Article **Journal of Business and SMEs**
December 2021, Vol.7 No.20 11-23

Administrative audit tool as support for the ISO 27001 standard towards managing the quality of information in SMSEs, 2021

Herramienta de auditoría administrativa como apoyo para la norma ISO 27001 hacia la gestión en la calidad de la información en las PYMES, 2021

RUÍZ-TAPIA, Juan Alberto†*, RUÍZ-VALDÉS, Susana, CRUZ-SOLÍS, Ivett del Rosario and ALCÁNTARA-CRUZ, Félix Héctor

Universidad Autónoma del Estado de México, Mexico.

ID 1st Author: *Juan Alberto, Ruíz-Tapia* / **ORC ID:** 0000-0003-1436-5214, **arXiv Author ID:** Juanalbertoruíz

ID 1st Co-author: *Susana, Ruíz-Valdés* / **ORC ID:** 0000-0001-6318-3009, **arXiv Author ID:** Susanaruíz, **CVU CONACYT ID:** 402668

ID 2nd Co-author: *Ivett del Rosario, Cruz-Solís*

ID 3rd Co-author: *Féliz Héctor, Alcántara-Cruz*

DOI: 10.35429/JBS.2021.20.7.11.23 Received July 15, 2021; Accepted December 30, 2021

Abstract

The problem is raised in which the drawbacks that Small, Medium-sized Enterprises (SMSESs) currently have that do not have an Information Security Management System (ISMS) in place are evidenced, the possible risks that are caused by various practices and the treatment of each one to minimize the negative impact. The objective of this research was to create a computer tool for conducting an administrative audit using the ISO 27001 standard in information quality management for (SMSESs), aiming to reduce computer risks and proposing a risk treatment plan. The methodology consists of determining the scope of the project that is limited by the control objectives obtained from ISO 27001:2013 standard. The project is structured by phases: the objectives of the ISMS to be developed, the reference framework from which the project dimensions and the proposed technological solution are measured, the theoretical and reference framework from which they are measured. the dimensions of the project to develop and implement it in an SMSESs. The contribution is a computer application with the aim of preventing vulnerabilities and threats to the quality of the security system. The information was collected and analyzed, documenting the results, generating a proposal for other SMSESs.

Computer application, ISO 27001, SMSESs

Resumen

El problema consiste en evidenciar los inconvenientes que tienen las Pequeñas, Medianas Empresas (PYME) que no cuentan con un Sistema de Gestión de Seguridad de la Información (SGSI), los posibles riesgos que se originan por diversas prácticas y el tratamiento de ellos para minimizar su impacto negativo. El objetivo fue desarrollar una herramienta informática para realizar una auditoría administrativa utilizando la norma ISO 27001 en gestión de la calidad de la información para (PYMES), para reducir los riesgos informáticos y proponer un plan de tratamiento de riesgos. La metodología consiste en determinar el alcance del proyecto que está limitado por los objetivos de control obtenidos de la norma ISO 27001:2013. El proyecto se estructura por fases: los objetivos del SGSI a desarrollar, el marco de referencia a partir del cual se miden las dimensiones del proyecto y la solución tecnológica propuesta, el marco teórico y de referencia desde el que se miden. las dimensiones del proyecto para desarrollarlo e implementarlo en una PYME. El aporte es una aplicación informática con el objetivo de prevenir vulnerabilidades y amenazas a la calidad del sistema de seguridad. La información fue recolectada y analizada, documentando los resultados, generando una propuesta para otras PYMES.

Aplicación informática, ISO 27001, PYMEs

Citation: RUÍZ-TAPIA, Juan Alberto, RUÍZ-VALDÉS, Susana, CRUZ-SOLÍS, Ivett del Rosario and ALCÁNTARA-CRUZ, Félix Héctor. Administrative audit tool as support for the ISO 27001 standard towards managing the quality of information in SMSEs, 2021. Journal of Business and SMEs. 2021. 7-20:11-23.

*Correspondence to the Author (Email: jart2005@gmail.com)
†Researcher contributing first author.

Introduction

Nowadays it is becoming easier for all the electronic information of an organization to be stolen or modified by multiple individuals, or even by organizations that have the objective of taking as much information as possible for their own benefit. For this, information security policies are constantly being created to prevent future and possible theft of information. Thinking of the different ways in which you can get away or that there is an opportunity for theft. As the use of the Internet is on the rise, more and more companies allow their users, partners and suppliers to access their information systems. Therefore, it is necessary to know which company resources need protection in order to control access to the system and the rights of users of the information system. In addition, due to the growing trend towards a nomadic lifestyle today, which allows people to connect to information systems almost from anywhere, so they are asked to take part of the information system with them outside. of the secure infrastructure of the Organization.

