A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard

Omar A. Fonseca-Herrera, Alix E. Rojas, and Hector Florez

***Abstract*—In an era of globalization, in which technology has allowed the development of companies to be promoted, data and information become essential assets in organizations, which are exposed to hackers, computer viruses, cyber espionage, and infrastructure failures are some of the problems organizations face daily. In this work, we aim to present a model of an information security management system, aligned with the NTC-ISO/IEC 27001:2013 standard, which applies to any organization and allows them to know their current status regarding the information security. Also, the proposed model will enable organizations to implement systemically and adequately controls, procedures, and policies required to preserve the integrity, confidentiality, and integrity of information assets. The model has been applied to an organization that provides technical information management and administration services in the hydrocarbon sector. The results of using the model in this organization, allowed to define its security structure, information security policies, and resources required to certify its management system. Additionally, information assets, technical vulnerabilities, and risks applied to all processes were identified.**

***Index Terms*—Information Security, Management System, NTC-ISO/IEC 27001:2013 Standard, Organizational Assets**

I. Introduction

CURRENTLY, risks and threats that can affect information security are frequent, affecting the confidentiality, availability, and integrity of companies' assets, disrupting both large and small companies [1], [2]. Malicious cyber activity manifests mainly as business disruption (denials of service attacks and data and property destruction), and theft of financial or sensitive data, among others [3], [4]. There are no enough good practices within organizations regarding information security. This fact may due to there are no secure code policies for software developed in-house [5], [6], or many companies now maintain their IT infrastructure in the cloud environment [7]–[9], or simply because human capital is not trained in information security [10]. All this translates into physical, digital, economic, psychological, reputational, and social damages for the victims daily [11].

Successful protection against cyber threats is a big challenge across all sectors, and the economic damage of lack of cybersecurity is evidenced in the Ninth Annual Cost of Cybercrime Study in which reported increases of 67% in security breaches, and 72% in the average cost that to deal with attacks, in the last five years [12].

Having said the above, the main objective of this work is to present an information security management system model aligned with the NTC-ISO/IEC 27001:2013 Standard [13]; since this standard makes it possible for companies to know their current status concerning information security and to systematically and effectively implement the controls, procedures, and policies necessary to preserve the integrity, confidentiality, and integrity of information assets [14], [15].

We have organized this document as follows. In section II, we presented the basis of an ISMS and its requirements according to the ISO Standard, and then detail the proposed model in section III. In section IV, we present the results of implementing the suggested model to an organization that provides technical information management and administration services in the hydrocarbon sector and discusses some security aspects of our proposed method. Finally, in section V, we end by concluding remarks and future work.

II. Information Security Management System

An Information Security Management System (ISMS) is a tool to manage and control security information. It is composed of a systematic process, documented and known by the entire organization. Its strategies and policies are developed to preserve and ensure the confidentiality, availability, and integrity of information assets, to keep a level of exposure less than the level of risk that the organization itself has decided to assume [16]. With the implementation of an ISMS, the organization might identify the risks of its information assets to tackle them by mitigating, transferring, or controlling them. The ISMS must be part of the organization's processes and structure of total information management, taking into account that information security is considered in the design of processes, information systems, and controls [17], [18].

Moreover, an ISMS allows any organization to implement a security government based on an organizational structure, where roles, responsibilities, policies, procedures, processes, and resources are defined to manage assets of information accurately [19]. Then, an ISMS provides a useful tool that enables organizations to establish information security policies, procedures, and controls aligned with the company's strategic objectives. Likewise, the implementation of an ISMS provides the company with a continuous improvement process, which allows reacting to any threat, taking corrective and preventive actions to control any incident that affects information security [20].

A model of an ISMS helps to identify existing and future vulnerabilities and risks. Also, it helps to establish security policies, elements, and procedures to have a possible minor impact in the case of a threat that is materialized [17]. Besides, a model of an ISMS can be aligned with best practices from one or more specifications such as ISO 27001, COBIT, or ITIL [21].

Manuscript received July 3, 2020; revised January 15, 2021.

Omar A. Fonseca-Herrera was Master Student at the Universidad Ean, Bogota, Colombia. E-mail: ofonsec05416@universidadean.edu.co

Alix E. Rojas is Associate Professor at the Universidad Ean, Bogota, Colombia. E-mail: aerojash@universidadean.edu.co

Hector Florez is Full Professor at the Universidad Distrital Francisco Jose de Caldas, Bogota, Colombia. E-mail: haflorezf@udistrital.edu.co

A. ISO-IEC 27001 Safety techniques: Requirements of an ISMS

The international standard ISO-IEC 27001 is the leading standard of the ISO 27000 series and contains the requirements of an ISMS [22]. It has been presented as a model for the design, establishment, implementation, operation, monitoring, control, maintenance, and continuous improvement of ISMS information in any kind of organization. ISO has reserved the 27000 numbering series for standards related to information security management systems [13], [14].

