Transactions on Energy Systems and Engineering Applications

Article

Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution

Leonel Hernandez[1,*], Andri Pranolo[2] and Aji Prasetya Wibawa[3]

[1] Faculty of Engineering, Institución Universitaria de Barranquilla, Barranquilla, Colombia.
[2] Informatics Department, Universitas Ahmad Dahlan, Yogyakarta, Indonesia.
[3] Faculty of Engineering, Universitas Negeri Malang, Malang, Indonesia
[*] Correspondence: lhernandezc@unibarranquilla.edu.co

Received: 24 January 2024; Accepted: 12 November 2024; Published: 20 November 2024

Abstract: This research was carried out to generate an implementation plan for the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis at the IUB university institution. The connotation of security has been extended over time due to technological advances and the introduction of new information systems, which simultaneously generate new security challenges. Likewise, the instruments to guarantee the confidentiality, integrity, and availability of information have become a fundamental strategy to ensure the security of public and private organizations. The preparation of this plan includes the methodological cycle, where they indicate a series of phases and their corresponding activities to implement the ISMS ISO 27001:2013, with procedural characteristics that support the entire implementation process from beginning to end, facilitating due process and continuity. Likewise, the information security risk plan is analyzed, and significant progress has been made. The result of this cycle will be a plan with a schedule of activities so that the organization links all the personnel around compliance with the standard, raising awareness regarding the importance of information security and the development of activities in phases that, within the stipulated times, will be able to have the ISMS fully operational.

1. Introduction

Over time, information has become one of the most valuable and essential assets for any organization; it only makes sense when available and ordered, maintaining its integrity to be used appropriately, responsibly,

How to cite this article: Hernandez, Leonel; Pranolo, Andri; Wibawa, Aji Prasetya. Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution. *Transactions on Energy Systems and Engineering Applications*, 5(2): 635, 2024. DOI:10.32397/tesea.vol5.n2.635

and safely. These qualities imply the need for organizations to manage their information resources and assets to ensure and control the access, treatment, and use of information. It has become a challenge to secure and protect the transmission of organizations, such as the personal data of users, employees, and suppliers, and to try to guarantee their confidentiality, integrity, and availability as much as possible. For this reason, information security has become a significant concern worldwide. For this reason, any organization, regardless of its size and nature, must consider and be aware of the diversity of threats and vulnerabilities that currently exist in our environment and that these threaten the security and privacy of information, representing a high risk that, when materialized, not only can lead to economic costs, legal sanctions, affect your image or reputation, but can directly affect the continuity of the business.

The preceding, added to a technological environment that becomes more complex to manage and secure daily, generates the idea that information security is increasingly part of organizations' objectives and strategic plans. Therefore, it is essential that those responsible within the organizations in charge of ensuring the protection and security of their resources, infrastructure, and information are constantly adopting, implementing, and improving security measures aimed at the prevention and detection of risks that may compromise the availability, integrity, and confidentiality of information, regardless of whether it is of an organizational, public, or private nature. "Global IT spending is projected to total $4.5 trillion in 2022, an increase of 8% from 2023, according to the latest forecast from Gartner, Inc." [1].

Organizations must carry out an adequate identification, classification, assessment, and management of the risks that may affect their security to implement effective measures that allow them to be prepared to mitigate adverse situations that may compromise the physical and logical security of their facilities, people, resources, and systems. Organizations are working to strengthen themselves on two fronts: comply with data protection regulations and, likewise, shield themselves from cyber-attacks [2].

For this reason, any organization, regardless of its size and nature, must consider and be aware of the diversity of threats and vulnerabilities that currently exist in our environment and that these threaten the security and privacy of information, representing a high risk that, when materialized, can not only entail economic costs, legal sanctions, damage to your image or reputation but can directly affect business continuity. The above added to a technological environment where managing and ensuring information security is increasingly part of organizations' objectives, and strategic plans become more complex daily.

It is crucial and essential that organizations carry out adequate identification, classification, assessment, and management of the risks that may affect their security to implement effective measures that allow them to be prepared to mitigate adverse situations that may compromise the security, physics, and logic of their facilities, people, resources, and systems.

Likewise, public or private University Institutions are obliged to guarantee the proper security, protection, and privacy of the information of their assets, which implies that they must have the highest standards and levels of security, making use of good practices to ensure the collection, treatment, storage, and use of information. The Information Technologies and Systems Process is currently considered a support process within the institutional macro, which depends directly on the Rectorate. Its primary function is to coordinate, manage, advise, evaluate, and control the tools, technological infrastructure, and Information Systems for the automation, support, and development of the academic and administrative processes of the Institution, the development of Science and Technology, by institutional goals and objectives.

The development of this work refers to the Technical Standard ISOIEC 27001: 2013 with the scope of making known the processes and activities that will be contemplated. This project proposes adopting the ISO 2701 standard to mitigate risks and threats. For the University Institution of Barranquilla, information security requires significant attention. Therefore, there is a need to use adequate controls on the confidentiality, availability, and integrity of the information to protect the information of the organization, which can be achieved through the implementation of the ISO 27001 standard that allows not only the protection of information, but also to make decisions aligned with the business, and that serves as a reference or consultation framework for any similar institution, thereby seeks to contribute to the state of the art of the standard in question.

2. Literature Review

The state of the art presented below seeks to show a national and international panorama of the current situation in which higher education institutions find themselves regarding the implementation strategies of an Information Security Management System. Likewise, it identifies the existing gaps regarding the implementation of the ISMS and how this research contributes to reducing these issues. Implementing an Information Security Management System (ISMS) can be complex and challenging, with several potential gaps and challenges often identified in various studies and industry reports. Implementing Information Security Management Systems (ISMS) based on the ISO/IEC 27001 standard has been widely adopted by organizations seeking to manage information security effectively. However, various gaps and challenges have been identified in academic literature over the past five years. Here are some key areas where these gaps have been noted:

- **Contextual and Organizational Factors:** Studies highlight that the effectiveness of ISMS implementation significantly depends on the specific context in which an organization operates. Factors such as the organization's size, industry sector, and cultural attitudes toward information security play crucial roles [3].
- **Cultural Challenges:** Implementing ISMS often requires a cultural shift within organizations. This involves moving from viewing information security as merely a technical issue to understanding it as an integral part of the business strategy. Organizations that are more open to innovation and change are generally more successful in implementing ISMS [2].
- **Emerging Technologies:** The rise of cloud computing, the Internet of Things (IoT), and platform-based business models presents new challenges for ISMS implementation. These technologies blur the boundaries of traditional IT environments, making it harder to define the scope of an ISMS. Consequently, while ISO/IEC 27001 provides a solid foundation, it may not be sufficient to address the security needs posed by these emerging technologies. Organizations often need to integrate additional standards and practices to achieve comprehensive security [2].
- **Standard Limitations:** The generic nature of ISO/IEC 27001 might not be suitable for all types of organizations. Specifically, it is designed for an "average organization" and may not adequately address the needs of companies that significantly deviate from this average, such as those with unique operational structures or highly centralized systems [4].
- **Measurement of Effectiveness:** There is also a gap in the literature regarding the measurement of the effectiveness of ISMS. While compliance with ISO/IEC 27001 can be assessed through audits and certifications, determining the actual improvement in security posture and reduction in risk remains challenging. More research is needed to develop robust metrics and methodologies for evaluating the real-world impact of ISMS implementations [5].

The extensive organizational reliance on information technology (IT) and the worsening impact of information security incidents have made information security a top management concern. The ISO 27001 standard guides a robust Information Security Management System (ISMS). However, implementation and accreditation costs can also be considerable [6].

Concerning the implementation of the ISMS, it managed to identify non-inventoried assets, imminent threats, and potential risks, allowing efficiency in the administration of the entity's resources. The

Institution's information security policies were not legalized, suggesting their certification. The proposed improvements enable the ISMS to reach higher maturity levels and possibly obtain its accreditation through the ISO/IEC 27001:2013 standard [7]. The standard ISO 27001 is highly respected and internationally recognized. But, while it has been around in various guises for over a decade, accreditation levels remain low due to its reputation for requiring a lot of time, effort, and money [8].

