International Journal for Innovation Education and Research

ONLINE ISSN: 2411-2933 PRINT - ISSN: 2411-3123

The Relevance of Information Security Policy in the Logical Part of the Company

Igor da Silva Corocher;Barbara Lopes Felsenthal;Bruno Pereira Gonçalves;Jean Mark Lobo de Oliveira;Rilmar Pereira Gomes;David Barbosa de Alencar

Abstract

The objective of this research is to analyze the relevance of the information security policy in the logical part of the company. It will be used data obtained from research conducted within various companies, which demonstrate the level of knowledge of employees and some wrong measures they taken which ended up harming the company. It will be possible to check not only the weight that an information policy has within any economic sector, but also to point out which areas of the company are most prone to data loss/theft. One of the most valuable assets in any business, is information, that is, data that is generated through trades made, revenue generated, productivity, etc., and however small the information seems, to the market it can be extremely relevant and the leakage of this information, due to a failure or lack of security, can lead to the bankruptcy of a company.

Keyword: Information Security Policy, Information Security Management, Data Loss;

Published Date: 11/30/2019 **Page.721-931** **Vol 7 No 11 2019**

DOI: https://doi.org/10.31686/ijier.Vol7.Iss11.1927

The Relevance of Information Security Policy in the Logical Part of the Company

Igor da Silva Corocher
igorcorocher@hotmail.com
Centro Universitário Metropolitano de Manaus – FAMETRO

Barbara Lopes Felsenthal
barbara@mapemi.com.br
Centro Universitário Metropolitano de Manaus – FAMETRO

Bruno Pereira Gonçalves (Advisor)
goncalves.bruno@gmail.com
Centro Universitário Metropolitano de Manaus – FAMETRO

Jean Mark Lobo de Oliveira
jeanlobolive@gmail.com
Centro Universitário Metropolitano de Manaus – FAMETRO

Rilmar Pereira Gomes
rilmargomes@hotmail.com
Centro Universitário Metropolitano de Manaus – FAMETRO

David Barbosa de Alencar
david002870@hotmail.com
Centro Universitário Metropolitano de Manaus – FAMETRO

Abstract

The objective of this research is to analyze the relevance of the information security policy in the logical part of the company. It will be used data obtained from research conducted within various companies, which demonstrate the level of knowledge of employees and some wrong measures they taken which ended up harming the company. It will be possible to check not only the weight that an information policy has within any economic sector, but also to point out which areas of the company are most prone to data loss/theft. One of the most valuable assets in any business, is information, that is, data that is generated through trades made, revenue generated, productivity, etc., and however small the information seems, to the market it can be extremely relevant and the leakage of this information, due to a failure or lack of security, can lead to the bankruptcy of a company.

Keywords: Information Security Policy, Information Security Management, Data Loss;

1. Introduction

The information security policy (PSI) is of significant importance within companies, no matter what economic sector it is in, as well-enforced, can prevent and prevent data loss and / or theft, which without them companies can simply let go. to exist.

According to ISO / IEC 17799 information is considered an asset (it comprises the organization's Assets and Rights set, having economic values and can be converted into money), i.e. it is of vital importance for the survival of corporations.

Over the years, a dependency on technology and information systems has emerged, and along with that dependency has come data vulnerability, creating a need to protect the corporation's knowledge and information.

Even with the rise of hackers, viruses, and other existing media that are used to harm companies / corporations, few companies in Brazil are concerned about information security, and many do not even know the relevance of data from A company has.

Thus, the purpose of this article is to demonstrate the relevance that the Information Security Policy (PSI) has in the logical part of a company.

2. Methodology

In the methodology were used bibliographical research such as, Information Security Policy, Information Security, The Importance of Information for Business, Damages in the Lack of Data Protection and Data Trafficking, this content will be extracted from articles, magazines, books, sites and study of ISOS.

We conducted bibliographic searches of ISOS regarding information security.

A quantitative survey was conducted, which consists of a questionnaire that must be completed by users of various companies, who consume a high number of information.

A PSI suggestion has been elaborated according to the best ISOS topics listed in this article.

