

Hybrid Information Security Framework Based on ISO/IEC 27005:2022 and the NIST Framework for the Ministry of Education of Ecuador (TIC)

Jayli De la Torre[1(✉)], Daisy Imbaquingo[1,2], and Jaime Llumiquinga[1]

[1] Facultad de Postgrados, Universidad Técnica del Norte, 100105 Ibarra, Ecuador
{jddelatorrer,jgllumiquinga}@utn.edu.ec,
daisy.imbaquingoe@info.unlp.edu.ar

[2] Universidad Nacional de La Plata, Posgrado de Ciencias Informáticas, 1900 La Plata, Argentina

Abstract. Currently, the National Directorate of Information and Communication Technologies (NDICT) of the Ministry of Education (MOE) of Ecuador faces significant security management challenges. Within its IT structure, the entity has implemented information systems and optimized processes to automate previously manual tasks. This article aims to design a hybrid framework to address three key security issues through a thorough research review. Prominent vulnerabilities include weak passwords and the risk of unauthorized physical access. ISO 27005 and NIST 800–53 offer a robust approach to manage information security risks. Validating the framework and controls' applicability ensures suitability for specific infrastructure and operations. Security tests and simulations identify weaknesses, strengthening controls against cyber threats. Leadership approval is crucial for a proactive security improvement approach. This combination provides a comprehensive approach to security risk management, ensuring confidentiality, integrity, and availability of information and systems at the National Directorate of ICT. Following these guidelines prepares the department to address current and future security challenges effectively.

Keywords: ISO/IEC · NIST · Framework

1 Introduction

In the current digital environment, inadequate access to Internet networks and business applications poses a significant threat to information security. To address this challenge, organizations can turn to two widely recognized frameworks: the ISO/IEC 27005:2022 standard and the NIST 800–53 Framework. The ISO/IEC 27005:2022 standard is an international standard that establishes principles and guidelines for information security risk management. It provides a structured and systematic approach to identify, assess, and address risks associated with unauthorized access, as mentioned in the ISO/IEC

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14820, pp. 71–85, 2024.
https://doi.org/10.1007/978-3-031-65285-1_6

27005 standard document [1]. By following the guidelines of the ISO/IEC 27005:2022 standard, organizations can implement appropriate security measures to protect their networks and business applications against unauthorized access. This involves the identification of critical information assets, analysis of threats and vulnerabilities, selection and application of appropriate security controls, and continuous monitoring of the security environment [2].

On the other hand, NIST 800–53, developed by the National Institute of Standards and Technology (NIST) in the United States, provides a set of security controls and recommendations for federal information systems [3]. This framework is based on risk management principles and provides guidance in areas such as access control, authentication, activity monitoring, and incident response [4]. The use of the NIST 800–53 Framework allows organizations to establish a robust foundation of security controls, taking into account internationally recognized best practices and standards. By combining the ISO/IEC 27005:2022 standard and the NIST 800–53 Framework, organizations can benefit from a comprehensive approach to address unauthorized access to their Internet networks and business applications. These frameworks provide a set of proven security controls, helping organizations identify and mitigate risks associated with unauthorized access [5]. By adopting these best practices and security controls, organizations can strengthen their ability to prevent and mitigate risks associated with unauthorized access, thereby protecting their critical information assets and ensuring trust and security in their digital environment [6].

The National Directorate of Information and Communication Technologies (NDICT) of the Ministry of Education (MOE), essential for educational modernization, it focuses on the effective implementation of information and communication technologies. It seeks to improve information accessibility and promote dynamic learning. Table 1 details the total number of registered students for the fiscal year 2022–2023, broken down by educational systems in Ecuador, guiding decisions in educational planning and management.

Table 1. Students enrolled in the Ministry of Education

	Coast - Galapagos	Sierra - Amazon	Levels
Baccalaureate	399,961	299,325	1ro, 2do, 3ero
Basic	1′405,997	925,955	1ro Básica a 10 Decimo
Total	1′805,958	1′225,280	3′031,238

Other Supports Information refers to Private, Fiscal-Commissioned, and Municipal institutions, with the information managed within the NDICT of the MOE, as shown in Table 2.

Table 2. Total enrolled students in Other Supports

	Total, Students Other Supports	Levels
Baccalaureate	204,315	1st to 3rd
Basic	716,888	1st Basic to 10th Tenth
Total	921,203	

Note: In the current data, the figures may increase as they are extracted during the enrollment process in the Sierra region

2 Methodology

Research focused on cybersecurity based on ISO/IEC 2022 and the NIST Framework. A qualitative approach and critical review of key articles will be employed. A validated framework will be designed within the NDICT systems to mitigate failures and vulnerabilities, particularly in the management of national student data, following the systematic review methodology known as SLR [7]. The research process was divided into four phases, detailed below.