On the other hand, the Universidad del Atlántico, in 2011, began designing and developing activities for implementing the ISMS Information Security Management System. In 2014, an ISMS policy was built that proposes a set of security policies to guarantee the proper use of information resources or assets [9]. A year later, the Pedagogical and Technological University of Colombia became the only public university in Latin America to obtain quality certification in the ISO 27001:2013 and ISO 20000-1:2011 standards, granted by the certifying firm SGS Colombia SA [10].

Following in the footsteps of the UPTC, in 2015, Francisco José de Caldas District University, according to rectoral resolution 632, created the Information Security Management Subsystem SGSI. In it, the policies, committees, and functions of the Information Security Management System, among others, were established. Despite the previous, according to the audit and follow-up report of July 28, 2016, which sought to follow up on the implementation of the ISMS, it was evidenced that the Francisco José de Caldas District University had not complied with eight criteria established in said Subsystem [11].

Organizations are working to strengthen themselves on two fronts: complying with data protection regulations and shielding themselves from cyberattacks. This is revealed by the "CIO 2018 Survey" by KPMG and Harvey Nash. Companies are transparent that avoiding inconveniences in these two aspects prevents difficulties in their operations and finances [12]. Without going too far, the WannaCry Ransomware from two years ago demonstrated how exposed the different organizations on the planet are when receiving an attack that involves the encryption of information and the extortion of payment to release valuable information. Spyware like Pegasus has shown that even brands with an excellent reputation in cybersecurity, like Apple, are not infallible and can compromise personal and corporate information. The most recent case, the hacking of the Cayman Islands, meant that financial institutions are not only vulnerable despite investing considerable amounts in network security and fraud prevention but also that so-called "hacktivists" can collaborate by sharing codes and vulnerabilities to steal information [13]

Today, 81% of the employees of large and small companies have access to the Internet. Yet, according to a recent study, the budget allocated to digital security is less than 1% of sales or investments. Meanwhile, cyber-attacks are increasing in sophistication and impact, so the only way out is to anticipate and broaden the spectrum when managing risks [14].

Likewise, the pandemic has changed reality and has defined new regulations for the protection of organizations' digital assets; some are even beginning to understand the dynamics of remote work as a reality that is here to stay, and that means rethinking how the functions of the security areas should be redesigned; this is shown in the report by the Ivati firm [15].

Regarding the research projects and its relationship with the ongoing study, the following degree theses stand out, which help to support or find the development of the research:

Among the new risks in this environment, there are aspects related to many different topics, such as virtualization, denial of service, or intrusion detection. Organizations are willing to adopt cloud computing services in any of their variants. Still, adequate security management is necessary to accelerate its adoption and respond to legal requirements. The main security problem holding back the adoption of Cloud Computing is the loss of control of the organization over its information assets, which means that an Information Security Governance strategy must be developed [16].

The Systems and Telecommunications office is the unit in charge of providing IT services at the University of Córdoba that help the normal functioning of internal processes and is the entity in charge of ensuring the computer assets and information security of the Institution. Therefore, through the planning phase, it is intended to establish the basis for the subsequent implementation of an Information Security Management System following the best practices of international security standards such as ISO / IEC 27001: 2013. Through risk analysis methodology, it is possible to identify which computer assets are the most critical. It has the most significant impact, requiring more excellent security controls and thus establishing a plan for the continuity of services [17]. The methodology used was based on three fundamental phases: the first, the diagnostic study, the second feasibility, and the third, the design of an Information Security Management System for Military Institutions, taking the ISO 27001:2005 Standard as a reference and using a combination of methodologies for risk assessment that helps decision-making on appropriate risk treatment options—design of an Information Security Management System for military institutions [18].

Over time, the quality management system has become a tool for organizing and certifying processes worldwide. Its purpose is to plan, control, and improve organizations' operations [19]. The procedures are created based on the domains of the ISO 27001 standard so that evidence of the user creation and change management processes can be maintained, making an audit more efficacious [20]. Talking about government in a public institution sounds redundant. However, many government institutions have not conceived a corporate business government, much less information technology. To manage information security effectively, it is necessary to implement an IT governance model that leverages said strategy. This is how its approach and management become essential for an organization that adjusts to the challenges and changes the environment presses [21].

In this order of ideas, an alternative solution is presented, and through a non-technical study that shows the current state proposing an implementation of an information system that meets the needs and, in turn, advised by specialist experts in information security to implement the proposed regulations, guidelines, standards, and thus counteract some risk and avoid the existing vulnerability in terms of access to information [22]. The problem is that the Secretary of Education of the Department of Nariño has not implemented an information security management system (ISMS). Up to now, an audit process of information systems, in general, has not been carried out, which allows for establishing the risks that arise in computer and information security. A control system is being developed to mitigate possible threats and dangers [23].

In conclusion, enhancing the implementation of ISMS in higher education institutions requires addressing gaps in digital maturity, developing tailored frameworks, integrating IT governance and digital transformation initiatives, and improving risk management practices. Addressing these gaps will help HEIs strengthen their information security and protect their data assets more effectively [24,25]. Special mention deserves the case of public institutions and developing countries, such as the current study, in which implementing an ISMS represents a challenge to overcome gaps and inconveniences in information security and optimize the processes [26–30].

3. Research Methodology

The type of research according to the object of study is applied and descriptive since it starts from the analysis of the results obtained from research carried out, which leads to the solution of the problem posed, to use what is indicated in each of the IT security processes of the Institution and likewise the design of a plan for the implementation of an ISMS in the educational Institution, under the ISO 27001:2013 standard. ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines the requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and sector with guidance for establishing, implementing, maintaining, and continually improving an information security management system. The effectiveness of the standard has been demonstrated across various sectors, as Fonseca-Herrera et al. and others discuss in their respective studies. ISO 27001 certification has become a widely recognized specification for an ISMS across industries worldwide [31, 32].

This research design is cross-sectional and longitudinal due to the study of the evolution of the IUB University Institution in terms of information security over the last ten years [33]. The information obtained by the ISMS implementation projects from other authors found on the Internet and freely accessible was analyzed, in addition to bibliographic material, books, journals, and the standard available at ICONTEC. Figure 1 shows the specific objectives and main activities of the methodological design, and Table 1 shows, in more detail, some techniques and expected results of each objective:

