ISSN:2230-9926

Availableonlineathttp://www.journalijdr.com

IJDR

InternationalJournalofDevelopmentResearch
Vol. 10, Issue, 06, pp. 37027-37033, June, 2020
https://doi.org/10.37118/ijdr.19225.06.2020

RESEARCH ARTICLE OPENACCESS

SUGGESTION OF APPLICABILITY OF ISO FOR THE IMPROVEMENT OF DATA SECURITY IN COMPANIES

[1]Moroni da Silva Cortez,[1]Patrícia Brasil Pantoja, [1]Bruno Pereira Gonçalves,[1]Rilmar Pereira Gomes, [1]Jean Mark Lobo de Oliveira, [1]Victor da Silva Almeida and *[2]David Barbosa de Alencar

[1]Academic Department, University Center FAMETRO, Amazon-Brazil
[2]Institute of Technology and Education Galileo of Amazon (ITEGAM), Brazil

ARTICLEINFO

ArticleHistory:
Received 17th March, 2020
Received in revised form
02nd April, 2020
Accepted 08th May, 2020
Published online 29th June, 2020

KeyWords:

ISO;Companies; Data; Security; Availability.

Corresponding author: David Barbosa de Alencar

ABSTRACT

Suggestion of applicability of ISO to improve the security of company information. Elaborated through a bibliographic research to understand the concepts applied in the present work, adopting a quantitative research through a questionnaire. Research directed to professionals and university students of information technology, and to a random audience. A documentary research was also carried out to collect data in informal *institutions*. The following technical standards were adopted: NBR-ISO-27001, NBR-ISO-27002, NBR-ISO-27008, NBR-ISO-27036, with distinct characteristics and with the intention of being useful in suggesting the applicability of ISO in company procedures. It was possible to evaluate the reliability of the companies in relation to the security of their employee data. With the suggestion of applying the ISO to companies, it is possible to obtain a greater security, as well as a greater availability, with more efficient data exchange. The information security policy is established through rules, standards, and procedures, which must be used internally and externally, providing more reliability. Company employees will begin to carry out processes more efficiently within the organizations. Therefore, the suggestion of using the ISO for information security in companies becomes significantly important because it is one more contribution so that they can have rules to protect both their data and those of their employees.

Citation: ***Moroni da Silva Cortez, Patrícia Brasil Pantoja, Bruno Pereira Gonçalves, Rilmar Pereira Gomes, Jean Mark Lobo de Oliveira and David Barbosa de Alencar.*** "Suggestion of applicability of iso for the improvement of data security in companies",*International Journal of Development Research*, 10, (06), 37027-37033.

INTRODUCTION

The flow of data in an organization can be characterized by the well-defined way of grouping them according to needs. The data constitute the atomic unit that information circulates, flowing in the organization though its information system. A study published by ESET points out that 65% of Brazilian companies have already had problems with information security, and the scariest of this is that more than half of the companies surveyed have a defined information security policy.With technology available to everyone and fully integrated into our daily lives, Has a very fertile environment been created for data thieves? According to the article published by PWC, the budget average with information security increased 51% in companies compared to last year. Today, organizations are increasingly interconnected, integrated, and interdependent. They employ technology and connectivity to share an unprecedented volume of information assets with customers, service providers, suppliers, partners and employees. But this evolution also puts them at risk by leaving them at the mercy of enemies who could exploit these technologies and processes to interrupt operations, obtain inside information and even destroy the company. As a result, security threats have become a critical risk for global companies. Data processing has brought companies into the habit of actively recording data for posterior treatment. Thus, new research, comparison and validation situations have been introduced, increasing the amount of information available about the company and its own the basic function of information security is to protect the information asset, minimizing risks to acceptable levels. In some organizations, this area is also responsible for elaborating the business continuity plan.

MATERIALS AND METHODS

It will be applied a bibliographic research for the construction of the study in the areas of Information Security, risk assessment,

operational controls, analysis and continuous improvement, within a company.We used a quantitative research, where a 15-questions questionnaire will be made that will be available to the public in the IT area to obtain data collection. In addition, the study had the character of a descriptive research, where ISO (International Organization for Standardization) techniques will be approached, resulting in a new alternative for the ISMS (Information Security Management System), with the objective of identifying risks and definition of controls to manage and overcome challenges related to Information Security.To carry out this study, we used ISO / IEC 27001 so that organizations opt for an suitable mode of establishing, implementing, operating, monitoring, and managing an information security management system, the ISO / IEC 27002 international standard that establishes a code of practice to support the implementation of the information security management system (ISMS) which has as its goal to establish general guidelines and principles to initiate, implement, maintain, and improve information security management within an organization, ISO / IEC 27008 guidelines for the assessment of information security controls, review and assessment of the implementation and operation of information security controls, including the technical evaluation of information system controls, in accordance with information security requirements established by an organization, ISO / IEC 27036 Information security for supplier relationships - Overview and concepts provides guidance destined to help organizations protect their information and information systems in the context of supplier relationships, and data collection through quantitative research, bibliographic materials and websites related to information security policy and standards, we used the google forms tool which is a google application for creating free online forms in the form of a link, we also used google forms to create 3D graphics in the form of Pizza.

