International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 1
ISSN: 2088-5334

The Implementation of Information Security for the Inventory System in a Municipality of Lima-Perú

Jorge Mamani Idme [a,*], Jhon Luis Valenzuela García [a], Shalóm Adonai Huaraz Morales [a], Laberiano Andrade-Arenas [a]

[a] *Department of Systems Engineering and Informatics, Universidad de Ciencias y Humanidades, Los Olivos, Lima, 15314, Perú*

*Corresponding author: *jormamanii@uch.pe*

Abstract— **In recent years, digital transformation has played an important role in all companies investing in technology. This investment greatly contributes to the daily tasks that companies carry out and can mean notable business growth. Also, it brings vulnerabilities that can be exploited by malicious people who, for any reason, seek to damage or appropriate the company's resources, thus directly or indirectly affecting business operations, which is why it is necessary to prevent these acts of vulnerability with the realization of information security. That is why the materials used to implement information security are explained in this work. The purpose of the research work is to identify, analyze, and evaluate to deal with the risks, thus better controlling the risks. This allowed us to land it in the conclusions made based on the objective and methodology used. It allowed us to have a sequence divided into three stages: initiation, planning, and execution. This helps us identify the infrastructure, times, risks, controls, policies, and information assets, in addition to evaluating and treating each risk identified in the District Municipality of Jesás María. This study showed that the implementation of information security has a positive impact since it helps make decisions for the protection of information assets.**

Keywords— **Information security; impact; methodology; protection; vulnerability.**

Manuscript received 7 Dec. 2020; revised 5 Jun. 2021; accepted 20 Sep. 2021. Date of publication 28 Feb. 2022.

I. Introduction

This paper analyzes a municipality in the international arena, that of Spain. It was observed that it is not called municipality in this country but "City Hall". Therefore, we study the Madrid City Council, where it has been possible to observe many services. Those that stand out the most are cultural, sporting, and economic activities. This is done to give great support to the community. That is why, resembling our paper, based on the District Municipality of Jesús María (MDJM), many similarities can be appreciated. These similarities are observed in citizen security, environment, housing, urban planning, and works. There are also social and health services that this "town hall" provides locally. For this, it needs materials, tools, and supplies that must be registered and controlled through inventories so that in this way, they can perform their services.

Thus, to begin with the implementation of information security, we have to know explicitly the process performed by the MDJM. Therefore, the various services that it provides to the community are detailed. Among them, it is in charge of the citizen security service to protect the inhabitants of the district. Video surveillance cameras are also used to detect any illegal activity to achieve a safe environment for the community of Jesús María. In addition, another service that it attends is the payment of the taxes made by the owners of the properties (Owners of the real estate).

This is located in the district's jurisdiction to keep the community safe with the serenade service. Moreover, thus providing services to the streets, parks, and gardens. In addition to providing lease inspection services, authorization or renewal of civil defense certificate; operating license for commercial establishments; and consent for marriage events [1]. That is why the municipality addressed in this paper wants to inspect and manage the inventory. Since this should give a detailed, orderly, and valued control of the supplies and products that the MDJM has in its warehouse. Therefore, it must be ensured that the organization has standards such as ISO 27001 [2].

To avoid possible errors, such as losses or theft, ISO 27001 must be followed, which helps detect and correct this promptly. That is why to keep correct use of the inventory. It is important to have ISO 27001, which helps us analyze and take the necessary steps to resolve any risks. Thus, generating an evaluation and a kind of control is done for risks related to information security [3]. According to the analysis that was made, many items (cleaning objects, video surveillance cameras, serenity clothing, and material for public infrastructure) are taken into consideration, which are stored in the MDJM. This aims to improve citizens' quality of life by taking care of public infrastructure, maintaining security cameras, and protecting them. Poor inventory management could cause significant damage, which happens when no controls. Therefore, there is a need to have efficient control of the number of articles in the inventories of the municipality. Since it could be evidenced that different problems have arisen. Such as poorly trained personnel that generate errors when conducting the review to the warehouse.

Other problems that arise are the loss or theft of warehouse items. Errors due to lack of verification, inadequate warehouse control (not generating reports of incoming materials), errors in the organization of warehouse items. Lack of security in the warehouse (to avoid theft of articles) and delays when searching for articles, thus generating a loss of time [5]. Therefore, we need information security, a unique and neutral endeavor that serves as advice and safeguarding assets. This was done to increase the value and strengthen the operations of the MDJM, reinforcing it to complete its goals. Information security contributes to a methodical orientation that classifies and puts order with which it is possible to assess and progress effectively and efficiently the risk management and control processes.

That is why information security becomes a support structure without losing professional independence and objectivity. We achieve this when executing the necessary procedures for evaluating and studying operational processes [6]. These problems arise when staff makes a mistake in the counting of objects. That is why the system does not allow to provide a quality service. For this reason, information security is implemented in the inventory system to protect the company's information. It also allows for a broad observation of defects within the company and the contingencies. Moreover, thus offer preventive operations suitable for each determined risk [7].

This work aims to identify, analyze, evaluate, and treat risks. This was achieved with the help of information security applied to the MDJM. It was done to mitigate the risks based on the heat map where the risks were established based on the probability and impact. This was achieved by following a methodology that consists of three stages (beginning of planning and execution). It contributes to the improvement of warehouse system management, the verification of the adequate procedures of the information security policies, and the diagnosis of the severity of the risks. Section II explains the material and method to be used, Section III the results and discussions, and finally Section IV the conclusions.

II. Materials and Method

This section explains the fundamental material for the preparation of this paper.

A. Information Security

In everyday life, we can appreciate that studies on information security are important. Since this is the cause of errors, risks, or information violations, they would not want to commit to an organization. Today all companies have to use technologies. Like Antivirus, Antimalware, Antispam, Antispyware, and Firewall. This helps the security of the information, but this "only", does not assure us a safe environment.

We must make use of the information security policies, which are responsible for protecting the information and reducing the risks that may arise in the areas of the organization and responding to events that carry risks, such as the elimination and loss of information. That is why organizations opt for seminars and conferences. As tools for learning information security in an organization, they can prevent and reduce events that negatively affect the information's security, privacy, and integrity. Information security carries already set up pillars: availability, confidentiality, and integrity, which we see below [8].

Pillars of Information Security are important in information security. Since they prevent unfortunate risks from happening in the information, helping to prevent these events that would put the organization at risk, this is done with early prevention, reducing the risks caused by lack of information security. Moreover, that is why the following pillars were born, represented in Fig. 1 Confidentiality, integrity and availability.

Fig. 1 Pillars of information security

The first pillar of confidentiality is keeping the data in the privacy of those authorized. Thus, only those responsible and in charge of these have access to them and not users outside of this responsibility. Integrity, the second pillar, tells us that the data must be complete. This means that unauthorized personnel must not alter the data. Availability, the third pillar, establishes that information must always be available to authorized personnel. This means that the information must be protected if an event compromises the availability of the information; this is covered against these incidents [9].

B. Computer Security, Cybersecurity, or Information Technology Security (IT Security)

We have to bear in mind that, unlike information security, which is responsible for the strategy. Computer security (IT Security) establishes its bases in the operational. As shown in Fig. 2, an organization that does not have computer security (IT Security) is exposed to risks because this is the one that manages the attacks that are presented. By working hand in hand with information security. Computer security, without a good strategy on the part of information security. Their protection efforts fall short of the levels necessary to protect an organization's information.

IT security is responsible for reducing the risks associated with unauthorized access and systems to protect the organization's computing resources, such as information, software, and hardware. Therefore, this allows the organization to benefit since, thanks to this, the organization protects its financial resources from expenses that a good IT security could deal with. It should be noted that computer security (IT Security) is supported by information security. It does not guarantee complete security since this objective is very difficult to achieve [10].

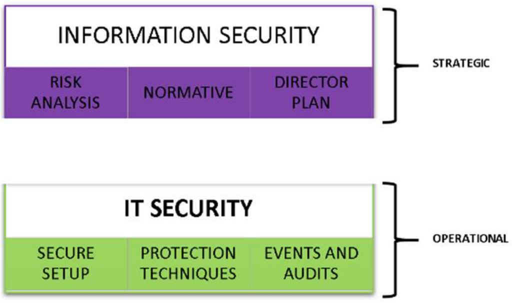


Fig. 2 Information security & Information Technology Security (IT Security)

C. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001

Every company has to be aligned with the principles and standards that are established worldwide; one of these is ISO 27001, which offers us international standards to reduce risks and protect data. Thus, managing information security and an acceptable way to establish, implement, operate, monitor, review, and manage information security. Thus, resulting in improved information security, this ISO 27001 offers many advantages to the organization. Such as identifying threats and vulnerabilities, providing security, and providing confidence to stakeholders (customers and partners). Thus, ISO 27001 sets up the improvement of information security in the organization, giving established international standards, thus allowing us to foresee disasters that may affect information security and reduce the costs of non-security information.

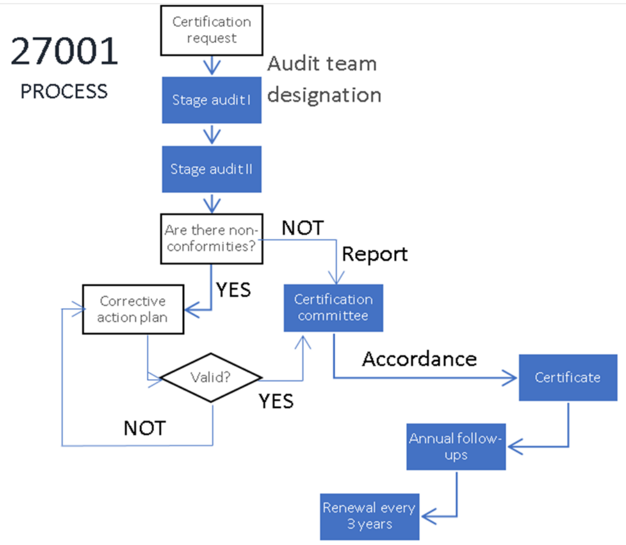


Fig. 3 Certification process of the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001

It also has security control clauses, such as information security policies, information security organization, human resources security, asset management, access control, cryptography, physical and environmental security, operational security, communications security; systems acquisition, development, and maintenance; supplier relationships, information security incident management, information security aspects of business administration and compliance. In Fig. 3, we can see the ISO 27001 certification process [11].

D. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002

As we discussed in the previous point, another of the standards to follow is ISO 27002, which is designed to be used by organizations or companies that intend to select controls to implement an Information Security Management System (ISMS) on the ISO 27001 standard. It also implements information security controls and develops its information security policies. Furthermore, ISO 27002 is divided into fourteen chapters. Within which, the areas to be taken into account are specified to guarantee the security of information within an organization or company. That is why, in Fig. 4, the security management model [12] is observed.

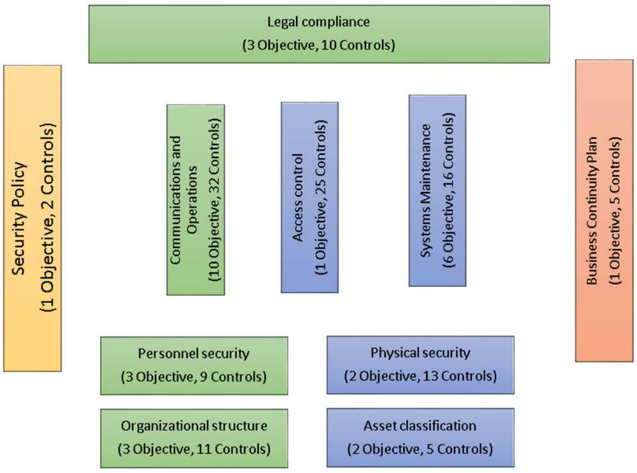

Legal compliance
(3 Objective, 10 Controls)
Security Policy
(1 Objective, 2 Controls)
Communications and Operations
(10 Objective, 32 Controls)
Access control
(1 Objective, 25 Controls)
Systems Maintenance
(6 Objective, 16 Controls)
Business Continuity Plan
(1 Objective, 5 Controls)
Personnel security
(3 Objective, 9 Controls)
Physical security
(2 Objective, 13 Controls)
Organizational structure
(3 Objective, 11 Controls)
Asset classification
(2 Objective, 5 Controls)

Fig. 4 Security management model International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27002: Information management

E. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27005

Among the main regulations, we have ISO 27005, whose main objective is to facilitate and provide guidelines for managing information security risks and ICTs (Information and Communication Technologies). This standard is compatible with or is related to the general notions described in ISO 27001. Moreover, it is outlined as an aid or support for the execution and satisfaction of information security aimed at risk management. ISO 27005 does not detail or recommend any specific risk analysis method. However, it explains an organized, methodical, and rigorous process from risk analysis to develop a mitigation plan. For this, we must be clear about the Risk Management Framework of Fig. 5 [13].

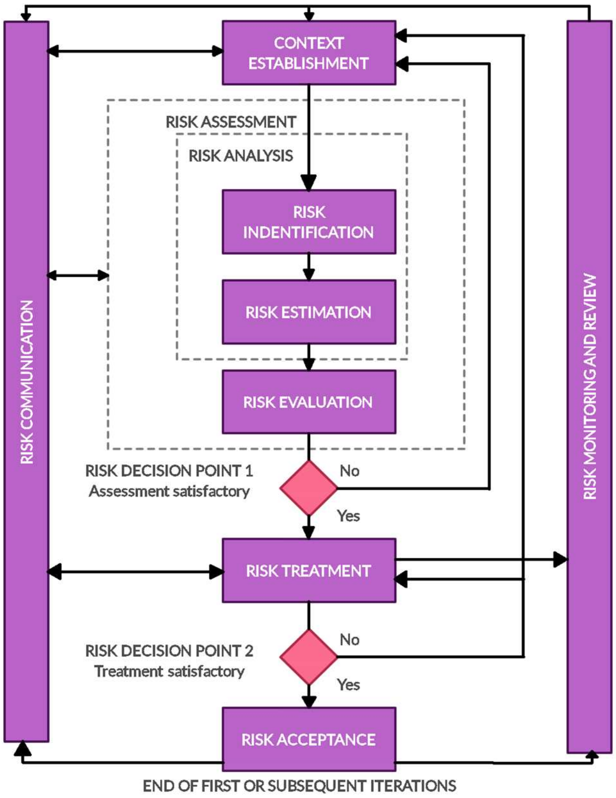


Fig. 5 Process International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27005

F. *Control Objectives for Information and Related Technology (COBIT)*

One of the main functions for the control objectives for information and related technologies (COBIT) was used. It is to apply to information systems throughout the enterprise, including personal computers and networks. It is based on the philosophy that information technology (IT) resources need to be managed by a set of naturally grouped processes to provide the relevant and reliable information that an organization requires to achieve its objectives.

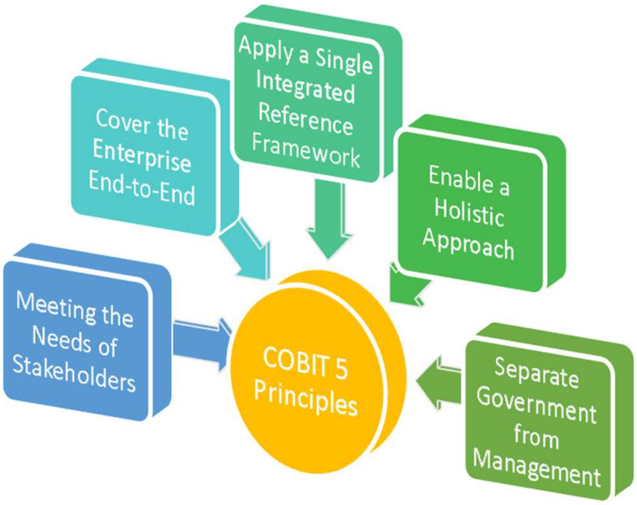

Apply a Single Integrated Reference Framework
Cover the Enterprise End-to-End
Enable a Holistic Approach
Meeting the Needs of Stakeholders
COBIT 5 Principles
Separate Government from Management

Fig. 6 Principles de COBIT 5

A primary objective of the Control Objectives Model for Information and Related Technologies (COBIT). It proposes a framework of action, where information criteria are evaluated, such as security and quality, the resources that comprise information technology are audited, such as human resources, facilities, systems, etc. Moreover, finally, an evaluation is carried out on the processes involved in the organization.

This model defines a frame of reference that classifies the processes of the information technology units of organizations in four main domains. Namely (Planning and organization, Acquisition and implementation, Support and service, and Monitoring). Moreover, the principles of COBIT 5 are detailed in Fig. 6 [14].

G. *Types of Malwares*

The different types of malwares that exist have a specific objective: to threaten the data network and affect the computer's functioning. That is why each malware's objectives and behaviors must be understood to design and implement a prevention mechanism in computer systems and the data network. These mechanisms are the best practices that may exist to reduce threats. In this way, it does not affect the functioning of the computer [15].

1) Phishing: It is a worldwide crime that aims to steal confidential user data. The way of operating is as it happens in fishing. There are several ways to catch the victim. The web pages made for phishing are cloud storage hosting sites and government websites. Currently, the demand for the fight against phishing from the hardware-based approach is poor. This is due to cost and operational factors. However, they prefer using the software-based approach [16].

2) Ransomware: This malware is the most dangerous that exists today in cyberspace. Ransomware is considered one of the most malicious attacks since its appearance. Because it not only corrupts and encrypts information with a password from a remote location. Rather, it steals information from the system by completely blocking the computer screen and showing a pop-up window where ask for payment to return the information. The currency used for payment is a cryptocurrency, which is considered highly dangerous for users or organizations [17].

H. *Computer Risk*

Organizations always are exposed to IT risks that are increasing every day. It is important to know the diverse types of computer risks. For this, social engineering was created, a common computer attack since the attacker persuades the user to allow him access to computers or passwords and extract information or install malicious applications.

Another source of computer attack is the keylogger, which is a tool that captures and records keystrokes when using the keyboard, extracting sensitive information. Other sources of computer attack are worms, Trojans, and spyware. It is a software dedicated to collecting and transmitting user information to another place without permission [18].

I. *Project Management Body of Knowledge (PMBOK)*

One of the main pillars of the Project Management Fundamentals Guide (PMBOK) is risk management. It is the process of explaining how to execute the risk management activities of a project. The key benefit of this process is to ensure that the level, type, and visibility of risk management are consistent with both the risks and the importance of the project to the organization. The entries to the process of planning risk management are plan for project management, the act of constitution of the project, registration of interested parties, environmental factors of the company, and assets of the processes of the organization [19]. In Fig. 7, it is shown the overview of risk management in a project.

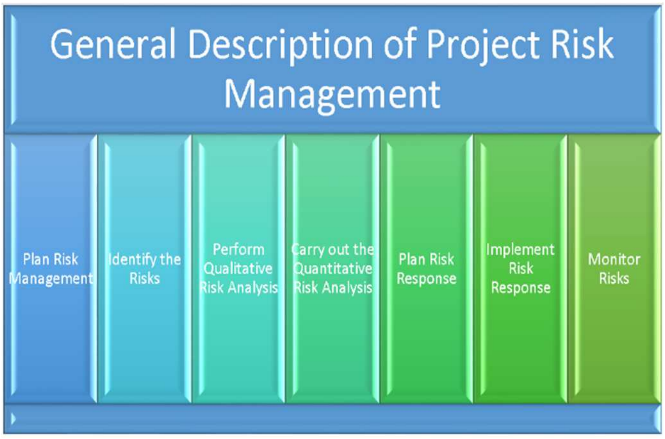

General Description of Project Risk Management
Plan Risk Management
Identify the Risks
Perform Qualitative Risk Analysis
Carry out the Quantitative Risk Analysis
Plan Risk Response
Implement Risk Response
Monitor Risks

Fig. 7 Overview of risk management in a project

J. *Internal audit*

Internal auditing is important because it is a unique and neutral task that serves as an advisor and safeguard assets. Since other companies were able to increase value and strengthen established operations, it can be emphasized that internal auditing serves as a reinforcement to achieve the proposed targets because it contributes to a systematic and orderly orientation that was able to assess and improve the risk management and control processes effectively and efficiently. That is why the internal audit becomes a support structure. Without losing independence and professional objectivity when executing the necessary procedures. For the evaluation and study of operational processes [20].