Currently, attacks and threats against information security in SMSESs do not take very seriously the risk involved in keeping all this information unprotected and do not have the security policies recommended by international standards. It is assumed that most of the Organizations in their IT departments do not have tools that help the people in charge of these areas to protect the information deposited in the Information Systems, so it is believed that there is a lack of technological knowledge to protect information from threats and attacks from both internal and external factors.

Social dynamics and technological growth have allowed SMSESs to apply the means and resources at their disposal to have timely information systems, which allow defining indicators, streamlining processes, design and monitor the degree of progress of lines of action, methods, techniques, and strategies, use resources efficiently and observe the changes we face in our environment for proper decision making. For all those involved in the organization, it is necessary to consider the information described above, to have elements of judgment that allow supporting or modifying an action plan proposal and that allows achieving the mission, vision and objectives established in the own organization.

It is necessary to know the importance of having quality in the information system in the administration of enterprise to generate reliable, valid, timely and accurate data that allow to support decision-making, which is why it is a necessity in the current context emphasizes the usefulness of computer tools and their implementation within enterprise because it allows optimizing elements and resources by carrying out in a timely, proper and more productive and efficient way a task that requires time, high costs and physical and mental effort.

It becomes necessary for those organizations, in which they have obviously forgotten the importance of human resource management, to solve the problem they face by implementing an information system on the dynamics of use of Enterprise resources with workers, that an Organization counts; The care of resources is essential, their allocation must be optimal and careful and the operational control of the process must be in charge of people committed to the ability to address the problem.

If we consider the enterprise entity as a properly organized structure, in which decision-making is applied on a large scale, in the different areas existing within it; it becomes a priority to identify the requirements that information systems must have on the administration of organization, since each area works in a different way, so the level of attention will vary depending on the analyzes carried out from the known information.

Therefore, the issue of information security quality for SMSESs is presented here.

Currently there are various risks in which information can be lost or extracted without the necessary security measures that affect organizations, however, this may be because there are not enough controls to meet these needs or they are not carried out cape.

ISSN: 2444-5010

Policies, procedures and controls are proposed more specifically to avoid loss of information as well as a good backup and protection of data since today it is very important to collect information and also make good use of it because security in networks and systems it is not a game since to be sure in the first place, it must be confidential, have competent people in addition to carrying out various controls that precisely help us to keep our databases and networks secure, additionally, keep our data updated software and hardware, as well as avoiding the loss of data, the theft of sensitive and confidential information or the disclosure of user data that can cause serious losses, both financial and credibility.

This research starts from the identification of risks, threats or vulnerabilities in the quality of information security to which an SMSE is exposed and which are caused by various situations within these organizations, proposing measures and controls, with the objective of maintaining the integrity, confidentiality and availability of information for a positive operation within the Organization.

At present, the information that organizations possess and generate is of vital importance and significance, in most Organizations not to mention that in all, confidentiality contracts are even signed where employees or former employees cannot speak about said information.

Therefore, it is necessary for organizations to have adequate control over the information and also to be able to control the handling of the information by the collaborators.

This computer tool is aimed at people related to the information technologies of an SMSE, either because of the responsibility assigned to them in relation to computer assets or because of the benefits they obtain from them. In addition, it is aimed at organizations that need to be careful to protect their information in order to offer them a proposal on how to avoid any risk of attacks within the Organization.

Theoretical framework

Quality of the information

Quality assurance begins with the actions that are carried out during planning such as the set of procedures, techniques and tools during the life cycle, audit activities such as technical reviews or inspections, optimizing previously defined criteria and the functions of management information, more oriented to documentation and development of tests.

Information systems make it possible to measure what is valuable, recognize the strengths and weaknesses that an SMSE has, compare it with other organizations, identify common indicators that measure the same with a high degree of reliability, which can be read and interpreted based on the degree development and evolution of both systems and organizations. Information security quality is the set of technical, operational, organizational and legal measures that allow organizations to safeguard and protect information. The concept of information security should not be confused with that of computer security, since the latter is only responsible for security in the computer medium, but the information can be found in different media or forms, and not only in computer media. The quality of information security (Wendy, Wang, 2019) is responsible for guaranteeing the: Integrity: property of safeguarding the accuracy and complete state of information assets, Availability: property of the information being accessible and usable by request from an authorized entity, and Confidentiality: property that determines that the information is not available or disclosed to unauthorized individuals, entities or processes.

Currently, companies have experienced high growth in information leakage, where confidential documents are exposed outside the company. The greatest challenge to control the leakage of information in companies are employees, since voluntarily or involuntarily, they cause information leakage. This creates a bad image or corporate reputation, since the inability to control attacks or leakage of critical information is questionable. Information security management is an important issue to guarantee the integrity of the information in the systems. These standards focus on a set of vulnerabilities or risks, internal and external, that must be addressed through the application of an associated set of controls.

ISSN: 2444-5010

These controls are physical or administrative safeguards suggested in the standards, aimed at avoiding or mitigating risks.