The ICONTEC (Colombian Institute of Technical Standards) adopts the ISO/IEC 27001:2013 [13] standard by translation under the reference NTC-ISO/IEC 27001:2013. The NTC-ISO/IEC 27001:2013 standard indicates that an ISMS must be made up of the following documents, which collect and transmit good practices among the employees in order to promote efficiency and effectiveness through the standardization of functions and activities [23]. These elements are identified in the Figure 1 with document icons and are described below:

- **Scope of the ISMS [S]**: it establishes the scope of the organization and includes a clear identification of the dependencies, relationships, and limits that exist between the scope and those parts that have not been considered.
- **Security policy and objectives [PG]**: a document with a generic content that establishes the Senior Management Commitment and the organization's approach to managing information security.
- **Standards, procedures, and guides that support the ISMS [SP]**: those documents and mechanisms that regulate the operation of the ISMS to ensure the planning, operation, and control of information security processes, as well as to measure the effectiveness of the implemented metrics.
- **Risk assessment methodology [RM]**: description of the methodology to be used in order to establish how the assessment of threats, vulnerabilities, probability of occurrence, and impacts will be carried out in relation to the information assets contained within the selected scope, treatment, and development of criteria for acceptance of risk and setting acceptable levels of risk.
- **Risk assessment report [RR]**: study resulting from applying the aforementioned assessment methodology to the organization's information assets.
- **Risk treatment plan [RP]**: document that identifies Senior Management actions, resources, responsibilities, and priorities to manage information security risks, based on the conclusions obtained from the risk assessment, objectives, available resources, etc.
- **Records [R]**: documents that provide evidence of compliance with the requirements and the effective operation of the ISMS.
- **Applicability statement [AS]**: document that contains the control objectives and the controls contemplated by the ISMS.

III. Proposed model for an ISMS

Based on the reference framework of the NTC-ISO/IEC 27001:2013 standard, we proposed the design and generation of a model of an ISMS composed of three phases, as is illustrated in Figure 1. In the first phase, the leading security elements of the organization are identified and contrasted with the information security model specified in the NTC-ISO/IEC 27001:2013 standard. In this phase, the existing information must be inspected; therefore, we proposed an instrument to help to identify the company's compliance status concerning the domains and controls of the standard. The second phase carries out the preparation of the ISMS. The context of the organization and the expectations of the stakeholders should be identified to generate the system scope. Additionally, in this phase, general information security policies, goals of the ISMS, and the company's organization structure regarding information security are defined. Finally, the third phase focuses on the planning of the ISMS that establishes four main activities: the identification and classification of assets, the identification of vulnerabilities, information security risk management planning, and definition of information security policies and controls, and declaration of applicability. It should be noted that this model considers continuous monitoring and control, so the last phase is expected to be iterative, and the artifacts will be updated.

A. Phase 1: Initial Diagnosis

Before making an in-depth diagnosis of the ISMS, it is crucial to have the support of the executive responsible or the leaders of the processes to be analyzed. To assess the requirements, control objectives, and controls of NTC-ISO/IEC 27001:2013, we collected data with the following instruments:

- Interviews with the leaders of the organizational units to determine the structure of the areas, organizational culture, and state of the processes.
- Questionnaire with twenty-six guiding questions to assess the status of compliance with the requirements of the standard.
- Review and reading of the existing documentation (mission, vision, organizational objectives, strategic planning, policies, processes, procedures, instructions, manuals, regulations, among others).
- Records of observation of daily activities.

1) Assessment of standard requirements: We proposed a specific interview with a questionnaire to determine the level of maturity of the organization regarding Information Security. These interviews should apply to the owners of the processes to evaluate all the mandatory requirements of the NTC-ISO/IEC 27001:2013 standard. Each item should be classified in one of the states described in Table I.

2) Assessment of the control objectives and controls of the standard: To determine the state of the controls of the NTC-ISO/IEC 27001:2013, we recommend using the existing document of the organization intended for the declaration of applicability. If the organization does not have this document, we suggest an evaluation format to classify the state of each control objective based on Table I.

Finally, this phase ends with the delivery of the final diagnosis report, which determines the percentage of compliance and non-compliance with the requirements, the standard

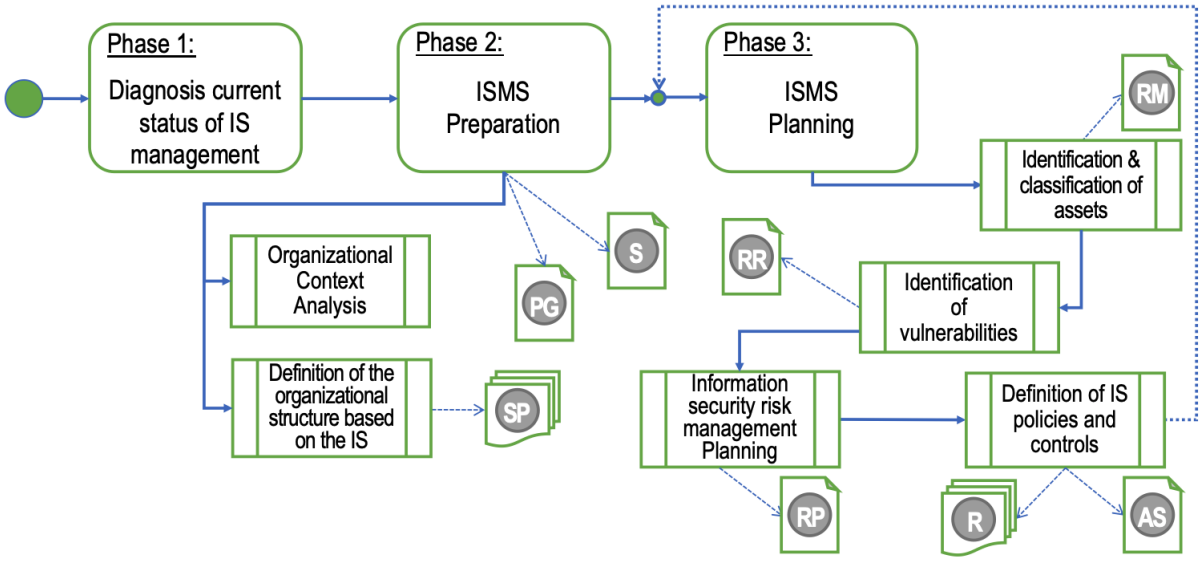

Figure 1. 3-Phase ISMS Model

Table I
DIAGNOSTIC EVALUATION CRITERIA

State	Description
Fully complies	It exists, it is managed, documented, complying with the requirements of the standard, known by all the personnel involved in the company. It complies 100%.
Partially fulfilled	According to what is required by the standard, it is being carried out partially, not fully documented, not managed, not known in the organization. It meets around 50%.
Non-fulfilment	It does not exist, it is not being realized, or its need has not been determined. It complies with 0%.