K. *Quality Management Principles*

It is especially important to know the ISO 9000 family of standards principles based on seven basic principles of quality management. Previously there were eight, but with the new revision of 2015, the principles have been seven. Next, let us mention each of them. The first is the customer focus, where we will focus entirely on the satisfaction of our customers. As a second principle, we have Leadership which focuses on the leader having to implement his ideologies to get benefits. The third principle is the Commitment to People, which reflects the participation of all the organization's staff.

Now we go with the fourth principal process approach, for this, the company must be structured by processes and have marked its objectives for each process. The fifth process is an improvement, where what stands out most is the continuous improvement that every company must have to keep growing. The sixth process is evidence-based decision making; this is very important since it allows a better understanding of the decisions made in the day to day. Moreover, finally, we have the principle of Relationship management as well as its name says it is the relationship that the company has with its customers and suppliers for better communication with each other [21].

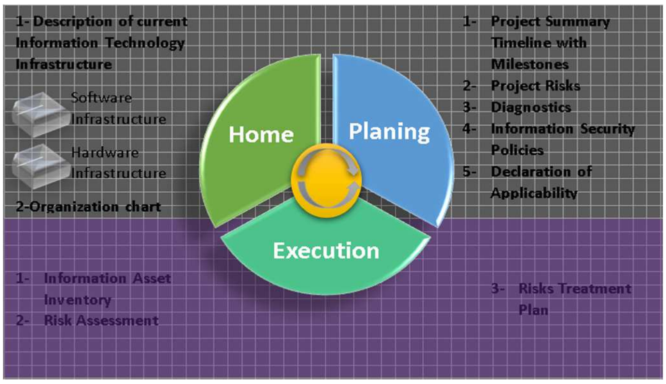

1- Description of current Information Technology Infrastructure
Software Infrastructure
Hardware Infrastructure
2-Organization chart
Home
Planing
Execution
1- Project Summary Timeline with Milestones
2- Project Risks
3- Diagnostics
4- Information Security Policies
5- Declaration of Applicability
1- Information Asset Inventory
2- Risk Assessment
3- Risks Treatment Plan

Fig. 8 Methodology for the implementation of Information Security

In this section, the method that was carried out in the implementation of information security is explained. For the inventory system of the MDJM, this study achieved the objectives with the support of this methodology shown in Fig. 8.

L. *Home*

Description of current Information Technology Infrastructure (TI):

- Software Infrastructure: The various open resource and licensed software portfolios for the productivity of all personnel deployed across the organization are shown here.
- Hardware Infrastructure: Here was the range of work equipment for hardware and Connectivity.

Organization chart: Here was shown the structural organization chart of the organization, which represent graphically, the organization, containing in it the distribution of the organization schematically and with its hierarchical levels.

M. *Planning*

1) Project Summary Timeline with Milestones: Project management software was used here. Thanks to this software known as Microsoft Project (MSP), the beginning and end of the project are known, which shows the progress of the activities and the date, duration, and work structure of the project [22].

2) Project Risks: Here, the value of probability, impact, and level of risk was used. The description of the risk, root cause, consequence, probability (This came out of the probability value), the affected target (Scope, time, cost and quality). Moreover, the impact estimate (This came out of the impact value). The probability per impact was also used (This came from multiplying the probability by the impact estimate and having a total probability per impact for each risk)—the type of risk (This came out of the risk level) and the risk owner. In addition, the response plan, the type of response and the person responsible for the response for each established risk were used.

3) Diagnostics: Here was the current level of compliance with the ISO 27001 standard; for this, two tables were used, one for clauses and one for the domain; individually (by table) contain the current compliance percentage.

4) Information Security Policies: These policies have to be organized, verified, and approved by the organization in order to comply to ensure the quality of the information, proceeding cautiously, inspecting the activity, and reacting promptly to the course of an incident interrupting it [23].

5) Declaration of Applicability: Here were the controls of the ISO 27001 standard, which were not applied in this paper, for which a table was made showing the subdomain, the control, the Apply? And the justification.

N. Execution

1) Information Asset Inventory: Here, a table was shown. The type, name, description, location, owner, manager of the information asset. Moreover, finally, to give the value of the information asset, a table of valuation of the information asset was used, which showed the level of impact on the three pillars of information security (Confidentiality, integrity, and availability).

2) Risk Assessment: Here was a table with the type of information asset, the description of the risk, the vulnerability. The probability of occurrence was assessed (a table was created having the frequency of the probability of occurrence expressed in values). The value of the impact was assessed (its impact on confidentiality, integrity, and availability or pillars of information security was used). The risk was also used, including the level of risk (two tables were created: the first called risk calculation and the second called risk acceptance criteria), the risk owner, and finally, the risk priority assessment.

3) Risk Treatment Plan: A table is shown with the treatment option and the action plan's description. The control, the percentage of the level of effectiveness of the control, the person responsible for the implementation were studied. The level of the residual risk, the risk acceptance, and the state of the risk were also studied.

III. Results and Discussion

A. Home

1) Description of Current Information Technology Infrastructure (TI):

- Software Infrastructure: The MDJM has a diverse software portfolio, which we can observe in Table 1. Both are open-source and licensed for the productivity of all personnel deployed throughout the district. These licenses are original and are installed by the technical staff trained for such work as showed by the ISO 27001 specifically in control A12.6.2 “Restrictions on software installation”.

TABLE I
Software infrastructure

N.º	System	Quantity
	Operating systems	
1	CentOS	1
2	Ubuntu 14.04.1	82
3	Ubuntu Server 14.04.1	4
4	Windows 10	49
5	Windows 7	147
6	Windows 8.1	87
7	Windows Server 2008 R2 Standard	3
8	Windows Server 2012 R2 Standard	8
9	Windows Server 2012 Standard	2
	Database Engines	
10	MySQL	3
11	PostgreSQL	2
12	SQL Server 2014 Standard	3
	Development tools	
13	Visual Studio 2015 Professional	3
	Office Tools	
14	Office 2016 Standard	110
	Web Design Tools	
15	Adobe Creative Cloud 2015	1
	Antivirus	
16	Comodo Endpoint Security	450
	Others	
17	AutoCAD LT 2017	8
18	Corel Draw Suite x7	1
19	GO1984 Camera Management	1
20	SATMUNxp Tax Administration System	285
21	Documentary Information System (SID)	285
22	Observatory and Coexistence System	285
23	Operating Licensing Web System	1
24	Zimbra Email Collaboration 8.7	1

- Hardware Infrastructure: The MDJM is clear that the software depends on something physical to process all the data. That is why it has good work teams, hardware and Networks, and Connectivity, which we can observe in Table 2; to keep information secure.

TABLE II
Hardware infrastructure

N.º	System	Quantity
	Operating systems	
1	Servers	19
2	Complete computers	365
3	Printers	115
4	Scanner	4
	Others	
5	Layer 2 switch	48
6	Layer 3 switch	17
7	Router	19
8	Equipment’s with Wi-Fi	7
9	Antennas	12
10	Radio Link Equipment	53
11	Firewall	1

2) Organization Chart: At this point we detail all the areas involved in the MDJM as shown in Fig. 9. The area in which we focus is in the Management. To which it must give all the results and benefits obtained from time to time for the benefit of all neighbors.