Currently, the different organizations face world-class competition, quality becomes an important differentiating point, in addition to increasing general customer satisfaction, reducing costs and optimizing resources. Products or services that have quality certificates are preferred by buyers because they convey security and trust. This is also a valuable attribute for overseas marketing strategies. The concept of total quality aims to seek excellence in everything that man, society and organizations do. This concept also applies to the development of information systems based on information processing equipment and man-made programs.

Existing software

The ISOTools Excellence Software for ISO / IEC 27001: 2013 for the Information Security Management System or ISMS is composed of different applications that, when put together, work so that the information handled by Organizations does not lose any of its properties. important: availability, integrity and confidentiality. In an internal software development scenario, an organization that claims to be certified or maintain a certification must take care of certain aspects of software development.

An IS standard (Tofan, 2019) is structured by a set of controls grouped into domains. The main reference for IS standards, ISO 27001 (Gilliam, 2009), is recognized as the most widespread standard throughout the world (Buecker, 2019). Other commonly mentioned models and also with a broader coverage than just security are the ITIL (Official ITIL) and COBIT (ISACA) standards]. Information security management must meet a clear objective: reduce the level of risk to which the SMSE is exposed. Having adequate security within the information management systems within SMSE is of great importance because, it avoids having any hacking and loss of information of valuable criteria due, to better implement the ISMS it is important to carry a control and this is where the audits come in where they review what is being done well and badly and for this to apply improvement and / or changes within the computer part of the Organization.

Unauthorized access to systems and infrastructures is another of the main risks to avoid. Much of this unauthorized access could be prevented if systems and applications were properly updated. Updating is considered a fundamental part of good management and corporate responsibility, since it provides greater security and denotes continuous improvement work that benefits the application and the user.

Organizations must take a proactive approach in order to identify and protect all of their most important assets. Establishing an information security risk treatment plan allows the Organization to evaluate what it wants to protect and use it as a support element to make the decision to identify different security measures. Comprehensive information security risk assessment enables an Organization to assess potential risks in the context of its needs. It is very important to keep in mind that the purpose of information systems and the data they contain is to support the Organization's processes, which in turn support the Organization's mission. Information is a fundamental element that contributes to the Organization's ability to sustain its operations.

To carry out the implementation of the ISO 27001 standard, the use of a specific risk management program is an excellent option that allows considerable cost and time savings on the one hand, and, on the other, the ability to carry out a exhaustive control of all the phases of the process, as well as of the results and the identification of possible points to improve and risks for the company. Implementing and certifying the ISO 2700 standard, for the SGCSI (Information Security Quality Management System) of the organization, it can be shown in a particular way that the entity meets all the minimum requirements to ensure security of the information. Organizations must have an Information security management model or system based on globally recognized security standards, in order to establish and maintain security aligned to the needs and strategic objectives of the organization, composed of an organizational structure, with roles and responsibilities and a coherent set of policies, controls, processes and procedures, which allow it to adequately manage the risks that may threaten the confidentiality, integrity, availability, authenticity, traceability and non-repudiation of the security of information.

ISSN: 2444-5010

To achieve an adequate quality of information, it is essential that organizations establish a structured, clear and rigorous methodology for the assesement and treatment of security risks, with the aim of: knowing the real state of the security of the information assets to through which business information is managed, identify and assess threats that may compromise information security and determine the security mechanisms and measures to be implemented to minimize the impact in case of possible losses of reliability, integrity and availability of the information.

Organizations handle large volumes of data belonging to third parties which must be treated in accordance with the requirements of the law, guaranteeing customers that their information is secure under the highest quality standards related to information security. Technologies and communications are becoming increasingly important in organizations due to the support they provide to the systematization and organization of information. However, due to various vulnerabilities and threats, Information Systems can put at risk the integrity, confidentiality and availability of the quality of the information, for which the risks must be managed to minimize damage to the organization through the prevention and reduction of the impact of security incidents. Currently, most companies that implement ISMS use tools such as spreadsheets to perform GAP analysis to determine the degree of compliance with the requirements set forth in the NTC-ISO-IEC-27001 standard.

The implementation of an ISMS allows the organization to carry out a risk analysis; identifying threats, vulnerabilities and impacts on Organizational activity, continuous improvement in security management, guarantee of business continuity and availability, reduction of costs related to incidents, increase in customer trust levels, increase of the commercial value and improvement of the image of the organization, comply with current legislation on the protection of personal data, information society services, electronic commerce, intellectual property and in general, that related to the security of information.

