https://dx.doi.org/10.22161/ijaers.73.8 *ISSN: 2349-6495(P) | 2456-1908(O)*

Security Mechanisms of Information in Companies

Larysson Luis Alves Araújo, Maria Celimar da Silva, Rosiane Rocha Oliveira Santos *

*Faculty of Social Sciences and Petrolina, Brazil. Campus s / n - Vila Eduardo, Petrolina - PE.

Abstract— *Information security is a feature that aims to protect, but also a management area. With the evolution of information and its rapid spread technologies, also increased the crimes related to it, with it, this article proposes a survey of information security mechanisms, influence and use of them by companies. It was also used a directed form the target audience to gather information on how companies deal with threats to their assets, data and services, also seeks to know whether there is effective use of information security mechanisms.*

Keywords— ***Companies, Threats, Information Security, Research.***

I. INTRODUCTION

Information Security (IS) is an important area of the organization, the neglect of this can extensively affect the entire operation of the same, resulting in large losses, such as unavailability of services and customer dissatisfaction (Mendes et al., 2013).

It consists of skill, resources, best practices and mechanisms used to protect information systems and data against cyber-attacks and misuse, as well as loss of integrity or theft in general (POSITIVE, 2017).

Information security is a strategic level theme and can never be left out, mainly because of the great constant technological advancement, the lack thereof in an organization can undertake routine activities, but can also influence the results obtained and the reputation of same (positive, 2017). Note that it is impossible to get one hundred percent practical way to control all possible threats to information and / or services. You should always prioritize what is most relevant.

To better understand how the information security, you must understand the principles on which it is based, which are: Integrity, Confidentiality, Availability and Authenticity (HINTZBERGEN et al, 2018.).

Integrity - It is the guarantee that the information manipulated keep all the original features that have been set by the owner of the information, as well as ensure it is complete, inviolable and protected against use or tampering (HINTZBERGEN et al, 2018.).

confidentiality- The information can only be accessed and updated only by legitimate entities, or those authorized and properly accredited (HINTZBERGEN et al, 2018.). If the company does not have security mechanisms that are able to ensure confidentiality will become vulnerable to threats, such as cyber attacks and theft of confidential information or customer (POSITIVE, 2017).

Availability- Ensure that the information is always accessible and available on demand and performance specifications to authorized users (Mendes et al, 2013.). Authenticity - Procedure to identify and register the user who is modifying or sending information, ensuring the correctness thereof and non-repudiation, which is the inability of the denial of that information written or manipulation (Mendes et al, 2013.).

Due to the constant evolution and technological innovation, we know how hard it is to keep a track hundred percent of every kind of threat that will affect the services and information of companies and organizations. Therefore, this article aims to bring together information gathered through a questionnaire on how companies deal with possible threats and what information security mechanisms used more frequently.

Threat is a term used to describe a situation that can cause the loss of important information or devices. There's no way to talk about without understanding information security possible threats, in which are very comprehensive and varied (SANTO, 2012). Among them, we can highlight:

- Virus - often responsible for irreversible damage to systems and applications.

https://dx.doi.org/10.22161/ijaers.73.8 *ISSN: 2349-6495(P) | 2456-1908(O)*

- Denial of Service (DoS) - Denial of service is an example of the threat that may affect the principle of availability by blocking access to a system and / or information.
- Fraud - Scam or Fraud can cover a lot of threats, the most common of these is the Phishing, where it is used for famous sites interfaces and / or sending emails to obtain confidential information.
- *malware*- They are responsible for theft of information through the invasions database and computers. As viruses are dangerous for the ability to spread rapidly.

Information Security mechanisms can be divided between Physical Security and Logical. They are used to ensure that the basic principles are not affected and inflicted by minimizing or blocking of possible threats to information. Mechanisms for Physical Security deal with methods to prevent access of unauthorized persons to areas where they are equipment and critical information. Some of them are restricted access, monitoring system and biometrics. Security The Logic aims to control access to passwords, files, data, applications and operating systems, as an example we have backups (backups), Firewalls, Information Security Policy, Redundancy Infrastructure and IT Risk Management .