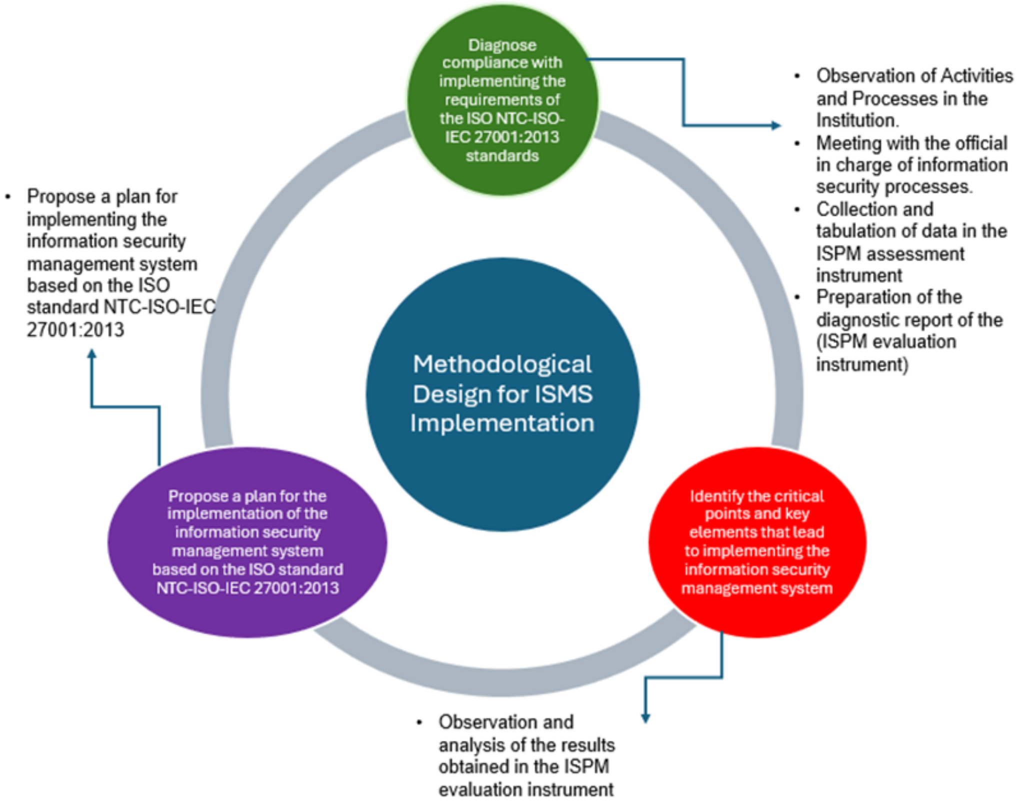

Diagnose compliance with implementing the requirements of the ISO NTC-ISO-IEC 27001:2013 standards
• Observation of Activities and Processes in the Institution.
• Meeting with the official in charge of information security processes.
• Collection and tabulation of data in the ISPM assessment instrument
• Preparation of the diagnostic report of the (ISPM evaluation instrument)
• Propose a plan for implementing the information security management system based on the ISO standard NTC-ISO-IEC 27001:2013
Methodological Design for ISMS Implementation
Propose a plan for the implementation of the information security management system based on the ISO standard NTC-ISO-IEC 27001:2013
Identify the critical points and key elements that lead to implementing the information security management system
• Observation and analysis of the results obtained in the ISPM evaluation instrument

Figure 1. ISO 27001 Compliance Steps.

The success of implementing an ISMS from any business perspective depends on the commitment and the changing mentality of the executive and managerial levels of the organizations. Therefore, the scope of the system requires a level of awareness of the strategic and tactical spheres of the business structure. In this way, training becomes a means of understanding that leads to internalization and commitment to change as a scenario of business competitiveness. Figure 2 shows the phases of the methodological cycle to implement the ISO 27001:2005 model. Each stage has a set of activities that must be carried out sequentially. It is essential to understand that the implementation of the model follows a project approach. The activities take place at a particular time, and it is necessary to have the support of the organization and adequate financial resources to start the project:

Table 1. Methodological Design Techniques and Results.

Specific Objective	Activities	Techniques Used	Results
• Diagnose compliance with implementing the requirements of the ISO NTC-ISO-IEC 27001:2013 standards.	• Observation of Activities and Processes in the Institution. • Meeting with the official in charge of information security processes. • Collection and tabulation of data in the ISPM assessment instrument. • Preparation of the diagnostic report of the (ISPM evaluation instrument).	• Process Diagram. • Review of company data and indicators	• ISPM (Information Security and Privacy Model) Assessment Instrument (Information Privacy and Security Diagnostic Tool)
• Identify the critical points and key elements that lead to implementing the information security management system.	• Observation and analysis of the results obtained in the ISPM evaluation instrument.	• Process Diagram. • Review of company data and indicators	• Formalized document with the list of critical points found.
• Identify the critical points and key elements that lead to implementing the information security management system.	• Propose a plan for implementing the information security management system based on the ISO standard NTC-ISO-IEC 27001:2013.	• Process Diagram. • Review of company data and indicators	• Document with proposals for implementing an ISMS based on the ISO 27001 standard.

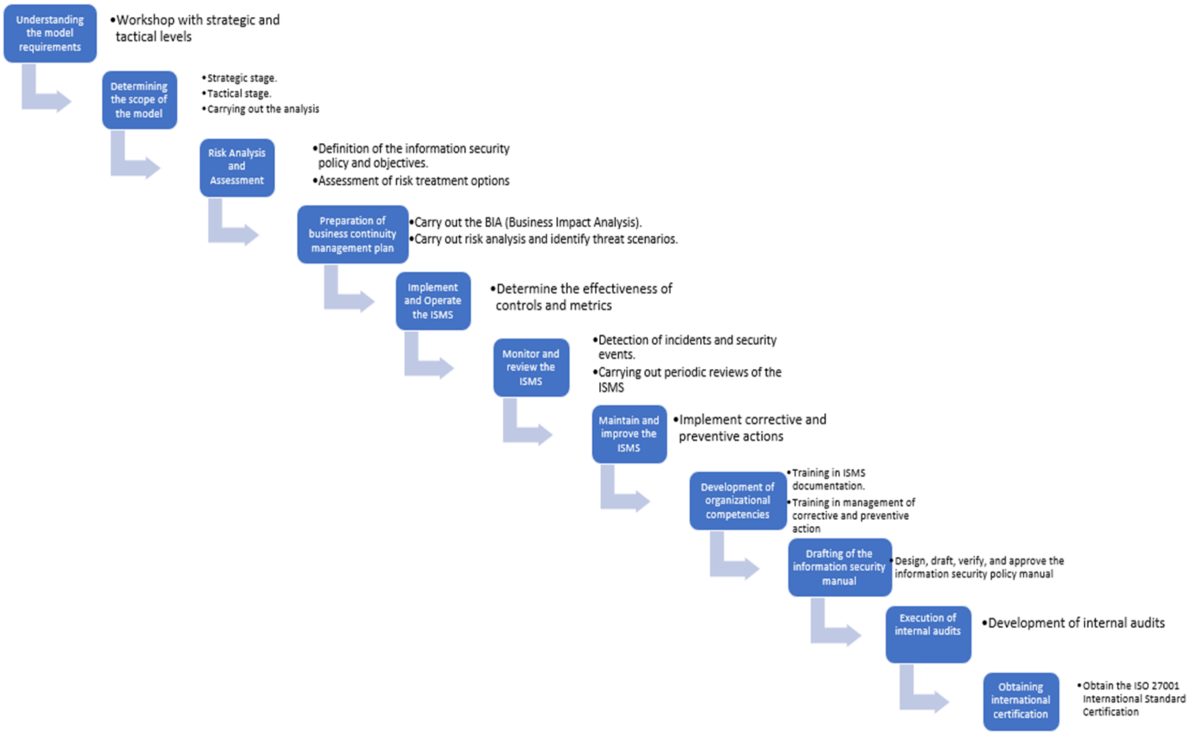

Understanding the model requirements
•Workshop with strategic and tactical levels
Determining the scope of the model
•Strategic stage.
•Tactical stage.
•Carrying out the analysis
Risk Analysis and Assessment
•Definition of the information security policy and objectives.
•Assessment of risk treatment options
Preparation of business continuity management plan
•Carry out the BIA (Business Impact Analysis).
•Carry out risk analysis and identify threat scenarios.
Implement and Operate the ISMS
•Determine the effectiveness of controls and metrics
Monitor and review the ISMS
•Detection of incidents and security events.
•Carrying out periodic reviews of the ISMS
Maintain and improve the ISMS
•Implement corrective and preventive actions
Development of organizational competencies
•Training in ISMS documentation.
•Training in management of corrective and preventive action
Drafting of the information security manual
•Design, draft, verify, and approve the information security policy manual
Execution of internal audits
•Development of internal audits
Obtaining international certification
•Obtain the ISO 27001 International Standard Certification

Figure 2. Methodological cycle for the implementation of ISMS 27001:2005.

The decision to implement the model must involve all levels of the Institution from a democratic and participatory perspective. Even more so, the process leader must be part of senior management, guaranteeing the level of responsibility and avoiding obstruction of the process [34].

After reviewing the documents, it was concluded that most Institutions need to establish an information security management system (ISO/IEC 27001) because it was possible to identify and apply information security concepts found in the different existing standards and methodologies, as well as their application and implementation in public and private sector entities. It is necessary to have all of them implemented and, if possible, combined with other quality management systems. All this will depend on the type of organization.