This implementation of the quality of the information is through a software tool accompanied by techniques for Data Visualization, makes it easier for people to interpret the information and make decisions for the management of quality systems in information security. To develop this computer tool, it was necessary to know technical and legal concepts that are directly related to the subject and have a theoretical and legal support that allows clarifying definitions in order to respond to the requirements of the project. Nowadays, companies and people tend to systematize the tasks they carry out repetitively to optimize time and make decisions intelligently, that is why management systems are not alien to this situation and computer tools must be implemented that allow data analysis and easy understanding by users at all levels. In order to carry out a simple analysis, it is easy to find templates in Excel that allow these diagnoses in an easy way, which is why a computer application is made to facilitate this process.

ISO 27001: 2013 standards

This standard is the international standard for information security management. Defines how to implement an independently assessed and certified information security management system. This enables you to more efficiently secure all financial and confidential information in a way that reduces the possibility of it being accessed illegally or without authorization. With ISO / IEC 27001: 2013, commitment and compliance with global best practice can be demonstrated, demonstrating to customers, suppliers and stakeholders that security is essential to the way the Organization operates.

The ISO / IEC 27001: 2005 standard is an internationally recognized standard, which specifies the requirements to establish, implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS), considering the risks of business (Official ISO 27000). In other words, it proposes a methodology to implement the ISO, specifying the requirements for the application of security controls to an ISMS. This standard segment security into eleven domains and proposes a set of controls within them.

ISSN: 2444-5010

Most organizations base their operations on computer systems. This situation is manifested through the IS standards, which present the security problem as a set of controls that represent guarantees for the different security vulnerabilities. On the other hand, it should be considered that there are also national regulations that do not necessarily align with international standards, which means that the organization must comply with both requirements. This is further aggravated, if it is considered a governmental organization, which also must comply with internal government regulations. This puts the organization in a problem as to which standard to apply or what level of compliance to achieve with the standards it is interested in achieving.

Given this situation, the incorporation of new systems within an organization that is certified according to a standard or that is on the way to do so, is an important decision, since the incorporation of systems that do not comply with the standard could lead it to lose the certification. . This phenomenon forces us to consider the effects or requirements of the standards in new systems developments, therefore, the controls established within the standards have an impact on the different stages of Software development.

ISO, (International Standardization Organization), is the body in charge of promoting the development of international manufacturing, trade and communication standards for all industrial branches. The main function is to seek standardization of product and safety standards for businesses, companies and organizations at an international level. The standards created by ISO are voluntary, they do not have the authority to impose their standards on any country since ISO is a non-governmental body and does not depend on any other international body. The ISO 27001 Standard is an international and open standard, the purpose of which is to establish a series of minimum requirements that an Information Security Management System (ISMS) must comply with in an organization, public or private, big or small. Companies are looking for efficient means that allow them to ensure and manage the security of information and the means that process it. The ISO 27000 series is the one that meets all the information security standards, the most important of which are the ISO 27001 and ISO 27002 standards.

The main difference between these two standards is that 27001 is based on continuous security management, supported by the identification of risks over time. It is a standard that organizations must certify. It contains a series of requirements that an organization must meet, to be in accordance with good practices. Today it is the most popular security certification applied by companies of all kinds at a universal level. Standard 27002 is a good practice guide that describes a succession of control and management objectives that should be recommended to provide security in the organization. It is a non-certifiable standard. The ISO 27003 standard provides instructions on how to approach management planning to implement the ISMS. The ISO 27004 standard provides a series of best practices to be able to measure the result of an ISMS. The ISO 27005 standard contains various general recommendations and guidelines for information security risk management. The ISO 27006 standard responds to a guide for certification bodies in the formal processes that must be followed when auditing ISMS. The ISO 27007 standard is a guide to auditing the ISMS. The ISO 27799 standard is a guide to be implemented in the healthcare industry. The ISO 27035 standard provides a best practice approach for managing security incident information for organizations.

The standards allow organizations to present and certify a level of quality to the general public, demonstrating that they have the appropriate controls and techniques to ensure the treatment of the data and information with which it is treated. At first they were considered of great interest to large companies, and ISO 27000 standards are currently being studied by medium-sized companies worldwide. This standard is applicable to any organization that has information systems. By complying with the legal data protection regulations, it is possible to reduce problems with customers and users. It offers a guarantee of business continuity based on the Contingency Plan. Increase the commercial value of the company and partners; as well as a great improvement in the image of the organization. Increase in the levels of trust of suppliers, customers, shareholders and partners.

ISSN: 2444-5010

Information Security Management Systems according to the ISO / IEC 27001: 2013 standard must be continuously improved following the philosophy by applying the PDCA cycle methodology (Plan, Do, Verify and Act), (Aldya: 2019) this is done when software, hardware, etc. are updated. A computer security management system (ISMS) guarantees the confidentiality, integration and availability of the data.

Method

The project is developed with a quantitative approach, where the different properties of the variables involved in the project will be quantified. The variables involved in the project are: information security organization, asset management, human resource security, physical and environmental security, communications and operations management, security controls, access, acquisition, development and maintenance of information systems, management of information security incidents, business continuity management and compliance with legal requirements, policies, security standards and the audit of the information systems.