2.1 Document Search

The following search string was used across various prominent scientific databases to locate documents related to the developing topic (refer to Fig. 1): ((“NIST computer security” OR “Information Security Risk Management Analysis Using ISO 27005” OR “Security Risk Management” OR “IS Analysis Using NIST “) AND (“Design of information security risk management using ISO/IEC 27005” OR “ security review “ OR “Assessing data cybersecurity using ISO IEC 25012”) AND (“Cyber Risk Management Planning Using NIST”)). In addition, variants were incorporated into the search strings with the aim of obtaining a minimum of 25 documents in each bibliographic database. In total, 40 relevant documents were retrieved in the area of interest.

2.2 Research Questions

To formulate the results, three research questions were addressed regarding challenges in Information Security, skills required for professionals in the field, and the role of auditing in data protection. Table 3 provides details and motivation for each research question. The information was gathered from specialized databases such as Science Direct, Scopus, IEEE Explore, Springer, and Google Scholar.

Table 3. Research Questions (RQ)

Number	Research Questions (RQ)	Motivation
RQ1	What are the most common cyber-attacks on computer systems?	Identifying and maintaining effective control over the most common attacks in the NDICT
RQ2	What are the recommended standards and regulations for mitigating computer attacks?	Proposing the application of norms and standards as a means to strengthen system security
RQ3	How to achieve more effective control and achieve high availability in information systems?	Detect vulnerabilities and address needs to achieve highly available systems

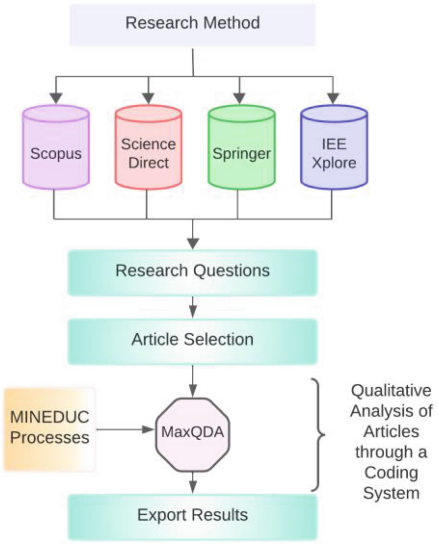


Fig. 1. Research Methodology.

2.3 Article Selection

In the article selection process, filtration criteria were implemented to choose documents obtained from research databases. These criteria addressed aspects such as content relevance, the inclusion of reviews, and their relation to cybersecurity and related topics. Additionally, during searches in bibliographic databases, an additional filter was applied covering classification by disciplines such as 'Science and Engineering,' 'Computer Science,' and 'Cybersecurity,' particularly in English.

2.4 Extraction of Relevant Data

At the end of the two document selection phases, 27 works were obtained. For the extraction of essential information from the Scopus, Science Direct, Springer, and IEE Xplorer databases, paragraphs were taken that helped answer the research questions using the MAXQDA qualitative analysis tool, following the guidelines proposed by Kuckartz in 2014 and the software specifications in 2019.

The articles analyzed with MAXQDA were organized into sections, labeling and extracting key data. They were grouped into areas of interest to design the research framework.

3 Analysis

In this research, a qualitative approach is employed through the collection of data from scientific journal articles and observations from the NDICT. A combined approach is used, integrating stages from the NIST Framework and ISO/IEC 27005:2022. The latest version of NIST 800–53, published in 2018, stands out for its improved organization in security areas, implemented through security profiles [8]. Its planned and business-focused structure makes it an effective tool to guide cybersecurity activities in risk management [9].

ISO/IEC 27005:2022 is a standard that provides guidelines for implementing a risk management approach to information security [10]. In this stage, ISO/IEC 27005:2022 is used to define priority and scope, thus establishing the fundamental criteria for the risk management process. This standard plays a crucial role in identifying assets, threats, vulnerabilities, and controls implemented by the organization [11].

Similarly, ISO/IEC 270005:2022 is used as a reference in the risk process, covering stages such as establishing context, risk assessment, risk treatment, and acceptance [12]. The results obtained in the cybersecurity risk management process undergo further analysis to provide control recommendations based on the NIST SP 800–53 standard [13].

NIST SP 800–53 is an assessment procedure and security controls for systems and information. It is used in the research due to its comprehensive reference [8]. Although it contains 20 control families, this study focuses on those necessary to provide control recommendations and enhance the security of the organization's information systems [14]. Figure 2 is an image of the flow of risk management stages along with the control recommendations used.