3.1. Organizational Structure of Technologies and Systems IUB Information

The organizational structure of the process is presented below in Figure 3. Technologies and Information Systems, which is made up of a leader of the process and three subprocesses that correspond to Infrastructure administration technology, Information Systems Administration and Software Development, and Microcomputer support:

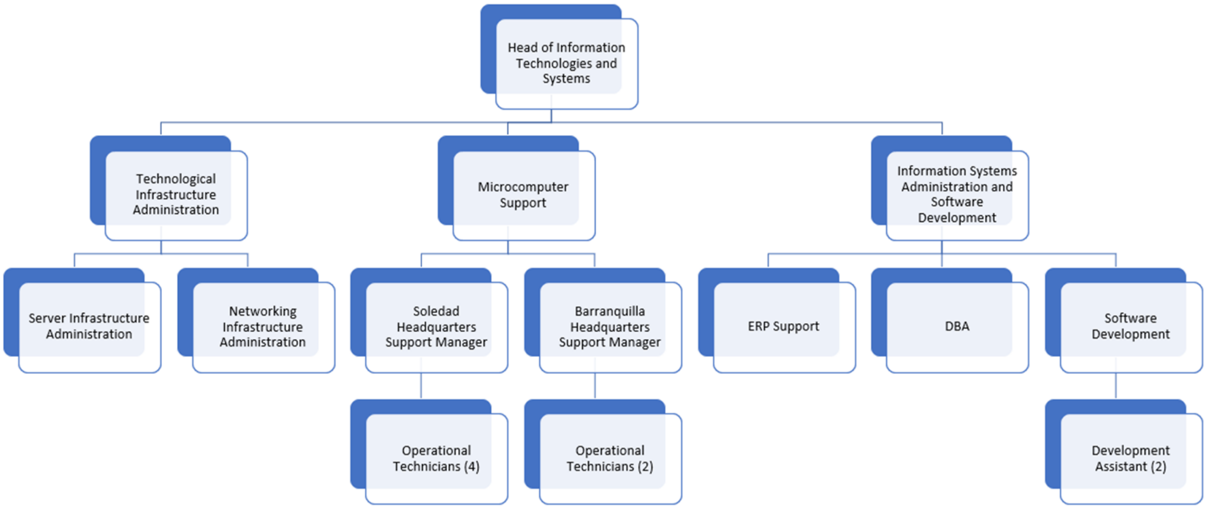

Head of Information Technologies and Systems
Technological Infrastructure Administration
Microcomputer Support
Information Systems Administration and Software Development
Server Infrastructure Administration
Networking Infrastructure Administration
Soledad Headquarters Support Manager
Barranquilla Headquarters Support Manager
ERP Support
DBA
Software Development
Operational Technicians (4)
Operational Technicians (2)
Development Assistant (2)

Figure 3. Technologies and Information Systems: Organic Structure.

Although the process has highly qualified human capital and is committed to achieving its essential functions, not all IT needs are covered in this order of ideas. The above answers, in turn, to the accelerated growth of the Institution during recent years, as well as the new challenges and demands of the environment in terms of Information Technologies Information.

3.2. IUB Basic Server Topology

Network and server infrastructure is fundamental in operating educational institutions like the IUB University. This infrastructure is the backbone that supports communication, collaboration, and access to essential digital resources for students, teachers, and administrative staff. Guaranteeing its stability, performance, and security has become a strategic priority to ensure the quality of education and the efficient functioning of the institution. Figure 4 shows the current topology of the servers at the IUB University Institution, in which the central information systems are housed:

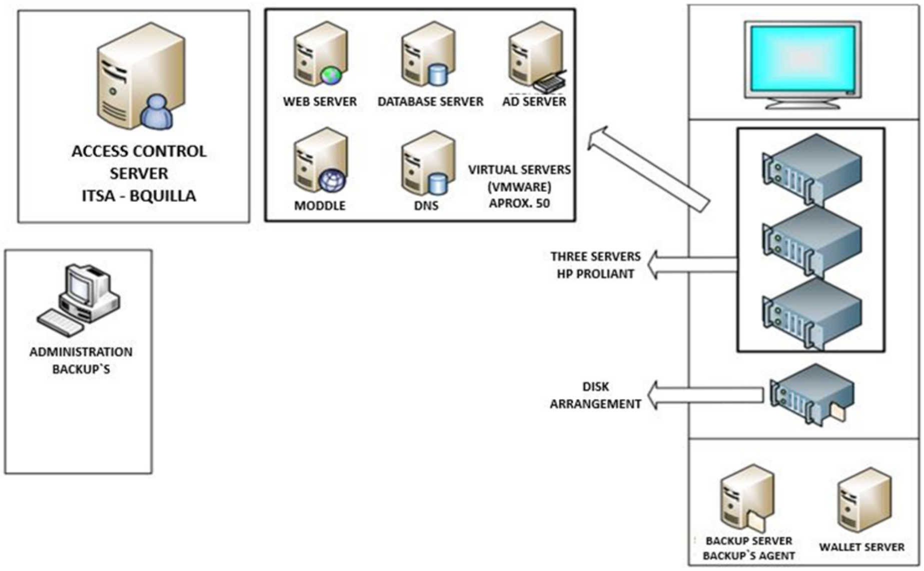


Figure 4. Topology of Servers in the University Institution – IUB.

4. Discussions and Results

4.1. Cyber-attacks on information systems in Higher Education Institutions in Colombia

Cyber-attacks on information systems in Colombia's higher education institutions (HEIs) have been a growing concern. Like global trends, Colombian universities face significant cybersecurity threats, which have implications for their operations and for the protection of sensitive data. According to the 2022 Cyber Security Breaches Survey [35], a significant proportion of HEIs globally reported cyber incidents. Higher education institutions are often targeted due to their vast amounts of valuable data and usually less stringent security measures than other sectors. While specific statistics for cyber-attacks on universities might not be extensively documented in Colombia, the global trends suggest similar vulnerabilities and threats exist. Colombian HEIs must, therefore, adopt robust cybersecurity frameworks to protect their information systems from potential attacks.

There are success stories of the implementation of ISMS in various entities. Severl authors highlight a common factor, the credibility generated among clients, suppliers, and society in general by obtaining certification in the implementation of ISMS, increasing profits and optimizing processes [35–37].

IUB has suffered some cyber-attacks. Some documented attacks were reconnaissance attacks in 2017, a denial-of-service attack in 2019, and XSS Scripting in 2020. Although they had a low impact on institutional information systems, they are incidents that should not be taken lightly and have given rise to the proposal of several strategies to improve information security, among them the implementation of the ISMS .

4.2. Key Performance Indicators (KPI) in the Implementation of ISO 27001:2022

Establishing key performance indicators to measure the success of implementation of ISO 27001:2022 is essential. Some relevant KPIs include:

- **Compliance Rate (CR):** This measure assesses the proportion of activities and controls that comply with the standard's requirements.

- **Incident Detection and Response Time (IDRT):** This measure evaluates the organization's efficiency in detecting and responding to possible security incidents.
- **Audit Performance (AP):** Measures the quality of internal and external audits regarding the standard.
- **Security Incident Rate (SIR):** Records the number of security incidents and their severity.

Implementing an ISMS under the ISO 27001:2022 standard is a fundamental process for guaranteeing the security of information in an organization. Proper documentation and tracking of key performance indicators are essential to success. By adopting this standard, organizations can strengthen security posture and protect their information assets effectively. Information security is an ongoing commitment, and ISO 27001:2022 provides a robust framework to address this challenge in a constantly evolving business environment.

4.3. Analysis of the ISMS

In the IUB University Institution, it is necessary to propose information security controls to mitigate risks, threats, and vulnerabilities, considering that the data must be protected. For this, efforts are being made so that the uses of Information Technologies contribute or add "value" to the organization's strategy in a VICA world (Volatile - Uncertain - Complex -Ambiguous). With this, previous solutions presented during the last years were sought to avoid information loss, such as exposure to data vulnerabilities, social engineering, and technical attacks.