It is a descriptive research because it measures the variables to generate data. The research is non-experimental and cross-sectional, the variables are studied in a defined time, where the most appropriate way to measure said set of variables was determined to be able to give an overview of the state of the information security controls and if they comply with ISO / IEC 27001 of 2013 and observe the quality of information.

To create the software for the Information Security Quality Management System (SGCSI) and measure the maturity model, the following was taken into account:

Gap Analysis (GAP) in ISO 27001

A gap analysis (GAP) is a method of evaluating performance differences between a company's information systems or software applications to determine if business requirements are being met and, if not, what steps to take to ensure they are met successfully. Gap refers to the space between "where we are" (now) and "where we want to be" (the goal to be achieved).

A deficiency analysis can also be called a needs analysis.In the case of our research, a gap analysis was applied using a SWOT matrix (Strengths, Opportunities, Weaknesses, Threats) determining what we lack and the necessary resources to achieve the goals. objectives based on the requirements of ISO 27001.

A gap analysis (GAP) or deficiency analysis therefore consists of an analysis of compliance with both the requirements of ISO 27001 and its controls. It is therefore something similar to an initial audit similar to the best auditing practices in an organization (Amogh Phirke, 2019), so you can have an idea of the degree of implementation of the ISO 27001 standard in the organization can serve to a double objective. Establish the starting point to implement the standard and evaluate the necessary effort as well as have a reliable tool to develop an ISO 27001 implementation plan, also to maintain a tool for evaluating the degree of implementation of the standard during the implementation process and evaluate the degree of progress of the project

Risk analysis vs gap analysis

An analysis of compliance with requirements and controls of ISO 27001 should not be confused with a risk analysis. The compliance analysis identifies what requirements and controls included in the standard we have implemented in the organization and to what degree. On the other hand, a risk analysis offers as a result, the information security controls that are really needed to implement. In other words, a risk analysis establishes the justification for the controls that must be implemented for information security.

Depending on the size and scope of the project, a gap analysis can be performed before starting the implementation of the standard in order to assess the initial situation and plan the necessary resources for the project. Previously, the GAP analysis standard was helpful when preparing the statement of applicability. However, in the current version ISO 27001: 2013 it is necessary to previously perform a risk analysis to determine the real scope of the controls to be implemented.

ISSN: 2444-5010

To obtain an initial audit report on compliance with the standard, a GAP gap or deficiency analysis can be performed before starting the project applied to the generic requirements of the standard. Based on a risk analysis, it is possible, through the analysis of compliance with the controls, to obtain the report to establish the plan for their application and their compliance status, in addition to helping us in the preparation of the Declaration of Applicability.

For the performance of the GAP deficiency analysis on information security, it may be advisable to use a maturity model for the evaluation of compliance. The most common maturity models such as NIST, CITI-ISEM, COBOT, SSE / CM and CERT / CSO propose a model of 5 to 6 levels of maturity or compliance. These maturity models commonly used as tools for IT service management are used to assess how well management processes are performing with respect to internal controls. This model is adapted to establish an audit model that allows us to measure your current level of maturity against the requirements of a specific standard, in this case ISO27001.

As a result, the GAP deficiency analysis will reveal best practices to the internal controls of the Information Security Management system. Maturity levels are not an objective, but rather are a means of evaluating the adequacy of internal controls against the objectives of the management system.

Among the advantages of performing a deficiency analysis using a maturity level model are the following:

- Provides a template for a complete safety program.
- Provides appropriate information to managers to implement security controls.
- Leads towards the use of best practice standards (ISO 27001).

In this model, both the existence or non-existence and the degree of implementation of the 11 controls (domains) that comprise the ISO27001 can be evaluated. The following 6 maturity levels were taken into account to develop the application in its management report:

(Level 0), Non-existence: there is no recognition of the need for the control or requirement.

(Level 1), Ad-hoc: There is some recognition of the need for internal control or requirement. It is applied for a specific problem or task, not generalizable.

(Level 2), Executed - Controls exist but are not documented.

(Level 3), Defined - Controls are in place and adequately documented.

(Level 4), Manipulable and measurable: There is internal control over the application of controls and compliance with the requirement.

(Level 5), Optimized: There is internal and continuous control over the application of controls and compliance with requirements. The effectiveness of the controls is measured by establishing improvement objectives.

To carry this out, a list of questions was used to obtain the level of compliance of the organization under different scenarios according to the defined maturity levels. This allows setting a maturity level for each of the 11 controls. This was solved by developing the questions used in the ISO 27001 standard controls to obtain their maturity values.

Evaluation criteria

If they assigned values according to the maturity levels from 0 to 5 for each control, obtaining for each control an average level of maturity that will be determined by:

Medium Level Compliance = Total score of each Control / Number of total controls

This formula will deliver an average value for each control between 0 and 5, with which the controls and their compliance can be classified among the following values:

Maturity score below 1.65: Does not comply.

