MANAGEMENT OF INFORMATION SECURITY IN ORGANIZATIONS

Author: Belén García Mesado

Tutor: Juan Darocha Huerta

DEGREE IN BUSINESS ADMINISTRATION

AE1049 – FINAL GRADE WORK

COURSE 2017-18

ÍNDEX

A. TABLE INDEX

B. INDEX OF ILLUSTRATIONS

1. INTRODUCTION

The present essay will try to provide more information about the regulations and good practices of information security in organizations, developing some of the ISO standards that complement this management of security and the governance frameworks that intervene in it.

Likewise, a risk analysis of a particular private company will be carried out, namely, Mediterránea Gestión Social y Cultural SA, in the specific context of the General European Regulation of Data Protection providing bases and recommendations for the future implementation of ISO 31000 in this organization.

Finally, the achieved conclusions after elaborating the presents essay will be exposed.

2. GENERAL OBJECTIVES

The general objective of this project is the study of the analysis of the technical risks that a specific company has, to facilitate its adaptation to the framework of the General European Regulation of Data Protection. The company under study is Mediterránea Gestión Social y Cultural S.A., which was born in 2004 as a limited company and in 2009 became an anonymous one. Its mission, according to the official website of the company is: "to ensure the satisfaction of all its clients from the optimal management of its social, educational, leisure and health services".

The company is dedicated to different educational, leisure, health and social activities. For the practical case, I will focus on the scope of the Home Help Service, which has ISO 9001 and 14001 certifications that guarantee a quality and effective management, always respectful of the sustainability of the environment.

Home Help Service is a municipal service in the city of Castellón that Mediterránea Gestión Social y Cultural S.A. has been managing since 2006, when it won the bidding.

Home Help Service is aimed at families or individuals who are in a situation of special need, because his/her family is unstructured and / or lacks personal autonomy, presenting in their own domestic environment social, educational and psychological care.

3. INTRODUCTION TO NORMATIVE AND GOOD PRACTICES OF INFORMATION SECURITY IN ORGANIZATIONS

This section will define the legal regulations that must be followed by both public and private bodies. Some technical measures associated with good information security practices in organizations will also be analyzed since in recent years, numerous frameworks have emerged: ISO standards for the government and management of the IT.

3.1. Legal

In the legal aspect we find the public sector, which will develop the Spanish National Security Scheme (SNSS) the private sector, which will detail the Organic Law on Data Protection (OLDP) and the General European Regulation of Data Protection (GERDP) -from now on I will call it General Regulation of Data Protection (GRDP)- in addition to its evolution over time and its main differences.

3.1.1. Public sector

The public sector is the set of administrative bodies through which the State complies or enforces the policy or will, expressed in the law of the country.

3.1.1.1. Spanish National Security Scheme

The Government's eGovernment Portal points that SNSS at the "aims, in the field of electronic administration, to establish the security policy in the use of electronic media and it is constituted by basic principles and minimum requirements that allow adequate protection of information ".

Law 40/2015, of October 1st of the Legal Regime of the Public Sector (Official State Gazette, 236, of Friday 2nd October, 2015) of electronic access of citizens to Public Services, established the Spanish National Security Scheme that , approved by Royal Decree 3/2010, of January 8th, which regulates the National Security Scheme in the field of Electronic Administration (Official Gazette of the State, 150, of June 23rd, 2007) aims to determine the security policy in the use of electronic media in its scope of application and will be constituted by the basic principles and minimum requirements that allow adequate protection of information.

In 2015, the modification of the Spanish National Security Scheme was published through Royal Decree 951/2015, of October 23rd, to amend Royal Decree 3/2010, of January 8th, which regulates the National Security Framework in the field of Electronic Administration (Official State Gazette, 264, of November 4th, 2015), in response to the evolution of the regulatory environment, in particular of the European Union, of information technologies and the experience of the implementation of the Scheme. The following new features are introduced:

Table 1: Introduced news Royal Decree 951/2015

Among others, the following novelties are introduced:	
Article 11	The continued management of security as a key aspect that must accompany the services available by electronic means.
Article 15	The requirement, in an objective and non-discriminatory manner, of qualified professionals to organizations that provide security services to Public Administrations.
Article 18	The use, in a proportionate way to the category of the determined system and security level, of those products that have certified security functionality related to the object of acquisition.
Article 24	The deployment of security incident management procedures, and weaknesses detected in the elements of the information system.
Article 27	The formalization of security measures in a document called “declaration of applicability” and the possibility of replacing security measures with compensatory ones when documentary evidence is justified.
Article 29	The figure of the "Safety Technical Instructions" that will regulate aspects

	such as the safety status report, the safety audit, the compliance with the Scheme, the notification of security incidents, the acquisition of security products, the cryptology used in the scope of the Scheme and the security requirements in outsourced environments, among others.
Article 34	The information systems referred to in the Royal Decree shall be subject to an ordinary regular audit, at least every two years that verifies compliance with the requirements of this Spanish National Security Scheme. In addition, with extraordinary character, this audit must be carried out whenever there are substantial changes in the information system that may affect the security measures required
Article 35	Express references to the articulation of the necessary procedures for the collection and consolidation of the information for the annual report of the state of the security and organisms responsible for its realization.
Article 36	Notification to the National Cryptological Center of those incidents that have a significant impact on the security of the information handled and the service provided.
Article 37	The evidences necessary for the investigation of security incidents by the National Cryptological Center.
Article 41	“The Bodies and Public Law Entities will publicize in the corresponding electronic offices the declarations of conformity and

	the security badges of those that are creditors, obtained with respect to compliance with the Spanish National Security Scheme".

Source: National Cryptological Center

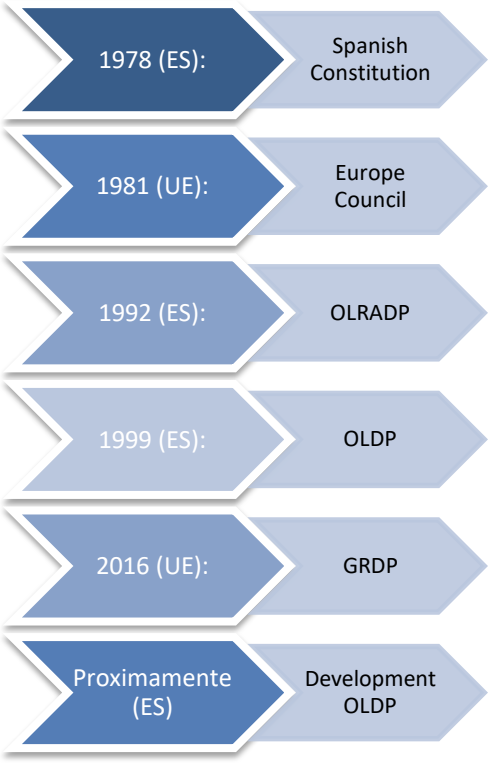
Own elaboration

3.1.2. Private sector

3.1.2.1. Evolution of the regulation of data protection

Before talking about the Organic Law on Data Protection and the new General Regulation of Data Protection (which came into force on May 24th, 2016, but is already mandatory since May 25th, 2018) it is convenient to know what the origin of these laws is, what their reason for being is and how they have evolved over time:

Table 2: Evolution of data protection regulation



Source: Techno Right Advisory

Own elaboration

- 1978 (ES): Art. 18.4 Spanish Constitution:

The first record of data protection regulation takes place in the Spanish Constitution of 1978. Specifically in Art.18.4, which reads as follows: "The law will limit the use of information technology to guarantee personal and family honor and intimacy of citizens and the full exercise of their rights".

- 1981 (EU): 95/46 / EC:

Later in 1981, the existence of an independent authority is expected to ensure this right regarding the protection of natural persons with regard to the processing of personal data and the free circulation of such data: Convention 108 of the Council of Europe, which obtains a greater configuration in the directive 95/46 / CE. "The creation of a control authority that exercises its functions with full independence in each of the Member States is an essential element of the protection of individuals with regard to the processing of personal data."

- 1992 (ES): Organic Law for the Regulation of Automated Treatment of Personal Data (OLRADP):

On October 29th, 1992, the organic law regulating the automated processing of personal data (OLRADP) was established. BOE: "The progressive development of techniques for collecting and storing data and access to them has exposed privacy, in effect, to a potential threat that was previously unknown." This Law prohibited making transfers (neither temporary nor definitive) of personal data that have been the object of treatment.