There is no known procedure before the one proposed in this document. However, in 2017, the university, by the guidelines of the national government, began the path towards implementing the ISO 27001 Standard, filling out shared documents on the online government portal.

Notably, since 2016, the awareness process has begun to protect the institution's information and computer systems. An attack on the institution's website was deemed appropriate that same year when a page redirection problem arose for purposes that perhaps are unknown to date but that were most likely to seek benefits at the expense of information. For 2021, some information thefts were recorded from some student community members through emails. Additionally, in 2022, there have been incidents such as SQL injection attacks for accessing, modifying, or obtaining information from databases and cases of attacks through malware.

For adequate implementation and operation of an Information Security Management System (ISMS), it is essential to have steadfast commitment and support from the Institution's senior management. According to the information obtained at the IUB University Institution, the rector is aware of the importance of having an Information Security Management System (ISMS), which is critical and in favor of establishing these planning and implementation processes of the ISO 27001 standard.

As can be seen in Table 2, according to the phases established in the standard and which are based on the PDCA cycle as a problem-solving strategy aimed at improving processes and implementing changes, the Institution in the initial planning phase is at 16% of 40%, which is the progress expected or suggested by the process. Notably, the difference is 24%, a considerably high percentage for the time elapsed since 2016 (the beginning of awareness).

About the next phase, called "Implementation," 6% of this process is observed, where the expected goal is 20%. It is notorious that this phase shows a gap that requires prompt management since, considering the gaps in the previous step (planning), it is likely that many of the processes are not implemented as directed by the standard; quantitatively, there is 14% pending completion, but this may be higher considering that the implementation phase is not considerably advanced. Regarding the last two phases, "Performance evaluation" and "Continuous improvement," it is logical that these depend directly on the first two phases, which must be fully managed to go from 0% to the desired 20%.

Table 2. PDCA operating cycle advance.

	Advance PHVA		
Year	**Component**	**% Current Progress Entity**	**% Expected Progress**
2015	Planning	16%	40%
2016	Implementation	6%	20%
2017	Performance Evaluation	0%	20%
2018	Continuous Improvement	0%	20%
TOTAL		**22%**	**100%**

Figure 5 compares the current progress versus the expected gain, which shows us the need for the Institution to implement controls that help safeguard the information urgently:

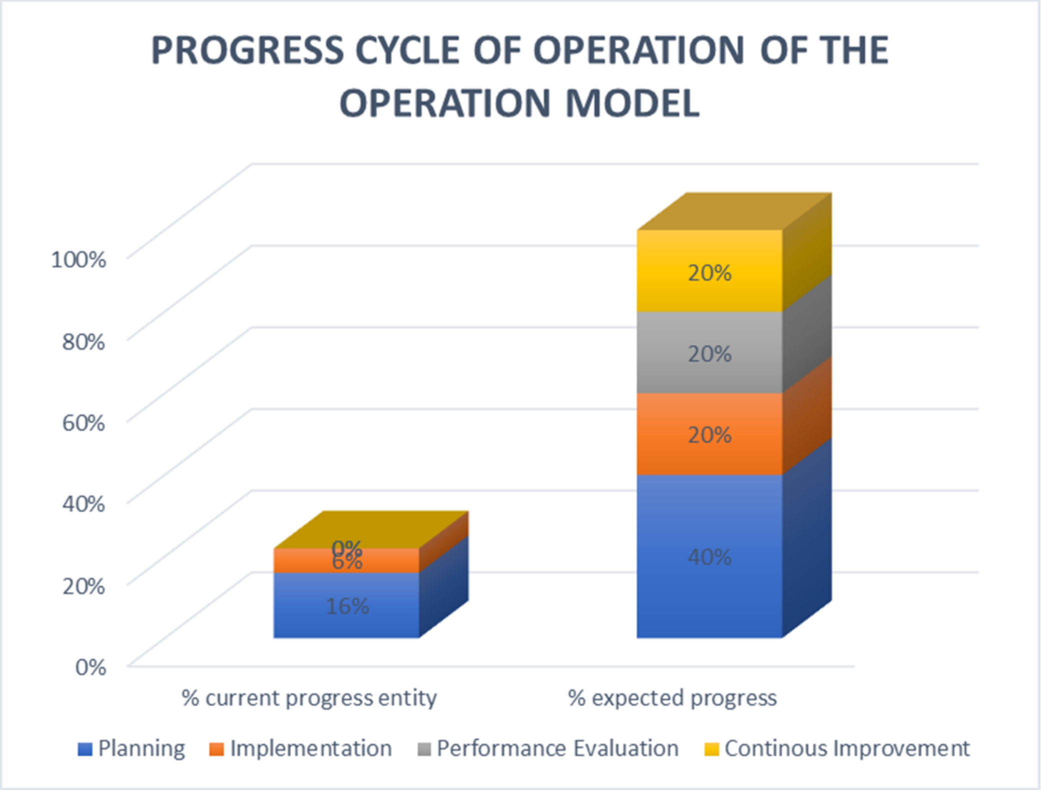


Figure 5. Progress of the Operation Model cycle.

The ISO 27001 standard has 14 domains, 35 control objectives, and 114 controls. According to the diagnosis made at the IUB University Institution, a managed evaluation instrument was found that shows the status of the documentation process regarding what is required by the standard in its early phases. Table 3 shows, in general, the 14 domains with a current rating well below the target rating, which shows an extensive margin in terms of the effectiveness of controls:

Table 3. Evaluation of effectiveness of controls.

No.	Domain	Current Rating	Target Rating	Control Effectiveness Evaluation
A.5	Information Security Policies	20	100	Initial
A.6	Organization of Information Security	18	100	Initial
A.7	Human Resources Security	18	100	Initial
A.8	Asset Management	0	100	Nonexistent
A.9	Access Control	15	100	Initial
A.10	Cryptography	12	100	Initial
A.11	Physical and Environmental Security	15	100	Initial
A.12	Safety of Operations	11	100	Initial
A.13	Security of Communications	20	100	Initial
A.14	Acquisition, Development and Maintenance of Systems	1	100	Nonexistent
A.15	Relations with Suppliers	0	100	Nonexistent
A.16	Information Security Incident Management	9	100	Initial
A.17	Information Security Aspects of Business Continuity Management	0	100	Nonexistent
A.18	Compliance	21.5	100	Repeatable
	Average evaluation of controls	**11**	**100**	**Initial**

This process evaluates the effectiveness of said controls, and it is evident that many of these are in an initial stage, and others are non-existent. Figure 6 shows the gap of annexes in addition to the information previously analyzed, allowing a comparison between the management and processes that the Institution has been carrying out and what the norm establishes.

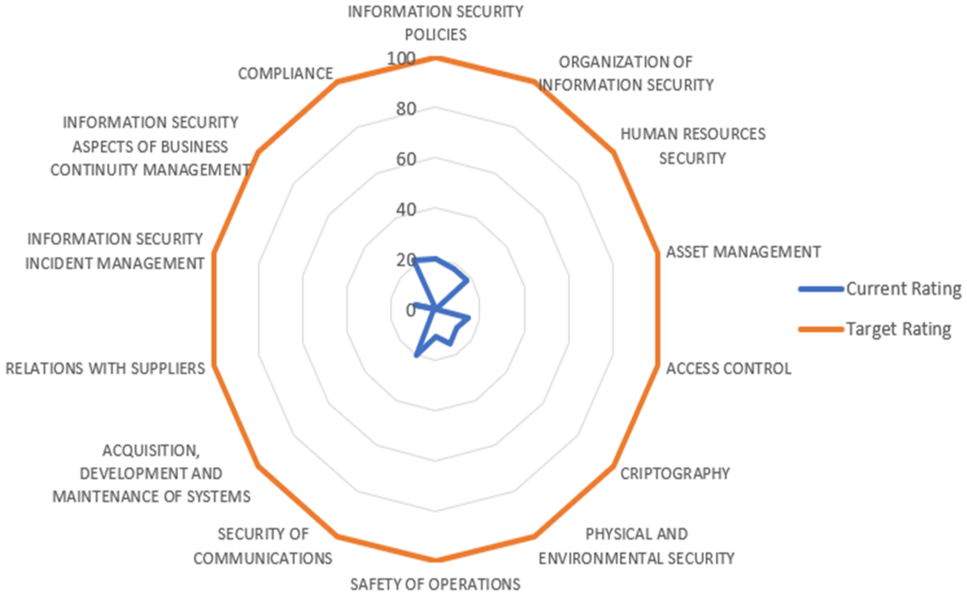


Figure 6. GAP ANNEX A ISO 27001:2013.