I. Prioritize Scope: In this phase, the scope is defined, and priority is established. The organizational structure, business objectives, mission, and priorities are identified. Fundamental criteria based on ISO/IEC 27005:2022, focused on the chapter of priority and scope include risk assessment, impact, acceptance, and risk treatment [15]. The data collection is done through scientific articles and observations of the NDICT and its processes.

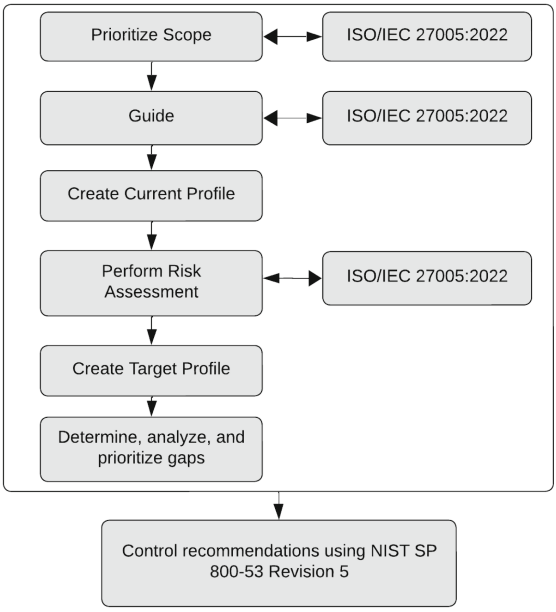


Fig. 2. Cybersecurity Risk Management Process and Provision of Control Recommendations.

II. Orientation: The stage aims to recognize resources and systems in the organization, identifying threats and vulnerabilities that affect assets. The process follows ISO/IEC 27005:2022 standard, in its risk analysis section, addressing the identification of assets, threats, vulnerabilities, and controls, as well as the analysis of the impact of posed risks [16].

III. Create Current Profile: This phase provides an insight into the perception and evaluation of cyber risk by the organization. Data were collected through scientific articles and observations of the NDICT and its processes. Evaluating perspectives on cyber risk involves positioning the organization according to the levels defined in the NIST Framework. [17].

IV. Conducting a Risk Assessment: This phase analyzes the operation of the organizational environment to identify and assess cybersecurity events, focusing on the MOE process. The risk assessment is divided into identification, analysis, and evaluation, followed by three additional stages: response, treatment, and prioritization, as depicted in Fig. 3. The results will guide treatment and control recommendations in the next management phase [18].

V. Create Objective Profile: In accordance with this phase, the aim is to define the objective profile that fits the specific needs and conditions of the organization. This profile is adjusted according to the levels established in the NIST [3]. Determining these levels ensures they are consistent with the organization's objectives, feasible to implement, and capable of reducing cybersecurity risks for critical assets of the organization [19].

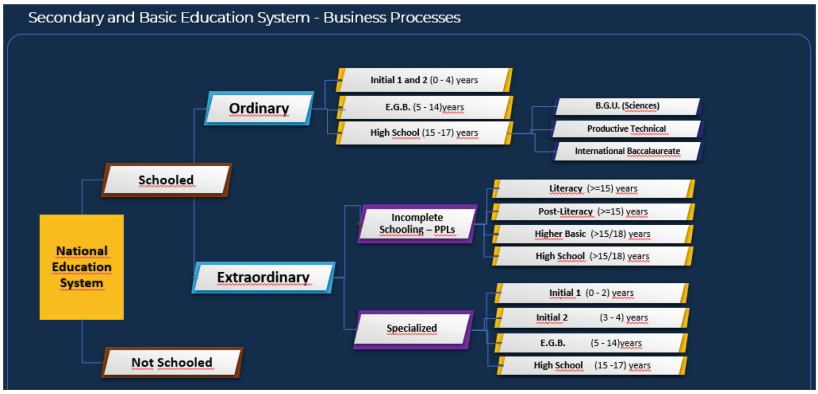


Fig. 3. Business Process - Ministry of Education (MOE)

VI. Determine, Analyze, and Prioritize Security Gaps: In this stage, profiles are compared, risks are analyzed, and a strategy is developed. The process at NDICT follows the EGSI, ensuring information security. Figure 4 illustrates the ISO/IEC 27005:2022 process [20].

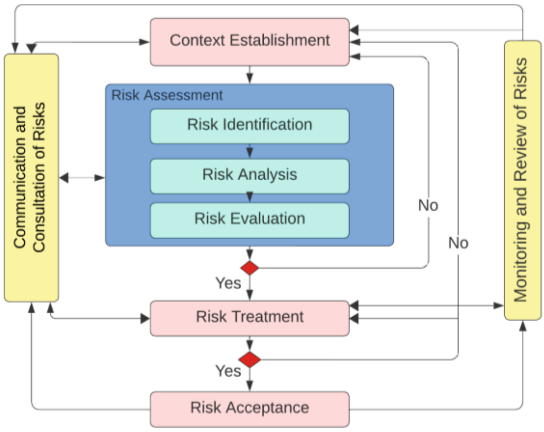


Fig. 4. ISO/IEC 27005:2022 Process.