controls, general security state, and analysis of the detected findings.

B. Phase 2: ISMS Preparation

1) Analysis of the organizational context: The first step of phase 2 corresponds to the preparation of the ISMS. The organization must determine the external and internal factors that generate some impact on the business to achieve the desired results of the ISMS. Thus, stakeholder identification is an essential part of context analysis because it defines the tacit, legal, regulatory, and contractual requirements of the organization, employees, financial institutions, customers, suppliers, government, community, and environment.

To identify the context and the interested parties, we propose a SWOT analysis to know the strengths, weaknesses, opportunities, and threats that may come from external elements. Additionally, all private and governmental entities that affect the ISMS must be listed, specifying their interests and needs.

2) Organizational structure based on Information Security: The second step in preparing the ISMS is to define the organizational structure concerning information security. At this stage, the organization chart of the company should be used as a basis.

Defining the information security roles and responsibilities of people involved in the different areas of an organization is the last activity of the planning stage. In this activity, it is crucial to define the profiles defined at each level and describe the general responsibilities and those condescending to information security from the brief and most detailed way possible. Likewise, essential aspects such as the department or area, immediate manager, and the number of equal roles must be specified.

III. Definition of resources.

The third step in the preparation of the ISMS is to define the necessary resources for the implementation and improvement of the ISMS. In this activity, senior management must demonstrate leadership and commitment by ensuring that the required people, teams, money, and supplies are available. In this step, it is crucial to define a budget detailing at least the following fields: type of resources, activity, description, year, and value.

C. Phase 3: ISMS Planning

1) Identification and classification of assets: Once the activities of the second phase are completed, the planning stage with the identification and classification of the organization's information assets begins. In this activity, the assets associated with the information, which correspond to the information processing facilities, infrastructure, knowledge of people in the company, and information in printed and digital media, must be identified in an inventory. For this inventory, we suggested a record table with at least the following eight columns: Asset Name, General Description, Asset Type, Security Objective, Criticality Level, Business Priority, Asset Manager, and Location.

The asset inventory must be accurate, current, consistent, and aligned with other records. The description of the suggested fields for the catalog are described as follows:

- Asset Name. It specifies the name of the information asset; For example, computer equipment, servers, printed documentation, valuable knowledge, etc.
- General Description. It describes as broadly as possible the description of that type of asset including its use and purpose. For example, Dell PowerEdge T30 server

connected to the network where all the documentation of the company's processes is stored.
- Asset Type. It determines whether this type of asset is information, infrastructure, people, or information systems.
- Security Objective. It defines the security objective in terms of the principles of information security Confidentiality (C), Integrity (I), and Availability (A) as high (H), medium (M), or low (L).
- Criticality Level. It refers to the level of criticality that corresponds to an automatic value as a result of the mathematical calculation of the rating given in the previous safety objectives, which is high (H = 3), medium (M = 2) and low (L = 1). Obtaining a value that can go from 3 to 9.
- Business Priority. It contains the business priority, which depends directly of critical level of each asset and can be 1, 2, or 3.
- Asset Manager. It includes the asset owner, which corresponds to the person in charge of its appropriate management throughout its life cycle.
- Location. It incorporates the physical or digital location of the asset.

2) Identification of Vulnerabilities: The vulnerabilities identified in an ISMS must be related to processes, people, and technology. The ISO 27005 standard presents a list of 63 common vulnerabilities in companies concerning their personnel, physical infrastructure, software, network, and processes.

The verification of the computer security state is essential in the tasks of assuring and monitoring the technological components that compose an ISMS. It is the starting point for the application of measures that guarantee the typical performance of the computing environments and the organization's processes.

The main objective in assessing vulnerabilities at the technology level is to identify potential computer security risks and opportunities for improvement by conducting internal security tests performed on workstations and servers. Finally, we establish the following recommendations according to reasonable information security practices.

1) Collection of information: In this first stage of vulnerabilities identification, it is suggested to carry out a survey of the technological information of the servers, desktops, laptops, and all connected equipment within the network. In addition, it is suggested to identify the IP addresses and domain name, enumeration of the users, identification of operating systems, and design of the network segmentation.
2) Vulnerability scan: In this second stage, it is suggested to inspect and review all elements of the network using a diagnosis software such as Microsoft Baseline Security Analyzer version 2.3.
3) Results and vulnerabilities: In this stage, findings by the diagnosis software are detailed.
4) Analysis of results and recommendations: In this last stage, the results of findings and recommendations are presented.

To obtain more accurate results in the identification of vulnerabilities, malicious code attacks, social engineering, denial of services attacks, among others, should be considered. This allows the organization to identify more risks, and implement more appropriate policies and controls. Although the model scope did not consider automatic methods for increasing cyber resilience or anticipating vulnerabilities and potential threats, this aspect is relevant for ISMS evolution [24], [25].

