literature review reveals the significant impact that information loss incidents have on organizational development, affecting key dimensions such as economic growth, competitive position, and corporate reputation. Studies [12] and [29] show consensus in identifying particularly serious consequences for competitiveness and business expansion when security breaches occur. These studies emphasize that maintaining rigorous IT protection standards is essential to preserving stakeholder confidence, while also quantifying the high costs associated with leaks, including both the operational costs of containing incidents and the intangible damage to the institutional image.

A relevant finding from authors in [29] indicates a positive correlation between ISO/IEC 27001 certification and corporate financial performance, reinforcing the strategic value of implementing robust security frameworks. This perspective is complemented by the analysis in [21], which examines in depth the cost-benefit ratio of investments in cybersecurity versus digital risks. The research quantifies how data breaches can slow business development in three main ways: reputational damage, loss of competitive advantage, and erosion of market confidence. While these results are consistent with the conclusions of [12] and [29], authors in [21] provide a more granular analysis of preventive cost structures and their effectiveness in neutralizing cyber threats.

The research in [30] and [31] shows that the consequences of data breaches transcend the economic and reputational spheres, extending even to the deterioration of public trust in public institutions when they are compromised.

As a final finding, the analysis in [32] identifies that low security awareness and the lack of effective strategies to promote it significantly increase exposure to cyber threats, affecting both staff and the organization as a whole. These results are supported by the work in [33], which analyzes organizational behavior patterns in information security. This study emphasizes three critical factors: adherence to established security policies, adequate perception of digital risks, and ongoing staff training. The results show that individual user practices are a determining factor in the effective protection of information assets.

D. Importance of Staff Awareness in Managing Incidents of Information Loss

Authors in [11] highlight the importance of continuously training employees in social engineering techniques and security protocols to mitigate threats such as phishing and malware, thereby reducing the risk of leaks. This perspective coincides with [34], which states that the effectiveness of security controls depends directly on the level of knowledge of the staff, as they are the ones who implement them in practice. Complementarily, authors in [35] analyze the cybersecurity behavior of young adults, identifying psychosocial factors that influence their practices and, therefore, organizational security. These findings broaden the understanding of how basic security training affects emotional and cognitive responses to cyberattacks, as demonstrated by authors in [36], who studied the psychological impact of digital victimization.

Such evidence suggests that awareness strategies should integrate both technical and emotional components, an approach supported by authors in [37] and [38], who propose personalized programs that combine specialized training with psychological principles and persuasive communication techniques. In this way, organizations can tailor awareness initiatives to individual needs, improving their effectiveness. In line with this, authors in [39] confirm that the degree of staff awareness is crucial to preventing, detecting, and responding to data loss incidents, highlighting how everyday practices (password management, account use) directly impact corporate security. The study underscores the importance of clear policies, ongoing training, and organizational support to strengthen the security culture in companies.

II. MODEL DESIGN

This section explores the tools used to develop the information security model, detailing the purpose of each and how it will be implemented during the model's adoption.

The hybrid integration of ISO/IEC 27001, NIST SP 800-53, FAIR, and CVSS v3.1 within the proposed model is grounded

in the complementary nature of these frameworks across strategic, operational, economic, and technical dimensions. ISO/IEC 27001 provides the governance and process foundation for an ISMS through its PDCA-based structure and risk management principles. However, its prescriptive guidance can be limited for SMEs operating in dynamic environments. To address this limitation, NIST SP 800-53 contributes operational granularity and explicit control implementation guidance, reinforcing the technical feasibility and practical depth of ISO-based programs [16, 20].

The integration is further strengthened by incorporating FAIR, which provides a quantitative method for estimating economic impact and aligning risk treatment with business tolerance, and CVSS v3.1, which supplies standardized metrics to assess technical vulnerability severity and prioritize remediation. Together, these frameworks bridge strategic risk quantification and operational vulnerability management, creating a closed loop between governance, control implementation, and measurable risk valuation.

Other frameworks, such as Control Objectives for Information and Related Technologies (COBIT) 2019 and ISO/IEC 27005, were reviewed but not included in the proposed model. COBIT 2019 was excluded due to its governance-centric focus and limited support for quantitative risk analysis, which would overlap with ISO/IEC 27001. ISO/IEC 27005, although conceptually relevant, was used only as a reference because its analytical components largely overlap with FAIR and NIST SP 800-53. As a result, the proposed layered architecture enables interoperability across governance, control, and data-driven approaches, addressing limitations of single-framework models while ensuring theoretical consistency and operational applicability.