Some of the mechanisms commonly used today in day are:

Detetecção Vulnerabilities -Vulnerabilities are flaws or gaps in a system that allows unauthorized users to manipulate it, as well, can be failures in technological resources of hardware or software, such as installing and / or wrong configuration (BUZZATE, 2014).

Detection would be a way to identify potential vulnerabilities and take preventive or corrective action. The outdated technology makes it vulnerable all the security and infrastructure, because all equipment is subject to obsolescence, misuse, poor maintenance or break, which can compromise more than a principle of information security and generating consequences as operational inefficiency, dissatisfaction client and availability of services, so should adopt specific safety practices for each iT component (Servers, Computers, Networking and Software).

Backup (Backup) -Backups, more commonly known as Backups are used to ensure the principle of availability and integrity of information and services if the basis on which they are located are damaged or stolen (MICROSOFT, 2008). The backup storage can be done in physical or cloud devices, it is advisable always several backups stored in different places. Note that companies that have good backup practices in case of loss of information can make the recovery of the same in a very short space of time.

Redundancy Infrastructure - A replicated infrastructure, whether physical or virtual, is another way to ensure the availability of information or services because if IT equipment (Server, UPS, Router) fails, there will always be a substitute to enter into immediate operation giving maintaining continuity and availability (pOSITIVE, 2017).

firewall - Mechanism that controls the data traffic of internal and external computer networks. It works by protocols (TCP / IP, UDP, HTTP) ensuring the correct functioning of the communication between one point and another, aiming to prevent intrusions (BUZZATE, 2014).

Restricted access - The use of restricted access to information, computers or sectors can be a way to ensure confidentiality and authenticity of the information. Some forms of application of this mechanism can be given for the use of biometrics (facial recognition, fingerprint), unique user identification and monitoring system with cameras (POSITIVE, 2017).

Security policy information - It is a document or manual that determines the most important actions to ensure information security,Also reaching the issue of behavior in the company and access to resources (Martins, 2005). Promotes the standardization of actions so that everyone knows what to do and what to avoid.

Management of IT Risks - Aims to identify the company's IT risks, analyzing them and sorting them according to likelihood, vulnerability to be exploited and impact on routine and their goals activities (TCU, 2018). From this it is preparing a response plan for each risk, defining actions. We can avoid the risk through actions that extinguish, reduce the probability and / or impact of it, accept the risk monitoring it continuously or transfer with the hiring of a cloud infrastructure to the security commitment be due to the provider. Some of the main risks are the lack of guidance, errors in internal processes, negligence and malicious activity.

Cloud computing - Cloud computing allows outsourcing of information technology services, ensuring agility, cost reduction and constant updating. After his appearance was possible to provide services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Hardware as a Service (Haas) (Pereira et al., 2016).

- Infrastructure as a Service (IaaS) - Outsourcing Servers and Datacenters scalable according to the needs of the company. Amazon

https://dx.doi.org/10.22161/ijaers.73.8 *ISSN: 2349-6495(P) | 2456-1908(O)*

Web Services (AWS), Microsoft Azure and Digital Ocean are examples.

- Platform as a Service (PaaS) - Outsourcing platforms for development and testing without the need to set up an infrastructure.
- Software as a Service (SaaS) - is the provision of software as a service over the Internet, is paid signature is used while the product. Google Drive and Office 365 are examples of SaaS.
- Hardware as a Service (HAAS) - Hiring and providing remotely hardware. AWS offers this type of service as well.

II. MATERIALS AND METHODS

This research aims to conduct a study on Security mechanisms of information and their use by companies. We conducted a survey of information in books, academic papers and dissertations available in the database and virtual libraries such as Google Scholar and various sites related to the topic of research.

It was also used a targeted questionnaire to the target audience, ie different segments companies (Automotive Center, Shop, Construction, IT) using a diverse range of IT services, making it thus necessary to use mechanisms for security its assets, data and information.

The proposals seek to take matters as much information about the segment, form the IT sector division, as well as, what mechanisms are used and review the efficacy and safety of their respective companies.

Participated in the data collection 20 companies, of which twelve (12) reported, including 2 of IT enterprises (17%) 0 Automotive centers (0%) 7 stores (58%) and 3 Builders (25%) .