3) IS Risk Management Planning: The organization must establish the actions to identify, evaluate, classify, and agree on the strategy to mitigate the information security risks to acceptable levels through mechanisms that facilitate its development in a permanent, repeatable, and measurable manner.

Later on, a model based on a PDCA management cycle is presented to carry out the analysis, assessment, risk treatment, and implementation of information security controls, which applies to all processes and services considered in the scope of any system. Table II presents the assessment criteria in the diagnosis based on the activities of the PDCA management cycle.

Table II
ASSESSMENT CRITERIA IN THE DIAGNOSIS

Cycle	Activities
P	Generate guidelines and guidelines on risk management, assessment, treatment, and information security controls.
	Design the necessary actions to deal with information security risks.
D	Execute the actions defined for risk treatment and information security controls following the proposed design.
	Ensure the generation and availability of the resulting evidence.
	Self-assess the effectiveness of the actions implemented to treat risks
C	Evaluate the effectiveness of the actions implemented to treat risks.
	Ensure that the ISMS achieves the expected results in terms of risk analysis, assessment, and treatment.
A	Develop the improvement actions required to address the risks and reduce the gaps identified in the evaluations and audits. If necessary, redesign the information security controls.

4) Definition of information security policies and controls: In this last activity of the third phase, we propose minimum policies and standards for ISMS concerning the use of information resources and assets based on the following elements [26].

- Secure Password Policy.
- Policy of Use of Cryptography Controls.
- Security Policy in Physical Systems.
- Legal Software Use Policy.
- Copyright Policy.
- Internet Use Policy.
- Email Use Policy.
- Desktop policy and clean screen.

IV. APPLICATION OF THE PROPOSED MODEL

The implementation of the model was done in a Colombian company with more than 20 years in the market that provides solutions for technical information management, projects audit services, and geoscientific consulting services for the oil and hydrocarbon industry. The identity of the company is kept anonymous since some confidential information about safety findings is presented as project results.

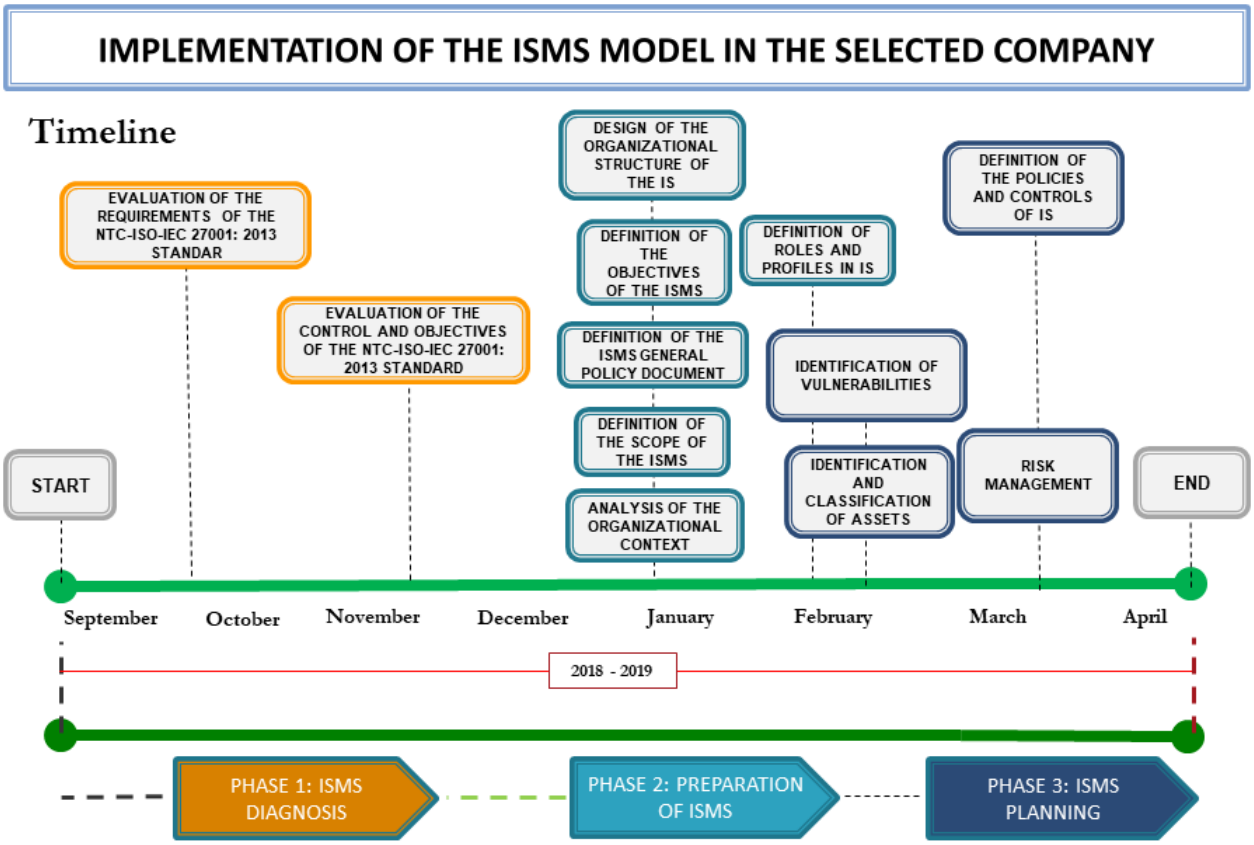

Figure 2. Model applied to the Organization

The model was implemented according to the reference framework of the NTC-ISO/IEC 27001:2013 standard. We strictly followed and respected all activities and steps detailed in the three phases of the ISMS model described in the previous section. The timeline of the implementation in the selected company lasted approximately eight months, as presented in Figure 1 in which all phases and activities are included.