- 1995 (EU): Directive concerning the protection of natural persons with regard to the processing of personal data and the free circulation of these data:

Three years later, on October 24th, 1995, the directive on the protection of natural persons was established with regard to the processing of personal data and the free circulation of these data, considering, according to the BOE that:

"Data processing systems are at the service of man; that they must, whatever the nationality or residence of natural persons, respect the fundamental freedoms and rights of natural persons and, in particular, privacy, and contribute to economic and

social progress, to the development of exchanges, as well as to the welfare of individuals. "

Therefore, Member States shall ensure, in accordance with the provisions of this Directive, the protection of the freedoms and fundamental rights of natural persons, and in particular of the right to privacy, with regard to the treatment of Personal information. In addition, Member States may not restrict or prohibit the free movement of personal data between Member States.

- 1999 (ES): Organic Law for the Protection of Personal Data (OLDP):

On December 14th, 1999, the organic law for the protection of personal data was implemented in Spain, which aims, according to the BOE, to "guarantee and protect, with regard to the processing of personal data, public liberties and the fundamental rights of natural persons, and especially their honor and personal and family privacy"

- 2016 (EU): General Regulation of Data Protection (RGDP):

According to the official newspaper of the European Union, on May 25th, 2016, the General Regulation of Data Protection was enacted. It aims:

"*To establish the rules regarding the protection of natural persons with respect to the treatment of data. Personal data and the rules relating to the free movement of such data. To protect the fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data. The free circulation of personal data in the Union can not be restricted or prohibited for reasons related to the protection of individuals with regard to the processing of personal data. "*

- Coming soon (ES): Development of an Organic Law for the Protection of Personal Data.

3.1.2.2. Organic Law on Data Protection

The Organic Law 15/1999 of December 13th, Protection of Personal Data (Official Gazette of the State, 298, of December 14th, 1999) states that "the present Organic Law 15/1999, of December 13th, Protection of Personal Data is intended to guarantee and protect, as regards the processing of personal data, public liberties and fundamental rights of natural persons, and especially their honor and personal and family privacy. That is, to limit the degree of intrusion into our privacy that new technologies can generate, as well as the indiscriminate traffic of personal data. Its last modification took place on March 5th, 2011.

Table 3: Main obligations of the OLPD

Main obligations of the OLPD
Notify the files to the Spanish Agency for Data Protection for registration in the General Data Protection Registry.
Ensure that the data are of adequate and truthful quality, obtained lawfully and legitimately and treated in a proportional way to the purpose for which they were collected.
Guarantee the fulfillment of the duties of secrecy and security.
The owners of personal data must be in formed when collecting them.
Obtain consent for the processing of personal data.
Facilitate and guarantee the exercise of the rights of opposition to the treatment, access, rectification and cancellation.
Ensure that in its relations with third parties that provide services which entail access to personal data, the provisions of the OLPD are complied with.

Source: Spanish Agency for Data Protection

Own elaboration

3.1.2.3. General Regulation of Data Protection

On May 25th, 2016, the General Regulation of Data Protection (GDPR) came into force, which began to be applied on May 25th, 2018 and replaced the Organic Law on Data Protection. This period of two years was aimed at allowing the States of the European Union, the Institutions and also the companies and organizations that

process data, to be prepared and adapted by the time when the Regulation was applied.

In general terms, the new Regulation seeks to strengthen the protection of the right of individuals to the protection of their personal data within the community environment, through the implementation of a single set of rules directly applicable to the legal systems of Member States.

This harmonization of data protection regulations favors the achievement of a true digital single market, by guaranteeing the confidence and security of consumers and the free circulation of personal data between the EU Member States. The novelties that this Regulation incorporates require, for the majority of countries, a conscientious reform of their respective legislations in force in this matter, hence the transitory period of two years for its entry into force.

As a result or the greater protection of people's rights over their data and the reinforcement of the different control mechanisms over them, entities that deal with their daily activity a large amount of personal data, must adapt their protection policy of data so as not to incur disciplinary responsibility.

Basic principles

GDPR aims to provide a single European framework for data protection, improve the process and reduce bureaucratic procedures to contribute to the freedom of movement of organizations that will acquire a greater commitment to the management and privacy of data. These are some of the basic principles on which this regulation is based:

- Relating to data protection: The information in the collection of personal data must be clear so that it is easily understood by the interested party. In addition, the data must be collected in a limited manner to what is necessary since they must have a previously established purpose that must also be legitimate. On the other hand, they must be kept updated and stored in a way that ensures their safety.

- Relating to the processing of data: The treatment of the data must be lawful. A lawful treatment occurs when we obtain the express consent of the interested party for its use.

- Relating to the international sending of personal data: It is prohibited to send personal data outside the European Economic Area to a country that does not offer sufficient protection to them. In the absence of a guarantee, that transfer may be limited by certain contractual clauses.

3.1.2.4. Differences between the OLPD and the GDPR

Trying to synthesize the main novelties and actions demanded by the new GDPR, regarding the OLPD we find the following questions:

1. Unmistakable consent

The new data protection regulation rejects the tacit consent that the client makes for the use of his data and oblige the revision of the clauses of the company so that the consent is free, specific, informed and unambiguous. That is to say: it is deduced from a clear affirmative action of the interested party. Therefore, data can only be used for the purposes stipulated from the beginning, since any other use will be considered illegal.

The consents that have been acquired before May 25th, 2018, will be valid as long as they have been made according to the criteria of the future regulation. After this date, all consents must be clearly expressed and revocable. An example of this is the cross that appears marked by default on web pages that refer to: "I accept the terms and conditions." This may continue to appear but in no case may it appear marked in advance.

2. Clauses and information policies

The right of people to know the purpose and treatment of their personal data when requested is extended. The novelties coming from the regulations must be transmitted to the client by means of habitual communication tools, such as the use of web pages,

e-mail, and it is convenient to carry out a formal review and adaptation of the information policies of the companies.

3. Delegate of data protection

The new regulation requires, only if the company in question carries out a habitual and systematic observation of stakeholders and if it deals on a large scale with special categories of data, that companies have a professional who acts as an internal auditor and identifies the risks in the protection of certain data and provide solutions to the company. This figure has the obligation to transmit to the Control Authorities the failures or breaches in the security in less than 72 hours and to request the previous authorization to implant.

In addition, this delegate of data protection will be responsible for establishing the culture of data protection within the entity and will have full access to the top management to advise and reform those processes or methods that are necessary for compliance with the new proactive policies in this matter.

4. Evaluation of the Impact on Data Protection (IDP)

There is an obligatory nature of launching an Impact Evaluation on the Protection of Personal Data in companies. This tool is very useful to advance the privacy of the entire life cycle of the data introduced when subjected to analysis to check whether it puts the fundamental right at risk.

5. Recognition of new rights:

In the previous OLPD the ARCO rights were recognized, namely: the right of access, rectification, cancellation and opposition. In the presence of the new GDPR, new rights are recognized: the right to be forgotten, the portability of data, the limitation of the processing of data, the extension of the right of access to interested parties (allowing obtaining a copy of the registration of them) and the freedom of circulation of data in the community environment. Entities must implement agile response mechanisms by the treatment manager that does not delay or slow these actions.

6. Measures of proactive responsibility:

The new GDPR does not establish specific control and security measures but invokes the principle of proactive responsibility or prevention of data processors according to the inherent risks of each organization. Among the main actions that are established, these are highlighted:

- Risk analysis, data protection from design and default.
- Maintenance of a record of treatment activities.
- Impact evaluation of data protection (known as EIPD): those responsible for the treatment must identify, before the implementation of a specific measure, those that may cause a serious risk to the rights and freedoms of the interested parties.

3.2. Technician: norms and governance frameworks

Within this section, governance frameworks will be developed which are a set of actions carried out by the area of information technologies in coordination with the top management of organizations to mobilize their resources more efficiently through processes and relational mechanisms. We will include within this scope the COBIT 5, the CSIRT and the ISO 38500.

On the other hand, we will analyze the ISO (27000, 27002 and 31000) that focus on the security systems of organizations and the management of their risks.