STUDY APPLICATION

Data and information: Before everything, identify and distinguish data and information, what differentiates data from information is the capacity of each one to provide understanding to the people who will use them. It can be said that the data is not able to provide a basis for important decisions in the business sector, although it has not been transformed in the way in which it will be viable for the company, that is, becoming information. Thus, giving relevance to understanding what is meant by information. Being able to say that the data do not cause and provide elements for business decision making, on the other hand, the information must be seen as the transformation of the data in a way that allows its interpretation and manipulation by the users, making possible their understanding in a form that can serve as a basis for business decision making (Oliveira, 2011 apud Andrade And Rabelo 2017, p.130).The data as a sequence of facts not yet analyzed, representative of events that occur in organizations or in the physical environment, before they have been organized and willing in a way that people can understand and use them. Corresponds to "data that has been modeled in a meaningful and useful format for humans". It is understood that information technology can be interpreted as methods and processes of technology that aims to develop and effectively use all information. Laudon and Laudon (2014, p.13) apud Andrade and Rabelo (2017).

Information Technology: Rezende and Abreu (2011, p. 54) apud Andrade and Rabelo (2017) define information technology as “any and all devices that have the capacity to process data and or information, both systemically and sporadically, whether applied to the product, whether applied to the process ”. It also includes “Hardware and its devices and peripherals; software and its resources; telecommunications systems and data and information management” .The component communicates with each other and has the need for the component that treat, that is, the users, who, in their conception, are not suitable as part of information technology, however, without the human factor, technology would not be achieved for the desired results.Albertin and Albertin (2010) apud Andrade and Rabelo (2017) explain that using technology to administer processes, improve growth and interact with the market as a whole. Therefore, it is understood that if subjected to technology it brings greater risks since this resource is becoming more difficult, looking for ways to conduct it in a way that its efforts involving technology bring expected results. It is needed that companies observe their methods and manners and that they are in accordance with the expected results, to obtain prominence using the available resources of technology.In order to obtain knowledge about information technology, its concepts and applicability in business areas, it is necessary to learn what is meant by information systems.

Information Systems: O'Brien (2004, p. 6) It is understood of information systems as “an organized set of people, hardware, software, communications networks and data resources that collect, transform and disseminate information in an organization”. Being important when inserted in the organization, as they modify the form in which the business will be demonstrated and managed, besides making significant changes in activities.It can be said that there are various definitions of information systems in addition to those mentioned here, but all of them conclude that the main focus is the information and the way it is being manipulated, transformed and passed on aiming to create information that will provide sufficient elements for organizational decisions and activities. In this context, it is interesting to say that organizations and information systems have a great interaction. Where organizations are using information systems with the purpose of collecting considerable information that will assist their employees in the most varied processes existing in the organization (JOÃO, 2012).After reporting on what an information system is and its applications, it is important to comprehend the information security role in the organizational environment, which will be shown in the next topic.

Information Security: Information Security is related to the protection of information, with the goal to preserve valuable information that an individual or organization could have.Sêmola (2014) apud Andrade and Rabelo (2017) emphasizes that there is a perception of the organization where it is necessary that the rules and norms defined through the security policy are connected with the methods that involve the duration of the information, making the information security an effective process in the organization.With what was discussed about information security, it is important to understand what is meant by information security policy, mentioned below.

Information Security Policy: Silva (2012) apud Andrade and Rabelo (2017) demonstrate that when it comes to information security in the organizational environment, it constitutes a security policy for the process to be effective. It applies, through the definitions of rules, standards and procedures using resources in a reliable way, whether internally or externally. Thus, the security policy involves subjects that deal with information security, such as "use of corporate e-mail, use of the internet, classification of information, use of mobile computers, security incidents and confidentiality agreements".Thus, Sêmola (2014)apud Andrade e Rabelo(2017) address that the security policy has an influence at the organizational ambit, where it substantiates the activities that involve the security issue. Reinforcing that the information security policy can be divided into three groups: "guidelines, standards, procedures and instructions", intended for strategic, tactical and operational layers within the organization.However, Silva (2012) states that the security policy can only bring the expected results when the main objectives are understood, providing mechanisms where the information used is safe to attend the demands of the organization. Therefore, it is necessary that the set of rules, standards, and procedures be disseminated and incorporated throughout the organization and not only in a specific sector. However, the author emphasizes that this awareness is a long process and requires continuous work.