The software used for the identification of vulnerabilities at a technological level was Microsoft Baseline Security Analyzer 2.3[1], which serves as a source for the identification, analysis, and monitoring of vulnerability tests [27].

A. Phase 1: Initial Diagnosis

In this section, the diagnosis made in the company selected is presented in order to know the current status of compliance with the NTC-ISO/IEC 27001:2013 standard. This validation was carried out under whit the instrument presented in Table IV and using the evaluation criteria established in Table I. Table IV partially shows the instrument we use for the measurement; We only include the first and last requirement per category required by the standard.

I. Assessment of the requirements of the NTC-ISO/IEC27001:2013 standard.

According to the review carried out on each of the minimal and mandatory requirements of numerals four to ten of the NTC-ISO/IEC 27001:2013 standard, the summary of the level of compliance and maturity is presented in Table III.

According to the results of the evaluation of all mandatory requirements of numerals four to ten of the NTC-ISO/IEC 27001:2013 standard, we could observe 21 deficiencies in the 22 evaluated requirements, specifically in a) the generation of the documented information required by the standard, b) the identification and actions to deal with the risks, and c) the low levels of awareness regarding the security of the information by the company's operating personnel.

The organization just considers compliance with the information security requirements in the IT process. In other areas of the company, aspects of IS have not been considered within the procedures and processes. However, areas owners and process leaders do consider the importance and benefits that an ISMS can bring them.

II. Evaluation of the control objectives and controls of the NTC-ISO/IEC 27001:2013 Standard.

The model applies a validation of the 114 control objectives and controls to execute a complete diagnosis of all the

Table III
LEVEL OF COMPLIANCE WITH THE REQUIREMENTS OF NTC-ISO/IEC 27001:2013

Requirement	It complies	It does not comply
Organization Context	37.5 %	63.5 %
Leadership	16.5 %	83.5 %
Planning	20 %	80 %
Support	31.25 %	68.75 %
Operation	16.5 %	83.5 %
Planning	16.5 %	83.5 %
Improvement	0 %	100 %

[1]https://docs.microsoft.com/en-us/previous-versions/cc184924(v=msdn.10)

Table IV
INSTRUMENT TO MEASURE THE STATUS OF COMPLIANCE WITH ISO/IEC 27001:2013

Req.	Criterion Description	Question	Status of Compliance	Evidence
4. Context of the Organization				
4.1	Knowledge of the organization and its context.	Has the company identified the internal and external aspects that may affect the ISMS?	Partially fulfilled	The organization has determined external issues that may affect the expected results of the ISMS (competitors, suppliers and customer requirements) but has not determined internal issues.
4.4	ISMS	Has the organization planned, established or implemented an ISMS?	Non-fulfilment	The organization does not currently have an ISMS.
5. Leadership				
5.1	Leadership and Commitment	Has senior management ensured the availability of the necessary resources for the ISMS, and, has it established the Information Security Policy and objectives?	Partially fulfilled	Senior Management has not established the Policy, nor the objectives of IS; But has defined a budget for the ISMS.
5.3	Roles, responsibilities, and authorities.	Has the organization defined a document of roles, responsibilities and authorities in Information Security?	Non-fulfilment	There is no evidence of definition of roles, responsibilities and authorities in Information Security
6. Planning				
6.1	Actions to deal with risks and opportunities	Has the organization carried out a risk identification with respect to the IS?	Partially fulfilled	No large-scale risks have been identified, nor is there a formal methodology to manage them.
6.2	Information security objectives.	Have the IS objectives been established in the organization?	Non-fulfilment	Information security objectives are not documented.
7. Support				
7.1	Resources	Has management determined the resources required for the ISMS?	Fully complies	A budget has been defined for the ISMS.
7.5.3	Control of documented information	Is the ISMS information adequately protected?	Partially fulfilled	The ISMS information is stored on a server that meets the appropriate security and protection conditions but is weakly documented. Configuration management is not performed either.
8. Operation				
8.1	Planning and operational control	Are aspects of information security considered in the different processes of the company?	Partially fulfilled	The organization only considers information security requirements in the ITC process; there is no planning or operational control concerning the ISMS in different areas.
8.3	Treatment of information security risks	Has the organization implemented an information security risk treatment plan?	Non-fulfilment	The organization doesn't have a documented risk treatment plan because it has not correct risk identification and evaluation.
9. Planning				
9.1	Monitoring, measurement, analysis, and evaluation	Does the organization evaluate the information security performance and the effectiveness of the ISMS?	Non-fulfilment	The organization does not have indicators to evaluate the performance of the ISMS.
9.3	Management review	Does management review the ISMS at planned intervals?	Partially fulfilled	The management periodically reviews the organization's processes, but this review has not been documented.
10. Continuous improvement				
10.1	Non-conformities and corrective actions	Have non-conformities been detected in the internal audits?	Non-fulfilment	An internal audit has never been carried out that provides information about the ISMS.
10.2	Improvement tracking	Has the organization continually improve the suitability, adequacy, and effectiveness of the ISMS?	Non-fulfilment	Since currently, it is not considered an ISMS; its improvement cannot be evaluated.

requirements standard. These were obtained directly from Annex A of the NTC-ISO/IEC 27002: 2013 standard was carried out, in the numerals 5 to 18. The categories covered in the diagnosis are described below with the indicative number of the standard, a name, and the quotient between the requirements met by the organization and those required by the standard.