Design of the Information Security Framework based on the comparison between ISO/IEC 27005:2022 and the NIST Framework from the NDICT of the MOE.

In this phase, the research focus at the NDICT shifts towards the planning of information security risks, based on the standards of ISO/IEC 27005:2022 and NIST 800–53. The relevant steps are detailed below, as illustrated in Fig. 5, according to the research questions. The resulting framework is presented subsequently:

Risk Assessment: ISO 27005 and NIST 800–53 are used to identify and manage risks. ISO 27005 focuses on analyzing assets, vulnerabilities, and assessing probability

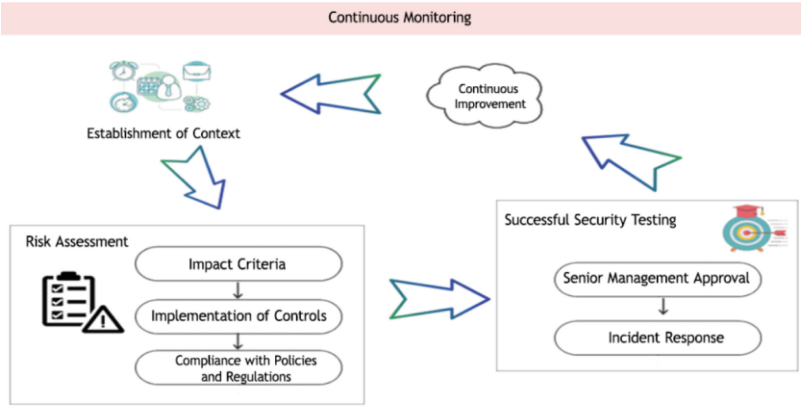


Fig. 5. Design of the resulting framework from the research.

and impact. NIST 800–53 employs controls such as authentication, access control, and encryption.

Evaluation Criteria for Risk: When assessing information security risks, key aspects such as strategic importance, asset criticality, operational interests, and stakeholder expectations must be considered. Additionally, impact criteria and risk events follow the guidelines of ISO 27005, as depicted in Table 4.

Table 4. Risk Probability Matrix

Probability of a threat event or occurrence	Probability that a hazard event will result in adverse impacts				
	Very low	Low	Moderate	High	Very High
Very low	Very low	Moderate	High	Very High	Very High
Low	Very low	Moderate	Moderate	High	Very High
Moderate	Very low	Low	Moderate	Moderate	High
High	Very low	Low	Low	Moderate	Moderate
Very High	Very low	Very low	Very low	Low	Low

Implementation of Controls: ISO 27005 and NIST 800–53 guide the implementation of controls based on the results of risk assessment. Measures such as multifactor authentication and robust password policies are applied to mitigate unauthorized access. In NIST 800–53, specific controls such as firewalls and intrusion detection systems are implemented to prevent unauthorized access.

Continuous Monitoring: ISO 27005: Establish a continuous monitoring process to detect potential unauthorized access activities on the network. Implement intrusion detection systems and audit logs to identify suspicious behaviors.[21]. NIST 800–53: Perform continuous network monitoring to detect unauthorized access attempts and anomalous activities [22]. Use security logs and alerts to respond promptly to potential incidents.

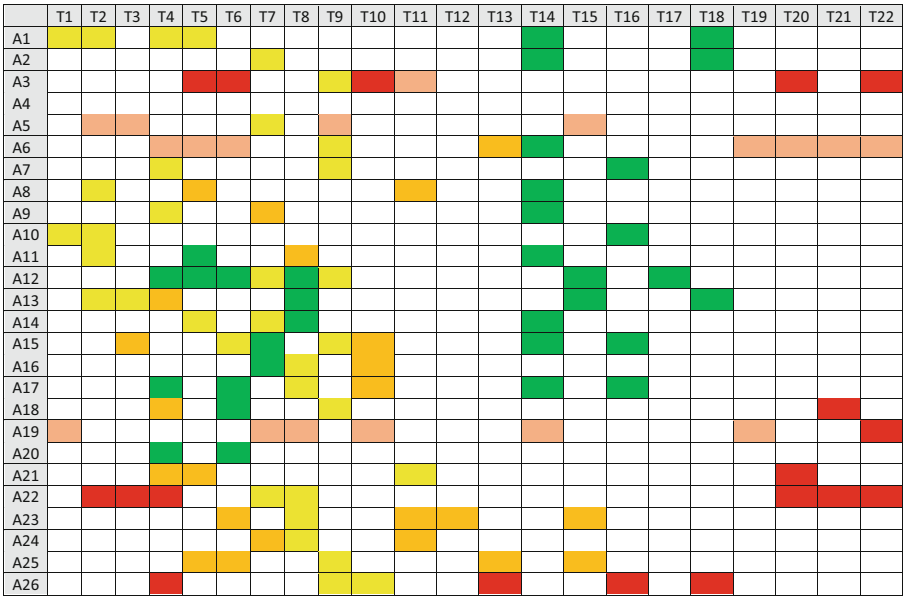
Asset Identification: Asset identification is carried out with the aim of determining the type of asset ownership and the value of the asset, a result obtained for 26 assets based on the results of risk identification.