3. Security Policy (PSI)

Information Security Policy (PSI) is a document that should contain a set of standards, methods and procedures, which should be communicated to all employees, as well as reviewed and critically reviewed at regular intervals or when changes become necessary. It is the ISMS that will ensure the viability and use of assets only by authorized persons who really need them to perform their duties within the company. (SOURCES, 2008).

It is increasingly important for an organization, even in its early stages, to formalize a document with its risk analysis, which provides top management with an indicator of the company's own future, in which assets that will be protected with investments will be listed. appropriate to their value at their risk (LAUREANO, 2005).

“Despite all care in defining security perimeters, this action will not produce positive results if employees are not in tune with the information security culture. This culture should be dispersed throughout the organization and especially consolidated within critical security areas. Information relevant to work within

these areas should be restricted to the area itself and only during the performance of activities where it becomes necessary. These activities should always be performed under supervision to ensure safety. When there is activity, these areas must remain validly closed, such as through the use of security seals, and regularly supervised (Campos, 2077, p.169) ".

4. Information Security

One of the most valuable assets in any business is information, that is, data that is generated through negotiations, revenue generated, customer registration, price formation, productivity, finance, etc.

As small and insignificant as information may seem to the market, it can be extremely relevant and the leakage of that information, due to a failure or lack of information security, can lead to the bankruptcy of a company.

Information security is made up of three pillars, confidentiality, integrity and availability.

Figure 1: 3 Pillars.
Source: ISO27001: 2013

As shown in Figure 1, confidentiality is one of the three pillars of information security, which is the guarantee that information will only be accessed by authorized persons, preventing documents from being available to everyone.

If access by an improper person occurs, even if unintentional, it may cause future problems.

The second pillar is integrity that ensures that information will not be modified or corrupted by third parties for the purpose of no data divergence. An example of a breach of integrity would be to change values in a seller's commission to a nonexistent higher value.

Availability, which is the third pillar, ensures that this same information is available to all users at any time without interruption. Maintaining the availability of information ensures continuous work on data provision.

5. The Importance of Information for the Company

The information is of paramount importance in an organization, because it is through it that the decision will be made, because without information would not have as the company conducts surveys, statistics and improvements that will contribute to its growth. For OLIVEIRA (1992), information helps in the decision

making process, because when properly structured is of crucial importance to the company, it associates the various subsystems and enables the company to postulate its objectives.

In the past, information was stored in a variety of ways: as in papers, archives, in the mind of a trusted employee or business owner, in large filing cabinets in folders and boxes. Today the information has gained so much value that it needs to be safely stored, because it will often depend on the useful life of the organization.

So, to have a protection, it would be necessary to have information security, with procedures, rules and standards that would have to be obeyed by all who represent the organization. This way the company will have great results by keeping the organization and its operation in perfect order and its successful business. For, one cannot have information as an end product, but the starting point that will lead to decision-making processing.

6. Loss in Lack of Protection of Information

The lack of an information security policy or its misapplication has serious consequences in both the business and even the world scenario. An example that demonstrates these consequences and the value an information has is the case of ransomware, which occurred in 2017 where 74 countries were invaded by this rogue software.

This malware acts as follows: it can first enter a corporate network disguised as a Word document and exploit networks that are misconfigured and have weak passwords, after gaining access it seeks valuable information for the corporation as a database of an ERP and kidnap it.

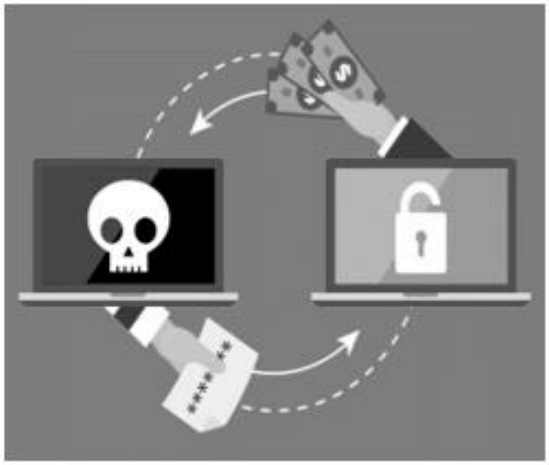


Figure 2 - Ransomware cycle.
Source: Analysis Informatic (2019).