NBR-ISO/IEC 27001: Decrease of the risk of liability when programming the ISMS or delimiting policies and processes. The objective of protecting the confidentiality, integrity and availability of an organization's information. Identify which potential problems may occur with the information, and thus define which needs must be met to prevent such problems that may occur. Requiring the company to

perform a security risk analysis periodically and whenever significant changes are established. For the analysis to be done correctly, it is needed to establish risk acceptance criteria as well as the definition of how these risks will be measured.

- The standard describes a process for systematically managing information risks.
- Specifies generic ISMS requirements suitable for organizations of any type, size or nature.
- Only ISO / IEC 27000 is considered absolutely essential for users of ISO / IEC 27001, the other ISO27k standards are optional.
- Understanding the organizational context, the needs and expectations of the 'stakeholders' and defining the scope of the ISMS, it clearly declares that the organization must establish, implement, maintain and continuously improve the ISMS.
- Senior management must demonstrate leadership and commitment to the ISMS, determine policies and assign roles, responsibilities and information security authorities.
- Describes the process to identify, analyze and plan the treatment of information risks and clarify the information security objectives.
- Competent and adequate resources must be assigned, as well as awareness and prepared and controlled documentation.
- In more detail on how to assess and treat information risks, manage changes and document things (in part so they can be audited by certification auditors).
- Evaluates, analyzes the controls, processes and the information security management system, systematically improving things whenever necessary.
- Address the conclusions of audits and reviews (for example, non-conformities and corrective actions), make continuous improvements in the ISMS.

NBR-ISO/IEC 27002

It has the purpose to establish general guidelines and principles for initiating, implementing, maintaining and improving information security management in an organization. This also includes the implementation and management of controls, taking into account the risk environments found in the company. Defining the code of good practice to give the necessary support for the implementation of the ISMS.The standard provides recommendations for those responsible for selecting, implementing and managing information security. Whether or not it can be used in support of an ISMS specified in ISO / IEC 27001.

- ISO / IEC 27000 is the only norm considered absolutely indispensable for the use of ISO / IEC 27002. However, several other standards are mentioned in the norm and there is a bibliography.
- All expert terms and definitions are now defined in ISO / IEC 27000 and the majority apply to the entire family of ISO27 standards.
- There is a pattern structure in each control clause: one or more subsections of the first level, each indicating a control objective and each control objective being supported, in turn, by one or more declared controls, each control followed by implementation guidance associated with additional explanatory notes.
- ISO / IEC 27002 specifies control objectives (one per 'security control category') related to the need to protect the confidentiality, integrity and availability of information.
- The control objectives are at a very high level and comprise a generic specification of functional requirements for the information security management architecture.
- Each of the control objectives is supported by at least one control, as the implementation guidelines recommend several real controls in detail.
- Management must define a set of policies to elucidate its direction and support for information security.
- The organization must define the roles and responsibilities for information security and allocate them to individuals.
- Information security responsibilities must be taken into account when recruiting permanent, contracted and temporary employees (for example, through appropriate job descriptions, pre-employment screening included in contracts).
- Managers must ensure that employees and contractors are made aware and motivated to fulfill their information security obligations. A formal disciplinary proceedings are necessary to deal with information security incidents supposedly caused by workers.
- All information assets must be inventoried and the owners must be identified as being responsible for their security. The "Fair use" policies must be defined and assets must be returned when people leave the organization.
- The organization's requirements for controlling access to information assets must be clearly documented in an access control policy and procedures. Network access and connections must be restricted.
- There should be a policy on the use of cryptography, beyond the cryptographic authentication and integrity controls, such as digital signatures, message authentication codes and cryptographic key management.
- Physical perimeters and barriers defined with physical entry controls and work procedures must protect facilities, offices, rooms, delivery areas, etc.
- IT operational responsibilities and procedures should be documented. Changes to IT facilities and systems must be controlled. Capacity and performance must be managed. The development, test and operational systems must be separated.
- Malware controls are necessary, including user awareness. The activities of user and system administrator, exceptions, failures and information security events must be recorded and protected. The clocks must be synchronized.
- IT audits must be planned and controlled to minimize adverse effects on production systems or inadequate access to data.
- Technical vulnerabilities must be corrected and there must be rules that govern the installation of the software by users. Security control requirements must be analyzed and specified, including applications and transactions on the web.
- There must be policies, procedures and awareness to protect the organization's information that is accessible to IT outsourcers, external suppliers and agreed in contracts or agreements.
- There must be responsibilities and procedures to manage (report, evaluate, respond to and learn from) information security events, incidents, weaknesses in a consistent and effective manner, and to collect forensic evidence.
- The continuity of information security must be planned, implemented and revised as an integral part of management systems.
- Information security arrangements should be independently reviewed and reported to management. The managers should also routinely review employees and systems conformity with security policies and procedures and initiate corrective action when necessary.