A. Description of the Proposed Model

The implementation of the proposed model (Table I) follows the PDCA continuous improvement cycle, also known as the Deming cycle, ensuring a systematic and structured approach to information security management, following the best practices stipulated by the ISO/IEC 27001 standard. This model was proposed in [40]:

- Plan: This phase begins with a gap analysis, the objective of which is to identify deficiencies in current security management and highlight the characteristics that separate it from the desired state. Based on this analysis, the scope of the ISMS is defined, specifying the areas and processes that will be addressed in the implementation. In addition, the current security policies are mapped, and the inventory of assets corresponding to the selected areas and processes is reviewed or prepared. This stage is key, as it lays the foundation for structured risk management aligned with the organization's strategic objectives. Likewise, the first audit is carried out in this phase, which will serve as a baseline to evaluate the effectiveness of the model and determine whether information security has improved with its implementation, by comparing the results with the audit that will be carried out in the Check phase.
- Do: During this phase, the risk treatment plans defined based on the gap analysis and the audit carried out in the Plan phase are implemented. The corresponding controls are applied, and training is provided to all personnel related to the areas and processes defined in the previous phase. This stage corresponds to the implementation phase and focuses on mitigating the identified risks.
- Check: During this phase, the results of the implementation in the Do phase are evaluated. To do this, a second audit of the company is carried out to evaluate the performance of the ISMS, assessing the effectiveness of the controls implemented through the use of performance metrics. Its purpose is to identify possible deviations from the plan, allowing informed decisions to be made and corrective measures to be applied in a timely manner, in order to ensure compliance with the security objectives established at the start of implementation.
- Act: Continuous improvements and corrective and preventive actions are applied based on the results obtained in the previous stage. This phase is essential to adapt the ISMS to the changing environment to which the organization is exposed and to continuously optimize the level of information security through policies and the structured system.

TABLE I. PDCA PHASES

Phase	Main activities in the proposed model
Plan	Gap analysis; ISMS scope definition; policy and asset inventory review; baseline audit (scored 0–100) to establish GMCM and identify <70% controls; initial risk matrix setup
Do	Implement risk-treatment plans for prioritized controls; deploy technical and organizational measures (e.g., access-control hardening, DLP configuration, logging); conduct awareness/training actions for relevant staff
Check	Six-month re-audit using the same instrument; compute GMCM and ARRI; compare cycles and compute IIEC; review FAIR×CVSS prioritization against observed improvements
Act	Corrective and preventive actions based on audit gaps; update risk matrix and control owners; adjust procedures and monitoring; feed lessons learned into the next PDCA cycle

The proposed model integrates ISO/IEC 27001:2022, NIST SP 800-53 [41], FAIR, and CVSS to support risk management and ISMS governance, primarily through a risk matrix and a web application designed to assist audit activities in the Plan and Check phases. The process begins with assessing the organization's current state and classifying information assets, which are then mapped to the corresponding ISO/IEC 27001 controls and their harmonized NIST SP 800-53 equivalents.

Aligned with ISO/IEC 27001:2022, the model incorporates updated controls addressing emerging threats and cloud-centric environments, enhancing organizational resilience and adaptability. Identified vulnerabilities, threats, and risks are evaluated using FAIR to estimate economic impact and CVSS to determine technical criticality, enabling prioritized mitigation and continuous updates to the risk matrix. As ISMS maturity increases, CVSS temporal and environmental metrics allow vulnerability severity to be contextualized to the organization.

To support audits, a web-based application assesses ISMS maturity through a structured questionnaire, stores historical

results, and facilitates longitudinal analysis of the evolution of the security posture.

B. Harmonization Device

To create a specialized model tailored to the specific needs of the selected technology sector, the study in [40] reduced the number of controls to be implemented. Initially, the ISO/IEC 27001:2022 standard provides a total of 93 controls, divided into four categories: organizational, people, physical, and technological. However, it was decided to reduce the number of controls based on two key criteria.

First, those controls directly related to the issue addressed—information leakage—were selected, prioritizing controls associated with confidentiality within the Confidentiality, Integrity, and Availability (CIA) triad. Second, all controls in the people category were included, given that, as mentioned in previous studies, the human factor is crucial to effectively address information leakage. After this selection process, 36 controls were obtained, which were used to evaluate companies in the sector.

This control set tailoring (93 to 36) process inevitably de-emphasizes controls related to Integrity and Availability, which could introduce potential bias in the resulting ISMS. To mitigate this effect, compensatory monitoring mechanisms were considered, as discussed in Section III, ensuring that the reduction in the number of controls does not compromise the organization's overall security posture.

To ensure proper implementation and compliance with the selected controls, the study in [40] decided to enrich the ISO/IEC 27001 standard using the NIST SP 800-53 framework, whose controls were aligned with the 36 previously selected controls (see Tables II, III, IV, and V).