- A5. Information security policies: 0/2
- A6. Information security organization: 3.5/6
- A7. Human resource security: 3/6
- A8. Asset management: 2/10
- A9. Access control: 4/14
- A10. Cryptography: 0/2
- A11. Physical security: 13.5/15
- A12. Operations security: 8.5/14
- A13. Communications security: 3.5/7
- A14. Systems acquisition, development and maintenance: 5/9
- A15. Relations with suppliers: 1.5/5
- A16. Information security incident management: 5.5/7
- A17. Information security aspects of business continuity management: 1/4
- A18. Compliance: 2.5/8

The global report of the level of compliance and maturity of the company presented a 49% fulfillment and a 51% non-fulfillment; regarding controls and control objectives of Annex A. Since we wanted to compare the simultaneous fulfillment of all the requirements demanded by the Standard

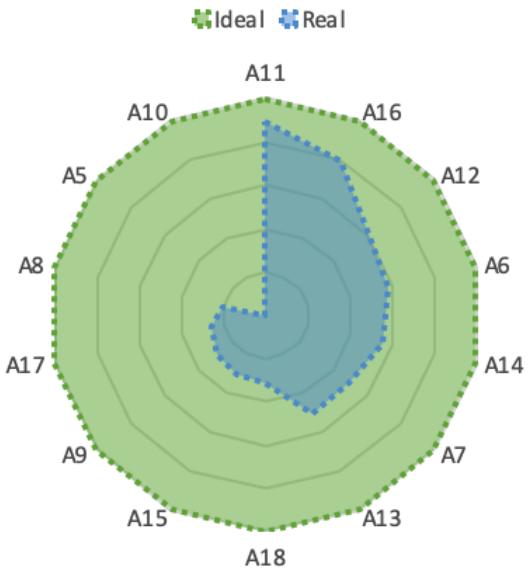

Figure 3. Requirements demanded by the standard vs. Requirements that the company meets

to contrast them with the requirements that the company actually fulfilled, we drew a radial graph to see the general shape, the scope, and the symmetry of the distribution (Figure 3). The radial chart provides an axis for each category, which has a score that ranges from 0% to 100% compliance regardless of the number of requirements that compose it. The blue area allows to see in which categories the organization performed well or poorly. The green area represents the requirements that are not yet being managed in the organization.

The evaluation of controls and control objectives (numerals 5 to 18 of Annex A), indicated significant progress with the accomplish 64 of the 114 controls. It is due to the actions implemented in the physical and environmental security and the management of information security incidents. However, many flaws were found, specifically in the generation of information security policies, asset management, cryptographic controls, and security aspects of business continuity management.

B. Phase 2: Preparation of the ISMS of the selected company

I: Analysis of the context of the selected company.

To identify the context of the organization, the following external and internal issues were determined with the a SWOT analysis presented in Table V.

Table V
SWOT ANALYSIS

Strenghts	**Weaknesses**
Interdisciplinary human talent committed, supported in a culture focused on achievement and the client's goals	Insufficient ICT platform and help desk.
Opportunities	**Threats**
National culture in increasing digital transformation.	Continuous growth of malware causing malicious to information systems.

II. Organizational structure of the selected company based on information security.

The roles and responsibilities for the information security of the people involved in the different areas of the company are defined as follows:

- President:
  - Perform the management review to the ISMS.
  - Establish and review the organization's IS policies and objectives.
  - Analyze the data produced by the ISMS and make the necessary decisions to guarantee the maintenance and improvement of the system.
  - Assign the necessary resources to the ISMS processes.
  - Report and identify risks, incidents or information security events.
  - Ensure effective communication within the organization.
  - Guarantee the achievement of the Information Security policy and objectives.
  - Respects and comply with the basic principles of information security.
- HSEQ Director:
  - Report and identify unsafe acts and conditions during the activities
  - Comply with the minimum training plan defined in the ISMS.
  - Respect and complies with the basic principles of information security (confidentiality, integrity, and availability).
  - Comply with the Information Security measures that are defined in the work procedures that are developed for the different activities that are carried out in the organization.
  - Implement the improvements identified in the ISMS.
- Administrative Director:
  - Comply with and enforces the principles of information security in the established procedure for purchases.
  - Verify that new candidates meet the designed job profiles.
  - Participate in the preparation of the ISMS training program and ensure compliance.
  - Report and identify unsafe acts and conditions during the activities.
  - Respect and comply with the basic principles of information security (confidentiality, integrity, and availability).
  - Comply with the minimum training plan defined in the ISMS
  - Comply with the Information Security measures defined in the work procedures that are prepared for the different activities that are carried out in the organization.
  - Implement the improvements identified in the ISMS.
- Marketing Manager:
  - Comply and enforce the principles of information

security in the procedure established for commercial.
  - Report and identify unsafe acts and conditions during the activities.
  - Comply with the Information Security measures defined in the work procedures that are prepared for the different activities that are carried out in the organization.
  - Implement the improvements identified in the ISMS.
  - Respect and comply with the basic principles of information security (confidentiality, integrity, and availability).
- Technology Director:
  - Generate the equipment maintenance schedule.
  - Asset Inventory Control.
  - Participate in the preparation of the ISMS training program and ensure compliance.
  - Comply with the minimum training plan defined in the ISMS.
  - Report and identify unsafe acts and conditions during the activities.
  - Respect and comply with the basic principles of information security (confidentiality, integrity, and availability).
  - Implement the improvements identified in the ISMS.
  - Comply with the Information Security measures defined in the work procedures that are prepared for the different activities that are carried out in the organization.
- IT Support:
  - Complete equipment resumes and update asset inventory.
  - Comply with the equipment maintenance schedule.
  - Implement corrective and preventive actions.
  - Report and identify unsafe acts and conditions during the activities.
  - Respect and comply with the basic principles of information security (confidentiality, integrity, and availability).
  - Comply with the minimum training plan defined in the ISMS.
  - Implement the improvements identified in the ISMS.
  - Comply with the Information Security measures defined in the work procedures that are prepared for the different activities that are carried out in the organization.