To determine a maturity level, it is necessary to have tools that help identify Security and Cybersecurity gaps [25]. In the collection of information and precisely in the evaluation instrument applied, the aspects of computer security are taken as a reference point, such as the controls established by the NIST Cybersecurity Framework, which are aligned with annexes A of the ISO 27001 standard, which exactly coincide with the 14 domains based by the standard. Evaluating the current behavior concerning the five pillars of the NIST Cybersecurity Framework (Identify, Detect, Respond, Recover, and Protect). Figure 7 allows us to observe the critical state that the Institution is currently going through regarding cybersecurity issues:

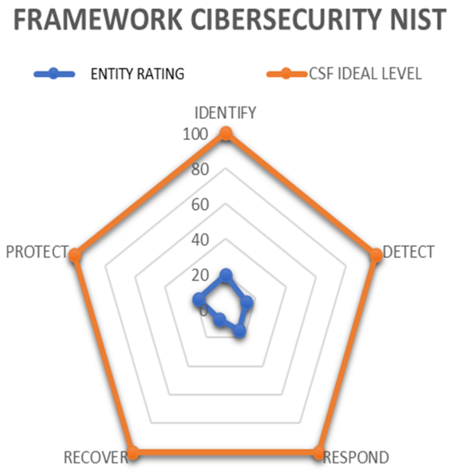


Figure 7. NIST Cybersecurity Framework.

Table 4 shows the NIST Framework Model, specifying the entity rating and CSF ideal level:

Table 4. NIST Cybersecurity Framework Model

Row Label	Entity Rating	CSF Ideal Level
IDENTIFY	20	100
DETECT	14	100
RESPOND	14	100
RECOVER	7	100
PROTECT	18	100

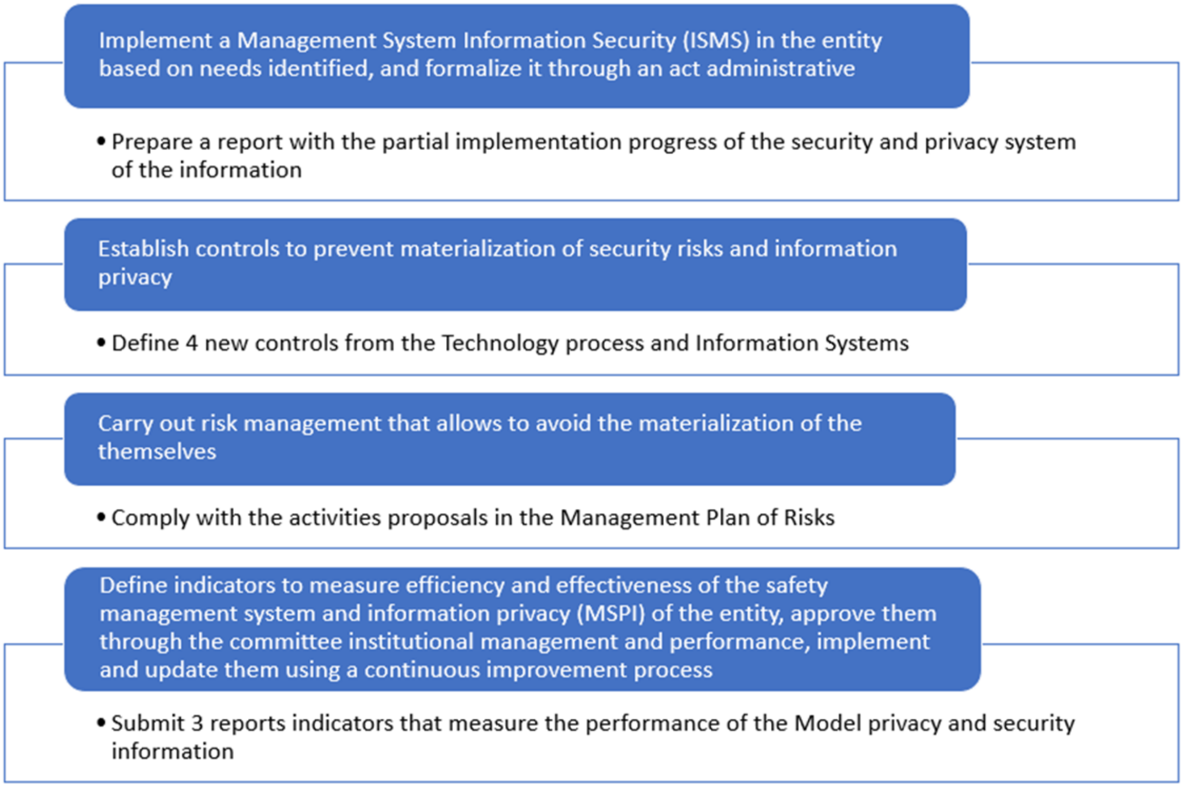
Following current regulations and the ISO 27001 standard, oriented towards the assurance, confidentiality, and integrity of information, the IUB University Institution establishes the following plan, determining a series of goals and activities pending execution, aligned with the institutional objectives and goals, thus continuing with the process of implementing the Information Security and Privacy Model, based on the previous diagnosis made on the level of maturity that the Institution has related to the management of information security and privacy.

Evidence shows that the Institution has recognized a problem that must be dealt with, but there are no standardized processes. The implementation of control depends on each individual and is mainly reactive. There are documented procedures, but they are not known or applied. However, since 2022, two documents called Information-privacy-risk-treatment-plan-IUB-2023 and PMSPI-IUB-2023 have been defined, and some conditions have begun to be outlined for the plan proposed in this study. The main objective of both documents is to emphasize strengthening the protection and security of information in the University Institution of Barranquilla, establishing a series of activities for the 2023 period, which seek to promote spaces for training work teams on the methodology of risk management to facilitate its implementation, establish new controls to reduce the materialization of risks related to the security and privacy of information, as well as define indicators to measure the progress of the implementation of the MSPI in the entity.

Continuing to strengthen the security and privacy policy of the information, the University Institution of Barranquilla contemplates complying with the following goals that will allow, to a greater extent, the control of risks related to digital security:

- Promote training spaces for leaders and work teams on risk management.
- Provide management information when designing controls.
- Establish new controls to prevent security risks from materializing and ensure information privacy.
- Carry out risk management to avoid their materialization.
- Define indicators to measure the effectiveness and efficiency of the Information Security and Privacy management system.

Figure 8 shows the goals and activities of the Annual Plan of the Information Security and Privacy Model, valid 2023:



Implement a Management System Information Security (ISMS) in the entity based on needs identified, and formalize it through an act administrative

- Prepare a report with the partial implementation progress of the security and privacy system of the information

Establish controls to prevent materialization of security risks and information privacy

- Define 4 new controls from the Technology process and Information Systems

Carry out risk management that allows to avoid the materialization of the themselves

- Comply with the activities proposals in the Management Plan of Risks

Define indicators to measure efficiency and effectiveness of the safety management system and information privacy (MSPI) of the entity, approve them through the committee institutional management and performance, implement and update them using a continuous improvement process

- Submit 3 reports indicators that measure the performance of the Model privacy and security information

Figure 8. Goals and activities of the Annual Plan of the Information Security and Privacy Model, valid 2023.

Table 5 shows the level of compliance according to the maturity levels and details the control assessment criteria using a table:

Table 5. Security Level Maturity Levels.