NBR-ISO/IEC 27008

Purpose: Provide guidance to all auditors on controls for information security management systems. It supports an ISMS's internal, external and third party information risk management and auditing process, explaining the relationship between the ISMS and its support controls.

- Supports any organization that uses ISO 27001 and 27002, because it focuses on verifying information security controls.
- It is applicable in organizations of all sizes.
- Adds value and improves quality, evaluates the security elements and IT operational environment.

- Provides guidance for auditing and information security controls in accordance with the ISO / IEC 27002 control guidelines.
- ISO 27008 complements ISO 27007 in the following way, manages the ISMS program, determines what to audit, designates appropriate auditors, and has a continuous improvement in the process.
- Provides support, planning and execution of ISMS audits and the information risk management process.
- Optimizes the relationships between the ISMS processes and the necessary controls.
- Ensures efficient use of audit resources.
- Provides information security governance support.
- Offer support in a governance approach based on ISMS.
- Guidelines for the assessment of information security controls.
- Provides guidance on assessing the controls in force to ensure they are fit for purpose.
- It is efficient and aligned with the company's objectives.
- Provides guidance on the review and evaluation of the application and functioning of the information security controls established by the organization.
- According to ISO / IEC 27008, technical compliance and evaluation criteria are based on the information security requirements established by the organization.
- The standard will help organizations to prepare against hackers.
- Perform an ISMS audit and controls.

NBR-ISO/IEC 27036

***Purpose*:** Address issues of relationship with suppliers and elaborate a risk analysis to improve security where both must adopt security policies and access permissions.

- It is possible to determine information security controls.
- The outsourced IT and cloud computing service will be covered by the standard.
- The standard will increase communication with suppliers.
- According to ISO / IEC 27036, the pattern improves relationship management.
- The pattern creates a safer and lasting environment.
- The standard also adopts security policies and access permission.
- This standard is aimed at suppliers.
- It is a standard where a risk analysis and survey is developed.
- ISO / IEC 27036 applies access policies;
- Applies up-to-date secure security protocols;
- Apply safe and updated security protocols;
- Extends the liability of assets in relation to valuable information.
- Assists in forensic audits and expertise.
- Requires suppliers to be certified in accordance with ISO / IEC 27001 in service level contracts or agreements.
- Information security management and procedures are important, such as risk analysis.
- According to ISO / IEC 27036, an optional stage must be updated to renew the contract, perhaps revising the terms, conditions, performance, problems and work processes.
- It is important to define requirements, including information security requirements.
- Holds special controls for unique risks, such as testing agreements.
- According to ISO / IEC 27036 you get visibility into information security associated with cloud services, and manage it effectively.
- Specifies the fundamental information security requirements regarding the relationship between suppliers and buyers of various products.
- The supplier obtains access to the acquirer's internal information.

DISCUSSION OF RESULTS

As can be seen in the survey conducted by this research, we observed that Information Security is important, we need to have standards that help to ensure the integrity and reliability of data within companies. Therewith, there is a concern with storing information and also with whom the data will be shared. We seek standards that we consider fundamental to assist management and decision making in companies. Therefore, it is important to stress that every company, whether small or large, needs to be careful with its information data.

ISO Suggestion

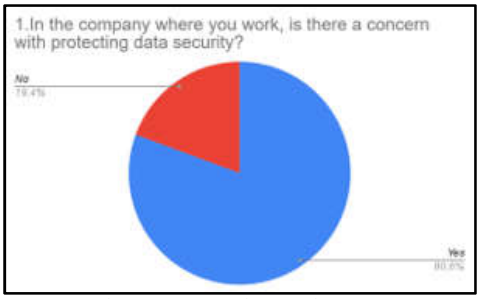
1. Business continuity;
2. Information Security Incidents;
3. Senior Management and its Commitment;
4. Risk analysis;
5. Definition of objectives and strategies;
6. Risk Identification and possibility to correct weaknesses;
7. Systems Maintenance;
8. Access Control;
9. Operational Procedures and Responsibilities;
10. Do not disclose confidential information at the time of login;
11. Technical vulnerability management;
12. Protection against brute-force "credibility strength" attacks;
13. Human Resources;
14. Benefits for customers and suppliers;
15. The importance of conformity;
16. Compliance with legal requirements;
17. Responsibility for assets;
18. Cost reduction due to the prevention of incidents in the area of information security;
19. Reduce costs;
20. Considerations about information systems audits;