C. Phase 3: ISMS Planning for the Selected Company

1) Identification and classification of assets of the company: The identification of the assets associated with the information in the organization was carried out with the instrument presented in the Table VI; only some records were included to show how the process was followed. The assets associated with the information, the employees, and the organization's infrastructure were identified under three security objectives: confidentiality, integrity, and availability. Each was classified in one of three categories: high, medium, or low; and into business priority.

2) Identification and Analysis of Vulnerabilities: Microsoft Baseline Security Analyzer 2.3 software was used to detect a higher number of vulnerabilities at the technology level. It was installed on a computer connected to the network to carry out a complete review of the active stations and servers. It was necessary to have the support of the technology department, headed by the IT Director, to carry out these tests.

Supported by the software, we scanned the company network and found technological level vulnerabilities in the domain server and some computers on the Intranet. This vulnerability identification tool was chosen at a technical level since all the computers in the organization have Windows as an operating system. Furthermore, the selected software is free and designed to identify vulnerabilities at the level of computer security in SMEs.

3) IS Risk Management Planning for the company: A document with the information security risk analysis, assessment, and the treatment procedure was presented to the company. Additionally, the record of the identification of thirteen information security risks with their respective treatment plan was presented.

4) Definition of information security policies for the company: The conceptual bases, principles and actions to protect or mitigate the risk of information and computer assets are known as information security policies [26]. The following are two examples of the suggested policies for the company in this case study.

Password Policy. Once the employee receives his username and password to enter his corporate email and active directory, he must proceed to change it on his first login. The following are some guidelines to follow to create strong passwords to prevent unauthorized persons from having access to the company's information systems:

- Use passwords that are not easy to guess.
- Construct passwords with a minimum length of eight characters. It must be composed of letters, numbers, specials that are not consecutive or identical characters.
- Refrain from using the same username as your password.
- Memorize the password: do not write it down
- Change your password at least every 60 days or when you feel it has been compromised.
- Avoid reusing old passwords
- Refrain from using obvious keyboard combinations, such as "qwerty"

Use of Cryptographic Controls Policy. Cryptographic controls will be used in the following cases:

- For the protection of access codes to systems, data, and services.
- For the transmission of restricted information on USB memory sticks or hard drives, outside the Agency's scope

V. Conclusion

In this project, a model for an information security management system was proposed and applied in a real

Table VI
IDENTIFICATION AND CLASSIFICATION OF THE ORGANIZATION'S ASSETS

Asset Name	General description	Asset Type	Security Objective C—I—A	Crit. Level	Business Priority	Asset Manager	Location
Quality Management Process Documentation	Procedures, records, manuals, documents	Information	[H] [L] [M]	6	2	HSEQ Director	Eniac-01 Server
CTO	Professional in charge of ensuring the correct use and administration of the company's computer resources.	People	[M] [M] [M]	7	2	Administrative Director	Company's Offices
Hardware IT	Set of technological physical components: keyboards, monitors, scanners, printers, routers.	Infrastructure	[L] [L] [H]	5	2	Manager IT Support IT	Company's Offices

organization. This kind of model serves as the basis for its implementation and subsequent certification in the NTC-ISO-IEC 27001:2013 standard [14], [15]. A model of an ISMS is a crucial element within the strategic plan of any organization because it allows obtaining a differential value within the operation of its services, fostering the positive perception of the company that contributes to improving processes and costs [15], [21].

The results and data obtained from the application of the model in this organization were successful. They allowed the organization to know and analyze its current state according to the requirements and objectives of the standard. Additionally, information assets, technical vulnerabilities, and risks applied to all processes were identified.

The case study shows the lack of a training and education plan in Information Security for people immersed in the processes. As argued in [6], [10], [17], influencing human factors inside organizations helps to create functional cybersecurity cultures. After model application, we also observed the necessity of adding certain strategic activities between phases. continuity plan to update the ISMS. These activities could be included in phase 2 and phase 3, respectively.

One important aspect to consider by organizations when the ISMS is running is to overhaul their Enterprise Architecture to ensure effective development between business processes and Information Technology. Previously, a strategy for managing imperfect models in the EA context has been proposed by Florez et al., [28] to address issues related to inconsistent, imprecise, uncertain, and incomplete information.

REFERENCES

[1] G. Tsakalidis and K. Vergidis, "A systematic approach toward description and classification of cybercrime incidents," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 4, pp. 710–729, 2019.

[2] A. Kigerl, "Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates," *International Journal of Cyber Criminology*, vol. 10, no. 2, pp. 147–169, 2016. [Online]. Available: http://www.vilabs.com/news-

[3] CEA, "The cost of malicious cyber activity to the u.s. economy," Executive Office of the President of United States, Tech. Rep., 02 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[4] M. Riek, R. Bohme, and T. Moore, "Measuring the influence of perceived cybercrime risk on online service avoidance," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 261–273, 2016.