III. RESULTS AND DISCUSSION

The questionnaire contained five questions, which were made with the purpose of collecting information about the subject matter of this article. Like all companies did not reply, graphics and information are based on responses from 12 companies that responded.

Fig. 1: Segments of the participating research companies

As shown in Figure 1, this question was drawn up in order to get information on the area of operation of the companies that answered the questionnaire. We see that the twelve companies 7 (58%) in the merchant operating area 3 (25%) act as builders and 2 (17%) are IT companies. None of the companies of the Automotive Center branch receiving the questionnaire responded.

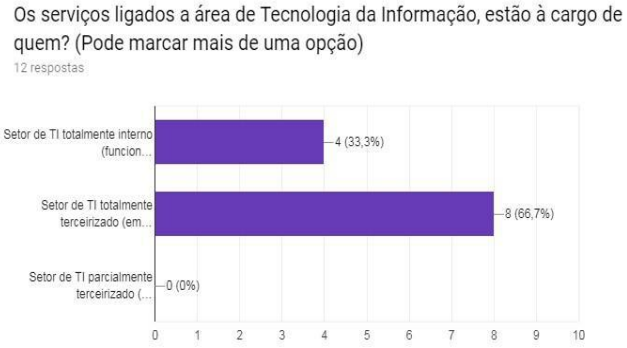

Fig. 2: Who performs the services of the Technology

4 of responding companies (33.3%) mentioned that they had fully domestic IT sector without outsourcing, 8 (66.7%) mentioned that they had fully outsourced IT Sector, 0% Sector IT outsourced partially as Figure 2. This happens because of the lack of knowledge of the companies in relation to information technology, or by the fact that today is more rewarding and less costly to have a third party looking after your assets and information without the need for new investments in an entire sector, such as the purchase of technological equipment and hiring a staff of trained employees to handle this type of service. There are several factors that can influence this decision,

https://dx.doi.org/10.22161/ijaers.73.8 *ISSN: 2349-6495(P) | 2456-1908(O)*

In Figure 3 we have the response that sought to assess the information which is the information security mechanisms used by most companies nowadays, but also see what the least used so comparing the differences between the values obtained.

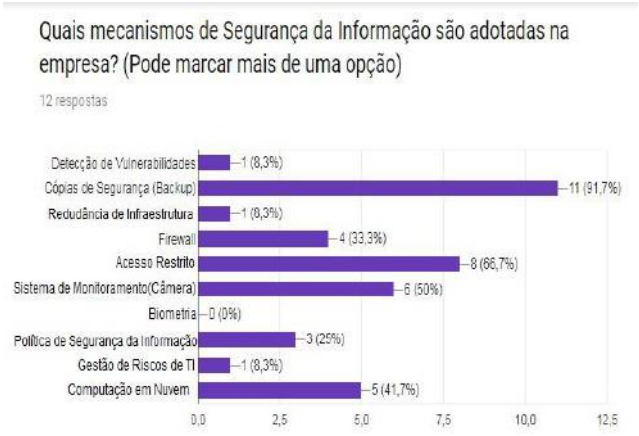

Fig. 3: What mechanisms of information security are adopted by companies

Among the information security mechanisms used in the first place was the Backup (Backup) with 11 (91.7%) responses from 12 companies, showing that today this mechanism is widely used for its ease and agility, followed Restricted access to 8 (66.7%) responses showing that companies are also concerned regarding access to its assets and general information.

The quantity of 6 companies (50%) responded that uses Monitoring System, 5 (41.7%) use Cloud Computing, a mechanism that is often used in conjunction with backups, seeking greater security against loss of it . 4 (33.3%) firewall uses to protect its information from viruses and potential cyber attacks.

Of the 12 companies that responded only five companies (25%) have an effective information security policy in the organization, showing that still lack information about how important an Information Security Policy can be for a company, it is through that it the company establishes guidelines and all possible actions to

threats on its assets and information.

Only 1 (8.3%) Response to Redundancy Infrastructure, Vulnerability Detection and IT Risk Management, showing once again that among those companies who responded, almost no understand the danger of doing vulnerability detection for through iT Risk management establish preventive and corrective actions for possible disasters to its assets and information, as well, it is through an infrastructure redundancy that you ensure greater availability of their services.