ISO Criteria Justifications

- The first criterion was chosen to create and implement a business plan to prevent the interruption of activities, so that there is a faster recovery of operations in case they are lost.
- The second criterion was chosen to establish formal procedures for employees, suppliers and third parties for make them aware through event notices and communications so that they can be corrected as soon as possible.
- The third criterion was chosen because it is important to have management's commitment to the ISMS, where leaders ensure resources for the implementation of systems that are correctly indicated and that have the obligation to guide their employees so that they have an efficient system.
- The fourth criterion was chosen for the company to make a periodic analysis whenever there are changes, establishing and defining acceptance criteria to know how the risks will be measured.
- The fifth criterion was chosen because it is necessary to clarify what are the objectives during the planning and what strategies will be defined to reach those objectives, which need to be determinant and considerable as requirements for security.
- The sixth criterion was chosen to improve relationship management, creating a more secure and lasting environment.
- The seventh criterion was chosen so that at the time of development or even when acquiring the system, security requirements must be identified, so that information is protected while maintaining the confidentiality, integrity and authenticity of encrypted data.
- The eighth criterion was chosen because care must be taken with unauthorized access to systems to prevent damage to documents and resources that are available to anyone.
- The ninth criterion was chosen because IT operational responsibilities and procedures must be documented and changes to IT facilities and systems must be controlled. In

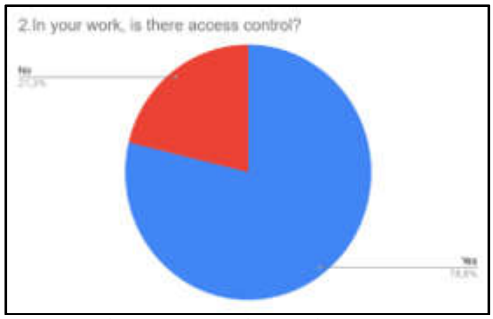
addition, capacity and performance must be managed and development, testing and operational systems must be separated.

- The tenth criterion was chosen because any employee who needs to have access to documents, e-mails or even a physical space that stores some type of information needs to have their login. And they must not let other people know about their password, to preserve themselves and even the company.



Source: Moroni Cortez e Patrícia Pantoja (2020)

Graph 1. In the company where you work, is there a concern with protecting data security?

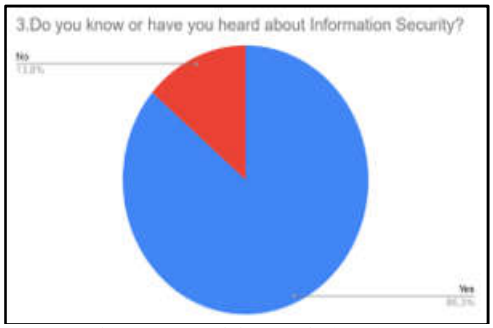


Source: Moroni Cortez e Patrícia Pantoja (2020).

Graph 2. In your work, is there access control?

- The eleventh criterion was chosen because the technical vulnerabilities must be corrected and there must be rules that govern the installation of the software by users.
- The twelfth criterion was chosen because it consists of generating possible combinations of passwords in sequence to access a system. Knowing that nowadays this type of attack is more and more common, we must always use a "strong" password in order to make any type of invasion more difficult.
- The thirteenth was chosen so that when hiring an employee or even a supplier, it is important to analyze their profile, especially if they have to deal with confidential information, and after being hired, they must be aware of their obligations, responsibilities and threats.
- The fourteenth criterion was chosen because with the implementation of the standard, customers will be sure that their information and data will be properly treated, knowing that the company has high levels of management and information security protection standards, being a company certified.
- The fifteenth criterion was chosen because it is important so that there is no violation of any law, ensuring regulations on information security requirements, and when it becomes necessary to hire a specialized consultancy to verify compliance and legal requirements, showing to future clients that it is a company that values its customers and assets.
- The sixteenth criterion was chosen because there are more and more laws, regulations and requirements related to information security, and the good news is that many of them can be solved by implementing ISO.
- The seventeenth criterion was established because all information assets must be inventoried and the owners must be identified as being responsible for their security. "Fair use" policies must be defined and assets must be returned when people leave the organization.
- The eighteenth criterion was chosen because it is important to invest in different aspects, observing the appropriate priorities where there may be possible losses of inverted resources, so that it is able to prevent unauthorized access. Thus, investments for prevention will be necessary.
- The nineteenth criterion was chosen because the philosophy of ISO 27001 is to prevent security incidents from occurring, and each incident, whether large or small, costs money. This way, by preventing incidents, organizations will save a significant amount of money.
- The twentieth criterion was chosen because IT audits must be planned and controlled to minimize adverse effects on production systems or on inadequate access to data.