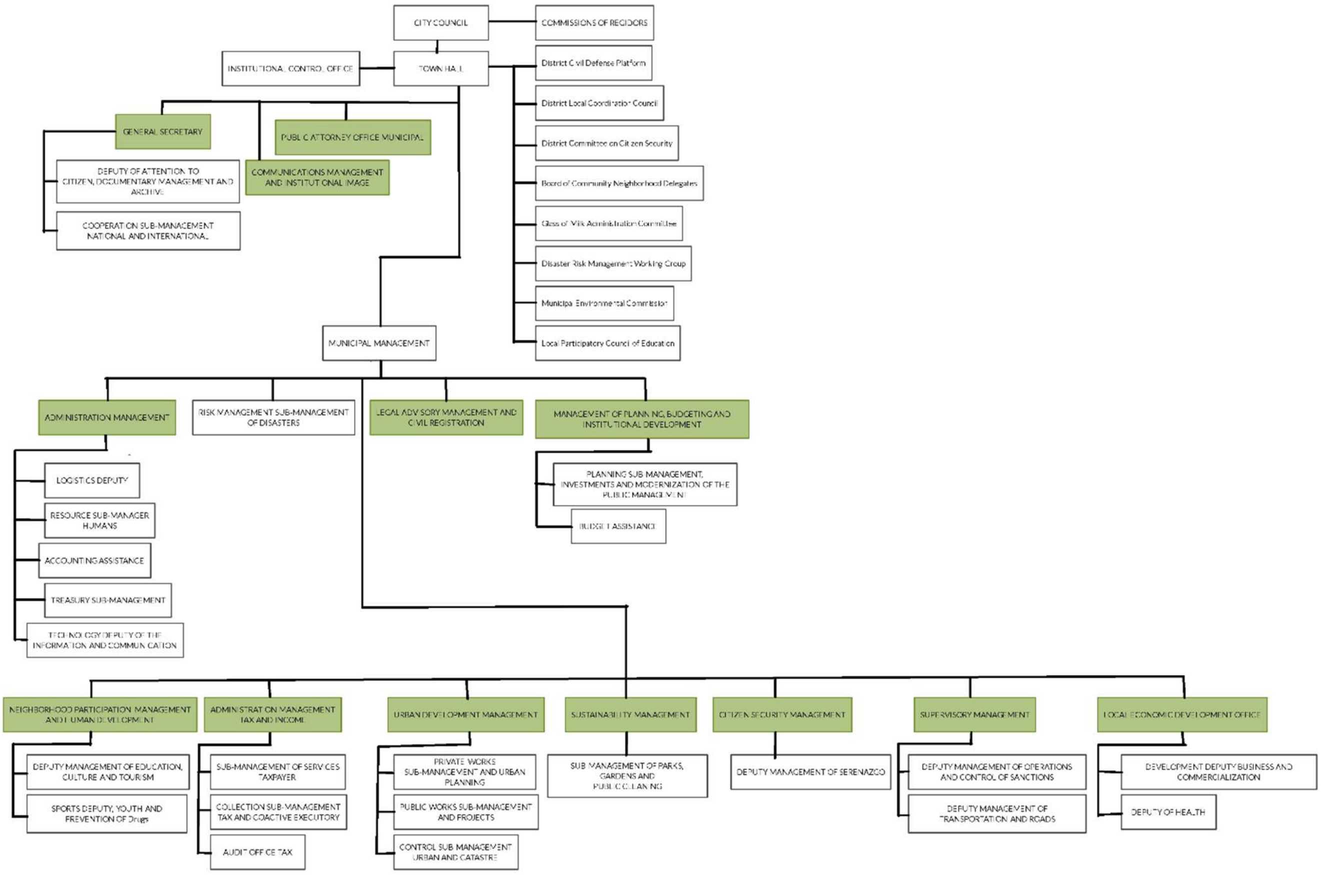

CITY COUNCIL
COMMISSIONS OF REGIDORS
INSTITUTIONAL CONTROL OFFICE
TOWN HALL
District Civil Defense Platform
District Local Coordination Council
District Committee on Citizen Security
Board of Community Neighborhood Delegates
Glass of Milk Administration Committee
Disaster Risk Management Working Group
Municipal Environmental Commission
Local Participatory Council of Education
GENERAL SECRETARY
PUBLIC ATTORNEY OFFICE MUNICIPAL
DEPUTY OF ATTENTION TO CITIZEN, DOCUMENTARY MANAGEMENT AND ARCHIVE
COMMUNICATIONS MANAGEMENT AND INSTITUTIONAL IMAGE
COOPERATION SUB-MANAGEMENT NATIONAL AND INTERNATIONAL
MUNICIPAL MANAGEMENT
ADMINISTRATION MANAGEMENT
RISK MANAGEMENT SUB-MANAGEMENT OF DISASTERS
LEGAL ADVISORY MANAGEMENT AND CIVIL REGISTRATION
MANAGEMENT OF PLANNING, BUDGETING AND INSTITUTIONAL DEVELOPMENT
LOGISTICS DEPUTY
RESOURCE SUB-MANAGER HUMANS
ACCOUNTING ASSISTANCE
TREASURY SUB-MANAGEMENT
TECHNOLOGY DEPUTY OF THE INFORMATION AND COMMUNICATION
PLANNING SUB MANAGEMENT, INVESTMENTS AND MODERNIZATION OF THE PUBLIC MANAGEMENT
BUDGET ASSISTANCE
NEIGHBORHOOD PARTICIPATION MANAGEMENT AND HUMAN DEVELOPMENT
ADMINISTRATION MANAGEMENT TAX AND INCOME
URBAN DEVELOPMENT MANAGEMENT
SUSTAINABILITY MANAGEMENT
CITIZEN SECURITY MANAGEMENT
SUPERVISORY MANAGEMENT
LOCAL ECONOMIC DEVELOPMENT OFFICE
DEPUTY MANAGEMENT OF EDUCATION, CULTURE AND TOURISM
SPORTS DEPUTY, YOUTH AND PREVENTION OF Drugs
SUB-MANAGEMENT OF SERVICES TAXPAYER
COLLECTION SUB-MANAGEMENT TAX AND COACTIVE EXECUTORY
AUDIT OFFICE TAX
PRIVATE WORKS SUB-MANAGEMENT AND URBAN PLANNING
PUBLIC WORKS SUB-MANAGEMENT AND PROJECTS
CONTROL SUB MANAGEMENT URBAN AND CATASTRE
SUB MANAGEMENT OF PARKS, GARDENS AND PUBLIC CLEANING
DEPUTY MANAGEMENT OF SERENAZGO
DEPUTY MANAGEMENT OF OPERATIONS AND CONTROL OF SANCTIONS
DEPUTY MANAGEMENT OF TRANSPORTATION AND ROADS
DEVELOPMENT DEPUTY BUSINESS AND COMMERCIALIZATION
DEPUTY OF HEALTH

Fig. 9 Organization Chart of the MDJM

B. *Planning*

1) Project Summary Timeline with Milestones: Here was a schedule of the project where the breakdown of the progress of the activities was known and the date of duration and work structure of the project.

2) Project Risks: We learned the uncertainty that an event might occur at this point. Which directly or indirectly affects our project resulting in the delay in the delivery times of commitments according to the planned schedule. A risk plan and treatment have to be made to reduce all this.

3) Diagnostics: This item shows the current level of compliance with the ISO 27001, using a table that described the initial diagnosis of clauses and domains; this can be seen in Table 3 and Table 4, respectively.

TABLE III
INITIAL DIAGNOSIS OF CLAUSES

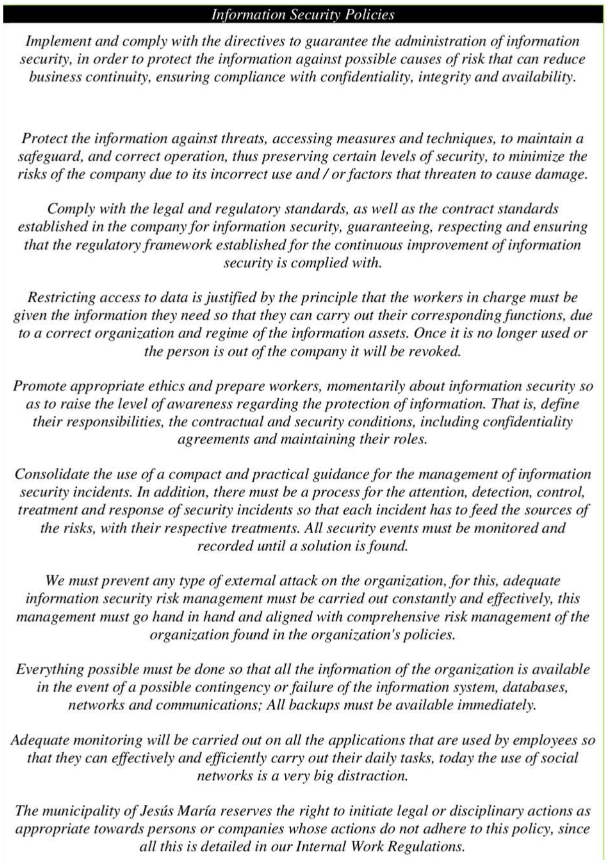
Description of the Clause	% Initial Compliance - Clauses
Context of the organization	38 %
Leadership	53 %
Planning	60 %
Support	68 %
Operation	56 %
Performance evaluation	42 %
Improvements	33 %
% Total Compliance	50 %

TABLE IV
INITIAL DIAGNOSIS OF DOMAINS

Domain Description	% Initial Compliance - Domain
Information security policies	50%
Information security organization	65%
Security linked to human resources	75%
Asset management	50%
Access control	55%
Cryptography	n/a
Physical and environmental security	65%
Security of operations	60%
Communications security	50%
System acquisition, development, and maintenance	40%
Relations with the supplier	45%
Information security incident management	40%
Information security aspects in business continuity management	40%
Compliance	50%
% Total Compliance	53%

4) Information Security Policies: The information security policy of the MDJM is a reference framework aimed at facilitating the definition, management, administration, and implementation of necessary mechanisms, regulations, procedures, and registries. Maintaining the confidentiality, integrity, and availability of information is allowed. To meet the strategic objectives indicated in the Institutional Strategic Plan 2018 – 2020, this is observed in Fig. 10.

5) Declaration of Applicability: Fig. 11 shows all controls of the ISO 27001 that were not used during the development of our paper, highlighting that such controls not shown in these figures are the ones we use.



Information Security Policies

Implement and comply with the directives to guarantee the administration of information security, in order to protect the information against possible causes of risk that can reduce business continuity, ensuring compliance with confidentiality, integrity and availability.

Protect the information against threats, accessing measures and techniques, to maintain a safeguard, and correct operation, thus preserving certain levels of security, to minimize the risks of the company due to its incorrect use and / or factors that threaten to cause damage.

Comply with the legal and regulatory standards, as well as the contract standards established in the company for information security, guaranteeing, respecting and ensuring that the regulatory framework established for the continuous improvement of information security is complied with.

Restricting access to data is justified by the principle that the workers in charge must be given the information they need so that they can carry out their corresponding functions, due to a correct organization and regime of the information assets. Once it is no longer used or the person is out of the company it will be revoked.

Promote appropriate ethics and prepare workers, momentarily about information security so as to raise the level of awareness regarding the protection of information. That is, define their responsibilities, the contractual and security conditions, including confidentiality agreements and maintaining their roles.

Consolidate the use of a compact and practical guidance for the management of information security incidents. In addition, there must be a process for the attention, detection, control, treatment and response of security incidents so that each incident has to feed the sources of the risks, with their respective treatments. All security events must be monitored and recorded until a solution is found.

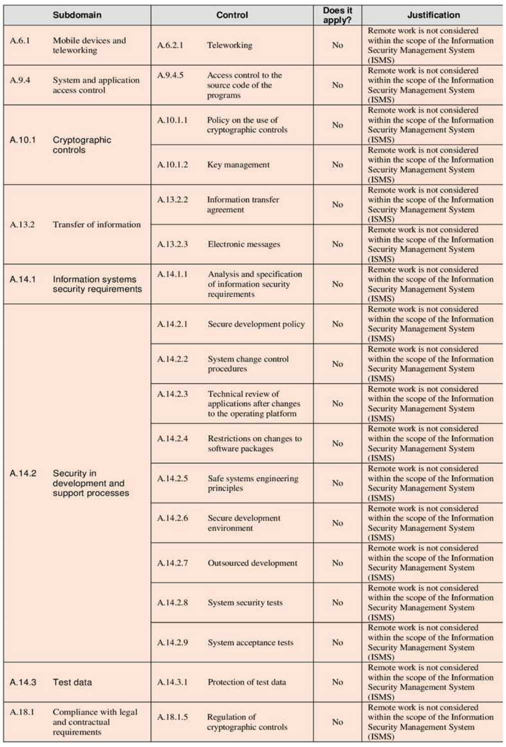
We must prevent any type of external attack on the organization, for this, adequate information security risk management must be carried out constantly and effectively, this management must go hand in hand and aligned with comprehensive risk management of the organization found in the organization's policies.