TABLE II. ISO/IEC 27001:2022 CONTROL 5 – NIST MAPPING

ISO control	ISO control name	Mapped NIST SP 800-53 controls/families
5.1	Policies for information security	All XX-1 controls
5.2	Information security roles and responsibilities	All XX-1 controls; CM-4; CP-2; PS-7; BS-8; SA-3; SA-9; PM-2; PM-10
5.3	Segregation of duties	AC-5
5.9	Inventory of information and other associated assets	CM-8
5.16	Acceptable use of information and other associated assets	MP-2; MP-4; MP-5; MP-6; MP-7; PE-16; PE-18; PE-20; PL-4; SC-8; SC-26
5.12	Classification of information	RA-2
5.13	Labeling of information	MP-3; PE-22
5.17	Authentication information	IA-5
5.18	Access rights	AC-2
5.19	Information security in supplier relationships	SR-1
5.20	Addressing information security within supplier agreements	SA-4; SR-3
5.22	Monitoring, review, and change management of supplier services	RA-3; SA-3; SR-6; SR-7
5.23	Information security for use of cloud services	SA-1; SA-4; SA-9; SA-2(3); SR-5

TABLE III. ISO/IEC 27001:2022 CONTROL 6 – NIST MAPPING

ISO control	ISO control name	Mapped NIST SP 800-53 controls/families
6.1	Screening	PS-3; SA-21
6.2	Terms and conditions of employment	PL-4; PS-5
6.3	Information security awareness, education, and training	AT-2; AT-3; CP-3; IR-2; PM-13
6.4	Disciplinary process	PS-8
6.5	Responsibilities after termination or change of employment	PS-4; PS-5
6.6	Confidentiality or non-disclosure agreements	PS-6
6.7	Remote working	None
6.8	Information security event reporting	AU-6; IR-6; SI-2

TABLE IV. ISO/IEC 27001:2022 CONTROL 7 – NIST MAPPING

ISO control	ISO control name	Mapped NIST SP 800-53 controls/families
7.7	Clear desk and clear screen	AC-11; MP-2; MP-4
7.9	Security of assets off-premises	AC-19; AC-20; MP-5; PE-17
7.10	Storage media	MA-2; MP-2; MP-4; MP-5; MP-6; MP-7; PE-16
7.14	Secure disposal or re-use of equipment	MP-6

TABLE V. ISO/IEC 27001:2022 CONTROL 8 – NIST MAPPING

ISO control	ISO control name	Mapped NIST SP 800-53 controls/families
8.1	User end point devices	AC-11
8.3	Information access restriction	AC-3; AC-24
8.4	Access to source code	AC-3; AC-11; CM-5
8.10	Information deletion	AU-13; PE-3(2); PE-19; SC-7(10); SI-20
8.11	Data masking	AC-4(25); AC-7(2); MA-2; MA-3(3); MA-4(6); MP-4; MP-6; MP-6(1); SI-21
8.12	Data leakage prevention	AC-4(23); SI-19(4)
8.13	Information backup	CP-9
8.24	Use of cryptography	SC-12; SC-13; SC-17
8.28	Secure coding	SA-4(3); SA-8; SA-11(1); SA-15(5); SI-10
8.32	Change management	CM-2; CM-5; SA-10; SI-2
8.33	Test information	SA-5(2)

This ISO–NIST harmonization protocol consisted of a three-step process: (i) semantic alignment, ensuring correspondence between the objectives and implementation scope of each control; (ii) granularity normalization, in which ISO and NIST controls were split or merged when necessary, given that NIST tends to provide finer-grained specifications; and (iii) a non-redundancy check, aimed at preventing overlapping or double-counting of equivalent controls.

Any disagreements in the mapping process were resolved by consensus and formally documented, establishing a replicable methodology that enhances transparency and traceability in the control harmonization process. Future iterations of the model propose the inclusion of inter-rater

reliability measurements to quantitatively assess the consistency of mappings among evaluators.

This alignment provides detailed guidance for the implementation of each control, combining the structured and strategic nature of ISO with the technical and operational specificity of NIST, thereby reinforcing the effectiveness of the model in protecting against information leakage and improving its adaptability to the operational context of the technology sector.

C. Asset Classification Methodology

Proper asset valuation is a critical phase in the effective implementation of organizational ISMSs. This methodological process facilitates the identification, classification, and prioritization of assets based on their intrinsic characteristics, functionality, and level of criticality, thus laying the foundation for developing accurate risk analyses, designing appropriate controls, and defining clear accountability frameworks.

Each organization must establish its own categorical framework for the systematic grouping of assets, which should reflect its specific needs and operational context. This customization ensures that the classification meets the particular requirements of the entity, optimizing the usefulness of the valuation process.

D. Vulnerability Assessment

Vulnerability assessment is a core component of information security management, enabling the systematic identification, measurement, and prioritization of weaknesses that may compromise confidentiality, integrity, and availability. By providing a realistic view of risk exposure, it supports the implementation of controls aligned with asset criticality. This process incorporates organizational and contextual factors—such as technological architecture, critical services, and operational conditions—and is operationalized through the application of CVSS metrics tailored to each risk scenario.

E. Threat Identification

Threat assessment and characterization are core components of IT security management, enabling organizations to identify, analyze, and prioritize risks that may compromise confidentiality, integrity, and availability. A structured evaluation process supports objective risk quantification, alignment of protection measures with asset criticality, and optimized allocation of security resources, while accounting for organizational context such as technological architecture, critical services, operating conditions, and sector-specific threat landscapes.