Level	Description	Qualification	Criteria
Non-existent	Complete lack of any recognizable process	0	The organization has not even recognized that there is a problem to be addressed. No controls applied.
Initial	At this level are the entities that do not yet have asset identification and risk management, which allows them to determine the degree of criticality of the information, with respect to its security and privacy. Therefore, the controls are not aligned with the preservation of the confidentiality, integrity, availability, and privacy of the information.	20	1) There is evidence that the organization has recognized that a problem exists and that it must be addressed. There are no standardized processes. The implementation of a control depends on each individual and is mainly reactive. 2) There are documented procedures, but they are not known and/or not applied.
Repeatable	At this level are the entities in which there are basic information security and privacy management processes. In the same way, there are controls that allow detecting possible security incidents, but they are not managed within the planning component of the MSPI.	40	Processes and controls follow a regular pattern. The processes have developed to the point where different procedures are followed by different people. There is no formal training or communication on procedures and standards. There is a high degree of confidence in each person's knowledge, so there is a probability of errors.
Defined	At this level are the entities that have the information security and privacy model documented, standardized, and approved by management. All controls are properly documented, approved, implemented, tested, and updated.	60	Processes and controls are documented and communicated. The controls are effective and are almost always applied. However, the detection of deviations is unlikely when the control is not applied in a timely manner or the way it is applied is not indicated.
Managed	At this level are the entities that have metrics, indicators, and audit of the MSPI, collecting information to establish the effectiveness of the controls.	80	Controls are monitored and measured. It is possible to monitor and measure compliance with procedures and take action steps where processes are not working efficiently.
Optimized	At this level are the entities where there is a continuous improvement of the MSPI, providing qualitative feedback from the model.	100	Good practices are followed and automated. Processes have been redefined to the level of best practices, based on the results of continuous improvement.

In addition to these analyses, the annual plans for 2020, 2021, and 2022 information security and privacy model of the Institution were socialized, where objectives, scopes, and strategies were found based on a set of activities planned for information security and privacy through a set of goals, activities and proposed and partially developed results, making use of schedules to organize such activities over time.

In the security risk treatment plan and information privacy - 2023, an inventory of information assets must be previously identified, which forms the basis of the risk assessment approach associated with information security and privacy. Once the risk assessment stage has been completed, there will be a list or matrix of risk with the identification of risk levels according to the location area, for which the strategies for risk treatment must be indicated to minimize the probability of materialization of this. The assessment of information security and privacy risks includes the following activities:

- **Risk analysis.** First, the information assets must be identified as institutional by the processes or activities of the institution, whose loss or damage affects the provision of the service or is required for compliance with contractual, legal, or regulatory requirements. We also know that we must identify those assets related to hardware, software, networks, personnel, sites, and organizational structures that contain, support, or use the information.
- Once all assets have been identified, the threats they pose must be determined to affect information, processes, and supports, and then the vulnerabilities (weaknesses) that could be exploited by threats and cause damage to institutional information assets. Finally, how these threats and vulnerabilities could affect information assets' confidentiality, integrity, and availability.
- **Risk estimation.** Here, we seek to establish the probability of the risk's occurrence and the impact of its consequences, assigning a rating to determine the risk's level, importance, and treatment strategy.

Probability indicates the number of times the risk has occurred or can be present in a certain period. Impact refers to the consequences that the materialization of the risk may cause in the institution. Once the analysis of the risks determined by their probability and impact has been carried out, you will assess the risk in a scenario without controls and the degree of exposure to the risk that the institution has. This exposition is nothing more than the weighing of the probability and impact that can be observed graphically in the risk matrix, which allows us to globally analyze the risks that must be prioritized by the area where they are located, making it easier to organize the risks, indicate their importance in determining your treatment and implementing action plans corresponding.

Based on the level of risks evaluated, one of the following options will be selected for treatment for each of the identified risks:

- **Avoid.** This option seeks to abandon the activity that causes the risk or choose other alternatives for the activity that do not incorporate the detected risk.
- **Share or Transfer.** This procedure seeks to deliver the risk management to a third party to reduce the probability and impact.
- **Reduce.** Establish controls to reduce the probability of risk occurrence and reduce its impact.
- **Accept.** No additional control measures will be implemented, and the risk will be constantly monitored to ensure it does not increase.

4.4. Monitoring of security and privacy risks of the information

The Risk Treatment Plan's follow-up and monitoring must periodically review the value of assets, impacts, threats, vulnerabilities, and probabilities because risks are dynamic and can change at any time. Continuous supervision is necessary to detect new assets or modifications, new threats, changes or new vulnerabilities, changes in the consequences of impacts, and security incidents, among others.

To determine compliance with managing information security and privacy risks, monitoring and measurement schemes must be defined, such as internal audits, that allow anyone to know the status of compliance with the goals at any time and make decisions promptly.

The resources required by the Information Security and Privacy plan are the following:

- **Human:** Process leaders, Person in charge of strategic planning, Manager of Internal Control, responsible for the Quality Management System, responsible for the Process of Information Technologies and Systems, Engineer in charge of the administration of server infrastructure, engineer in charge of network administration, engineer specializing in computer security.
- **Physical:** Firewall, network equipment, servers, desktop computers.
- **Software:** Information systems.
- **Financial.**

Table 6 shows the activities of the Information Security and Privacy Risk Treatment Plan to mitigate the risks on the institutional information assets:

Table 6. Activities of the Information Security and Privacy Risk Treatment Plan

Management	Activities	Task	Responsible
Treatment of Risks	Identification	• Documentation review of the organization to identify critical assets. • Interviews with those responsible for the assets to gain a deeper understanding of them.	TSI Manager / Leaders or representatives of the two processes missionary
	Identification	• Generate a report of 3 assets' information that have corrected vulnerabilities (weaknesses) which actors could exploit externally to cause damage to these institutional information assets.	TSI Manager / Engineer of TSI plant / Responsible Managers Process Missionary
	Assessment	• Identification of impacts and potential security gaps in each asset.	TSI Manager / Engineer of TSI plant / Responsible Managers Process Missionary
	Assessment	• Design of 3 additional controls to mitigate identified risks. • Improvement of 2 existing controls to increase their effectiveness.	TSI Manager / Engineer of TSI plant
	Sensitization	• Perform periodically simulated engineering exercises for the entity's staff, including campaigns (phishing, smishing, etc.), to raise awareness, education, and training based on results.	Staff involved in the Processes of Missionary / Engineer of the TSI plant

The source of information contained in the results of this document was obtained thanks to the collaboration of some of the representatives of the IT department of the Institution through telephone video calls, meetings, emails, and personal conversations to record truthful and consistent information that leads to the fulfillment of the objectives of this case study.

5. Conclusions

The present study can be used as a framework for developing an ISMS implementation plan under the ISO 27001 standard to strengthen the security of organizations' information systems and significantly higher education institutions. The research can serve as a guide that promotes continuous improvement in managing the security of assets as essential as information systems.

According to the results obtained in the investigation, it can be concluded that in the IUB University institution, short-term and effective measures must be implemented to guarantee the security of the information. Such measures could mean the investment of resources, time, and extensive training days, but that will allow the Institution to guarantee that the management and use of information technologies are under the online government requirements to protect and ensure the security and privacy of information. It is essential to highlight the work carried out by the IT group of the IUB University institution to mitigate some identified weaknesses.

Those mentioned above will improve the quality and continuity of the service and guarantee the security of the information, bringing significant benefits to the Institution since the needs of students, teachers, contractors, officials, and external personnel who use the services provided by the university can be met [38]. Assets can be protected, and the strengthening of information and communication technologies will be promoted according to the global trends required by the electronic government. Additionally, it is vital to generate training work for interest groups, especially for the areas that directly manage the information, as an initial preparation for implementing the system. Samiei et al. Highlight the importance of the participation of managers and directors of organizations in these processes. While many frameworks exist for other industries, HEIs need customized solutions considering their unique organizational structures, diverse user groups, and specific regulatory requirements. At this point lies the importance of the study, which aims to be a mandatory reference for the correct development of the institutional ISMS and optimize the academic and administrative processes [39].