With the encrypted database the company loses all information of years, customer registration, accounts receivable, accounts payable and etc. So there is no alternative but to pay the ransom to get the data back, the payment is charged in cryptocurrencies where it is impossible to track the fate of money and the values vary a lot, but they are always high and yet the company has no guarantee that you will get your files again after payment of the ransom.

7. Information Trafficking

According to the UN, in 2018 more than half of the world's population currently uses the Internet, which is equivalent to almost 4 billion people, in developing countries they are 45% of the population while in developed countries more than 80% of people.

Hootsuite surveyed the number of people using social networks and reached the following numbers: 3.1 billion (42%) people are active users of social networks, 2.9 billion (39%) use social networks via smartphones . In Brazil alone, over 96% of internet users are on some social network according to Social Media Trends.

Do you know that cell phone that was researched the price on the Internet and then began to see these same products on all sites that visited in the form of advertising? Cookies are to blame for this happening, they are files created by the browser for every website the user visits and can be used by hackers for web scam applications.

Policy writers in an organization will need to choose appropriate policies based on their companies' environment and business objectives. Each organization, with its different security requirements, based on the needs, legal requirements, organizational culture, and information systems used, will establish the policies presented and omit the rest. You also need to make choices about the rigidity of policies in each category. A smaller company located in a single facility where most employees know each other need not be too concerned that the attacker calls and impersonates an employee (although, of course, an impostor may impersonate a vendor). Similarly, despite the greater risks, a structured company with a more liberal and loose corporate culture may want to adopt only a limited subset of the recommended policies to meet its security objectives.

Facebook is currently involved in some scandals involving the sale of data from social network users, one of the accusations being the sale of data to Cambridge Analytica, which is a data analytics company for political campaigns, and has provided service to the campaign team. current President of the United States Donald Trump in 2016. According to the New York Times, the company had access to data from more than 50 million Facebook users, it happened even though Facebook itself was against and forbid
the sale and sale of this data.

8. Iso Technical Standards

8.1. ISO / IEC 27001

ISO / IEC 27001 is a standard that establishes the premises for an Information Security Management System (SGSI).

In accordance with ISO / IEC 27001 the main requirements are:

• Organizations should establish, implement, operate, monitor, critically analyze, maintain and improve a documented Information Security Management System (ISMS) within the context of the organization's global business activities and the risks it faces.

• Select controls within the process of implementing an ISO / IEC 27001 based ISMS;

• Implement commonly approved information security controls.

• Develop their own information security management guidelines.

8.2. ISO / IEC 27005

ISO / IEC 27005 provides information security risk management instructions, including guidance on risk assessment, risk treatment, risk acceptance, risk communication, monitoring, and critical risk analysis. Controls may be selected from this standard or other sets of controls, or new controls may be designed to meet specific needs as appropriate.

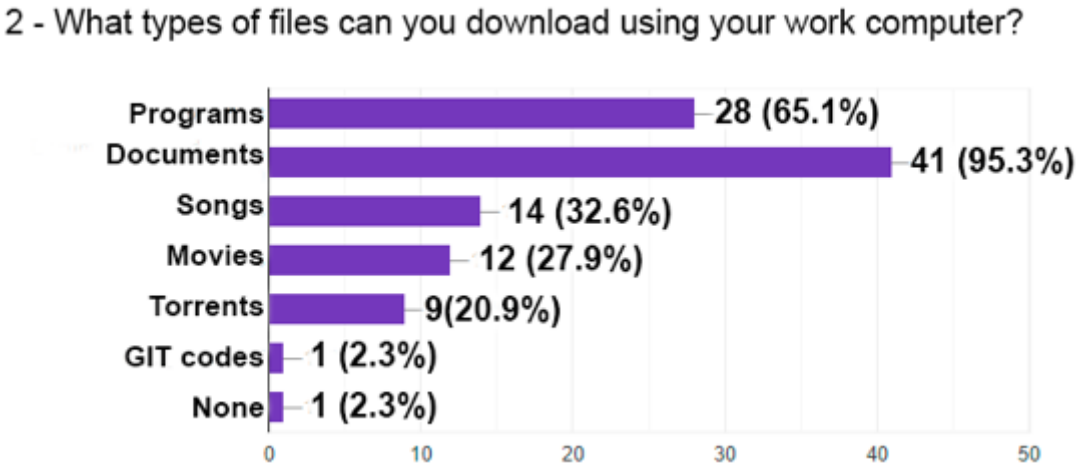
The standard defines the assessment, considering the likelihood of the threat and ease of fragility of controls and prioritizing actions over risks, considering impacts.