In the proposed model, risk evaluation combines FAIR and CVSS to integrate financial and technical perspectives within a unified decision framework. FAIR is used to estimate the potential economic impact of risk materialization for each asset–threat pair, based on historical data, internal records, and expert input, whereas CVSS v3.1 provides standardized severity scores for associated vulnerabilities, incorporating Base metrics and contextual temporal or environmental adjustments when applicable.

The outputs of both models are consolidated into a FAIR×CVSS matrix, enabling objective prioritization of remediation actions according to financial exposure and technical severity. Scenario-based FAIR analysis estimates loss event frequency and magnitude, using calibrated ranges when empirical data are limited, whereas CVSS scoring relies on observable evidence and conservative assumptions to ensure consistency and reproducibility.

Finally, to integrate the results of both methodologies, a Decision Logic (FAIR×CVSS) matrix was developed. Rather than aggregating FAIR's monetary outputs and CVSS's numerical scores (0–10) into a single value, a bi-criteria prioritization matrix was constructed:

- Quadrant I (high impact & high severity): top-priority remediation actions
- Quadrant II (high impact & low severity): strategic controls and monitoring
- Quadrant III (low impact & high severity): quick-win mitigations
- Quadrant IV (low impact & low severity): deferred actions or backlog

This dual-criteria approach preserves interpretability and auditability, allowing decision-makers to balance financial risk and technical exposure without oversimplifying the underlying data relationships.

F. Context of Application of the Research

The model was implemented over a six-month period in a technology consulting SME in Metropolitan Lima serving approximately 51 client companies. The organization, with around 20 employees and a centralized management structure, represents a typical SME environment; specific details are omitted for confidentiality. The implementation covered all functional areas, providing a representative setting to validate the model's effectiveness under common SME constraints such as limited resources, high client interdependence, and the need for efficient information security management. The ISMS scope for this study focused on the internal processes and assets directly involved in service delivery and information handling (e.g., access management, endpoints used for operations, service documentation repositories, incident-handling routines, and supporting administrative records). The study was designed to reflect common SME constraints, including limited dedicated security roles, constrained training time, and a preference for measures that can be evidenced through auditable artifacts (policies, configurations, logs, tickets, and records) rather than informal practices.

III. CASE STUDY PROTOCOL AND DATA COLLECTION

This study follows a single-case design to evaluate the feasibility and short-term effects of the proposed hybrid ISMS model in a real SME setting. The case organization is a technology consulting SME located in Metropolitan Lima (Peru) that provides IT services to approximately 51 client companies. At the time of implementation, the SME had ~20

employees and a centralized management structure. The company name and certain operational details are withheld for confidentiality.

- Scope and timeline: The implementation covered all functional areas (administrative, operational, and technical) over a six-month window. Two evaluation cycles were performed: (i) a baseline assessment during the Plan phase (T0) and (ii) a follow-up assessment after six months of treatment implementation (T1) during the Check phase.
- Data collection and audit instrument: Compliance with the selected ISO/IEC 27001:2022 controls was measured through structured internal audits using the same questionnaire and scoring rubric in both cycles. Each control was scored on a 0–100 scale based on observable evidence (policies, configurations, logs, records, and interviews with control owners). Evidence was recorded and validated by peer review to reduce evaluator bias. Controls scoring <70% were classified as non-compliant for the purpose of ARRI.
- Implementation actions between T0 and T1: Based on the baseline gap analysis and the FAIR×CVSS prioritization logic, the organization executed risk-treatment actions aligned with the selected controls, including access-control hardening and account lifecycle adjustments, improvements in logging/monitoring practices, deployment/configuration of DLP capabilities, and procedural updates for asset handling. Awareness activities were planned; however, the execution of training sessions was constrained by operational workload, as discussed in Section V.A.
- Metric computation traceability: GMCM was computed as the mean compliance across the implemented control set. IIEC represents the change in GMCM between T0 and T1. ARRI was computed as the proportion of controls below 70% compliance at each cycle. These metrics provide an auditable link between raw audit scores and the summarized results reported in Section V.

IV. METRICS

To evaluate the evolution of the proposed model over time and determine whether there have been significant improvements in the company in terms of compliance with controls, three aggregate metrics have been defined that allow for a comparative analysis between the different evaluation cycles.

A. Global Model Compliance Metric

The GMCM provides an overview of the model's implementation status, considering the percentage of compliance with all controls applied:

$$\text{GMCM} = \left(\frac{\sum_{i=1}^{n} C_1}{n}\right) \times 100 \quad (1)$$

where:

- C_i: percentage of compliance with control i
- n: total number of controls implemented (36 in this model)

Interpretation:

- ≥ 90% → Excellent implementation
- 80–90% → Good implementation
- 70–79% → Acceptable with improvements
- <70% → Needs immediate intervention

B. Improvement Index per Evaluation Cycle

The IIEC allows for the quantification of progress made between two consecutive evaluation cycles, reflecting progress or regression in the implementation of the model:

$$\text{IIEC} = \text{GMCM}_n - \text{GMCM}_{n-1} \quad (2)$$

where:

- GMCM_n: current evaluation cycle
- GMCM_{n-1}: the previous cycle

Interpretation:

- IIEC > 0 → Improvement
- IIEC = 0 → No change
- IIEC < 0 → Decline

C. Associated Residual Risk Index

The ARRI measures the proportion of critical controls (those with less than 70% compliance) that remain unresolved, allowing the level of residual risk present in the organization to be identified:

$$\text{ARRI} = \left(\frac{N_{controls<70\%}}{n}\right) \times 100 \quad (3)$$

Interpretation:

- <10% → Low risk
- 10–20% → Medium risk
- 20% → High risk

The three metrics proposed in this study—GMCM, IIEC, and ARRI—were conceptually derived from the performance measurement principles outlined in ISO/IEC 27004:2016, which establishes quantitative indicators for evaluating the effectiveness of information security controls, and from the control effectiveness metrics described in NIST SP 800-55 Rev. 1.

Their operationalization followed a three-stage process: (i) construct definition, specifying the dimension of performance each metric represents (compliance, improvement rate, residual risk); (ii) scaling and normalization, ensuring comparability between cycles and organizations; and (iii) content validation through expert judgment. Three independent information-security specialists reviewed the indicators for clarity, relevance, and consistency, achieving full consensus on their interpretability and applicability to SMEs.

The metrics were empirically tested during the pilot phase through pre- and post-implementation assessments, confirming their ability to capture observable maturity progression. For future validation, we propose correlating GMCM, IIEC, and

ARRI with actual incident frequency and external audit outcomes across multiple SMEs, thereby establishing criterion-related validity and longitudinal reliability.

V. RESULTS

Based on the assessment carried out on the company during the planning phase, as well as after a period of six months following the implementation of the proposed model, a significant improvement was observed in the level of compliance with the controls established by the ISO/IEC 27001:2022 standard. The model included a total of 36 selected controls, which were evaluated using three predefined metrics: GMCM, IIEC, and ARRI.

A. Compliance with ISO 27001 Controls

During the initial assessment, 15 controls with a rating below 70% were identified and considered non-compliant. In the second assessment, carried out six months after the model was implemented, this number was reduced to 7 controls, reflecting an improvement in the level of compliance and greater maturity in information security management.

In operational terms, the number of non-compliant controls decreased from 15 at T0 to 7 at T1 (out of 36 total controls). This indicates that eight controls crossed the 70% compliance threshold within a single PDCA cycle. The remaining non-compliant controls were largely those requiring sustained organizational effort (e.g., workforce screening and structured awareness programs) or those associated with software-development practices that were not core to the company's operating model.

The controls that continued to receive a failing score were as follows:

- 6.01 – Background checks
- 6.03 – Information security awareness, education, and training
- 8.04 – Access to source code
- 8.24 – Use of cryptography
- 8.28 – Secure coding
- 8.33 – Test information

Each of these controls had specific limitations:

- Control 6.03 declined because, during the implementation period, no staff training sessions were held due to the company's high operational workload.
- Control 8.04 remained disapproved because the company does not develop code centrally; rather, certain coding tasks are performed individually by the operations department, without direct supervision.
- Control 8.24 also declined, as the implementation of cryptographic methods was not prioritized, since efforts were focused on the implementation of DLP tools.
- Controls 8.28 and 8.33 remained disapproved, as software development is not an essential function in the company's operations, and secure coding and test data handling are not considered relevant in its current processes.

B. Evaluation Metric Results

The results obtained by applying the defined metrics show an improvement in overall compliance:

1. Global Model Compliance Metric:
   - Initial evaluation: 74.36%
   - Subsequent evaluation: 83.36%
   - Increase: 9 percentage points
2. Improvement Index per Evaluation Cycle:
   - Calculated value: 9, corresponding to the difference between the two GMCM evaluations.
3. Associated Residual Risk Index:
   - Initial evaluation: 41.67% of controls with less than 70% compliance.
   - **S**ubsequent evaluation: 19.44%, which shows a significant reduction in the risk of non-compliance.

Beyond the aggregate values, the audit evidence at T1 showed a shift toward more consistent governance traceability (i.e., artifacts and records supporting the existence and repeatability of controls), which is a key precursor of sustained ISMS maturity in SMEs. However, improvements were not uniform across control types, reinforcing the need to interpret GMCM gains alongside the specific controls that remained below the threshold.

These results suggest preliminary improvement trends rather than conclusive effectiveness, given the limited six-month observation window. The findings should be interpreted as indicative evidence of short-term maturity gains. Future longitudinal replications (18–24 months, multi-company) are necessary to evaluate sustained impact and validate causal relationships between model adoption and security posture improvement.

VI. DISCUSSION

The implementation of the proposed ISO/IEC 27001:2022–based model led to a measurable improvement in information security compliance, with a 9-percentage-point increase in GMCM and a reduction of over 22 percentage points in ARRI, indicating a more mature security posture. Unlike traditional audit-based approaches, the model uses metric-driven monitoring (GMCM, IIEC, and ARRI) to enable quantitative tracking and informed decision-making. Although derived from a single case study, the use of 36 representative controls suggests that the model is adaptable to SMEs with similar resource constraints.