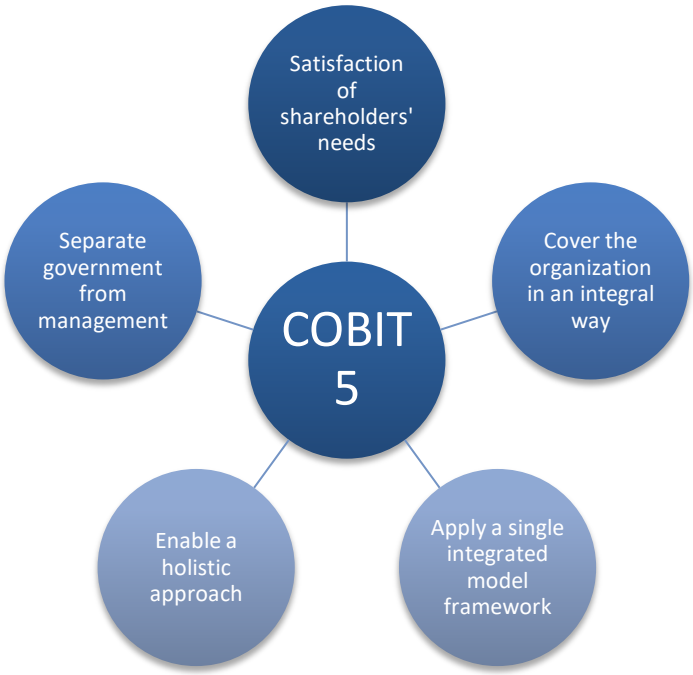
For a better understanding and organization, ISO standards have been grouped into one section and numerically ordered from lowest to highest.

3.2.1. COBIT 5

The global non-profit association ISACA defines COBIT 5 (Control Objectives for Information and related Technology) as "a global management and business framework for the governance and management of IT (information technology) of the company". That is, a set of support tools used by managers to reduce the gap between control requirements, technical issues and business risks and thus develop a clear policy that allows the control of IT in the organization.

The COBIT 5 has 5 main principles which are the following:

Table 4: Five main principles of COBIT 5



Source: COBIT 5, 2012 ISACA

Own elaboration

Satisfying the needs of shareholders: the needs of shareholders are aligned with specific business objectives, IT objectives and enabling objectives. In this way it is possible to optimize the use of resources when obtaining benefits with an acceptable level of risk.

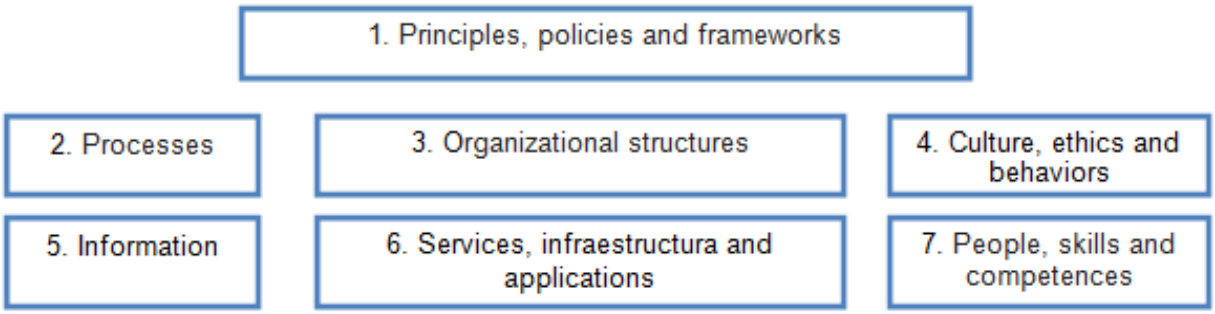
Covering the organization in an integral way: IT governance and IT management are assumed from a global perspective in such a way that all corporate IT needs are covered.

Apply a single integrated model framework: COBIT 5 integrates the best Information Systems Audit and Control Association (ISACA) frameworks as Val IT, which relates the COBIT processes with the management processes required to achieve a good value of IT investments.

Enable a holistic approach: the COBIT 5 enablers are identified in seven categories that cover the company from end to end. Individually and collectively, these factors

influence how IT governance and IT management operate based on business needs. They are the following:

Table 5: COBIT 5 Enablers



Source: COBIT 5, 2012 ISACA

Own elaboration

Separate government from management: COBIT 5 clearly distinguishes the areas of IT governance and IT management.

- IT governance is understood as the functions related to the evaluation, management and monitoring of IT. In this way, it seeks to ensure the achievement of business objectives, it assess the needs of shareholders and the existing conditions and options.

- Management is more related to the planning, construction, execution and monitoring of activities aligned with the direction established by the government agency for the achievement of business objectives.

3.2.2. CSIRT

CSIRT (Computer Security Incident Response Team) is a forum whose main objective is to protect cyberspace by exchanging information on cybersecurity and acting quickly and in a coordinated manner before any incident that may simultaneously affect different entities worldwide, state, business...

This forumisan independent, trustworthy and non-profit platform, made up of CSIRT / CERT security incident response teams, whose scope of action or community of users in which it operates, is located within Spanish territory.

As the CSIRT.es Forum shows, these are some of its main objectives:

- Promote cooperation between Spanish CSIRTs, both in the field of response to incidents and in the development of joint projects that contribute to the improvement of security both in its scope of action and in the Spanish community.
- Share relevant information about security incidents and any other type of intelligence information deemed useful.
- Launch coordinated actions and recommendations in situations that require so.
- Encourage the creation of new CSIRTs in the national territory.
- Serve as a safety event reference site.
- Collaborate with other similar Forums and initiatives at national and international level.

Purposes of the CSIRT:

- Control and minimize any type of damage to the organization and its information.
- Evidence what happened and document it.
- Coordinate activities for a fast and efficient recovery of activities that have been affected.
- Achieve the least tolerable impact.
- Prevent similar events from occurring in the future.
- Maintain a knowledge base to record the lessons learned from these events.
- Implement activities to share information related to security incidents with other CSIRTs, for dissemination purposes, and trying to mitigate the impact of new threats, vulnerabilities or attacks

CCN-CERT

An example of a center attached to the CSIRT is the CCN-CERT (National Cryptological Center) which, according to its official website, is defined as "the ability to

respond to information security incidents at the National Cryptological Center, attached to the National Intelligence Center."

This service was created in 2006 and its mission is to contribute to the improvement of Spanish cybersecurity, being the national response alert center that helps to respond quickly to cyber attacks and to effectively confront cyber threats.

3.2.3. ISO

As we have mentioned before, within the ISO standards to analyze, we will study the ISO 38500 standard that refers to the section on governance frameworks and the ISO 27001, 27002 and 31000 standards. The practical case that is shown ahead will be carried out based on the latter.

According to the UNE-ISO standard (AENOR) it defines the ISO (International Organization for Standardization) as "a worldwide federation of national standardization bodies

As indicated by the UNE-ISO (AENOR) regulation:

The preparation work of the international standards is normally done through the ISO technical committees. Each member body interested in a subject for which a technical committee has been established, has the right to be represented on that committee. International organizations, public and private, in coordination with ISO, also participate in the work.

3.2.3.1. ISO 27001

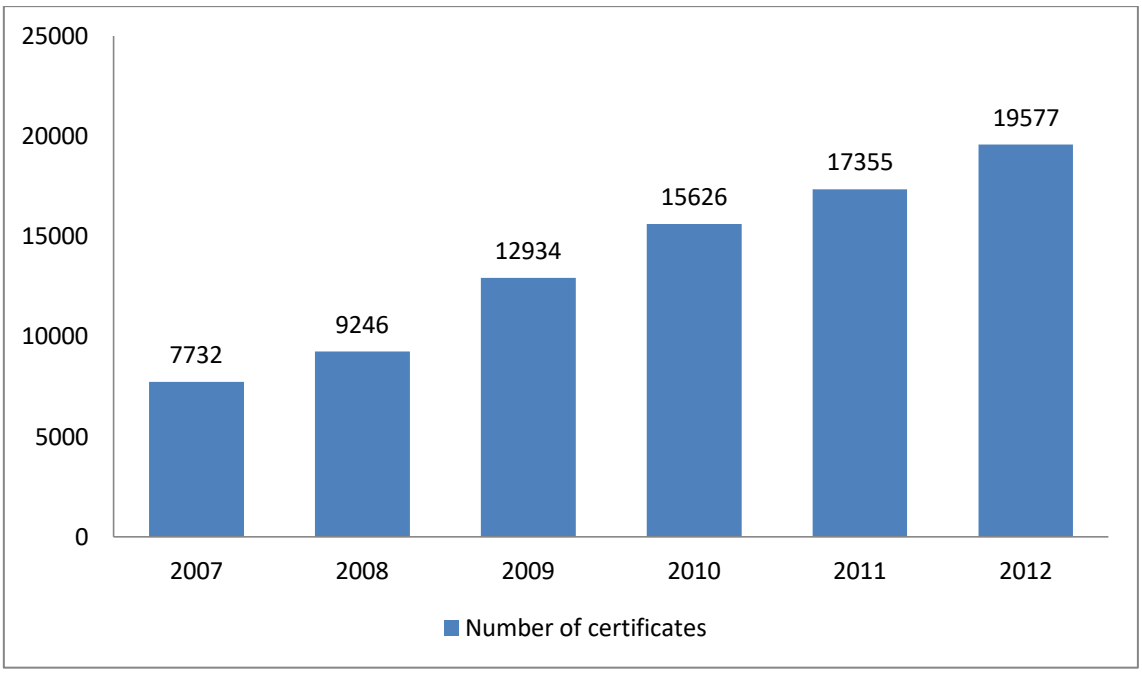
This international standard provides a model for the creation, implementation, operation, supervision, review, maintenance and improvement of an information security management system (ISMS).