Everything possible must be done so that all the information of the organization is available in the event of a possible contingency or failure of the information system, databases, networks and communications; All backups must be available immediately.

Adequate monitoring will be carried out on all the applications that are used by employees so that they can effectively and efficiently carry out their daily tasks, today the use of social networks is a very big distraction.

The municipality of Jesús María reserves the right to initiate legal or disciplinary actions as appropriate towards persons or companies whose actions do not adhere to this policy, since all this is detailed in our Internal Work Regulations.

Fig. 10 Information Security Policies



Subdomain		Control		Does it apply?	Justification
A.6.1	Mobile devices and teleworking	A.6.2.1	Teleworking	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.9.4	System and application access control	A.9.4.5	Access control to the source code of the programs	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.10.1	Cryptographic controls	A.10.1.1	Policy on the use of cryptographic controls	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.10.1.2	Key management	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.13.2	Transfer of information	A.13.2.2	Information transfer agreement	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.13.2.3	Electronic messages	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.14.1	Information systems security requirements	A.14.1.1	Analysis and specification of information security requirements	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.14.2	Security in development and support processes	A.14.2.1	Secure development policy	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.2	System change control procedures	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.3	Technical review of applications after changes to the operating platform	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.4	Restrictions on changes to software packages	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.5	Safe systems engineering principles	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.6	Secure development environment	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.7	Outsourced development	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.8	System security tests	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
		A.14.2.9	System acceptance tests	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.14.3	Test data	A.14.3.1	Protection of test data	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)
A.18.1	Compliance with legal and contractual requirements	A.18.1.5	Regulation of cryptographic controls	No	Remote work is not considered within the scope of the Information Security Management System (ISMS)

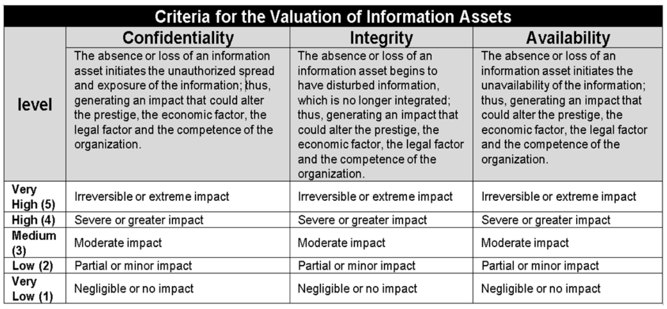
Fig. 11 The declaration of applicability

C. Execucion

1) Information Asset Inventory: The table of information asset inventory is represented in Fig. 13. This table contains the types of information assets shown in Table 5, their respective description. The information asset valuation table shown in Fig. 12 mentioned in the method showed the level of impact on the three pillars of information security (confidentiality, integrity, and availability).

TABLE V
INFORMATION ACTIVES

Type of Information Assets	Description
Data and Information	Databases, Electronic files, Paper documents, and records
Software	Operating systems, Business applications, Utilities
Hardware	Servers, Computers, Imaging Devices
Communication networks	Routers, Switches, Radio link equipment, Firewall
Installations	Clients, suppliers, employees
People	Data center, offices, auditoriums



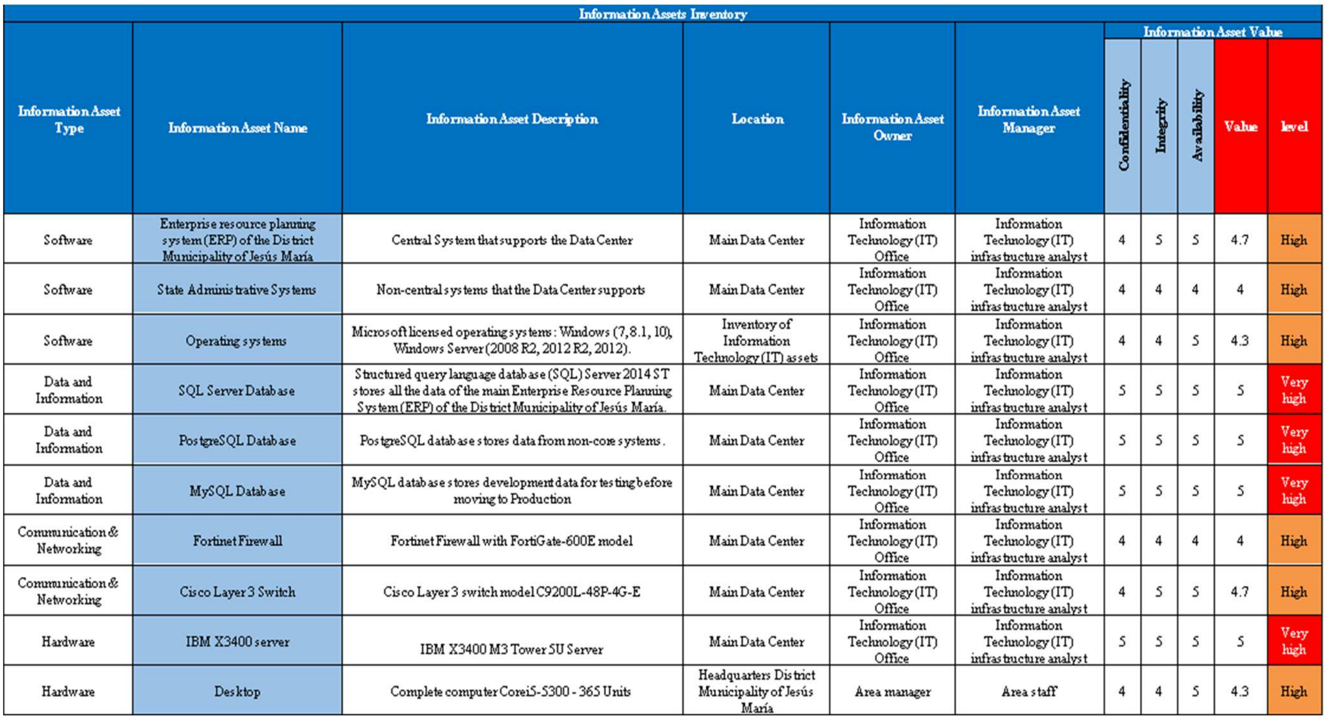
Criteria for the Valuation of Information Assets			
level	Confidentiality	Integrity	Availability
	The absence or loss of an information asset initiates the unauthorized spread and exposure of the information; thus, generating an impact that could alter the prestige, the economic factor, the legal factor and the competence of the organization.	The absence or loss of an information asset begins to have disturbed information, which is no longer integrated; thus, generating an impact that could alter the prestige, the economic factor, the legal factor and the competence of the organization.	The absence or loss of an information asset initiates the unavailability of the information; thus, generating an impact that could alter the prestige, the economic factor, the legal factor and the competence of the organization.
Very High (5)	Irreversible or extreme impact	Irreversible or extreme impact	Irreversible or extreme impact
High (4)	Severe or greater impact	Severe or greater impact	Severe or greater impact
Medium (3)	Moderate impact	Moderate impact	Moderate impact
Low (2)	Partial or minor impact	Partial or minor impact	Partial or minor impact
Very Low (1)	Negligible or no impact	Negligible or no impact	Negligible or no impact

Fig. 12 Valuation of Information Assets

2) Risk Assessment: Here is a table of risk identification and analysis. This is represented in Fig. 14; to achieve optimal results, this table has to consider the probability of occurrence that we can observe in Table 6. The value of the impact that we can see in Table 7 (It shows us that the value of the impact is averaging its impact on confidentiality, integrity, and availability or each pillar of information security). The risk calculation can be observed in Table 8, and the risk acceptance criteria can be observed in Table 9. So, in this way, everything mentioned above is a fundamental part of the risk assessment. Thus, by applying this optimally, we prevent the risk from materializing.

TABLE VI
PROBABILITY OF OCCURRENCE

Probability of Occurrence	
Value	**Frequency**
5	Very frequent
4	Frequency
3	Normal
2	Infrequent
1	Rarely



Information Assets Inventory										
Information Asset Type	Information Asset Name	Information Asset Description	Location	Information Asset Owner	Information Asset Manager	Information Asset Value				
						Confidentiality	Integrity	Availability	Value	level
Software	Enterprise resource planning system (ERP) of the District Municipality of Jesús María	Central System that supports the Data Center	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	4	5	5	4.7	High
Software	State Administrative Systems	Non-central systems that the Data Center supports	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	4	4	4	4	High
Software	Operating systems	Microsoft licensed operating systems: Windows (7,8.1, 10), Windows Server (2008 R2, 2012 R2, 2012).	Inventory of Information Technology (IT) assets	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	4	4	5	4.3	High
Data and Information	SQL Server Database	Structured query language database (SQL) Server 2014 ST stores all the data of the main Enterprise Resource Planning System (ERP) of the District Municipality of Jesús María.	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	5	5	5	5	Very high
Data and Information	PostgreSQL Database	PostgreSQL database stores data from non-core systems.	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	5	5	5	5	Very high
Data and Information	MySQL Database	MySQL database stores development data for testing before moving to Production	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	5	5	5	5	Very high
Communication & Networking	Fortinet Firewall	Fortinet Firewall with FortiGate-600E model	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	4	4	4	4	High
Communication & Networking	Cisco Layer 3 Switch	Cisco Layer 3 switch model C9200L-48P-4G-E	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	4	5	5	4.7	High
Hardware	IBM X3400 server	IBM X3400 M3 Tower 5U Server	Main Data Center	Information Technology (IT) Office	Information Technology (IT) infrastructure analyst	5	5	5	5	Very high
Hardware	Desktop	Complete computer Corei5-5300 - 365 Units	Headquarters District Municipality of Jesús María	Area manager	Area staff	4	4	5	4.3	High

Fig. 13 Inventory of Information Assets

TABLE VII
IMPACT VALUE

Impact			
Confidentiality	Integrity	Availability	Impact Value

TABLE VIII
RISK CALCULATION

IMPACT						
Extreme	5	5	10	15	20	25
Higher	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Less	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5
		1	2	3	4	5
		Rarely	Infrequent	Normal	Frequent	Very frequent
		PROBABILITY				

TABLE IX
RISK ACCEPTANCE CRITERION

Risk Acceptance Criterion		
level	Rank	Description
High	[15 - 25]	Unacceptable risk
Medium	[9 - 12]	Unacceptable risk
Low	[1 - 8]	Acceptable risk

3) Risk Treatment Plan: Here is a table of the risk treatment plan, represented in Fig. 15. This table helped us know the correct way to treat risks; that is, after performing the risk assessment (Identification and risk analysis), we have to choose the most optimal option to treat the risk. These options can be seen in Table 10. The risk treatment action plan had to also be described. As well as the control, the level of control effectiveness (where the risk treatment option and action plan were applied), the implementation manager, the date (Start and End), acceptability, and the state of risk. The residual risk calculation was also applied to define whether the treatment has reduced the calculated risk.