A relevant implementation insight is that the observed gains were driven mainly by controls that can be improved through discrete, evidence-friendly actions (documentation, configuration hardening, operational records), whereas people-centric controls remained more sensitive to time availability and workload. This is consistent with the decline observed in

Control 6.03, where formal training sessions were not executed during the implementation window due to operational constraints, illustrating a typical SME barrier that directly affects human-factor maturity.

From a practical perspective, the proposed model offers step-by-step guidance for SMEs seeking to strengthen their information security posture without undergoing the costly implementation of the full ISO/IEC 27001 standard. The process can be summarized as follows:

1. Scope definition and gap analysis, including clause review and Annex A preselection.
2. Asset inventory and classification, linking assets to relevant ISO controls and corresponding NIST SP 800-53 families.
3. ISO↔NIST harmonization mapping following the protocol described in Section II.B.
4. Baseline audit, using a structured instrument with observable rubrics (scored 0–100).
5. FAIR scenario construction and CVSS scoring, as detailed in Sections II.D and II.E.
6. Risk-treatment planning, applying the bicriteria FAIR×CVSS prioritization matrix.
7. Training and awareness programs, focusing on human-factor controls.
8. Re-audit and metric reassessment (GMCM, IIEC, ARRI) to track improvement and adjust the security plan.

An illustrative risk schedule links common data leakage vectors to their corresponding ISO/NIST controls, enabling SMEs to directly associate mitigation efforts with relevant threat scenarios. Certain controls received lower ratings due to the organization's operating context—particularly those related to secure software development, which were not prioritized given the absence of a formal development function—highlighting the need to adapt ISO/IEC 27001 implementations to avoid inefficient resource allocation.

The proposed hybrid approach contributes to ISMS research by bridging compliance-oriented frameworks (ISO/NIST) with quantitative risk evaluation methods (FAIR/CVSS), operationalizing metrics-driven security governance and extending existing theory toward practical, evidence-based application in resource-constrained SMEs.

Finally, several threats to validity were identified during the study:

- Internal validity: potential Hawthorne effect, concurrent organizational changes, and evaluator bias—mitigated through standardized rubrics and peer review.
- Construct validity: reliance on bespoke metrics (GMCM, IIEC, ARRI) without external validation; future research should correlate these with actual incident data.
- External validity: results are limited to a single SME in Metropolitan Lima; cross-sector replications are recommended.
- Conclusion validity: the short observation window (N=1, T=2) precludes statistical inference, though trends suggest positive outcomes.

VII. CONCLUSION

The implementation of the proposed model resulted in a measurable improvement in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 compliance, with a 9-percentage-point increase in the Global Model Compliance Metric (GMCM) and a reduction of the Associated Residual Risk Index (ARRI) from 41.67% to 19.44%, indicating a strengthened security posture. These results show that an adaptive hybrid model aligned with ISO/IEC 27001:2022 and supported by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Factor Analysis of Information Risk (FAIR), and Common Vulnerability Scoring System (CVSS) effectively guides Small and Medium-sized Enterprises (SMEs) in improving their Information Security Management System (ISMS) under resource constraints, enabling short-term, quantifiable progress with limited operational overhead.

The model's practical value lies in its applicability to resource-limited organizations, offering metric-based prioritization, contextual flexibility, and scalable adoption. A limitation identified was the low adoption of certain controls with limited operational relevance, highlighting the need for sector- and context-specific customization. Future work should include longitudinal validation over 18–24 months, assessment of inter-rater reliability, and the incorporation of visual statistical monitoring tools, as well as the publication of anonymized instruments and datasets to support broader validation.

ACKNOWLEDGMENT

The authors are grateful to the Dirección de Investigación of the Universidad Peruana de Ciencias Aplicadas for the support provided for this research work through the UPC-EXPOST-2026-1 incentive.

REFERENCES

[1] "Cost of a data breach 2025." IBM. https://www.ibm.com/reports/data-breach.

[2] "Rising threats: cybercriminals unleash 411,000 malicious files daily in 2023." Kaspersky. https://www.kaspersky.com/about/press-releases/rising-threats-cybercriminals-unleash-411000-malicious-files-daily-in-2023.

[3] "CrowdStrike 2024 Global Threat Report." CrowdStrike. https://www.crowdstrike.com/en-us/resources/reports/crowdstrike-2024-global-threat-report/.

[4] "CrowdStrike 2025 Global Threat Report." CrowdStrike. https://go.crowdstrike.com/2025-global-threat-report.html.

[5] "Ciberdelincuencia: Reporte de información estadística y recomendaciones para la prevención." Ministerio de Justicia y Derechos Humanos del Perú. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf.

[6] "La ciberdelincuencia en el Perú: Estrategias y retos del Estado." Defensoría del Pueblo. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf.