One of the main aspects of ISO 27001 is that it allows a company to be certified, that is, an independent certification entity confirms that information security has been implemented in that organization in compliance with ISO 27001. Thank you to this the

ISO 27001 has become the main norm worldwide for the security of the information and many companies have certified its fulfillment.

The following graph, extracted from the ISO survey on certifications of the Standard for management systems, shows the impact that the implementation of ISO 27001 has had worldwide in the organizations.

Illustration 1: Evolution of ISO 27001 certificates worldwide



Source: ISO survey on certifications of the standard for management systems

Own elaboration

In the following chart we can see how the level of ISO 27001 certifications shows annual growth. In 2007 there were 7,732 worldwide certifications, while in 2012 there were 19,577 certifications.

The latest figure recorded in 2016 regarding the level of global certifications of ISO 27001 amounts to 33,290 certifications, which suffered an increase of 21% over the previous year.

A. ISO 27001 Process

The central axis of ISO 27001 is to protect the confidentiality, integrity and availability of information in a company, investigating what are the potential problems that could

affect the information through a risk assessment. After this, it defines what must be done to prevent these problems from occurring. In Table 5 we can see that ISO 27001 is divided into seven processes that the company in question must implement and the content of each process. They are the following:

Table 6: ISO 27001 Processes

Context of the organization	The organization must determine the external and internal issues that are relevant to its purpose and that affect its ability to achieve the expected results of its information security management system. In addition, the organization must determine the interested parties that are relevant to the information security management system and the requirements of these interested parties that are relevant to the security of the information.
Leadership	Top management must demonstrate leadership and commitment regarding the information security management system as well as establishing an information security policy that, in a few words, is adequate for the purpose of the organization.
Planning	When planning, the organization must consider the context of the organization and determine the risks and opportunities in order to ensure that the information security management system can achieve its intended results.
Support	The organization must determine and provide the necessary resources for the establishment, implementation, maintenance and continuous improvement of the information security management system.
Operation	The organization must plan, implement and control the processes necessary to comply with the information security requirements and to implement the determined actions. The organization must maintain documented information to be confident that the processes have been carried out as planned.
Performance evaluation	The organization must evaluate the performance of

	information security and the effectiveness of the information security management system. This can be achieved through internal audits that must be carried out at planned intervals, to provide information about whether the information security management system meets its own requirements.
Improvement	When a non-conformity occurs, the organization must react to it by taking actions to control and correct it and face the consequences. On the other hand, the organization must continuously improve the suitability, adequacy and effectiveness of the information security management system.

Source: Standard UNE-ISO 27001

Own elaboration

B. Advantages of ISO 27001

There are 4 essential business advantages that a company can obtain with the implementation of this standard for information security:

- Comply with legal requirements: there are increasingly more laws, regulations and contractual requirements related to information security. By implementing ISO 27001, you have the guarantee of being compliant.

- Obtain a commercial advantage: when comparing two companies from the point of view of potential customers, a competitive advantage would be the fact of having the ISO certificate in relation to their safety. Which would cause them to opt for this option as a secure company.

- Lower costs: the penalty for committing failures in the security of the clients will have higher cost each time. Investing in obtaining ISO 27001 certification helps us to control that this information is well insured so that we can avoid paying the corresponding fines.

- Better organization: in general, fast-growing companies do not have time to pause and define their processes and procedures. As a result, employees often do not know what to do, when and who should do it. The implementation of ISO 27001 helps to solve this type of situation since it encourages companies to write their main processes, which allows them to reduce the lost time of their employees.

3.2.3.2. ISO 27002

This international standard is designed for organizations to use it as a reference when selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO 27001 or as a guide document for organizations that implement commonly accepted information security controls.

This standard consists of 14 chapters of security controls that contain a total of 35 main security categories and 114 controls. Below, the 14 relevant chapters and the objectives they seek to achieve are shown:

- Chapter 1: Information security policies

Provide guidance and support to information security management in accordance with business requirements, relevant laws and regulations.

- Chapter 2: Organization of information security

Establish a management framework to initiate and control the implementation and operation of information security within the organization.
Guarantee security in teleworking and in the use of mobile devices.

- Chapter 3: Security related to human resources

Ensuring that employees and contractors understand their responsibilities and these employees or contributors in turn, are suitable for the functions for which they are considered.
Ensure that employees and contractors know and comply with their responsibilities in information security.

Protect the interests of the organization as part of the process of change or termination of employment.

- Chapter 4: Asset Management

Identify the assets of the organization and define the appropriate protection responsibilities.
Ensure that the information receives an adequate level of protection according to its importance to the organization
Avoid the unauthorized disclosure, modification, elimination or destruction of information stored on supports.

- Chapter 5: Access control

Limit access to information processing resources and information
Guarantee the access of authorized users and avoid unauthorized access to systems and services.

- Chapter 6: Cryptology

Guarantee an adequate and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of the information.

- Chapter 7: Physical security of the environment

Prevent unauthorized physical access, damages and interference to the information of the organization and resources for processing information.
Avoid the loss, damage, theft or compromise of the assets and the interruption of the operations of the organization.

- Chapter 8: Security of operations

Ensure the correct and safe operation of information treatment facilities.
Ensure that information and information processing resources are protected against malware.
Avoid data loss.

Record events and generate evidence.
Ensure the integrity of the software in operation.
Reduce the risks resulting from the exploitation of technical vulnerabilities.
Minimize the impact of audit activities on operating systems.

- Chapter 9: Security of communications

Ensure the protection of information in networks and information processing resources.
Maintain security in the information that is transferred within an organization and with any external entity.

- Chapter 10: Acquisition, development and maintenance of information systems

Ensure that information security is an integral part of information systems throughout the life cycle. This also includes the requirements for the information systems that provide the services through public networks.
Guarantee the security of the information that has been designed and implemented in the information systems development lifecycle.
Ensure the protection of test data

- Chapter 11: Relationship with suppliers

Ensure the protection of the assets of the organization that are accessible to suppliers.
Maintain an agreed level of security and provision of services in line with agreements with suppliers.

- Chapter 12: Information Security Incident Management

Ensure a consistent and effective approach to the management of information security incidents, including the communication of security events and weaknesses.

- Chapter 13: Information security aspects for business continuity management

The continuity of information security should be part of the organization's business continuity management systems
Ensure the availability of information processing resources.

- Chapter 14: Compliance

Avoid breaches of legal, statutory, regulatory or contractual obligations related to the security of information or security requirements.
Ensure that information security is implemented and operated in accordance with the policies and procedures of the organization.

3.2.3.3. ISO 31000

This international standard recommends that organizations continuously develop, implement and improve a framework that aims to integrate the process of risk management into the processes of governance, strategy, planning, management and reporting, as well as in the policies, values and culture of the entire organization. This international standard establishes a series of principles that must be met in order for risk management to be effective.

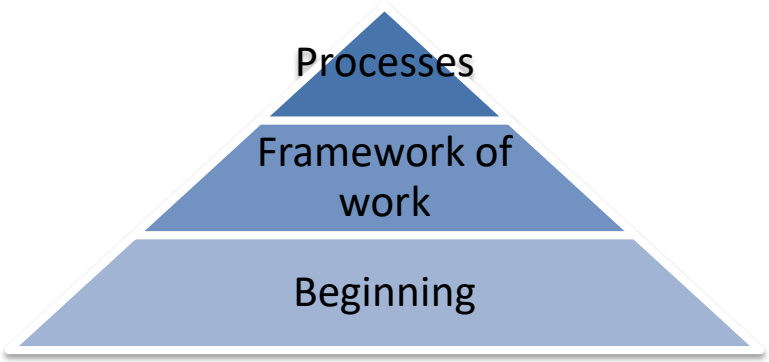
Risk management is defined as the set of processes carried out by organizations that lead to identifying, analyzing and responding to risk factors throughout the life of the project and seeking the benefit of the organization. Adequate risk management implies the control of possible future risks and their reduction.