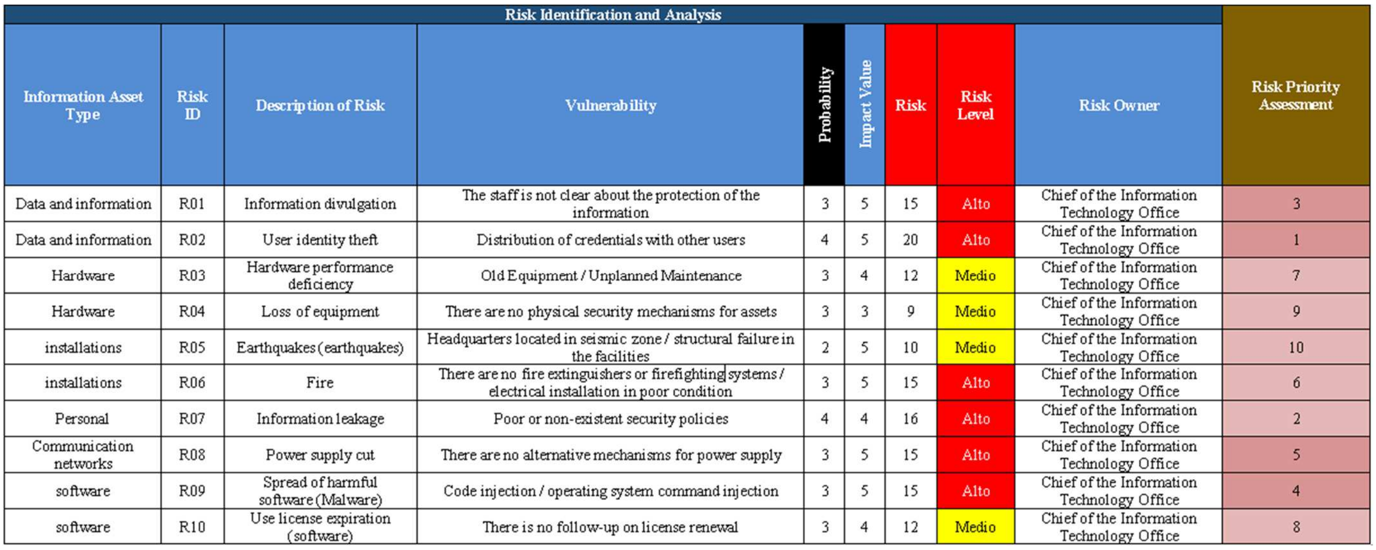
TABLE X
RISK TREATMENT

Risk Treatment	
Avoid	Do not continue with the activity that causes the risk
To mitigate	Reduce the probability of risk occurrence
Share	Transfer the risk to a third party
To accept	Assume the consequences of risk

This table of "final diagnosis of clauses" depicted in Table 11. The results obtained from the "Initial Diagnosis of Clauses" are represented in Table 3. Only in this table was added the final diagnosis of the clauses obtained after the development of the method applied in this study. This was done based on the clauses specified in the ISO 27001, which generated a Comparative Chart of Clauses (Start and End). It can also be seen in Fig. 16 that it was initiated with 50% compliance with the clauses. Moreover, in the end, the method complies with the clauses was increased by 95% leaving only 5% non-compliance.

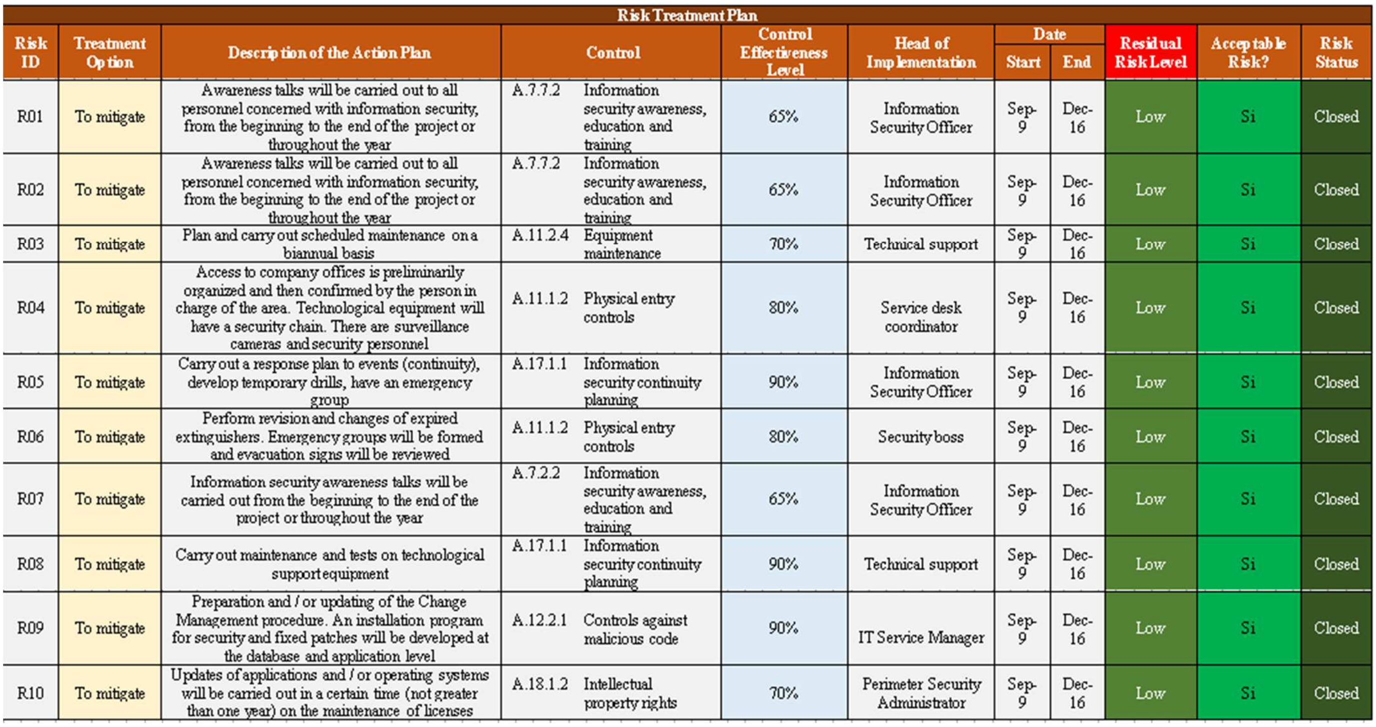
TABLE XI
FINAL DIAGNOSIS OF CLAUSES

Clauses	Start	Final
Context of the organization	38 %	96%
Leadership	53 %	94%
Planning	60 %	94%
Support	68 %	95%
Operation	56 %	92%
Performance evaluation	42 %	94%
Improvements	33 %	98%
% Total Compliance	50 %	95%



Risk Identification and Analysis									Risk Priority Assessment
Information Asset Type	Risk ID	Description of Risk	Vulnerability	Probability	Impact Value	Risk	Risk Level	Risk Owner	
Data and information	R01	Information divulgation	The staff is not clear about the protection of the information	3	5	15	Alto	Chief of the Information Technology Office	3
Data and information	R02	User identity theft	Distribution of credentials with other users	4	5	20	Alto	Chief of the Information Technology Office	1
Hardware	R03	Hardware performance deficiency	Old Equipment / Unplanned Maintenance	3	4	12	Medio	Chief of the Information Technology Office	7
Hardware	R04	Loss of equipment	There are no physical security mechanisms for assets	3	3	9	Medio	Chief of the Information Technology Office	9
installations	R05	Earthquakes (earthquakes)	Headquarters located in seismic zone / structural failure in the facilities	2	5	10	Medio	Chief of the Information Technology Office	10
installations	R06	Fire	There are no fire extinguishers or firefighting systems / electrical installation in poor condition	3	5	15	Alto	Chief of the Information Technology Office	6
Personal	R07	Information leakage	Poor or non-existent security policies	4	4	16	Alto	Chief of the Information Technology Office	2
Communication networks	R08	Power supply cut	There are no alternative mechanisms for power supply	3	5	15	Alto	Chief of the Information Technology Office	5
software	R09	Spread of harmful software (Malware)	Code injection / operating system command injection	3	5	15	Alto	Chief of the Information Technology Office	4
software	R10	Use license expiration (software)	There is no follow-up on license renewal	3	4	12	Medio	Chief of the Information Technology Office	8