[5] R. M. Nivia, P. E. Cortés, and A. E. Rojas, "Implementation phase methodology for the development of safe code in the information systems of the ministry of housing, city, and territory," in *Computational Science and Its Applications – ICCSA 2018*, ser. LNCS, O. Gervasi, B. Murgante, S. Misra, E. Stankova, C. M. Torre, A. M. A. Rocha, D. Taniar, B. O. Apduhan, E. Tarantino, and Y. Ryu, Eds. Melbourne, Australia: Springer, July 2018, vol. 10961, pp. 34–49.

[6] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Computers & Security*, vol. 98, p. 102003, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404820302765

[7] M. Arafat, "Information security management system challenges within a cloud computing environment," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, ser. ICFNDS '18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3231053.3231127

[8] M. Marwan, F. AlShahwan, F. Sifou, A. Kartit, and H. Ouahmane, "Improving the Security of Cloud-based Medical Image Storage," *Engineering Letters*, vol. 27, no. 1, pp. 175–193, 2019.

[9] Z. Kartit and M. El Marraki, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage," *Engineering Letters*, vol. 23, no. 4, pp. 277–282, 2015.

[10] J. A. Rodríguez-Corzo, A. E. Rojas, and C. Mejía-Moncayo, "Methodological model based on gophish to face phishing vulnerabilities in sme," in *2018 ICAI Workshops – ICAIW*, O. García, C. Díaz, and J. Chavarriaga, Eds. Bogota, Colombia: IEEE, November 2018, pp. 1–6.

[11] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, 10 2018, tyy006. [Online]. Available: https://doi.org/10.1093/cybsec/tyy006

[12] K. Bissell, R. M. LaSalle, and P. D. Cin, "Ninth annual cost of cybercrime study," Accenture, Tech. Rep., 3 2019, an optional note. [Online]. Available: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[13] ISO/IEC, "Iso/iec 27000:2013 family - information security management systems," Geneva, Switzerland: ISO/IEC, 2013. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[14] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," *Journal of Information Security*, vol. 4, pp. 92–100, 2013. [Online]. Available: http://dx.

[15] C.-S. Park, S.-S. Jang, and Y.-T. Park, "A study of effect of information security management system[isms] certification on organization performance," *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 3, p. 10, 2010. [Online]. Available: http://asia.bsi

[16] M. Heru Susanto and N. Almunawar, *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard*. Apple Academic Press, 2018.

[17] A. Qusef, M. Arafat, and S. Al-Taher, "Organizational management role in information security management system," in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: https://doi.org/10.1145/3231053.3231064

[18] N. I. of Standards and Technology, *Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce,

8 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[19] C. Balsa, C. V. Rodrigues, I. Lopes, and J. Rufino, "Using analog ensembles with alternative metrics for hindcasting with multistations," *ParadigmPlus*, vol. 1, no. 2, pp. 1–17, 2020.
[20] J. Areitio Bertolín, *Seguridad de la información: redes, informática y sistemas de información.* Paraninfo, 2008.
[21] Y. Ozdemir, H. Basligil, P. Alcan, and B. Kandemirli, "Evaluation and comparison of cobit, itil and iso27k1/2 standards within the framework of information security," *International Journal of Technical Research and Applications*, vol. 11, pp. 22–24, 01 2014.
[22] E. Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*, 1st ed. USA: Artech House, Inc., 2007.
[23] ICONTEC, *NTC-ISO/IEC27001 Técnicas de Seguridad, y Requisitos para un Sistema de Gestión de Seguridad de la Información*, 2013. [Online]. Available: https://www.icontec.org/rules/tecnologia-de-informacion-tecnicas-de-seguridad-gestion-riesgo
[24] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
[25] R. Dorado, A. Bramy, C. Mejía-Moncayo, and A. E. Rojas, "Automatic acquisition of controlled vocabularies from wikipedia using wikilinks, word ranking, and a dependency parser," in *Advances in Computing*, A. Solano and H. Ordoñez, Eds. Cham: Springer International Publishing, 2017, pp. 32–43.
[26] Angraini, R. A. Alias, and Okfalisa, "Information security policy compliance: Systematic literature review," *Procedia Computer Science*, vol. 161, pp. 1216 – 1224, 2019, the Fifth Information Systems International Conference, 23-24 July 2019, Surabaya, Indonesia. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050919319465
[27] M. E. Whitman and H. J. Mattord, *Hands-On Information Security Lab Manual*. Cengage Learning, 2011. [Online]. Available: 978-1-435-44156-9
[28] H. Florez, M. Sánchez, and J. Villalobos, "Embracing Imperfection in Enterprise Architecture Models," *CEUR Workshop Proceedings*, vol. 1023, pp. 8–17, 2013.

Omar A. Fonseca-Herrera received his M.Sc degree at the Universidad Ean. This article summarizes his research project, which represents the full research processes.

Alix E. Rojas is Associate Professor at the Universidad Ean, Bogota, Colombia. She is M.Sc. in Systems and Computing Engineering at the Universidad Nacional de Colombia. Her research interests are: agile practices, industry 4.0 technologies, and education.

Hector Florez is Full Professor at the Universidad Distrital Francisco Jose de Caldas, Bogota, Colombia. He is Ph.D. in Engineering at the Universidad de los Andes. His research interests are: enterprise modeling, model driven engineering, and enterprise analysis.