Organizations face factors such as internal and external influences that make it uncertain to know when they will achieve their objectives and if they will achieve them. The incidence that this uncertainty has on the achievement of the objectives of an organization constitutes the "risk".

Throughout this process, organizations communicate and consult with interested parties. They monitor the risk and modify the control to ensure that no additional risk treatment is necessary.

For the implementation of ISO 31000 we can differentiate three fundamental sections that make up this standard:

Illustration 2: Fundamental sections ISO 31000 standard



Source: Standard UNE-ISO 31000

Own elaboration

A. Principles: for risk management to be effective, organizations must comply at all levels with the following principles:

Table 7: Principles of risk management

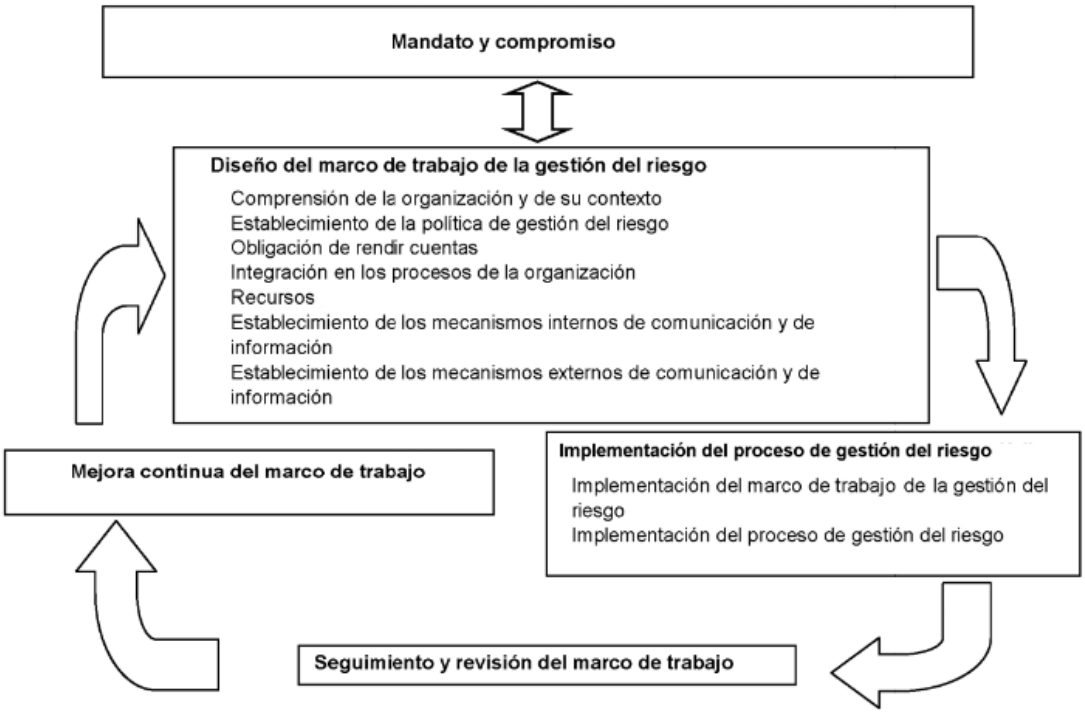
Create and protect the value	An integral part of the organization's profits	Part of decision making	Explicitly deals with uncertainty
Systematic, structured and timely	Based on the best training available	Adaptable	Integrates human and cultural factors
Transparent and participatory	Dynamic, interactive and responds to changes	Facilitates the continuous improvement of the organization	

Source: Standard UNE-ISO 31000

Own elaboration

B. Framework: provides the basis and provisions that will allow its integration at all levels of the organization. This framework facilitates effective risk management by applying the risk management process at different levels within the context of the organization. In addition, it guarantees that information about the risk obtained from this process is communicated and used appropriately as a basis for decision-making and accountability at all relevant levels of the organization.

Illustration 3: Components of the framework and their relationships



Source: Standard UNE- ISO 31000

C. Process: its hould be an integral part of the management, its hould be integrated into the culture and practices and its hould adapt to the business processes of the organization.

We can divide it into 5 fundamental steps:

Step 1: Establishment of the context

By establishing the context, the organization defines the external and internal parameters to be taken into account in risk management. In this way, political and social factors that involve the organization and influence its decision-making, will be identified. Trends in the sector or relations with groups outside the organization will also influence it.

Step 2: Focus

It will determine the scope of application of the rule: if the organization seeks to focus on all existing risks in an organization or on a specific sector.

Step 3: Identification, analysis and risk assessment

In this step, the risks are identified, the probability of their occurrence is analyzed and evaluated in order to determine a series of procedures to follow that may mitigate or eliminate them.

Step 5: Follow up and review

It is a continuous process of verification, supervision and critical observation, which aims to identify changes in the situation that could generate new risks, or affect the effectiveness of the risk management plan. This verification may be periodic or eventual.

The results of the monitoring and the review should be recorded and included in internal and external reports, as appropriate, and should be used as inputs to the revision of the risk management framework.

Step 6: Risk management process

It is a set of decisions regarding the creation of risks that should take into account: the needs of the organization, the benefits of reusing information for management purposes, the costs and efforts involved in the creation and maintenance of risks, ...

3.2.3.4. ISO 38500

As stated in the UNE-ISO / IEC (AENOR) standard:
It is a principled advisory standard that provides general guidance on the role of the governing body and encourages organizations to use the standards that are most appropriate to strengthen their governance of IT.

The purpose of this standard is to provide a framework of principles for managers when evaluating, directing and supervising the use of Information Technology (IT) in their organizations.

It is aimed mainly at the governing body, but also allows that, in some organizations (usually the smallest ones) the members of the governing body can play key functions in the management. In this way, it ensures that the standard is applicable to all organizations, from the smallest to the largest, regardless of the purpose, design and corporate structure. This ISO is closely related to COBIT 5, mentioned above.

This norm also aims to inform and guide those involved in the design and implementation of the management system on policies, processes and structures that support governance.

Framework for corporate governance of IT

The framework for governance is composed of six principles and three models, which, when combined, give rise to guidelines for implementing these principles in organizations.

The principles express the desirable behavior to guide decision making. The definition of each principle refers to what should happen, but does not prescribe how, when or by whom it would be put into practice, since these aspects depend on the nature of the organization that implements them. Administrators should demand the application of these principles in their organization.

Table 8: Principles ISO 38500

Principe 1: Responsibility	Individuals and groups within the organization understand and accept their responsibilities with respect the demand and supply or IT products and services.
Principle 2: Strategy	The organization's business strategy takes into account current and future IT capabilities; IT strategic plans meet the current and future needs of the business strategy.
Principle 3: Acquisition	IT acquisitions are made for valid reasons, based on adequate and continuous analysis through clear and transparent decisions.
Principle 4:Performance	IT fulfills the purpose of supporting the organization through the provision of services, service levels and quality of service required to meet present and future business requirements.
Principle 5: Compliance	IT complies with all mandatory legislation and regulations. The policies and practices are clearly defined, implemented and enforced.
Principle 6: Human behavior	IT policies, practices and decisions related to IT, show respect towards human behavior including the current and future needs of all "people involved in the process.

Source: Standard UNE- ISO / IEC 38500

Own elaboration

On the other hand, administrators should govern IT through three main models:

Table 9: ISO 38500 main models

Evaluate	•The current and future use of IT
Lead	•The preparation and execution of plans and policies to ensure that the use of IT meets the objectives of the organization
Monitor	•Compliance with policies and performance in relation to what was planned

Source: Standard UNE- ISO / IEC 38500

Own elaboration

Guidelines for the corporate governance of IT

The following sections provide guidance on the general principles of IT governance and the good practices needed to implement these principles. Therefore, the practices described are an orientation guide for the governance of IT.

Table 10.1.: Principle 1 – Responsibility

Principle 1: Responsibility	
Evaluate	Administrators should evaluate what options exist when assigning responsibilities related to the current and future use of IT in the organization.
Directing	Administrators should direct with the objective that the plans are carried out in accordance with the responsibilities assigned to IT and in order to receive the information they need to fulfill their responsibilities.
Monitor	Managers should monitor that the appropriate IT governance mechanisms have been established

Source: Standard UNE- ISO / IEC 38500

Own elaboration

Table 10.2.: Principle 2 – Strategy

Principle 2: Strategy	
Evaluate	Administrators should evaluate the evolution of IT and business processes to ensure that IT will provide support for the future needs of the organization
Directing	Administrators should direct the creation and use of plans and policies that ensure that the organization benefits from IT development.
Monitor	The administrators should monitor the use of IT to ensure that the objectives are achieved within the established deadlines, using the assigned resources and the expected benefits.