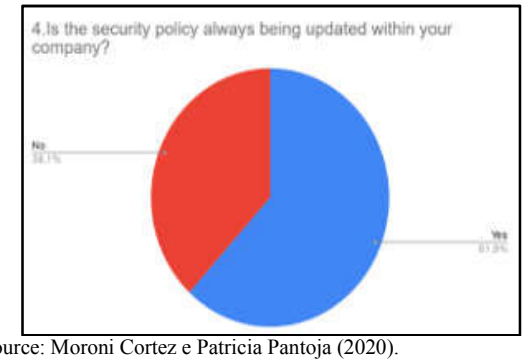
Questionnaire Answers: The result of the following quantitative research aims to identify the behavior and attitudes adopted by employees of companies, random audience, and students of information technology, we conducted a questionnaire with 15 questions with 161 people to analyze if they have information about the ISO information security, and whether the information security of the companies where they work is being performed. Thus, having a base in the answers we can propose solutions.According to the graph below, we can observe that 80.6% of people answered yes, that in the companies where they work they are concerned with data security, and 19.4% answered no. According to what was exposed in the survey, 86.3% affirm that they have heard about information security, and 13.8% answered that they did not.



Source: Moroni Cortez e Patricia Pantoja (2020).

Graph 3. Do you know or have you heard about Information Security?

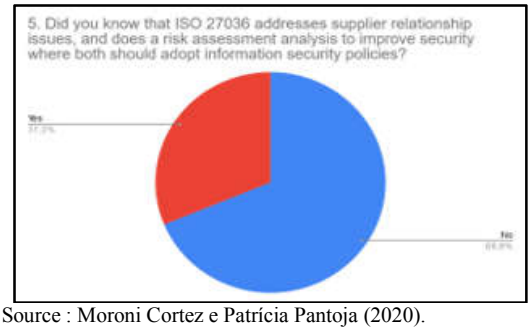
According to the survey, 61.9% answered yes and 38.1% answered no.



Source: Moroni Cortez e Patricia Pantoja (2020).

Graph 4. Is the security policy always being updated within your company?

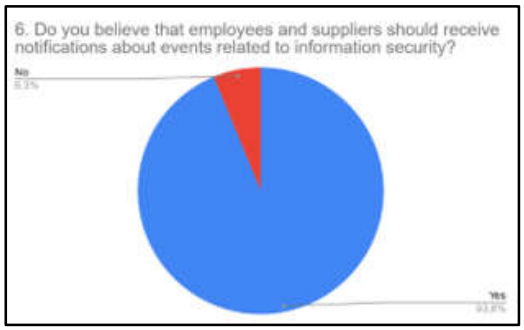
According to the survey, we can see that 68.8% answered no and 31.3% answered yes.



Source : Moroni Cortez e Patrícia Pantoja (2020).

Graph 5. Did you know that ISO 27036 addresses supplier relationship issues, and does a risk assessment analysis to improve security where both should adopt information security policies?

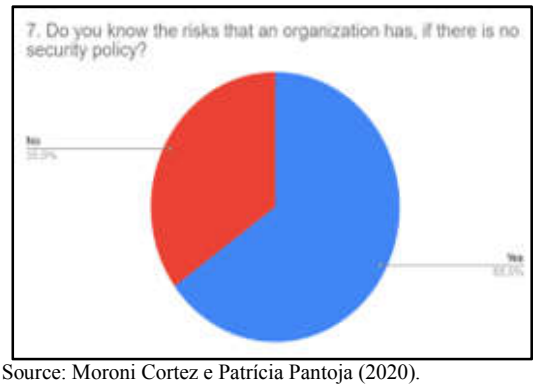
We can observe that 93.8% of people answered yes and 6.3% answered no.



Source: Moroni Cortez e Patrícia Pantoja (2020).

Graph 6. Do you believe that employees and suppliers should receive notifications about events related to information security?

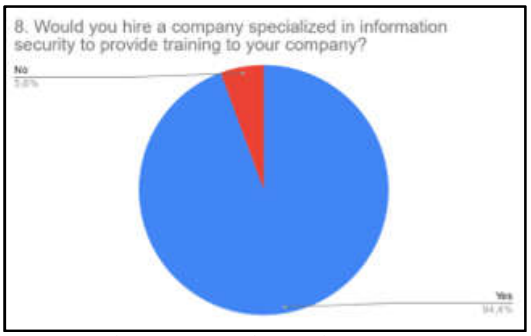
According to the survey, 65.0% answered yes and 35,0% answered no.



Source: Moroni Cortez e Patrícia Pantoja (2020).

Graph 7. Do you know the risks that an organization has, if there is no security policy?

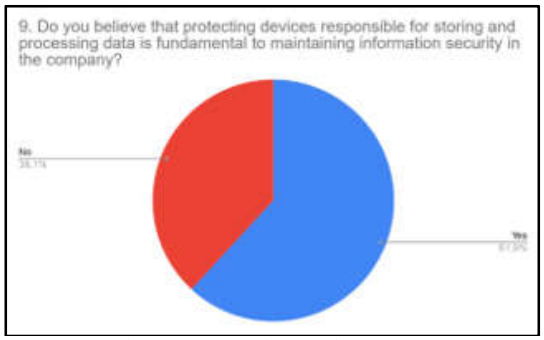
According to the graph below, we can see that 94,4% answered yes and 5.6% answered no.