[7] "LatAm Orgs Face 40% More Attacks Than Global Average." Dark Reading. https://www.darkreading.com/cybersecurity-analytics/latin-american-orgs-more-cyberattacks-global-average.

[8] C. Tse, B. Lu, and B. S. Ghuman. "Real-Time Anti-Phishing: Essential Defense Against Evolving Cyber Threats." Fortinet Blog. https://www.fortinet.com/blog/threat-research/real-time-anti-phishing-essential-defense-against-evolving-cyber-threats.

[9] A. F. Al-Qahtani and S. Cresci, "The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19," *IET Information Security*, vol. 16, no. 5, pp. 324–345, July 2022, https://doi.org/10.1049/ise2.12073.

[10] Y. Hong, M.-J. Kim, and T. Roh, "Mitigating the Impact of Work Overload on Cybersecurity Behavior: The Moderating Influence of Corporate Ethics—A Mediated Moderation Analysis," *Sustainability*, vol. 15, no. 19, Sept. 2023, Art. no. 14327, https://doi.org/10.3390/su151914327.

[11] T. Li, C. Song, and Q. Pang, "Defending against social engineering attacks: A security pattern-based analysis framework," *IET Information Security*, vol. 17, no. 4, pp. 703–726, July 2023, https://doi.org/10.1049/ise2.12125.

[12] M. Iaiani, A. Tugnoli, S. Bonvicini, and V. Cozzani, "Analysis of Cybersecurity-related Incidents in the Process Industry," *Reliability Engineering & System Safety*, vol. 209, May 2021, Art. no. 107485, https://doi.org/10.1016/j.ress.2021.107485.

[13] J. García-Rodríguez, S. Krenn, and D. Slamanig, "To pass or not to pass: Privacy-preserving physical access control," *Computers & Security*, vol. 136, Jan. 2024, Art. no. 103566, https://doi.org/10.1016/j.cose.2023.103566.

[14] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, June 2021, Art. no. 102248, https://doi.org/10.1016/j.cose.2021.102248.

[15] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustainability*, vol. 15, no. 7, Mar. 2023, Art. no. 5828, https://doi.org/10.3390/su15075828.

[16] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Mar. 2021, https://doi.org/10.1108/TQM-09-2020-0202.

[17] F. Djebbar and K. Nordström, "A Comparative Analysis of Industrial Cybersecurity Standards," *IEEE Access*, vol. 11, pp. 85315–85332, 2023, https://doi.org/10.1109/ACCESS.2023.3303205.

[18] J. Zhang *et al.*, "ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks," *Computer Networks*, vol. 245, May 2024, Art. no. 110376, https://doi.org/10.1016/j.comnet.2024.110376.

[19] S.-H. Choi, J. Youn, K. Kim, S. Lee, O.-J. Kwon, and D. Shin, "Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement," *Sustainability*, vol. 15, no. 18, Sept. 2023, Art. no. 13404, https://doi.org/10.3390/su151813404.

[20] B. Valkenburg and I. Bongiovanni, "Unravelling the three lines model in cybersecurity: a systematic literature review," *Computers & Security*, vol. 139, Apr. 2024, Art. no. 103708, https://doi.org/10.1016/j.cose.2024.103708.

[21] I. Lee, "Cybersecurity: Risk management framework and investment cost analysis," *Business Horizons*, vol. 64, no. 5, pp. 659–671, Sept. 2021, https://doi.org/10.1016/j.bushor.2021.02.022.

[22] A. Abdiraman, N. Goranin, S. Balevicius, A. Nurusheva, and I. Tumasonienė, "Application of Multicriteria Methods for Improvement of Information Security Metrics," *Sustainability*, vol. 15, no. 10, May 2023, Art. no. 8114, https://doi.org/10.3390/su15108114.

[23] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "When Security Risk Assessment Meets Advanced Metering Infrastructure: Identifying the Appropriate Method," *Sustainability*, vol. 15, no. 12, June 2023, Art. no. 9812, https://doi.org/10.3390/su15129812.

[24] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers & Security*, vol. 120, Sept. 2022, Art. no. 102820, https://doi.org/10.1016/j.cose.2022.102820.

[25] M. Weiss and F. Biermann, "Cyberspace and the protection of critical national infrastructure," *Journal of Economic Policy Reform*, vol. 26, no. 3, pp. 250–267, July 2023, https://doi.org/10.1080/17487870.2021.1905530.

[26] W. Yeoh, S. Wang, A. Popovič, and N. H. Chowdhury, "A systematic synthesis of critical success factors for cybersecurity," *Computers & Security*, vol. 118, July 2022, Art. no. 102724, https://doi.org/10.1016/j.cose.2022.102724.

[27] J. Fenech, D. Richards, and P. Formosa, "Ethical principles shaping values-based cybersecurity decision-making," *Computers & Security*, vol. 140, May 2024, Art. no. 103795, https://doi.org/10.1016/j.cose.2024.103795.

[28] A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity Enterprises Policies: A Comparative Study," *Sensors*, vol. 22, no. 2, Jan. 2022, Art. no. 538, https://doi.org/10.3390/s22020538.