Source: Standard UNE- ISO / IEC 38500

Own elaboration

Table 10.3.: Principle 3 - Acquisition

Principle 3: Acquisition	
Evaluate	Administrators should evaluate what the options are to obtain the IT they need to develop the approved proposals, balancing the risks and the economic value of the proposed investments.
Directing	Administrators should direct that provision agreements (whether internal or external) support the business needs of the organization.
Monitor	Managers should monitor IT investments to ensure that the required capabilities are provided.

Source: Standard UNE- ISO / IEC 38500

Own elaboration

Table 10.4.: Principle 4 - Performance

Principle 4: Performance	
Evaluate	Administrators should evaluate the means proposed by management to ensure that IT will sustain business processes with the required capabilities and skills.
Directing	Administrators should ensure the allocation of sufficient resources for IT to meet the needs of the organization, according to agreed priorities and budget constraints
Monitor	Managers should monitor the degree to which IT supports the business.

Source: Standard UNE- ISO / IEC 38500

Own elaboration

Table 10.5.: Principle 5 - Compliance

Principle 5: Compliance Evaluate Directing Monitor	
Evaluate	Administrators should periodically evaluate the organization's internal compliance with its IT governance system.
Directing	Administrators should direct those in charge to establish periodic and routine mechanisms to ensure that the use of IT complies with the relevant obligations (regulatory, legislative, customary, and contractual), norms and established policies.
Monitor	Administrators should monitor compliance and accordance of IT through appropriate auditing and reporting practices.

Source: Standard UNE- ISO / IEC 38500

Own elaboration

Table 10.6.: Principle 6 - Human behavior

Principle 6: Human behavior	
Evaluate	Administrators should evaluate IT activities to ensure that human behaviors are properly identified and considered.
Directing	Administrators should direct so that the risks, opportunities, problems and concerns related to the business can be identified and notified by any individual at any time.
Monitor	Managers should monitor work practices to ensure they are consistent with the proper use of IT.

Source: Standard UNE- ISO / IEC 38500

Own elaboration

4. METHODOLOGY

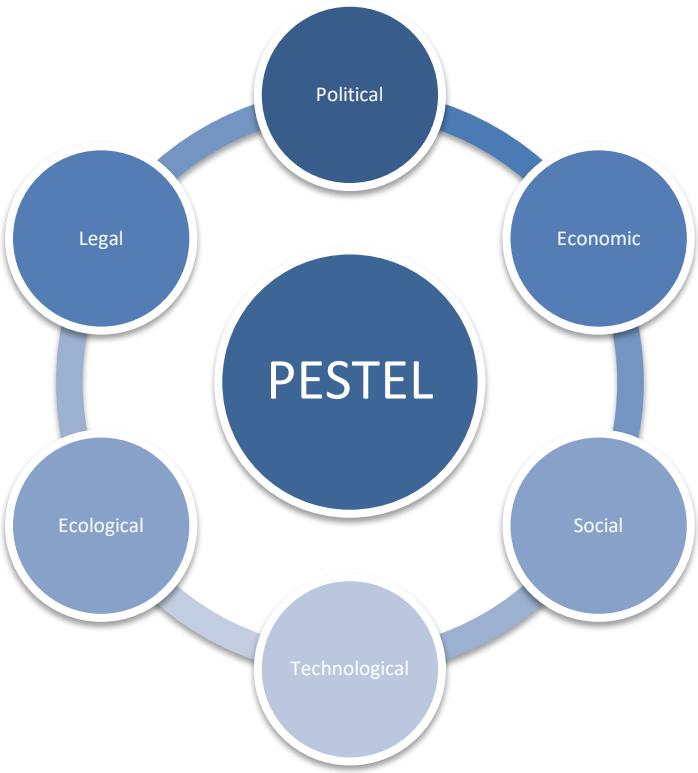
Within this section I will mention the tools or mechanisms that will be used for the development of the practical case.

4.1. PESTEL Analysis

First I will talk about the PESTEL analysis. Pascual Parada in his web: *PESTEL analysis, a business strategy tool to study the environment,* defines such analysis as "strategic analysis technique to define the context of a company through the analysis of a series of external factors."

The application of this tool consists in identifying and reflecting about the different factors of study to analyze the environment in which we will move and act accordingly in a strategic way about them. The factors that intervene are the following:

Illustration 4: PESTEL factors



Own elaboration

- **Political:** it refers to the degree of intervention by the government in the economy. It includes areas such as tax policies, labor laws, environmental laws, trade restrictions, rates and political stability. That is, al l those factors associated with the political class that can determine and influence the activity of the company in the future.

- **Economic**: it analyzes, thinks and studies current and future economic issues that may affect us in the execution of our strategy. You have to think about issues such as the following: economic cycles of our country, government economic policies, interest rates, inflation, income levels...

- **Social:** it includes cultural aspects, health awareness, rate of growth... It analyzes what elements of society can affect our organization and how they are combined. They would be changes in tastes or fashions that affect the level of consumption, changes in the level of income...

- **Technological**: it focuses on technological progress, that is, how the impact of new technologies affects our organization. For example, the appearance of new technologies related to the activity of the company that may cause some kind of innovation, the emergence of disruptive technologies that change the rules of the game in many sectors, etc.

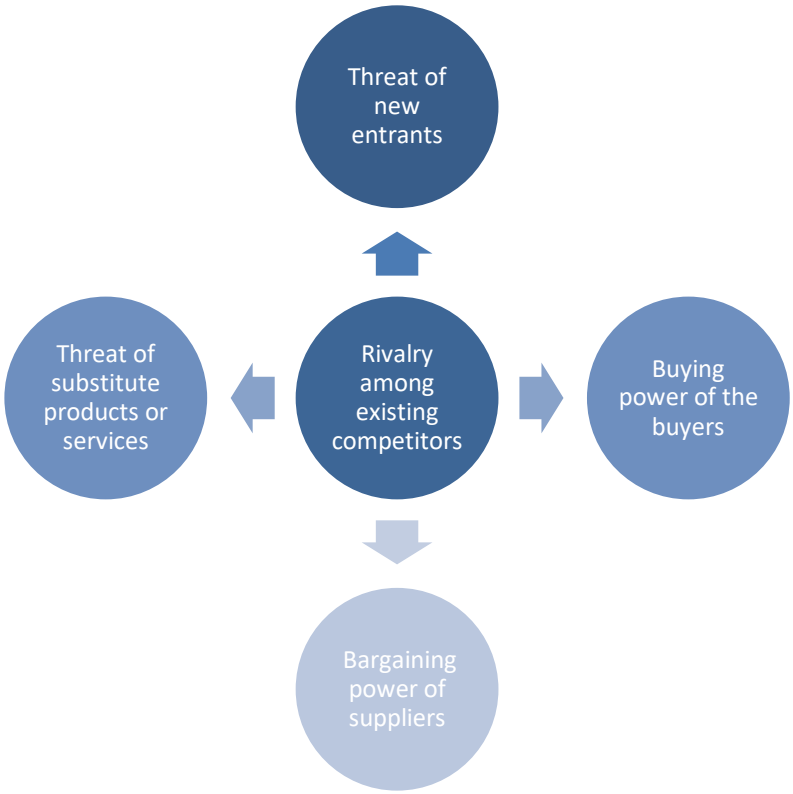
- **Ecological:** it refers to possible normative changes referring to ecology and social conscience. It would be for example, environmental protection laws, regulation on energy consumption, and concern about global warming...

- **Legal:** these factors refer to all those changes in the legal regulations related to our organization, which may affect you positively or negatively. For example, new laws or licenses.

4.2. Five Porter forces

Secondly, I will discuss the 5 forces of Porter.
Porter (1979) defines the five forces as “a strategic model that establishes a framework for analyzing the level of competition within an industry, in order to develop a business strategy”.
These 5 forces determine the intensity of the competition and their rivalry in an industry to determine their position with respect to these ones. The 5 forces are the following:

Illusion 5: The 5 forces of Porter



Source: The five competitive forces that shape the strategy

Own elaboration

1. Threat of new competitors: this refers to the barriers to new products / competitors. The easier it is to enter, the greater the threat. The seven barriers to entry that Porter identified are the following: economies of scale, product differentiation, capital investments, access to distribution channels, government policy, barriers to entry and cost disadvantage regardless of scale.