Fig. 14 Risk Assessment



Risk Treatment Plan											
Risk ID	Treatment Option	Description of the Action Plan	Control		Control Effectiveness Level	Head of Implementation	Date		Residual Risk Level	Acceptable Risk?	Risk Status
							Start	End			
R01	To mitigate	Awareness talks will be carried out to all personnel concerned with information security, from the beginning to the end of the project or throughout the year	A.7.7.2	Information security awareness, education and training	65%	Information Security Officer	Sep-9	Dec-16	Low	Si	Closed
R02	To mitigate	Awareness talks will be carried out to all personnel concerned with information security, from the beginning to the end of the project or throughout the year	A.7.7.2	Information security awareness, education and training	65%	Information Security Officer	Sep-9	Dec-16	Low	Si	Closed
R03	To mitigate	Plan and carry out scheduled maintenance on a biannual basis	A.11.2.4	Equipment maintenance	70%	Technical support	Sep-9	Dec-16	Low	Si	Closed
R04	To mitigate	Access to company offices is preliminarily organized and then confirmed by the person in charge of the area. Technological equipment will have a security chain. There are surveillance cameras and security personnel	A.11.1.2	Physical entry controls	80%	Service desk coordinator	Sep-9	Dec-16	Low	Si	Closed
R05	To mitigate	Carry out a response plan to events (continuity), develop temporary drills, have an emergency group	A.17.1.1	Information security continuity planning	90%	Information Security Officer	Sep-9	Dec-16	Low	Si	Closed
R06	To mitigate	Perform revision and changes of expired extinguishers. Emergency groups will be formed and evacuation signs will be reviewed	A.11.1.2	Physical entry controls	80%	Security boss	Sep-9	Dec-16	Low	Si	Closed
R07	To mitigate	Information security awareness talks will be carried out from the beginning to the end of the project or throughout the year	A.7.2.2	Information security awareness, education and training	65%	Information Security Officer	Sep-9	Dec-16	Low	Si	Closed
R08	To mitigate	Carry out maintenance and tests on technological support equipment	A.17.1.1	Information security continuity planning	90%	Technical support	Sep-9	Dec-16	Low	Si	Closed
R09	To mitigate	Preparation and / or updating of the Change Management procedure. An installation program for security and fixed patches will be developed at the database and application level	A.12.2.1	Controls against malicious code	90%	IT Service Manager	Sep-9	Dec-16	Low	Si	Closed
R10	To mitigate	Updates of applications and / or operating systems will be carried out in a certain time (not greater than one year) on the maintenance of licenses	A.18.1.2	Intellectual property rights	70%	Perimeter Security Administrator	Sep-9	Dec-16	Low	Si	Closed

Fig. 15 Risk Treatment Plan

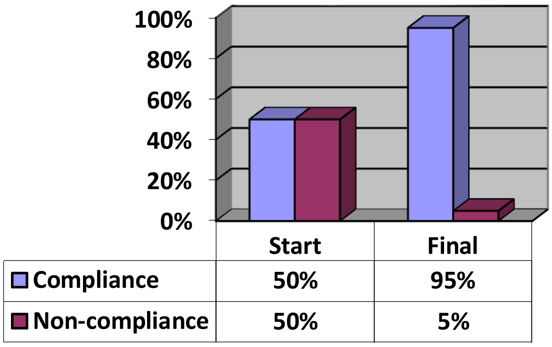


Fig. 16 Comparative Chart of Clauses

In this "final domain diagnostics" table depicted in Table 12. The results obtained from the "Initial Domain Diagnostics" are represented in Table 4. The initial controls that were implemented were determined. This way aims to ensure that no control already established was set aside. In this table, what was done was to add the final diagnosis of the domains, which were obtained after the development of the method was applied in this study. This was done based on the domains specified in the ISO 27001. A comparative graph of domains (start and end) can also be seen in Fig. 17, highlighting that it was started with 53% domain compliance, and after the completion of the method, domain compliance was increased by 94%, leaving only 6% non-compliance.

TABLE XII
FINAL DOMAIN DIAGNOSTICS

Domain Description	Start	Final
Information security policies	50%	99%
Information security organization	65%	97%
Security linked to human resources	75%	96%
Asset management	50%	95%
Access control	55%	93%
Cryptography	n/a	n/a
Physical and environmental security	65%	96%
Security of operations	60%	91%
Communications security	50%	90%
System acquisition, development and maintenance	40%	97%
Relations with the supplier	45%	99%
Information security incident management	40%	90%
Information security aspects in business continuity management	40%	92%
Compliance	50%	91
% Total Compliance	53%	94%

In figure of "Analysis of Indicators" as represented in Fig. 18. The information security policies are shown in Fig. 10, with their indicator, formula, goal, and before and after. The results obtained based on the development of the method applied in this paper. A comparative chart of indicator analysis (before and after) can also be seen in Fig. 19. Highlighting that there was further change in some indicators (Employees trained to fully follow information security policies, preparing employees from all areas on information security issues, and preparing employees who took the information security review). As well as a slight change in the indicator "Compliance with all stipulated to prevent fines and penalties" than S/. 120,310 low to S/. 10,000.

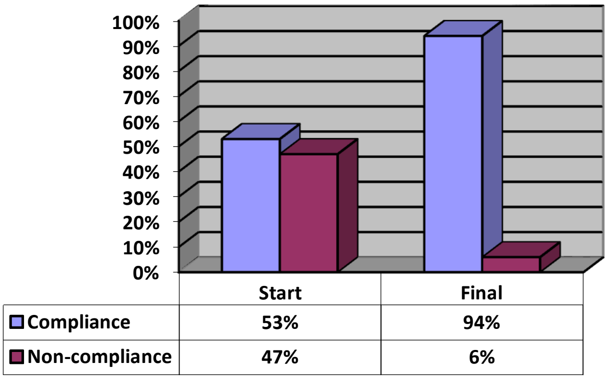
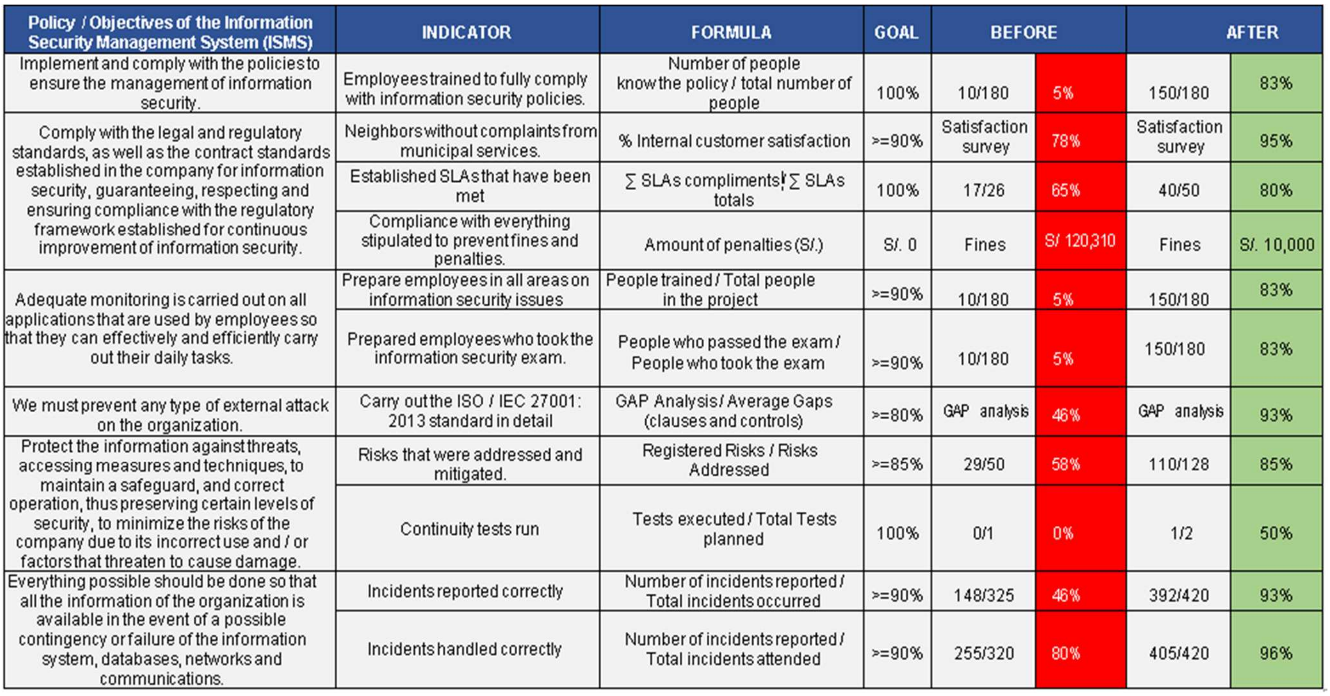
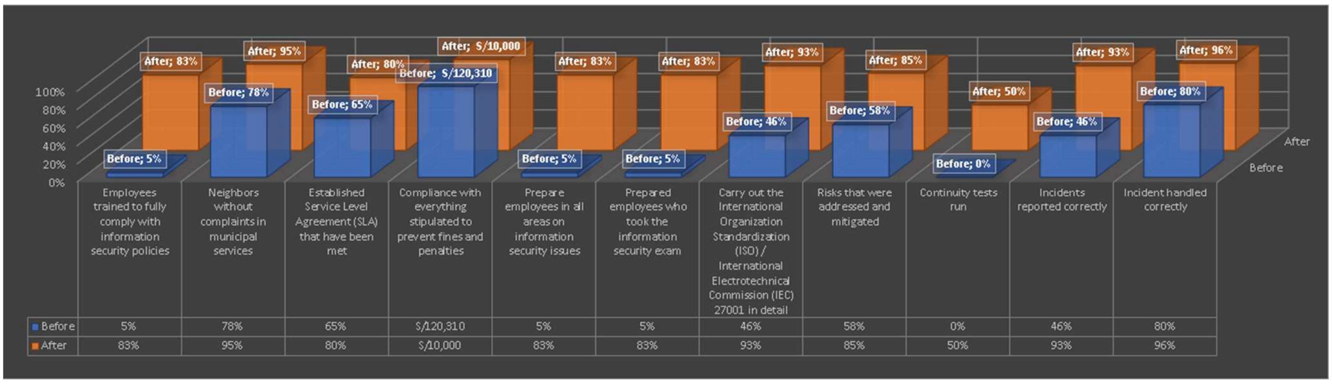