9. Questionnaire Analysis

Graph 1 - Information security - exchange - 2019

SOURCE: Own questionnaire development on google platform Forms, based on responses from users of organizations in general.

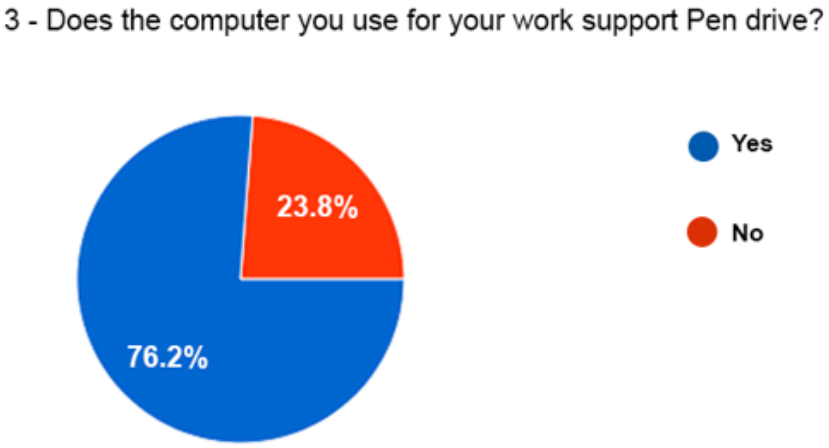
According to graph 1, it was found that there is still a high number of approximately 50% of users which leaves the organization information vulnerable, where 27.9% never changed the password of the computer they work in and 20.9% It does not require a password to access the company's computer, having vulnerability and giving the visibility of information to unauthorized persons having irregular definitions as to the confidentiality of information access in accordance with ISO / IEC 27002: 2005.



Graphic 2 - Information Security

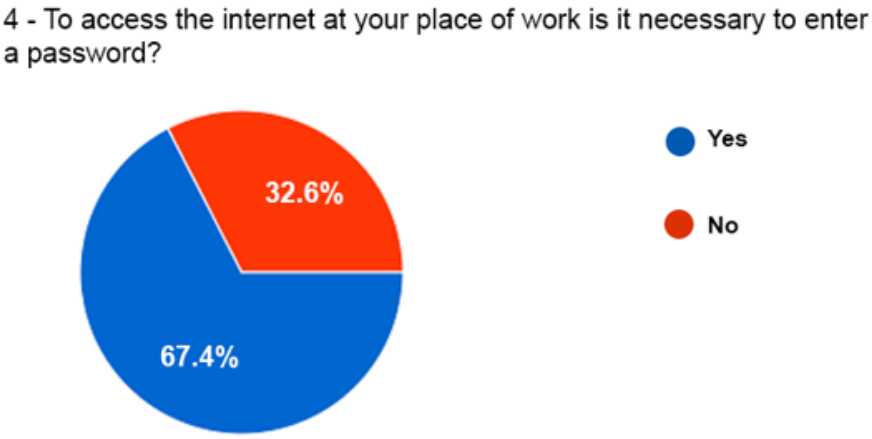
SOURCE: Own elaboration of questionnaires in google forms platform, from answers of users of organizations in general, 2019.

According to graph 2, a high number of 65.1% can be seen where the user can download any type of program opening a range for various threats, according to ISO / IEC 17799: 2005 the threats related to security. information, are increasingly frequent, ambitious and sophisticated, and may therefore cause greater damage to organizations that do not have an adequate security policy such as a filter to download which may bring infiltrated hosts.