Maturity score between 1.66 and 3.25: Partially compliant.

Maturity score above 3.26: Compliance with requirements of the Standard.

ISSN: 2444-5010

All of the above influenced the development of software to measure the quality of Information Security in an Organization and to know if it meets the maturity levels required in the ISO 27001 Standard.

Development of the computer application

The software made allows the establishment of information security measures in any type of organization. For this, it has a modular system that allows the entry of information through the collaboration of managers, area managers and support staff. It is fed back with information and allows the person in charge of information security to carry out an analysis and obtain immediate reports that, when analyzed by the Directors, will allow taking adequate measures to minimize the risks to which the critical assets of the organization are exposed, in its different aspects in information security. Senior managers have realized that information is a critical resource, and perhaps the most important of the organization and for this reason it must be treated appropriately like any other asset in the organization.

Information security is based on the availability, integrity and confidentiality of information assets. There is a manual that provides the logic with which the software has been designed and its technological components on which it works correctly, as well as its proper installation. In the computer application that was developed, photos, videos, documents and notes can be uploaded by USB or by cell phone. The documents that can be obtained are: Policies, Measures, Procedures, Controls, Risks, Suggestions, a Book containing information on each point of the ISO 27001 Standard to clarify any doubts about it in more detail. Documents can be registered for a possible audit, each of the control points of the ISO 27001 Standard can be printed separately, agreements can be signed and saved through the union of the Adobe Reader application, they can be send documents by email for each of the points of the Standard, you can have reports on service providers, you can obtain reports for the Organization's Management, you can obtain missing follow-up reports for each point of the Standard , the different analyzes and reports allow timely decisions to be made for the different people involved.

The design of the database is carried out, taking into account the structure of the controls provided in the ISO-IEC-27001: 2013 standard. This computer application was developed for the information requested in ISO 27001. It is an application so that each user can capture their information related to the questions of the questionnaire for SMSEs with ISO 27001 and also allows to view suggestions.

It starts with a screen where it says security warning, then click on AF_principal and presents an introduction, after having read that, click on the button: Start. (See Figure 1). In this development, the responses of both public and private organizations were taken as a basis so that the responses obtained can be taken as an example. (Here the names of the Organizations and those responsible were intentionally deleted). In each question you can see suggestions for Policies, Measures, Controls and Procedures (See Figure 3), to exit the suggestions click on return to survey to continue capturing the information related to the Organization. It continues with the 151 questions (See Figure 2) and finally in suggestion 151 you can also see a book with the theoretical framework on the content of the ISO 27001 Standard (See Figure 4), to complement all the information, bibliographic references , glossary as well as consult the credits of the authors and research assistants involved. To exit the application, click on finish capture. You also have the option of printing the information captured in detail for each item or in summary.

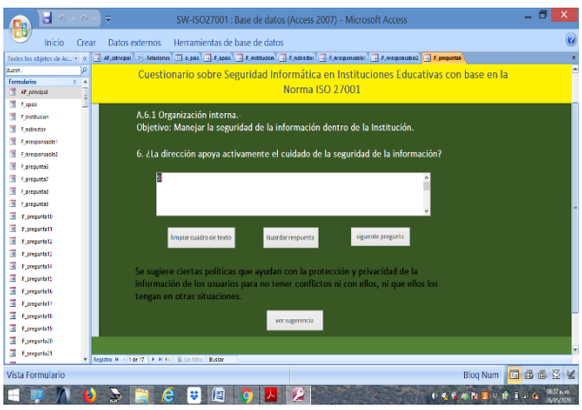

Figure 1 Start screen of the computer application
Source: Own elaboration

ISSN: 2444-5010

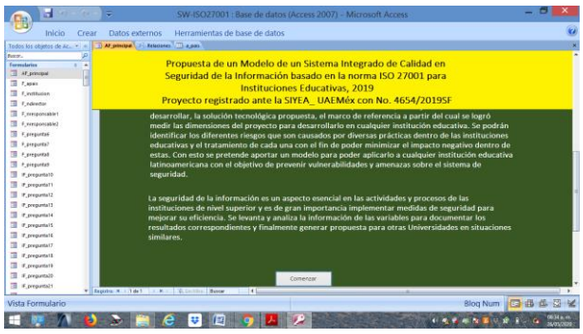

Figure 2 Example of questions from the 151-item questionnaire
Source: Own elaboration