2. Bargaining power of buyers: the smaller the number of users, the more power they will have. This is so because they will acquire the possibility of being planted at a price that will be lower than what the company is willing to offer. If in addition, there are many suppliers they will have more power since there is the option to change companies.

3. Power of negotiation of suppliers: this is a threat imposed because of their power, either by their concentration or by the characteristics of their products. This negotiation capacity is usually low since there are many providers that can perform the same functions.

4. Threat of substitute products or services: markets with many similar products suppose a low profitability by the amount of similar products that exist. The opposite occurs in smaller markets where there is little variety.

5. Rivalry among existing competitors: it is the result of the combination of the previous four forces. It defines the profitability of a sector: the fewer the competitors, the more economically profitable, and vice versa.

4.3. ISO 31000 and GRDP

On the other hand, ISO 31000 will be used to delimit the risks that the company may incur focusing on data protection, as I have mentioned above.

The purpose of ISO 31000 is for the organizations to develop, implement and improve the framework by integrating the risk management process in the different processes of the organization.

The General Regulation of Data Protection seeks to strengthen the defense of the right of individuals to the protection of their personal data within the community environment. To that end, a single set of rules directly applicable to the legal systems of the Member States will be implemented.

Therefore the union of these two concepts, the analysis of the risks and the General Regulation of Data Protection, will lead to an assessment of risks applicable to the company in question, with a specific focus on data protection.

5. PRACTICAL CASE

In this section, the risk analysis of ISO 31000 will be developed in a real private company, Mediterránea Gestión Social y Cultural SA, in its scope of Home Help Service in the context of the General Regulation of Data Protection.

Risk management, as defined by the Spanish Agency for Data Protection (Practical guide to risk analysis in the processing of personal data subject to GDPR): "It is the set of activities and tasks that allow controlling the uncertainty related to a threat through a sequence of activities that include the identification and evaluation of risk, as well as, the measures for their reduction or mitigation ".

Based on ISO 31000, the risk assessment comprises three fundamental parts. The principles, the framework and the process.

- Principles: every company must comply with some basic principles before implementing the ISO 31000. These principles were previously mentioned in section 3.2.3.3., and have as their goal that the company internally implements values that get the support and the implication of all areas.

- Framework: provides the bases and provisions that will allow its integration at all levels of the organization.

- Process: it must be an integral part of the management, integrating itself into the culture and practices and adapting to the business processes of the organization.

Due to the fact that both the principles (which is something subjective of the company) and the framework (which is basically a theoretical concept) have already been established by Mediterránea Gestión Social y Cultural S.A., this section will focus exclusively on the processes involved in risk analysis.

The process will be structured in six steps which are the following:

Table 11: Steps in the risk analysis process

Own elaboration

Step 1: Establishing the context

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account in risk management and establishes the scope and risk criteria for the remaining process.

External context: the external context is the external environment in which the organization seeks to achieve its objectives. Within this section we find the PESTEL analysis and the relationships with stakeholders based on the 5 Porter Forces.

The PESTEL analysis, described in the methodology, helps us to situate ourselves in the context of the organization. In this case, the factors that have an impact on it are defined in the context of data protection.

- **Political:** they refer to governmental aspects that directly affect the company. The new GDPR refers to the policy since it is a topic not only of Spanish application as the old OLDP; but it acquires a European character. And it must be implemented compulsory in all organizations.

- **Economic**: this variable would refer to inflation, thereof employment... But if we focus on the environment of data protection, we could identify that an economic variable to take into account would be the sanctions to be applied by the state in cases of bad management, violation or breach of the GDPR.

- **Social:** a factor to take into account in this case is the knowledge of the new technologies that the population possesses. Individuals are aware of the progress of new technologies and the effects they have on their lives. So, the knowledge and application of these new mentioned standards are available to all people and you must be careful when managing your data.

- **Technological:** this factor is one of the most important when talking about the regulation of data protection since this regulation has entered into force to protect individuals from the technological advances experienced by organizations in relation to the management of their data. Technology plays a fundamental role both in the management of data and in the mechanisms that are implemented to protect them.

- **Ecological:** regarding this area I do not consider it relevant to mention any specific aspect.

- **Legal:** finally, we find the law itself. The current GDPR, which is in the official bulletin of the state and includes a series of scopes and guidelines to follow that organizations must implement from May 25th, 2018.

The 5 Porter Forces, also described in the methodology, help to determine the relationships with the interested parties. In this aspect we will analyze the 5 Porter Forces for the service of the Home Help Service, taking into account the perspective of data protection.

- **Power of negotiation of the buyers**: focusing on the Home Help Service, the City Council (only "buyer"), is the one who values and selects the company in charge of carrying this service. Although there is only one buyer, its decision-making power is universal and is based on different criteria established by a sheet of administrative clauses. The company that best performs its guidelines and improves them will be the one who takes the service. Having an ISO certification in terms of data protection will be an incentive to select one company over the others.

- **Power of negotiation of the suppliers**: the suppliers of Home Help Service have a low negotiation capacity, since the tools needed to work are basic and can be purchased from any company with similar characteristics. The company Mediterránea Gestión Social y Cultural S.A., will prefer a provider that complies with the data protection regulations so that they are not disclosed.

- **Threat of new competitors**: Home Help Service has several competitors since new companies can appear whenever they want to get the regulation of this service. So this threat is significant. The presence of companies that have certifications that comply with data protection regulations will be more important and will cause a tough competition between them.

- **Threat of substitute products**: currently there are no substitute services for Home Help Service, since it is the only service offered by the Local Corporation

that meets the needs of users who have certain physical and economic deficiencies.

- **Rivalry between competitors:** given the characteristics described above, Home Help Service has a high level of competence and a great negotiating power for the clients. The rivalry between competitors is high.

Internal context: within the internal context we can find the awareness that exists in the company regarding data protection, if they have protocols of action regarding such protection and the computer systems they have to regulate it.

The company Mediterránea Gestión Social y Cultural S.A., has become aware of this new change in data protection, that is why it has established an action protocol that includes the actions that its workers must follow since they receive information from the City Council about the users to be treated, until finally the service ends.

On the other hand, the computer systems they have are adapted to the needs of the company and the service, detecting possible external threats and possessing an effective documentation management system that avoids both loss, theft and filtering.

Step 2: Focus

The focus of the risks for this essay is data protection. That is, how to manage the risks that the company Mediterránea Gestión Social y Cultural S.A., may have within the General Regulation of Data Protection.

Step 3: Identification and risk assessment

Identify threats and risks

We define threat as any risk factor with the potential to cause harm. Focusing on data protection we find:

- Illegitimate access to the data: the impact or damage that would cause if the data were known by undocumented persons. It refers to confidentiality.

- Unauthorized modification of data: the prejudice that would cause the possession of a damaged or corrupted data. It refers to integrity.
- Elimination of data: the consequences of not having data or not being able to use it. It refers to its availability.

According to the Spanish Agency for Data Protection (Practical guide to risk analysis in the processing of personal data subject to GDPR):

A risk can be defined as the combination of the possibility of a threat materializing and its negative consequences. The level of risk is measured according to its probability of materializing and the impact it has in case of doing so. The threats and associated risks are directly related, therefore, identifying the risks always implies considering the threat that may originate them.

The risks that have been identified, based on what has been established in the Spanish Agency for Data Protection and the indications of the Responsible Person for Security of the company Mediterránea Gestión Social yCultural S.A. ,are the following:

- *Unintentional modification or alteration of personal data:* alteration of data due to poor data entry or due to hacking.

- *Information filtering*: any leakage of information that occurs in the organization, taking into account the importance of such information. Data such as the name would be a slight failure but data such as illnesses that the user could suffer would be a leak of greater nature.

- *Illicit treatment of personal data*: action of transferring personal data of users in a company to other companies to manage them, as long as the users have not authorized such transfer. Without such authorization, we would be at high risk.

- *Human errors*: mistakes made by workers, such as forgetting a document in an inappropriate place, such as sending information to a customer who has not requested it by mistake ... Depending on the severity of the faults, it will be classified as greater or lesser risk.

- *Non-confidentiality of the workers:* when the workers, despite having signed the confidentiality agreement, do not keep the "professional secret".

- *Appointment of security director*: the new GDPR includes the figure of a security director to address in case of problems or incidents. The lack of this figure could lead to the lack of coordination of the employees.

- *Documentation delivery notification*: any user must be informed of the use that the company is going to make with his/her data and in case of not having his/her authorization, not doing so due to the fact that this non-compliance would have negative consequences for the organization.