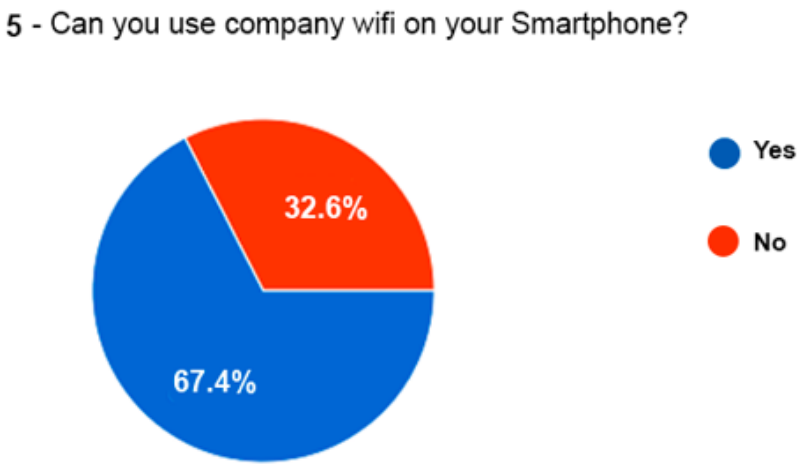
Graph 3 - Information Security - Pen drives - 2019.
SOURCE: Self-made questionnaires on google platform forms, based on responses from users of organizations in general.

The visualization in graph 3 is clear as to the danger it applies to about 76.2% of users according to the graph showing authorization to insert pen drivers on corporate computers, according to researchers Karsten Nohl and Jakob Lell released in G1. .com, there is a huge chance of attacks through these devices, one of them being the badUSB technique, modifying the firmware of a USB to malicious achievements.



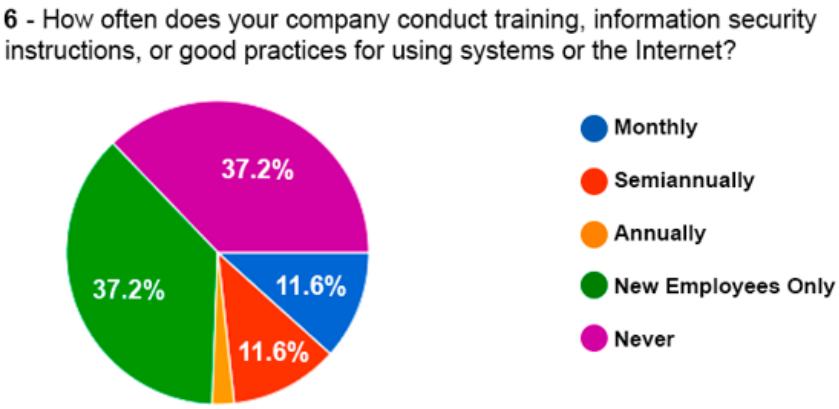
Graphic 4 - Information Security - Internet Passwords - 2019
SOURCE: Own survey on google platform forms, based on responses from users of organizations in general.

According to Graph 4, we have 67.45% of users who do not need to enter a password to access the internet, so any unauthorized person can have access to information and data on the company's internal network.



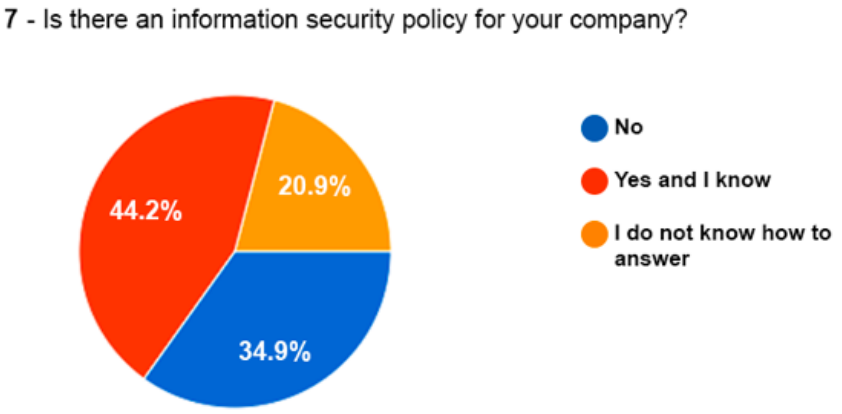
Graph 5 - Information Security - Enterprise Wi-Fi - 2019.
SOURCE: Own survey on google platform forms, based on responses from users of organizations in general.