Threat Identification: Identification of threats that could occur on each asset and threat source. A total of 22 threats that could impact the risk were identified.

Identification of Implemented Controls: Potential negative risks can occur due to vulnerability resulting from a lack of control over negative risks or controls that already exist but are missing or ineffective or inefficient in handling occurring threats.

Identification of Vulnerabilities: A total of 26 assets were identified, resulting in 126 vulnerabilities: 18 very high, 18 high, 23 moderate, 34 low, and 33 very low.

Table 5. Risk Assessment Value Matrix.



- Incident Response: ISO 27005 and NIST 800–53 require incident response plans, definition of roles, and mitigation procedures [23].
- Continuous Improvement: Both standards propose regular reviews and adjustments of controls to maintain network security.
- Security Testing: Tests are conducted to verify the effectiveness of the adopted controls according to ISO 27005 and NIST 800–53.
- Compliance: ISO 27005 and NIST 800–53 help comply with international standards and security regulations.
- Risk Assessment: It is based on impact and uses probability levels, highlighting high-impact risks. The risk assessment value matrix can be seen in Table 5.

Validation of the Designed Framework with Data Collected from the NDICT of the MIEDUC.

Risk Assessment: Critical assets of the ICT department, such as servers, workstations, databases, applications, and networks, are identified. Outdated servers used in the ICT department have not received the latest security updates, which could expose them to known vulnerabilities and exploits. According to prior authorization from the highest authority, network access is not properly controlled, increasing the possibility of an employee downloading a malicious file or opening a compromised link, potentially resulting in malware infection on workstations and compromising network security. Figure 6 illustrates the blockages within the MOE network.

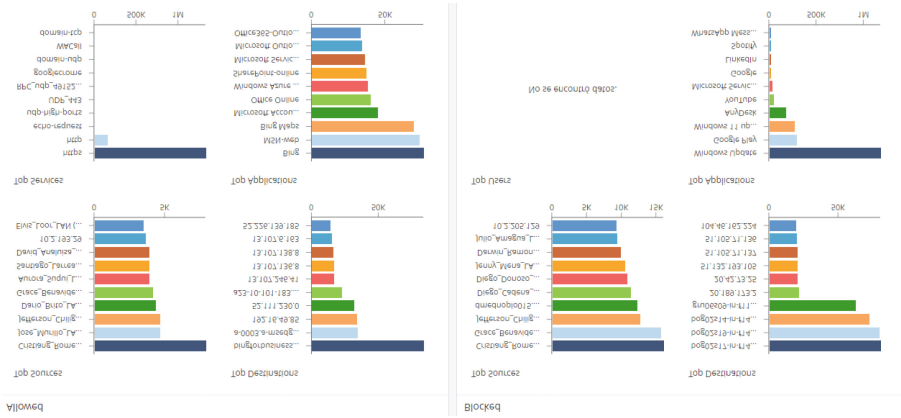


Fig. 6. Blocked Users and Pages within the NDICT Network.

Implementation of Controls: Proposal of controls based on risk assessment, including strong password policies and firewalls to strengthen security. Validating these controls through proof-of-concept testing will help mitigate risks and protect the organization's assets, following the recommendations of ISO 27005 and NIST 800–53.

Continuous Monitoring: Continuous monitoring verifies the effectiveness of implemented controls, identifies and mitigates emerging risks, and responds quickly to threats. It provides data for trend analysis and informed decision-making, as depicted in Fig. 7.

The NDICT of MOE responds to incidents with detection of unusual activity, risk assessment revealing vulnerabilities, and validation of the response through intrusion detection. Continuous improvement includes lessons learned, updating procedures according to ISO 27005 and NIST 800–53, and successful security testing.

4 Results

After conducting the validation of the resulting Framework based on the combination of ISO 27005 and NIST 800–53, the NDICT of MOE significantly improved information security and mitigated risks associated with unauthorized network access.