Source: Moroni Cortez e Patrícia Pantoja (2020).

Graph 8. Would you hire a company specialized in information security to provide training to your company?

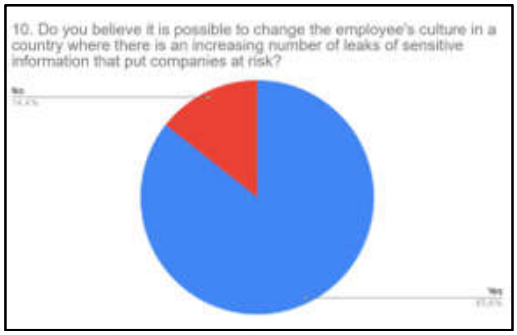
According to the questionnaire, 61.9% answered yes and 38.1% answered no.



Source : Moroni Cortez e Patrícia Pantoja (2020).

Graph 9. Do you believe that protecting devices responsible for storing and processing data is fundamental to maintaining information security in the company?

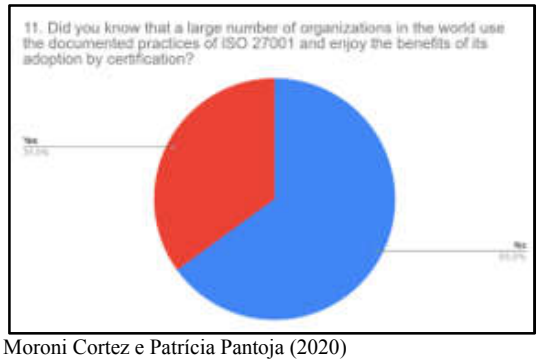
According to the questionnaire, 85.6% answered yes and 14.4% answered no.



Source: Moroni Cortez e Patrícia Pantoja (2020).

Graph 10. Do you believe it is possible to change the employee's culture in a country where there is an increasing number of leaks of sensitive information that put companies at risk?

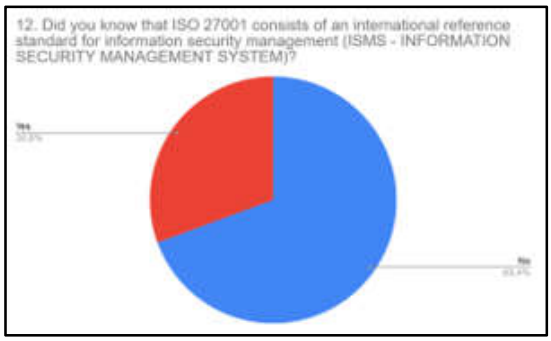
According to the questionnaire, 65.0% of people answered no and 35.0% answered yes.



Source: Moroni Cortez e Patrícia Pantoja (2020)

Graph 11. Did you know that a large number of organizations in the world use the documented practices of ISO 27001 and enjoy the benefits of its adoption by certification?

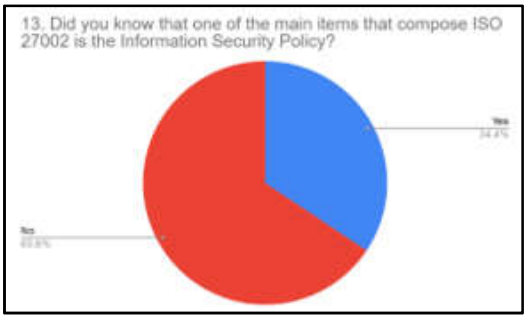
According to the questionnaire, 69.4% answered no and 30.6% answered yes.



Source: Moroni Cortez e Patrícia Pantoja (2020)

Graph 12. Did you know that ISO 27001 consists of an international reference standard for information security management (ISMS - INFORMATION SECURITY MANAGEMENT SYSTEM)?

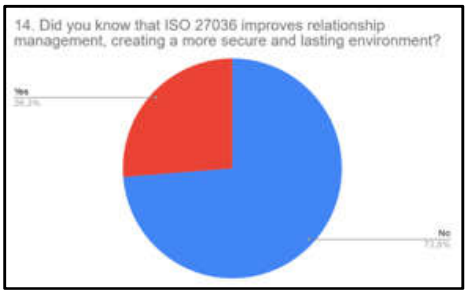
According to the questionnaire, 65.6% answered no and 34.4% answered yes.



Source: Moroni Cortez e Patrícia Pantoja (2020)

Graph 13. Did you know that one of the main items that compose ISO 27002 is the Information Security Policy?