Fig. 17 Comparative Chart of Domains



Policy / Objectives of the Information Security Management System (ISMS)	INDICATOR	FORMULA	GOAL	BEFORE		AFTER	
Implement and comply with the policies to ensure the management of information security.	Employees trained to fully comply with information security policies.	Number of people know the policy / total number of people	100%	10/180	5%	150/180	83%
Comply with the legal and regulatory standards, as well as the contract standards established in the company for information security, guaranteeing, respecting and ensuring compliance with the regulatory framework established for continuous improvement of information security.	Neighbors without complaints from municipal services.	% Internal customer satisfaction	>=90%	Satisfaction survey	78%	Satisfaction survey	95%
	Established SLAs that have been met	∑ SLAs compliments/∑ SLAs totals	100%	17/26	65%	40/50	80%
	Compliance with everything stipulated to prevent fines and penalties.	Amount of penalties (S/.)	S/. 0	Fines	S/ 120,310	Fines	S/. 10,000
Adequate monitoring is carried out on all applications that are used by employees so that they can effectively and efficiently carry out their daily tasks.	Prepare employees in all areas on information security issues	People trained / Total people in the project	>=90%	10/180	5%	150/180	83%
	Prepared employees who took the information security exam.	People who passed the exam / People who took the exam	>=90%	10/180	5%	150/180	83%
We must prevent any type of external attack on the organization.	Carry out the ISO / IEC 27001: 2013 standard in detail	GAP Analysis / Average Gaps (clauses and controls)	>=80%	GAP analysis	46%	GAP analysis	93%
Protect the information against threats, accessing measures and techniques, to maintain a safeguard, and correct operation, thus preserving certain levels of security, to minimize the risks of the company due to its incorrect use and / or factors that threaten to cause damage.	Risks that were addressed and mitigated.	Registered Risks / Risks Addressed	>=85%	29/50	58%	110/128	85%
	Continuity tests run	Tests executed / Total Tests planned	100%	0/1	0%	1/2	50%
Everything possible should be done so that all the information of the organization is available in the event of a possible contingency or failure of the information system, databases, networks and communications.	Incidents reported correctly	Number of incidents reported / Total incidents occurred	>=90%	148/325	46%	392/420	93%
	Incidents handled correctly	Number of incidents reported / Total incidents attended	>=90%	255/320	80%	405/420	96%

Fig. 18 Indicator Analysis



	Employees trained to fully comply with information security policies	Neighbors without complaints in municipal services	Established Service Level Agreement (SLA) that have been met	Compliance with everything stipulated to prevent fines and penalties	Prepare employees in all areas on information security issues	Prepared employees who took the information security exam	Carry out the International Organization Standardization (ISO) / International Electrotechnical Commission (IEC) 27001 in detail	Risks that were addressed and mitigated	Continuity tests run	Incidents reported correctly	Incident handled correctly
🟦 Before	5%	78%	65%	S/120,310	5%	5%	46%	58%	0%	46%	80%
🟧 After	83%	95%	80%	S/10,000	83%	83%	93%	85%	50%	93%	96%

Fig. 19 Comparative Chart of Indicator Analysis

The information security policy conducted has consistency and coherence because it allows having a solid basis to comply with it. Since they were approved by the experts in the field and the person in charge of the organization, they have a contingency plan to the risks and respond to the risks if we compare it with another organization's information security policy [8]. They are based on the information security policy after and not before, as it was done in our research work. This study is based on the ISO 27000 standards using the triple restriction such as confidentiality, integrity, and availability [24]. However, it is limited in using the control objectives of the ISO 27001 standards where the research article carried out if implemented by comparative analysis to narrow the gap through risk diagnoses.

IV. Conclusion

The implementation of information security has been developed, achieving optimal results, as shown in the final diagnosis of the clauses. It was observed that the municipality had only 50% of the clauses at the beginning and the end of the case study; this rose to 95%. It is also shown in the final diagnosis of the domain that the municipality initially had only 53% of the domains, and at the end of the case study, it rose to 94%. Likewise, when comparing the analysis of indicators, an increase is observed in its entirety. Equally important, when looking at the results shown, a continuous improvement is visualized. Future research suggests monitoring the risk assessment to analyze its effectiveness and thus implement improvements. In addition to teaching how to implement information security, the staff is educated through brochures and videos that help them safeguard information assets. Moreover, finally, implement storage of risks, incidents, and events that compromise the well-being of information security to collect evidence that describes the appropriate actions to be taken against these negative factors to establish continuous improvements and count with prevention measures.

References

[1] J. A. Orjuela Castro and W. Adarme Jaimes, "Dynamic impact of the structure of the supply chain of perishable foods on logistics performance and food security," Journal of Industrial Engineering and Management, vol. 10, no. 4, pp. 687–710, Oct. 2017, DOI: 10.3926/jiem.2147. [Online]. Available: http://jiem.org/index.php/jiem/article/view/2147.

[2] I. M. Lopes, T. Guarda, and P. Oliveira, "How iso 27001 can help achieve gdpr compliance," in 2019 14th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2019, pp. 1–6, DOI: 10.23919/CISTI.2019.8760937.

[3] K. J. Moncayo L´opez and C. A. Ortiz Lozada, "Propuesta de iso 27001 para salvaguardar los inventariosde peter pc," B.S. thesis, Universidad de Guayaquil Facultad de Ciencias Administrativas, 2018.

[4] M. Nieles, K. Dempsey, V. Y. Pillitteri et al., "An introduction to information security," NIST special publication, vol. 800, p. 12, Jun. 2017, DOI: 10.6028/NIST.SP.800-12r1.

[5] A. da Veiga and N. Martins, "Defining and identifying dominant information security cultures and subcultures," Computers Security, vol. 70, pp. 72–94, 2017, DOI: 10.1016/j.cose.2017.05.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817300937.

[6] Z. Tumwebaze, V. Mukyala, B. Ssekiziyivu, C. B. Tirisa, and A. Tumwebonire, "Corporate governance, internal audit function and accountability in statutory corporations," Cogent Business & Management, vol. 5, no. 1, p. 1527054, Jan. 2018, doi = 10.1080/23311975.2018.1527054. [Online]. Available: https://doi.org/10.1080/23311975.2018.1527054.

[7] E. F. Alvarado Meza, "Propuesta para la implementación de un sistema de gestión de seguridad de la informaci´on aplicando la norma iso 27001 para industrias ales" PhD thesis, Universidad de Guayaquil.Facultad de Ingenierıa Industrial, 2016.

[8] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," Computers Security, vol. 56, no. Complete, pp. 70–82, Feb. 2016, DOI: 10.1016/j.cose.2015.10.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404815001583.

[9] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," Computers Security, vol. 61, no. C, pp. 169– 183, 2016, DOI: 10.1016/j.cose.2016.06.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816300670.

[10] V. Gil Vera and J. Gil Vera, "Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas," Scientia et Technica, vol. 22, no. 2, pp. 193– 197, Jun. 2017, DOI: 10.22517/23447214.11371. [Online]. Available: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/11371.

[11] V. P. Rathod, "Project implementation of information security management system in tata chemicals ltd," Ph.D. dissertation, Instytut Organizacji Systemow Produkcyjnych, 2019.

[12] W. M. Contero Ramos, "Diseño de una polıtica deseguridad de la información basada en la norma iso27002: 2013, para el sistema de botones de seguridaddel ministerio del interior," 2019.

[13] F. Cabrera and R. Isidro, "Análisis del riesgo de las ticsen el laboratorio de computo de la unidad educativapueblo nuevo mediante la aplicaci´on de la norma iso27005.," B.S. thesis, Babahoyo, UTB-FAFI 2020, 2020.

[14] J. J. Santacruz Espinoza, C. R. Vega Abad, L. F. Pinos Castillo, and O. E. Cardenas Villavicencio, "Sistema cobit en los procesos de auditorías de los de sistemas informáticos," Journal of Science and Research: Revista Ciencia e Investigacion. ISSN 2528-8083 ´ , vol. 2, no. 8, pp. 65–68, Dic. 2017, DOI: 10.26910/issn.2528-

8083vol2iss8.2017pp65-68. [Online]. Available: https://revistas.utb.edu.ec/index.php/sr/article/view/342.

[15] A. D. D. Quintana, "Relación entre los virus informáticos (malware) y ataques en países vulnerables de seguridad en informática utilizando análisis de componentes principales (acp)," Logos, vol. 6, no. 1, 2016, DOI: 10.21503/log.v6i1.1316.

[16] T. Nathezhtha, D. Sangeetha, and V. Vaidehi, "Wc-pad: Web crawling based phishing attack detection," in 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019, pp. 1–6, DOI: 10.1109/CCST.2019.8888416.

[17] J. S. Aidan, H. K. Verma, and L. K. Awasthi, "Comprehensive survey on petya ransomware attack," in 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS), IEEE. Los Alamitos, CA, USA: IEEE Computer Society, Dec. 2017, pp. 122–125, DOI: 10.1109/ICNGCIS.2017.30.

[18] F. M. Arevalo Moscoso, I. P. Cedillo Orellana, and S. A. ´ Moscoso Bernal, "Metodología Ágil para la gestión de riesgos informáticos," Killkana Técnica, vol. 1, no. 2, pp. 31–42, ago. 2017, DOI: 10.26871/killkanatecnica.v1i2.81.[Online].Available : https : //killkana.ucacue.edu.ec/index.php/killkanatecnico/article/view/81.

[19] E. A. Morales Quispe, "Validación metodologıa pmbok en gestión de riesgos del proceso de desarrollo de software empresa sector educación," 2018.

[20] H. C. y Marcelo Mendoza-Vinces y Christian Vera Alava, "Importancia de la auditoría interna para el perfeccionamiento de los niveles eficiencia y calidad en las empresas," Dominio de las Ciencias, vol. 3, no. 2, pp. 908–920, 2017, DOI: 10.23857/dc.v3i2.457. [Online]. Available: https://www.dominiodelasciencias.com/ojs/index.php/es/article/view/457.

[21] S. Sirvent Asensi, V. Gisbert Soler, and E. Perez Bernabeu, "Los 7 principios de gestión de la calidad en iso 9001," 3C Empresa. Investigación y pensamiento crítico, no. 1, pp. 10–18, dic. 2017, DOI: 10.17993/3cemp.2017.especial.10-18. [Online]. Available: http://ojs.3ciencias.com/index.php/3c-empresa/article/view/572.

[22] V. B. Somawarad and J. Rashmi, "Planning and scheduling multi storeyed residential building using microsoft project and application of material management technique," Planning, vol. 6, no. 07, 2019.

[23] A. Merlos, "Polıticas de seguridad y defensa en la erade la posverdad,"Cuadernos de estrategia, no. 197,pp. 83–106, 2018.

[24] A. Nechai, E. Pavlova, T. Batova, and V. Petrov, "Implementation of information security system in service and trade," IOP Conference Series: Materials Science and Engineering, vol. 940, p. 012048, Oct. 2020, DOI: 10.1088/1757-899x/940/1/012048. [Online]. Available: https://doi.org/10.1088/1757-899x/940/1/012048