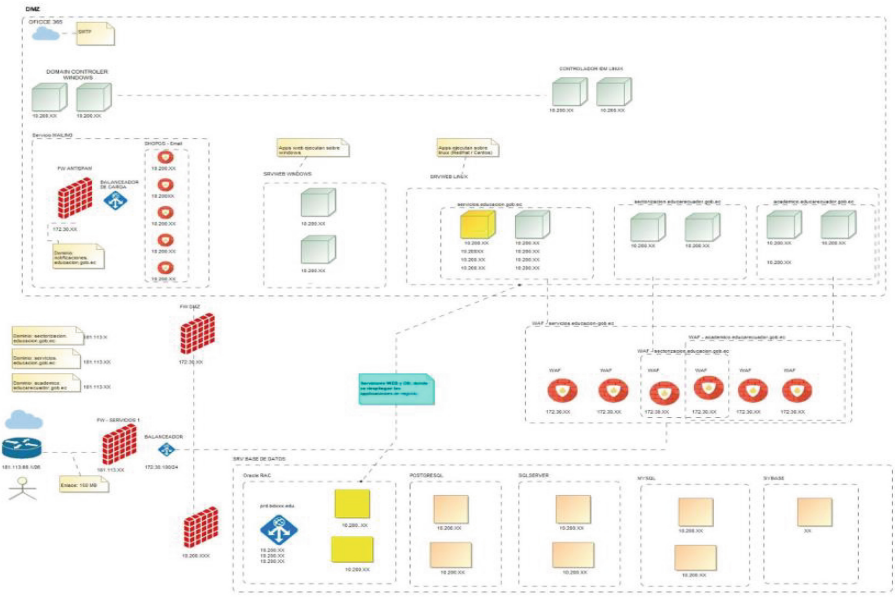


Fig. 7. General Infrastructure Diagram of Ministry of Education Applications.

Risk Assessment: A comprehensive risk assessment was conducted across the entire IT infrastructure, identifying key vulnerabilities and threats that could compromise the confidentiality, integrity, and availability of data and systems, as outlined in Table 6.

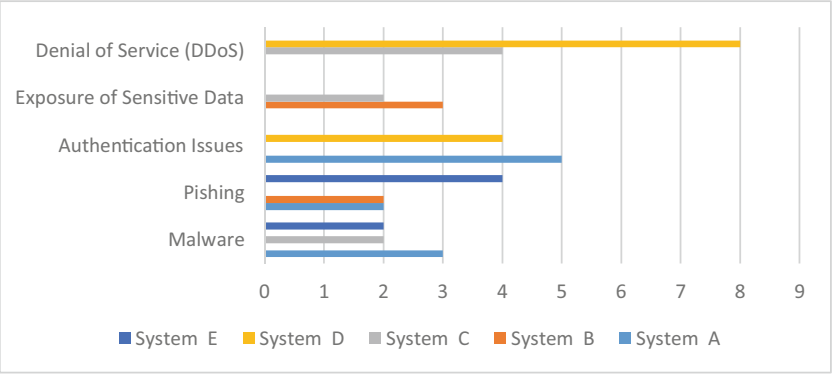
Implementation of Controls: Measures were adopted based on the assessment, such as multifactor authentication and strong password policies, aligning with ISO 27005 and NIST 800–53. Continuous Monitoring and Rapid Response: Establishment of a continuous monitoring system with intrusion detection and audit logs. Improvement in incident response for quick reactions to threats and prevention of institutional failures, as shown in Table 7.

Using the TOAD tool (Tool for Oracle Application Developers), transaction times and interruptions are extracted. As shown in Table 8, it is possible to identify peaks susceptible to system downtimes during registration and update processes.

Successful Security Testing: Penetration tests and vulnerability assessments were conducted, demonstrating the effectiveness of the implemented controls. Vulnerabilities were identified and addressed before they could be exploited. Table 9 analyzes the before and after of the research in the NDICT.

Responsibles: The Security Advisory Committee leads the implementation of the new research framework, providing guidance to the highest authority in information security. The Information Security Officer proposes key documentation for the framework, ensuring compliance with institutional standards and controls, and ensures continuous alignment of the framework with the objectives of the NDICT of the MOE, as seen in Fig. 8.

Table 6. Statistics of Vulnerabilities in the Main Systems of MOE.



System A: Grade Reporting System.
System B: MOGAC System.
System C: COLMENA System.
System D: Enrollment System.
System E: Teacher Assignment System.

Table 7. Statistics of Failures due to Attacks in the Period March-November 2023.