- *Action protocol*: it is convenient for workers to have an action protocol for each new user, document management, etc, so that there is a clear outline of the steps to follow.

- *Duration*: the current law prohibits users' data from being stored indefinitely in the databases of organizations. Not proceeding to the elimination of this documentation in the indicated period of time would have consequences.

- *New user rights:* the old OLDP allowed users the use of ARCO rights. The new law also grants the users the right to request the elimination of data permanently from the organizations in which such data are processed and also the transfer of these to other organizations. Not offering these rights to users would be an attempt against the law.

- *Destruction of documentation:* once the period of custody of personal data has passed they must be destroyed. The same happens if it is a manifest wish of the user. It will be necessary to determine if it is an automated or non-automated file, and guarantee its destruction.

- *Modification of data protection law*: this law is susceptible to be modified as it has already happened with the new Regulation and as we have seen in the evolution of the data protection law. The company must be prepared for this event and adapt its company for that purpose.

- *Lost or erased documentation by third parties*: this would be the case if The Local Corporation had a leak of information of data of the users of Home Help Service that will have Mediterránea Gestión Social y Cultural S.A. In this case, as the company has not signed the receipt for recieving this documentation, the

City Council will be responsible. If not (having signed the acknowledgment of receipt), the City could hold the company responsible.

- *Loss or deletion of personal data on their own*: if personal documents are deleted or lost, this could cause a serious problem, so extreme caution should be used.

- *User information*: all users must be informed, be aware of their rights and authorize the processing of their data. For this reason all the relevant clauses must be accepted (use of data, transmission authorization to other companies...). Otherwise, the data could not be used.

- *Unauthorized access to personal data*: every organization must regulate the use of their passwords and access to documentation. In this way only authorized people can have access to data protected by passwords for personal use that meet a series of basic requirements. The loss of passwords could give access to people outside the knowledge of personal data.

Evaluating risks

Evaluating the risks involves considering the scenarios in which such risks will be effective. This evaluation consists in assessing the impact, the probability of its materialization and the impact it will have. The latter is determined by analyzing the damage that the risk will cause when it occurs, if it does.

The evaluation of the risks must be the result of a reflection on the implications that the treatment of personal data have on the interested parties.

Table 12: Risk assessment

Source: Spanish Agency for Data Protection

The probability of the occurrence of any of the aforementioned risks and their impact within the organization based on the previous table will be taken into account. Scoring from 1 to 4 according to whether it is negligible, limited, significant or maximum, the combination of both ranges will serve to obtain the level of risk: low, medium, high or very high and act accordingly.

For a greater synthesis, we will present in summary form a table that combines the criteria mentioned above:

Table 13: Identification and risk assessment

Risk identification	Impact	Probability	Real risk
Unintentional modification or alteration of personal data	2	2	Low
Filtering information	3	2	Medium
Illegal treatment of personal data	4	1	Medium
Human errors	2	1	Low
Non-confidentiality of workers	3	1	Medium
Appointment of security director	1	1	Low
Documentation delivery notification	2	1	Low
Action protocol	1	1	Low
Duration	1	1	Low
New user rights	3	1	Medium
Destruction documentation	2	1	Low
Modification of data protection law	2	4	High
Lost or erased documentation by third parties	1	2	Low
Loss or deletion of personal data on their own account	2	1	Low
User information	2	1	Low
Unauthorized access to personal data	2	2	Medium

Own elaboration

Step 4: Treatment and communication of risks

The aim of the treatment is to reduce the level of exposure with control measures that reduce the likelihood and / or impact of these risks materializing. In this section, decisions are made about the actions that must be undertaken to modify the risk, that is, to prevent, eliminate or mitigate it.

We will analyze three of the risks described above. Each one will represent a level of risk, namely: low, medium and high. Since the very high risk is not contemplated in this case.

- Low: loss or deletion of personal data on their own account.

To avoid a definitive loss caused by an accidental deletion of information, a solution to be adopted is the making of backups on a frequent basis to avoid the loss of this data. In addition storing those copies in different places should also be done.

- Medium: unintentional modification or alteration of personal data.

This risk could be mitigated through the implementation of network threat monitoring controls which identifies possible external threats destined to produce damages in the company.

- High: modification of law Data Protection.

The amendment of the law is not a risk in itself. It would be the breach of this Law which was implemented for all of Europe on May 25th. This does not mean that it can not change again. So organizations should establish a safety officer and train him to take the necessary measures whenever necessary.

Step 5: Follow up and review

This process involves a continuous verification, supervision and critical observation, whose objective is the identification of changes in the situation of the organization that may generate new risks or affect the efficiency of the risk management plan.

Step 6: Risk management process

It is the set of decisions related to the creation of risks that must take into account: the needs of the organization, the benefits of reusing information for management purposes, the costs and efforts involved in the creation and maintenance of risks…

Definitely, it is an evaluation of the plan itself.

6. CONCLUSIONS

The general objective of this study has been to analyze the technical risks of a specific company in order to facilitate adaptation to the framework of the General Regulation of Data Protection.

After reviewing the different rules and practices of security in both public and private organizations, it is observed that there are different practices and tools that can be useful to regulate the information they have and adapt to the standard in which they are nowadays.

From this analysis, we also realize that laws are constantly changing, and these organizations must adapt to them efficiently. That is why the State puts at their disposal different instruments to adapt to it.

On the other hand, focusing on Mediterránea Gestión Social y Cultural S.A., we observe that although this first risk assessment may be useful to carry out a risk analysis in a general way, this is only the first step they must follow to get an efficient company in the field of data protection.

7. RECOMMENDATIONS

In this essay, a risk analysis based on ISO 31000 has been carried out, focusing only on data protection. Thus, the recommendations for this company in the future would be the following:

A) The company should not only carry out a more exhaustive analysis of its risks at the level of data protection, but also focus on the appearance of new future risks so as to mitigate their impact or eliminate them permanently. Therefore, the company should continue with the implementation of ISO 31000.

B) In addition, the company should work with the governance framework of information technologies; that supposes the management and evaluation of the plans by using IT, giving support to the organization to reach its objectives integrating and institutionalizing good practices.

In this way the company would make the most of its information maximizing the benefits.

C) Finally, it would also be advisable for the company to start applying ISO 27001, since it provides a model for the creation, implementation, operation, supervision, review, maintenance and improvement of an information security management system. All this would allow the company to obtain a better risk management and expand and improve its competences unifying the government frameworks with this ISO 27001.

8. BIBLIOGRAPHY

Cybersecurity and Incident Management Spanish teams. Retrieved on May 9 from https://www.csirt.es/index.php/es/

Diaz, E (e.D.). New Organic Law on Data Protection: legal adaptation to digital reality. Retrieved on April 16, 2018 from http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/nueva-ley-organica-de-proteccion-de-datos-adaptacion-legal-a-la-realidad- digital

ISACA (2012). COBIT 5 CSIRT

Martínez, M (m.M.). Seven keys of the RGPD for the self-employed and the SME. Retrieved on May 4, 2018 from https://infoautonomos.eleconomista.es/blog/claves-del-rgpd-autonomo-pyme/

Mediterránea Gestión Social y Cultural S.A. Retrieved on May 25, 2018 from http://mediterraneagestion.es/

Michael, E. Porter (2008) The five competitive forces that shape the strategy

National cryptological center. (National Security Scheme). Retrieved on May 25, 2018 from https://www.ccn-cert.cni.es/ens.html

National Institute of CIberseguridad (INCIBE). Retrieved on April 20, 2018 from https://www.incibe.es/protege-tu-empresa

Organic Law 15/1999, of December 13, on Protection of Personal Data.

Paschal Stop (p.P.). PESTEL analysis, a business strategy tool to study the environment. Retrieved on June 13, 2018 from http://www.pascualparada.com/analisis-pestel-una-herramienta-de-estudio-del-entorno/

Practical guide on risk analysis in the processing of personal data subject to the RGPD (Spanish Agency for Data Protection).

Regulation (EU) 2016/679 of the European Parliament and Council 27 April 2016

Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration.

Spanish Agency for Data Protection. Retrieved on May 22 from https://www.aepd.es/

TechnoRightAdvisory (2018). Evolution of data protection regulation. Unpublished material

UNE-ISO/IEC 27001 (2014) Information technologies, Security techniques, Information security management systems and Requirements.

UNE-ISO/IEC 27002 (2015) Information technology, Security techniques and Code of practice for information security controls.

UNE-ISO 31000 (2010). Risk management, Principles and guidelines.

UNE-ISO/IEC 38500. (2013) Corporate governance of information technology.