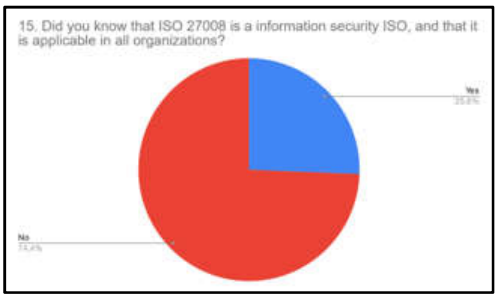
According to the questionnaire, 73.8% answered no and 26.3% answered yes.



Source: Moroni Cortez e Patrícia Pantoja (2020)

Graph 14. Did you know that ISO 27036 improves relationship management, creating a more secure and lasting environment?

According to the questionnaire, 74.4% answered no and 25.6% answered yes.



Source: Moroni Cortez e Patrícia Pantoja (2020).

Graph 15: Did you know that ISO 27008 is an information security ISO, and that it is applicable in all organizations?

Conclusion

According to what has been seen, an information security specialist in an organization is of fundamental importance so that he can make improvements, implement and evaluate the applicability of ISO in the organization's information security. Every day new attacks on companies appear, as well as new technologies, a constant innovation. It is necessary to be attentive and protected, always seeking to update technical standards that benefit current and future actions. The companies need to make clear to their employees and suppliers about how important and valuable their information is, as well as the urgency to protect it. Therefore, according to the evaluation of the quantitative questionnaire applied, it became evident an alert for the existing risks that may arise in an organization, as well as the need to protect its information. It was an exploratory work where the objective was to show that information security is necessary in all types of organizations, as well as a more efficient use through the suggestion of applicability of the information security ISSO.

Acknowledgments

First of all, to God who allowed this to happen throughout our lives, not only in these years as university students, but who at all times is the greatest teacher that anyone can know. Thanks to our family members who, at the time of our absence dedicated to higher education, always made it clear that the future is made from the constant dedication in the present, we thank all teachers for providing us with not only rational knowledge, but also the manifestation of the character and effectiveness of education in the process of professional qualification, for they have dedicated themselves a lot to us, not because they taught us, but because they made us learn.

REFERENCES

Andrade, S.N; Rabelo, S.H.M. Segurança da Informação: Um estudosobre o processo de segurança da informaçãoeminstituiçõesfinanceiraslocalizadasnaregiãocentro-oeste de minas gerais.MinasGerais:FASF, 2017. Available at: http://revista.fasf.edu.br/index.php/conecta/article/view/54. Accessed in: 04.04.2020.

AssociaçãoBrasileira de NormasTécnicas. NBR ISO/IEC 27001. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. 2006 https://www.academia.edu/36980100/ABNT_NBR_ISO_IEC_27001_Tecnologia_da_informação_Técnicas_de_segurança_Sistemas_de_gestão_de_segurança_da_informação_Requisitos. Accessed in: 08/02/2020.

AssociaçãoBrasileira de NormasTécnicas. NBR ISO/IEC 27002. Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. 2013. https://www.academia.edu/35031704/ABNT_NBR_ISO_IEC_27002_2005. Accessed in: 11/02/2020.

Bardin, L. Análise de conteúdo. 1. ed. São Paulo: Almedina, 2011.

Carneiro, A. Introdução à segurança dos sistemas de informação. Porto, Portugal: FCA, 2002.

Ferreira F., N. F., & Araújo, M. T. Política de segurança da informaçãoguiaprático para elaboração e implementação. 2. ed. Rio de Janeiro: CiênciaModerna, 2008.

Fontes, E. Políticas e normas para segurança da informação. Rio de Janeiro: Brasport, 2012.

Fontes, E.. Segurança da Informação. São Paulo:Saraiva. 2006.

ISO / IEC 27008 Controles de segurança da informação. https://www.academia.edu/35644434/ISO_IEC_27008_Controles_de_segurança_da_informação. Acesso: 20/03/2020.

ISO. "ISO27036-2013".2020 Available at: https://www.iso.org/standard/ 59688.html Accessed in:22.03.2020.

ISO."ISO/IEC27036-3".2020.Available at:https://www.iso.org/standard/59688.html. Accessed in :22/03/2020.

Ltd, IsecT. "Iso/Iectc 27008 ".2020. Available at: https://www.iso27001security.com/html/27008.html. Accessed in: 30.03.2020.

Peixoto, A."Lei de Proteção de dados".2020.Available at:https://www.politize.com.br/lei-de-protecao-de-dados/. Accessed in:19/03/2020.

Solutionsti. "ISO 27036 Relação com Fornecedores". 2020. Available at: https://debsolutionsti.com/iso-27000/iso-27036/Accessed in:13.03.2020.

Tanenbaum, A. Computer Networks, 4 ed. New Jersey: Prentice Hall, 2003. 27000. "Introdução á ISO 27008".2020. Available at: https:// www.27000.org/ iso-27008.htm. Accessed in: 30.03.2020.

****