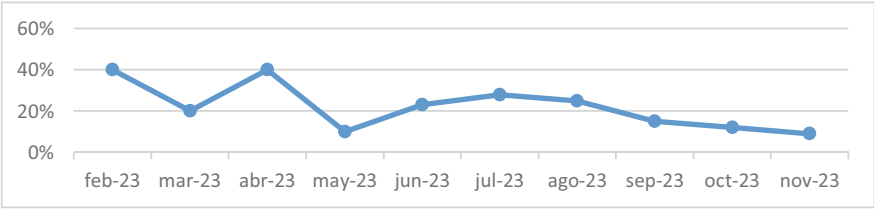


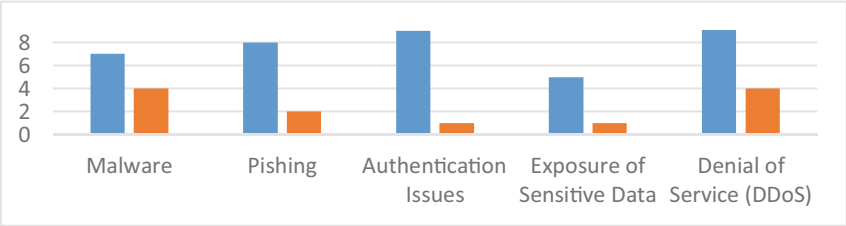
Table 8. Transaction Times and System Downtime-Prone Interruptions.

	Transaction Peak Points Coast - Galapagos	Transaction Peak Points Sierra - Amazon	Transaction Type
Baccalaureate	220,000 approx	180 000 aprox	Insert
Basic	125,000 approx	90 000 aprox	Update

Note: The number in the Sierra-Amazonia period may increase by approximately + - 8 thousand records in entries and updates as the data is extracted during the enrollment period

After validating the ISO 27005 and NIST 800–53 framework, the NDICT of MOE improved security and mitigated risks. They identified vulnerabilities, adopted measures,

Table 9. Before and after the attacks detected after the validation of the proposed Framework.



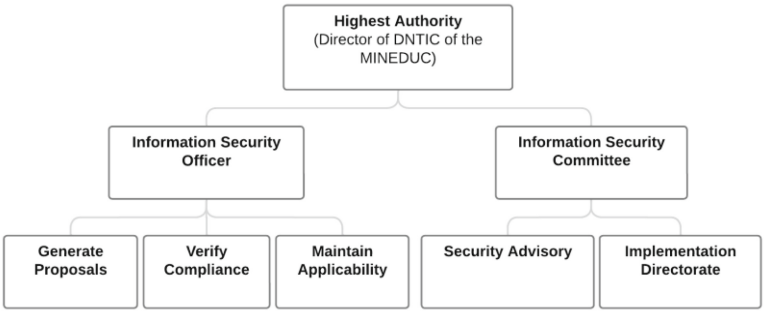


Fig. 8. Organizational chart of responsibilities according to the validation of the Framework.

established continuous monitoring, conducted penetration tests, and ensured regulatory compliance. The support of top management ensured effectiveness and cost control.

5 Conclusions

In the National Directorate of Information and Communication Technologies (NDICT) of the Ministry of Education (MOE), information security is of utmost importance to protect the organization's critical assets, data, and systems against potential threats and unauthorized access. The combination of ISO 27005 and NIST 800–53 provides a robust and comprehensive approach to manage and effectively mitigate information security risks. During this critical period, validating scenarios and attacks was challenging due to the constant change of information, as the Ministry of Education was in the process of enrolling and registering students in the different educational modalities and regimes in Ecuador.

It is concluded that the combination of ISO 27005 and NIST 800–53 provides a comprehensive and robust approach to information security risk management at the National Directorate of ICT of the Ministry of Education. By following these guidelines, the department will be better prepared to address current and future security challenges, ensuring the confidentiality, integrity, and availability of information and systems. This guarantees effective protection against potential unauthorized access and cyber threats.

Additionally, future research could explore the adaptation of security standards to specific environments. Investigating how to tailor and implement ISO 27005 and NIST 800–53 security standards to the unique infrastructure and operational requirements of diverse educational and governmental organizations would provide valuable insights. This line of inquiry aligns with the proactive approach advocated in the conclusion, ensuring that security measures remain effective and relevant amidst evolving challenges.