According to Graph 5, it is observed that 67.4% of users interviewed use the company's WI-FI without any kind of restriction or network divisions, so there may be data hijacking, confidential and important in the organization. One of the requirements of ISO / IEC 27001 is that the organization must carry out information security risk assessments, implementing a risk management plan.



Graph 6 - Information Security - Training and Good practices - 2019. SOURCE: Own questionnaire elaboration in the google forms platform, based on responses from users of organizations in general.

According to graph 6, it is noted that 37.2% never had the user trained or received any kind of training for the handling of corporate equipment. According to ISO / IEC 27002: 2013, information security management requires at least the participation of all employees in the organization so that users can understand how to proceed with any given data.



Graph 7 - Information Security - PSI - 2019.
SOURCE: Own survey on google platform forms, based on responses from users of organizations in general.

According to graph 7, by merging the two negative responses it is concluded that almost 50% do not know your company's security policy, putting at risk and exposing sensitive data. NBR ISO / IEC 17799, suggests the creation of a document entitled "information security policy document", with management approval, making it available and disseminating to all employees, considering its relevance to the organization, should be easy. understanding by the target audience and accessible.

10. Administrative Guidelines and Standards

The guidelines and standards cited are based on the recommendations proposed by the standard ABNT NBR ISO / IEC 27002: 2005, recognized worldwide as a code of practice for information security management.

• Information technology (IT) officers within the company can access other users' files and data, but only when needed to perform operational activities such as maintaining computers, making copies of security, audits, deployment / installation of systems and applications.

• Every employee must have his or her own account or device to access computers, systems, databases and any other information assets, being identified by full name and social security number.

• Each employee is responsible for their login and password. Passwords are for personal and non-transferable use, and the holder is prohibited from sharing or providing them to third parties.

• Adopt a password expiration standard, i.e. program that every 30 days, for example, the user is required to renew their passwords, and cannot repeat any previously used.

• Identify the administrative and operational functions of each sector in order to restrict the powers of each user and reduce or eliminate the existence of individuals who can exclude logs and histories from their own actions.

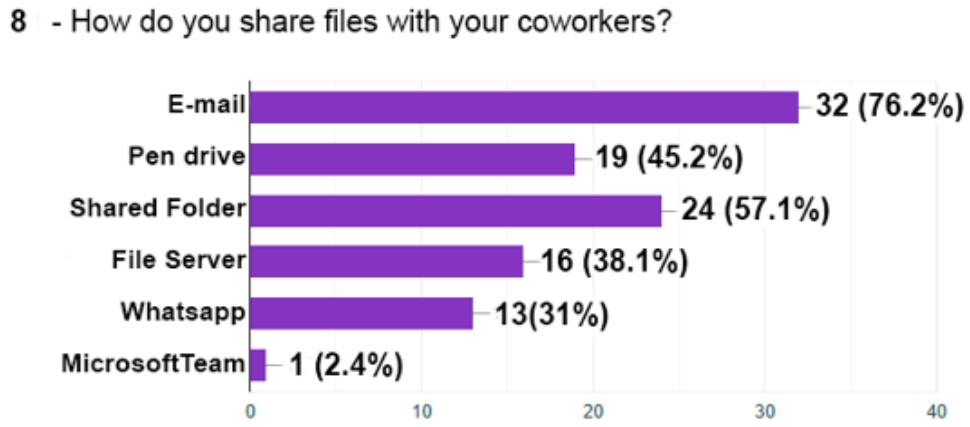
• Inform through a formal request, which may be via email, the blocking of access for users who have been disconnected from the company or for any other situation that requires restrictive measures to safeguard the company's assets.

• For the use of private equipment such as smartphones, laptops and pen drivers, as well as access to the internet, it is necessary to have a prior authorization from the manager / director of the company.