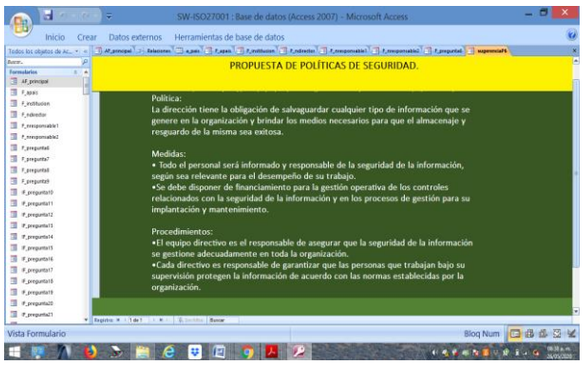

Figure 3 Example of Policies, Measures, Controls and Procedures in each of the questions.
Source: Own elaboration

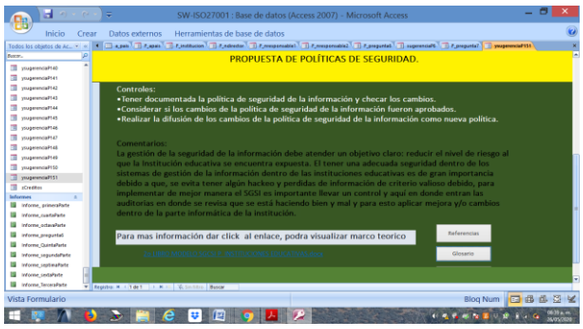

Figure 4 Example of proposal for review of the book link also containing the theoretical framework on the content of the ISO 27001 Standard.
Source: Own elaboration

Results

The construction of a theoretical reference was developed, which starts from the quality of information security to the standards to be studied and the requirements of the tool to be developed. Information collection techniques formats were applied and designed: content analysis and unstructured observation; The analysis of the results delimited the project towards the implementation of fundamental stages for the process of development and implementation of the ISMS.

The selection of international quality standards for information security was made, common aspects were identified that characterize them and allow describing their purposes and way of working. In this way advantages and disadvantages were known. The development of the methodology section corresponds to the description of the technical and theoretical strategies applicable to the scheme required for the development of the software. With the theory, the definition of the methodology to be applied in the selection of characteristics and component elements of the software model was established, moving from theory to practice (Ionna Topa, 2019). The software architecture that corresponds to the implementation of the software model was designed.

SW reports

The reports available to the software are: Project planning, Document on the scope of the SGCSI, Initial Diagnosis, Quantitative Diagnosis of SGCSI, Information Security Policy, Information Security Policies, Roles and Responsibilities, Management of ISMS Risks, Risk Treatment Software (Own development to manage risks), Documentation, ISMS Risk Management, Risk Treatment (Own development to manage risks), Audit reports for review by Management. The statistics report presents a comprehensive view of the Organization showing the status of information security for each of the control points or if you prefer a particular report on any of the control objectives in particular.

Conclusions

The software implementation process implies commitment on the part of the entire organization, so if only the ICT department is involved, this does not lead to the successful implementation of the ISMS. It is necessary that the corresponding roles and tasks be assigned to each of those involved in the organization. Each and every one of the people must be linked to actively participate in the development of quality for the security system, because in one way or another the information is accessible to all those involved. The total commitment at the time of implementing an ISMS must have its knowledge by the managers, to minimize dependency and the way to see this process as a responsibility not only of the ICT department.

ISSN: 2444-5010

It is necessary to know the risks to which the organization is exposed and through an analysis establish the treatment that is considered most appropriate. Remembering that a risk analysis is a process that allows identifying the threats and vulnerabilities of an organization with the aim of generating controls that minimize the effects of risks, which implies determining what or which assets to protect, from what or from whom protect them and how to do it. Some of the main information security risks in organizations are: targeted attacks and exploitation, internal file and database theft, reckless browsing by employees, Phishing, Use of smartphones, tablets and other devices, reckless use of WiFi, weak security keys, misuse of technology, theft of assets such as technological devices, private security systems and CCTV (closed circuit television, computer viruses, theft of confidential information, financial fraud, damage to the image of the organization, modification of files and databases, information leaks, fraud and data theft, vulnerability on the web.

Some organizations describe a "risk analysis", where they have only subjectively evaluated some threats on the assets they know best, without having a clear idea of their value and on the other hand without constituting the totality of the organization's assets. Knowing what can happen and the consequences that this event would generate are key aspects when defining a good security strategy.

The analysis of the proposed variables allowed the software to be better structured, as well as the most appropriate way of defining the ideas that were had for the programming of said software. The possibility of assigning managers in the SMSE was raised to enter only the appropriate information to the software with respect to the functions of those involved. After analyzing the various situations that could arise when entering the information in the software, the use scheme was raised with the ICT manager for his knowledge and experience that gives added value, this in order to be a support and help to capture the requested data in terms of information security, thus obtaining the creation of aids in the software to enter only the requested information and obtain good results in the final reports.