References

1. Iso. Information security, cybersecurity and privacy protection-Guidance on managing information security risks (2022)
2. Asamblea Nacional. Ley Orgánica De Protección De Datos Personales (2021)
3. Ibrahim, A., Valli, C., McAteer, I., Chaudhry, J.: A security review of local government using NIST CSF: a case study. J. Supercomputing **74**(10), 5171–5186 (2018). https://doi.org/10.1007/s11227-018-2479-2
4. Asamblea Nacional. Ley Orgánica De Telecomunicaciones (2015)
5. Verdugo, J., Rodríguez, M.: Assessing data cybersecurity using ISO/IEC 25012. Softw. Qual. J. **28**(3), 965–985 (2020). https://doi.org/10.1007/s11219-019-09494-x
6. Gutiérrez-Martínez, J., Núñez-Gaona, M.A., Aguirre-Meneses, H.: Business model for the security of a large-scale PACS, compliance with ISO/27002:2013 standard. J. Digit. Imaging **28**(4), 481–491 (2015). https://doi.org/10.1007/s10278-014-9746-4
7. Atymtayeva, L., Bortsova, G., Inoue, A.: Methodology and Ontology of Expert System for Information Security Audit. SCIS-ISIS 2012 (2012)
8. Safitri, E.H.N., Kabetta, H.: Cyber-risk management planning using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800–53 Revision 5 (A Study Case to ABC Organization). In: 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), pp. 332–338. IEEE (2023). https://doi.org/10.1109/ICoCICs58778.2023.10277652
9. Amiruddin, A., Afiansyah, H.G., Nugroho, H.A.: Cyber-risk management planning using NIST CSF v1.1, NIST SP 800–53 Rev. 5, and CIS Controls v8. In: Proceedings - 3rd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2021, Institute of Electrical and Electronics Engineers Inc., pp. 19–24 (2021). https://doi.org/10.1109/ICIMCIS53775.2021.9699337
10. Agrawal, V.: A framework for the information classification in ISO 27005 standard. In: Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, Institute of Electrical and Electronics Engineers Inc., pp. 264–269 (2017). https://doi.org/10.1109/CSCloud.2017.13
11. Terán Tamayo, L.F., Meier, A.: Escuela Superior Politécnica del Litoral (Ecuador), IEEE Computer Society, Institute of Electrical and Electronics Engineers. Region 9, and Institute of Electrical and Electronics Engineers. In: 2018 Fifth International Conference on eDemocracy & eGovernment (ICEDEG) : Quito, Ecuador : eDEM & eGOV : April 4–6, 2018 (2018)
12. Zhang, H.G., Han, W.B., Lai, X.J., Lin, D.D., Ma, J.F., Li, J.H.: Survey on cyberspace security. Science China Information Sciences, vol. 58, no. 11. Science in China Press (2015). https://doi.org/10.1007/s11432-015-5433-4
13. Sharma, G., Vidalis, S., Menon, C., Anand, N.: Analysis and implementation of semi-automatic model for vulnerability exploitations of threat agents in NIST databases. Multimed. Tools Appl. **82**(11), 16951–16971 (2023). https://doi.org/10.1007/s11042-022-14036-y

14. Herath, T.C., Herath, H.S.B., Cullum, D.: An information security performance measurement tool for senior managers: balanced scorecard integration for security governance and control frameworks. Inf. Syst. Front. **25**(2), 681–721 (2023). https://doi.org/10.1007/s10796-022-10246-9
15. Putra, I.M.M., Mutijarsa, K.: Designing information security risk management on Bali regional police command center based on ISO 27005. In: 3rd 2021 East Indonesia Conference on Computer and Information Technology, EIConCIT 2021, Institute of Electrical and Electronics Engineers Inc., pp. 14–19 (2021). https://doi.org/10.1109/EIConCIT50028.2021.9431865
16. Putra, F.A., Setianwan, H.: Design of information security risk management using ISO/IEC and NIST SP 800–30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute (2017)
17. Fahrurozi, M., Tarigan Agrina, S., Tanjung, M.A., Mutijarsa, K.: ICITEE 2020 : Proceedings of the 12th International Conference on Information Technology and Electrical Engineering : October 6th-8th 2020 (2020)
18. Rico Martínez, M.A.: Universidad Católica de Colombia, Institute of Electrical and Electronics Engineers. Region 9, Institute of Electrical and Electronics Engineers. Colombia Section. Technology and Engineering Management Chapter, and Institute of Electrical and Electronics Engineers, 2019 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI) : conference proceedings : 2nd October - 4th October 2019, Bogotá, Colombia (2019)
19. Putra, S.J., Muslimin, J.: Information Security Risk Management Analysis Using ISO 27005: 2011 For The Telecommunication Company (2011)
20. Hugo del Pozo Barrezuela. Esquema Gubernamental de Seguridad de la Información (EGSI)
21. Ñauta Benavidez, R.G.: Plan de seguridad informática para mejorar la gestión de la información en la sociedad financiera visionfound fodemi de la ciudad de Ibarra (2015)
22. Francisco, I., Zapata, X.F.: Implementación Del Modelo De Gestión De La Seguridad De La Información Aplicando ISO 27000 En La Empresa COKA TOURS, AMBATO-ECUADOR (2014)
23. Zuñiga Paredes, A.R., Serrano Quevedo, I.M., Molina Chalacán, L.J.: Seguridad informática en las PyMES de la ciudad de Quevedo. J. Bus. Entrepreneurial Stud. **4**(2), 232–241 (2020). https://doi.org/10.37956/jbes.v4i2.97