Implementing ISMS in the institution is a multifaceted challenge that requires addressing various gaps and obstacles. These include the need for tailored frameworks, better risk management practices, strong IT governance, and regulatory compliance strategies. By focusing on these areas, IUB can enhance its information security posture and protect its data assets more effectively, taking the results obtained in this research as a starting point.

Likewise, it is crucial to sensitize university personnel through communication campaigns that strengthen the sense of belonging to the entity and, simultaneously, allow them to know the information security recommendations and tips based on the risks that may arise. Future training is also recommended to guarantee the constant updating of officials in managing the Information Security Management System and compliance with the standard. In addition, the Institution can implement a more in-depth cybersecurity risk analysis, such as the one presented by Corredor et al. [40], or other strategies, such as implementing the diamond model for intrusion analysis, a system for managing cybersecurity incidents, or the phases for controlling cyber kill chain intrusion.

Funding: This research received no external funding.

Author contributions: Andri Pranolo: Introduction and Literature Review; Aji Prasetya Wibawa: Research Methodology and 4.1 Cyber-attacks on information systems in Higher Education Institutions in Colombia; Leonel Hernández: Research Methodology, Discussions and Results, and Conclusions.

Disclosure statement: The authors declare no conflict of interest.

References

[1] Luis Enrique. El gasto mundial en TI crecerá un 8% en 2024 según Gartner, Feb 2024.

[2] Giovanna Culot, Guido Nassimbeni, Matteo Podrecca, and Marco Sartor. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, 33(7):76–105, Mar 2021.

[3] Yasmin Kamil, Sofia Lund, and M Sirajul Islam. Information security objectives and the output legitimacy of iso/iec 27001: stakeholders' perspective on expectations in private organizations in sweden. *Information Systems and e-Business Management*, 21(3):699–722, Aug 2023.

[4] Lukas Grenefalk and Norén Wallin. Security management: Investigating the challenges and success factors in implementation and maintenance of information security management systems, 2023.

[5] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. Information security challenge and breaches: novelty approach on measuring iso 27001 readiness level. *International Journal of Engineering and Technology*, 2(1):67–75, 2012.

[6] Carol Hsu, Tawei Wang, and Ang Lu. The Impact of ISO 27001 Certification on Firm Performance. Jan 2016.

[7] ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online., 2017.

[8] Jangirala Srinivas, Ashok Kumar Das, and Neeraj Kumar. Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92:178–188, Oct 2018.

[9] Universidad del Atlántico. Sistema de gestión de seguridad de la información - universidad del atlántico, July 2024. Accessed: 2024-07-07.

[10] Gestion Web. La UPTC, única universidad pública latinoamericana que ha conseguido la ISO 20000 y 2700, Apr 2016.

[11] Mosquera C. *Resolución Rectoral Creación SGSI Universidad Distrital Francisco Jose De Caldas*. 2015.

[12] KPMG. CIO Survey 2018: Insights for technology leaders in Colombia, June 2018. Accessed: 2023-07-07.

[13] La Ciberseguridad en el Día Internacional de la Seguridad de la Información - 30 de noviembre 2022, 2022.

[14] Universidad del Rosario. Ciberataques en colombia ¿está colombia preparada para uno?, July 2024. Accessed: 2024-07-07.

[15] Ivanti. Ciso priorities shift: Navigating changes post-pandemic, July 2024. Accessed: 2024-07-07.

[16] O. R. Martínez. *Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing*. PhD thesis, Universidad de Castilla - La Mancha, 2014. [Online].

[17] J. D. Camargo Ramirez. Diseño de un sistema de gestión de la seguridad de la información (SGSI) en el área tecnológica de la comisión nacional del servicio civil - CNSC basado en la norma ISO27000 e ISO27001, 2017. [Online].

[18] J. A. Guaman Seis. *Diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares*. PhD thesis, Escuela Politécnica Nacional, Quito, 2015.

[19] Erick Guerra, Harold Neira, Jorge L. Díaz, and Janns Patiño. Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica*, 32(5):145–156, Oct 2021.

[20] F. Becerra and A. Villamil. Diseño de procedimientos de gestión de usuarios y gestión del cambio en el sistema kactus-hr aplicando iso 27001. Master's thesis, Universidad Distrital Francisco Jose de Caldas, 2019.

[21] B. Gambin and L. Carreño. Marco de trabajo para la gestión de la seguridad de los sistemas de información en la universidad pública colombiana - caso de estudio universidad del magdalena. Master's thesis, Universidad del Norte, 2017.

[22] R. Betancourt, P. Monroy, and J. Davila. Implementación de sistemas de control de la información en el sena regional tolima, 2015. [Online].

[23] R. Aguirre and A. Zambrano. Estudio Para La Implementación Del Sistema De Gestión De Seguridad De La Información Para La Secretaría De Educación Departamental De Nariño Basado En La Norma ISO/IEC 27001, 2015. [Online].

[24] Jorge Merchan-Lima, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, and Dorys Quiroz. Information security management frameworks and strategies in higher education institutions: a systematic review. *Annals of Telecommunications*, 76(3-4):255–270, Jul 2020.

[25] Antonio Fernández, Beatriz Gómez, Kleona Binjaku, and Elinda Kajo Meçe. Digital transformation initiatives in higher education institutions: A multivocal literature review. *Education and Information Technologies*, 28(10):12351–12382, Mar 2023.

[26] L. A. Mutchler and M. Hines. Effective practices in implementing isms in higher education: A case study. *Education and Information Technologies*, 2018.

[27] J. El-Khoury and C. Kesserwan. Digital transformation and it governance in higher education: A case study. *International Journal of Education and Development Using Information and Communication Technology*, 2018.

[28] N. Ismail and A. N. Zainab. Implementation of information security management system framework in public universities. *Journal of Information Systems Research and Innovation*, 2018.

[29] F. A. Aloul and S. Zhioua. Compliance challenges for isms in higher education. *Journal of Information Security and Applications*, 2020.

[30] G. Tarekegn. Information security management in higher education institutions in developing countries. *Journal of Information Security*, 2019.

[31] O. A. Fonseca-Herrera, A. E. Rojas, and H. Florez. A model of an information security management system based on ntc-iso/iec 27001 standard. *IAENG International Journal of Computer Science*, 48(2):1–10, 2021.

[32] Pangondian Prederikus, Stefan Gendita Bunawan, Ford Lumban Gaol, Tokuro Matsuo, and Andi Nugroho. Standard analysis of document control as information according to iso 27001 2013 in pt xyz. *Lecture Notes in Networks and Systems*, page 721–732, 2022.

[33] Rúsbel Domínguez-Domínguez, Omar A Flores-Laguna, and del Valle-López. Evaluation of an information security management system at a mexican higher education institution, 2023.

[34] Zaydi Mounia and Nassereddine Bouchaib. A new comprehensive solution to handle information security governance in organizations. *Proceedings of the 2nd International Conference on Networking, Information Systems Security*, page 1–5, Mar 2019.

[35] Adrian Ellison. How to prepare and protect your institution against a future cybersecurity attack, July 2024. Accessed: 2024-07-08.

[36] BSI Case Study Fredrickson International. How fredrickson has reduced third party scrutiny and protected its reputation with iso 27001 certification, 2024. [Online].

[37] Inprosec. Caso de Éxito: Adaptación a la ISO 27001 (Gradiant) - Inprosec, July 2024. Accessed: 2024-07-09.

[38] A Aguilar, T Velásquez Pérez, and Silva. Information security model. case study higher education institution. *Journal of Physics Conference Series*, 1257(1):012014–012014, Jun 2019.

[39] Ehsan Samiei and Jafar Habibi. Toward a Comprehensive IT Management Methodology. *IEEE Engineering Management Review*, 50(1):168–185, Dec 2021.

[40] Felipe Andrés Corredor-Chavarro, Diana Cristina Franco-Mora, and Diego Izquierdo-Dussan. Implementation of cybersecurity risk analysis systems in colombia. *Visión electrónica*, 2(2):334–342, Dec 2019.