Therefore, it is concluded that the development of the software meets the expectations of functionality and quality parameterization in information security because it has been formulated under the parameters of the ISO 27001: 2013 standard. This software development complies with carrying out an analysis of the quality of information security, this being the basis for establishing an SGCSI in this SMSE, as well as for any Organization that wants to establish measures for the security of its information. The support modules presented as part of the solution in this software, were defined by several investigations that, in addition to confirming the complexity associated with the selection and application of standards, allowed to respond to the objectives set, through different methods, of computer security , formal techniques for data collection, statistical analysis of reports, and the determination of standards evaluation criteria for the consolidation of the modules.

The software model presented for the implementation of the ISMS is a tool that offers risk analysis, specific suggestions, methodological documentation, frequent review, handling of non-conformities. In the software developed, tasks of information collection, data analysis, understanding and application of theories were carried out, among others, which allowed the exchange of knowledge and skills. The final product constitutes a software and tool for the facilitation and consolidation of goals that describes processes to support the implementation process of the Quality System in Information Security measures. With the computer application presented in this document, different statistics, procedures, policies, types of controls, security measures for the control of the information and the systems that are a key piece in the organizations for the decision-making of the managers of the organization. After analyzing the computer risks that organizations currently have to live with, the following results were achieved: proposing policies, measures, procedures and controls for the use, statistics, control and safeguarding for the quality of the information security of the systems in the organization at the time of implementing a computer application of the ISMS, to protect the risks to which they are subjected and at the same time propose solutions that follow up on possible present and future problems that may arise.

ISSN: 2444-5010

References

Acosta Torres, A. T. (2021). Plan de mejora continua para el área de compras y logística de la empresa COMWARE SA enfocado en la gestión de la calidad.

Aldya et al, Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard, 2019 IOP Conf. Ser.: Mater. Sci. Eng. IOP Conference Series: Materials Science and Engineering, doi:10.1088/1757-899X/550/1/012020

Amogh Phirke, Best practices of auditing in an organization using ISO 27001 standard, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S3, July 2019

Buecker, A., Borrett, M., Lorenz, C. and Powers, C., "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," Report REDP-4528-01, 2019.

Fernández Orozco, G. P. (2021). Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.

Gilliam, D.P.; Wolfe, T.L.; Sherif, J.S.; Bishop, M.; "Software security checklist for the software life cycle," Enabling Technologies: Infrastructure for Collaborative Enterprises, 2020. WET ICE 2019, pp. 243- 248, 9-11 June 2020, doi: 10.1109/ENABL.2003.1231415

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). 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.

Ioanna Topa, "From theory to practice: guidelines for enhancing information security management", Information and Computer Security, ISSN: 2056-4961, Publication date: 8 July 2019

ISACA: Control objectives for information and related technologies (COBIT)," http://www.isaca.org/Knowledge-Center/cobit/Pages/Products.aspx.

ISO 10006 (2003). Sistemas de gestión de la calidad — Directrices para la gestión de la calidad en los proyectos.

ISO 21500 (2012). Orientación sobre la gestión de proyectos.

ISO 25000 (2006). Requisitos, evaluación de la calidad del sistema y del software.

ISO 27002 http://iso27000.es/iso27002.html, https://www.isotools.org/software/riesgos-y-seguridad/iso-27001

ISO/IEC 27000 (2005). Dominios y Controles de gestión ISO 27000. Portal ISO 27000 en español. http://www.iso27000.es/download/ControlesISO27002-2005.pdf.

ISO/IEC 27000 (2013). Standard ISO 27000. Portal ISO 27000 en español. Recuperado de http://www.iso27000.es/iso27000.html.

ISO/IEC 27001:2005, "Information technology -- Security techniques -- Information security management systems -- Requirements," Edition: 1 | Stage: 90.92 | JTC 1/SC 27 ICS: 35.040.

Montoya-Quintero, D. M., García-Marín, J., & Moreno-Jimenez, S. J. (2021). Relación entre algunas normas ISO en un modelo conceptual de gestión del conocimiento. *Aibi revista de investigación, administración e ingeniería*, *9*(3), 10-22.

Norma UNE-EN ISO 27001:2005. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Project Management Institute.
Official ISO Website, http://www.iso.org/
Official ITIL Website, http://www.itil-officialsite.com/

PMBOK (2020). Guía de los Fundamentos para la Gestión de Proyectos. 5º Edición. Project Management Institute.

ISSN: 2444-5010

Rodriguez Diaz, J. A., & Ruiz Rojas, Y. A. (2021). Diseño de un sistema de gestión de seguridad de la información para el área de talento humano de la secretaria de educación de Fusagasugá basado en la norma NTC-IEC ISO 27001: 2013.

Tofan, D., "Information Security Standards," Journal of Mobile, Embedded and Distributed Systems, vol. 3, pp. 128-135, 2019

Wendy, Wang,Measuring information security and cybersecurity on private cloud computing, Journal of Theoretical and Applied Information Technology, 15th January 2019. Vol.96. No 1, ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ISSN: 2444-5010