[29] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, "Information security and value creation: The performance implications of ISO/IEC 27001," *Computers in Industry*, vol. 142, Nov. 2022, Art. no. 103744, https://doi.org/10.1016/j.compind.2022.103744.

[30] R. Shandler and M. A. Gomez, "The hidden threat of cyber-attacks – undermining public confidence in government," *Journal of Information Technology & Politics*, vol. 20, no. 4, pp. 359–374, Oct. 2023, https://doi.org/10.1080/19331681.2022.2112796.

[31] A. Alharbi *et al.*, "Analyzing the Impact of Cyber Security Related Attributes for Intrusion Detection Systems," *Sustainability*, vol. 13, no. 22, Nov. 2021, Art. no. 12337, https://doi.org/10.3390/su132212337.

[32] D. Baltuttis, T. Teubner, and M. T. P. Adam, "A typology of cybersecurity behavior among knowledge workers," *Computers & Security*, vol. 140, May 2024, Art. no. 103741, https://doi.org/10.1016/j.cose.2024.103741.

[33] E. Thron, S. Faily, H. Dogan, and M. Freer, "Human factors and cyber-security risks on the railway – the critical role played by signalling operations," *Information and Computer Security*, vol. 32, no. 2, pp. 236–263, Jan. 2024, https://doi.org/10.1108/ICS-05-2023-0078.

[34] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry," *Sustainability*, vol. 14, no. 3, Jan. 2022, Art. no. 1269, https://doi.org/10.3390/su14031269.

[35] M. Alanazi, M. Freeman, and H. Tootell, "Exploring the factors that influence the cybersecurity behaviors of young adults," *Computers in Human Behavior*, vol. 136, Nov. 2022, Art. no. 107376, https://doi.org/10.1016/j.chb.2022.107376.

[36] A. Palassis, C. P. Speelman, and J. A. Pooley, "An Exploration of the Psychological Impact of Hacking Victimization," *Sage Open*, vol. 11, no. 4, Oct. 2021, Art. no. 21582440211061556, https://doi.org/10.1177/21582440211061556.

[37] J. Kävrestad, S. Furnell, and M. Nohlberg, "User perception of Context-Based Micro-Training – a method for cybersecurity training," *Information Security Journal: A Global Perspective*, vol. 33, no. 2, pp. 121–137, Mar. 2024, https://doi.org/10.1080/19393555.2023.2222713.

[38] M. Alshaikh, S. B. Maynard, and A. Ahmad, "Applying social marketing to evaluate current security education training and awareness programs in organisations," *Computers & Security*, vol. 100, Jan. 2021, Art. no. 102090, https://doi.org/10.1016/j.cose.2020.102090.

[39] S. Saeed, "Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia," *Sustainability*, vol. 15, no. 7, Mar. 2023, Art. no. 6019, https://doi.org/10.3390/su15076019.

[40] G. O. Quispe, C. K. Zuloaga, and P. S. Castañeda, "Mitigating Information Leakage in Tech-Sector SMEs: Implementing ISO 27001:2022 for Comprehensive Security," in *11th International*

Conference on Information Management, London, UK, 2025, pp. 273–285, https://doi.org/10.1007/978-3-031-99353-4_24.

[41] L. Biggi, J. Rioja, P. Castaneda, J. Mansilla-Lopez, and A. D. Garcia-Nunez, "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," *Engineering, Technology & Applied Science Research*, vol. 15, no. 6, pp. 30015–30025, Dec. 2025, https://doi.org/10.48084/etasr.12948.

AUTHORS PROFILE

Gabriel Quispe-Kobashikawa is an Information Systems Engineering student at Peruvian University of Applied Sciences (UPC) in Lima, Peru. (Email: u20201a402@upc.edu.pe)

Cesar Zuloaga-Estrada is an Information Systems Engineering student at Peruvian University of Applied Sciences (UPC) in Lima, Peru. (Email: u201914170@upc.edu.pe)

Pedro Castaneda is a RENACYT Researcher and holds a PhD in Systems Engineering, a Master's degree in Management and Information Technology from UNMSM and in Business Administration (MBA) from ESAN. He has completed doctoral studies in Public Policy and State Management at the Centro de Altos Estudios Nacionales (CAEN). He leads projects in e-brokerage, software development, and process improvement, using agile and traditional methodologies. Certifications include Project Management Professional (PMP), Scrum Certified Developer (CSD), IBM Certified Professional in Rational Unified Process, and ORACLE certifications. His research interests include Artificial Intelligence, Software Productivity, Business Intelligence, Data Analytics, Machine Learning, and 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 (1997) and a Master's degree in Finance from Universidad ESAN (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 Garcia-Nunez is a doctoral student in Technology and Innovation Management at Universidad Pontificia Bolivariana (UPB) and holds a Master's degree in Information Technology Management (ITESM). (Email: alberto.garcia@upb.edu.co, ORCID: https://orcid.org/0000-0002-9402-3785)