• Deploy workstation, server, e-mail, internet network, mobile or wireless monitoring systems. Information generated by monitoring may be used to identify users and their access, as well as material manipulated.
• Create an automated backup routine at set intervals according to the generation and flow of business data.
• The storage of this information must be in geographically distinct locations, because if something happens with the main backup has the "reserve".
• Always administer, protect and test the integrity of copies.
• Backups should be performed, preferably, before or after business hours, as the system can be slow, impairing the operation of the company.
• Use of corporate email is for work-related activities only and may not be used for personal purposes, or as a sign-up for commercial websites, social networks or any other platform for particular interests.
• Work information cannot be transmitted using personal emails.

11. Conclusion

In the data collected it was found that basic security procedures are not respected, as shown in graph 11, which asks what are the file sharing methods within the corporation, and the second most used method, representing 45.2% was the pen drive for information exchange. Using USB storage devices, such as a USB flash drive, poses a significant risk and can aggravate problems not only with information loss, but with information leakage and virus spread between corporate stations.



Graphic 8 - Share Files - PSI - 2019.
SOURCE: Own survey on google platform forms, based on responses from users of organizations in general.

According to graph 9 (topic 3.3) most of the users interviewed have had their work hampered by loss of document, and almost 50% lost their files due to viruses.
A company with a well-deployed PSI becomes a safer environment and reduces the risk of being infected with viruses, and if so, there will still be a data backup policy where a secure copy of company documents will be stored.
Given these facts, it was possible to highlight the relevance that information security policies have for the proper functioning of companies. In addition, research has shown that security and / or concern for company data is not yet considered a priority and that a lack of knowledge of the importance and value that

information carries with it interferes with the company's future.

12. References

[1] OLIVEIRA, Djalma de Pinho Rebouças de. Sistemas de informação gerenciais: estratégias, táticas, operacionais. 8. ed., São Paulo: Atlas, 1992.

[2] Disponível em <http://www.san.uri.br/~regiane/wp-content/uploads/2010/11/artigo.PDF> acesso em: 10 Ago. 2019.

[3] CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em informática e de Informações. São Paulo: SENAC/SP, 2006.

[4] Entenda o problema de segurança dos dispositivos USB. G1. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/entenda-o-problema-de-seguranca-dos-dispositivos-usb.html>. Acesso em: 10 agosto 2019.

[5] Revista conhecimento contábil, vol 06, ISSN 2447-2921, n 01, p 70-80 Jan/Jun, 2018.

[6] Boas Práticas de Segurança da Informação, Disponível em <http://www5.sefaz.mt.gov.br/documents/6071037/6412633/Boas_Praticas_de_Seguranca_da_Informacao.pdf> acessado em: 15 ago. 2019.

[7] Plano de Implementação da Norma ISO/IEC 27001 no INEM, Carlos Manuel Rosa Correia Disponível em <https://run.unl.pt/bitstream/10362/19605/1/TGI0069.pdf> Acessado em: 20 ago. 2019.

[8] MARCELO,A; PEREIRA, M. A ARTE DE HACKEAR PESSOAS. Rio de Janeiro: Brasport, 2005.

[9] ARAUJO, Eduardo. A VULNERABILIDADE HUMANA NA SEGURANÇA DA INFORMAÇÃO. 2005

[10] FONTES, Edson. POLÍTICAS E NORMAS PARA A SEGURANÇA DA INFORMAÇÃO: Como desenvolver, implantar e Manter regularmentos para a proteção da informação nas organizações. São Paulo. Brasport. 2012

[11] DANTAS, M. SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM FOCADA EM GESTÃO DE RISCOS. 1 ed. Olinda: Livro rápido, 2011

[12] FREITAS, F; ARAUJO, M. POLITICAS DE SEGURANÇA DA INFORMAÇÃO: Guia prático para elaboração e implementação. 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008

[13] FONTES, E. PRATICANDO A SEGURANÇA DA IONFORMAÇÃO. Rio de Janeiro: Brasport, 2008

[14] SENAC. PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO. V.1.0. São Paulo. Disponível em: <http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf>. Acesso em: 01 de outubro 2019.