Fig. 4: preparation of business level

In Figure 4 we sought answers to the question elaborated in order to identify if companies feel prepared to face possible threats and risks to their information and assets may suffer, in which 6 (50%) said yes, they were prepared even taking into account that almost do not use effective prevention mechanisms such as Vulnerability Detection and iT Risk Management, as well raise the question if these companies are aware of your current situation or if you just do not feel interest in the subject.

Only one company (8%) replied that he was not prepared and 6 (42%) responded that they did not stop to assess it, even knowing that what was at stake was their valuable information assets and reputation.

Fig. 5: View of the companies on the importance of information security

Figure 5 shows the opinion of companies on the effectiveness of the security mechanisms of information, including, 6 believe that the use bring good results, 4 opined that relies heavily on the practices of the staff, one said he did not believe in the efficacy of use of the mechanisms and the other that there is no review, because everything changes very fast.

It was noticed that even though the importance of using safety mechanisms for the companies that responded do not engage in investment in IT the same as in the third question clearly shows the lack of use of the wide range of available mechanisms, apoiando- only the most simple, such as backups, restricted access and monitoring system, which is the basic for any company that wants to have a control over your assets and information, and a deficit in the use of more

https://dx.doi.org/10.22161/ijaers.73.8 *ISSN: 2349-6495(P) | 2456-1908(O)*

elaborate and recommended mechanisms such as Policy Information Security and IT Risk Management.

IV. CONCLUSIONS

The conclusion section must be included and shouldnt Indicate Clearly the advantages, limitations, and possible applications of the paper. Although a conclusion may review the main points of the paper, do not replicate the abstract to the conclusion. The conclusion might elaborate on the importance of the work or suggest applications and extensions.

Throughout the work we have seen the importance of information security in organizations and companies, basic security concepts, potential threats and mechanisms for information security to combat such threats. Through research we have seen how companies deal with the threats taking into account all that has been presented previously.

It is necessary to combine the largest number of possible mechanisms, so that they can carry out a well-planned work, and thus combat the security threats of information and ensure the quality of work provided by third parties with the necessary efficiency.

The expectation is that the research described here is received as a warning for professionals Technology and even the managers of companies who care and are responsible for information security in organizations that best practice and mechanisms should be used as a manual.

REFERENCES

[1] Aikpo, F., Ahouanse, M., Agbandji, L., Edorh, P., & Houssou, C. (2017). Assessment of contamination of soil by pesticides in Djidja's cotton area in Benin. *International Journal Of Advanced Engineering Research And Science*, *4*(7), 1-5. doi: 10.22161/ijaers.4.7.1BUZZATE Patricia Monego. (2014). Vulnerability Analysis by detectors scanners. Accessed on November 5, 2018, available at UFSM:

[2] http://www.redes.ufsm.br/docs/tccs/TCC_Final_Patricia.pdf

[3] HINTZBERGEN, Jule; HINTZBERGEN, Kess; SMULDERS, Andrew; BAARS, Hans. (2018). Information Security Fundamentals: based on ISO 27001 and ISO 27002, 10-35.

[4] MARTINS, Alaíde Barbosa; SANTOS, Alberto Celso Saibel. (2005). A methodology for the implementation of a Safety Management System Information. access

[5] 05 in November in 2018 available in JISTEM: http://www.jistem.fea.usp.br/index.php/jistem/article/view/10.4301%252FS1807177520050002000002/15

[6] MENDES, Ricardo; OLIVEIRA, Romulus RL; COSTA, Anderson FBF; GOMES, Reinaldo. (2013). A methodology for implementation of a Safety Management System Information (ISMS) based on standards ISO / IEC 27001 and 27002.

[7] MICROSOFT (2008). Resource IO: Data Protection and Recovery - Basic to Standardized. Accessed on November 5, 2018, available at Microsoft: https://docs.microsoft.com/pt-br/previous-versions/infrastructureoptimization/bb821259(v=technet.10).

[8] PEREIRA, Lucio Adan; PENHA, Elton Wagner Machado; GOMES, Nazur Amorim; FREITAS, Rodrigo Randow. (2016). Cloud Computing: Information Security Environments Cloud and Physical Networks. Accessed on November 5, 2018, available at UFES: http://periodicos.ufes.br/BJPE/article/viewFile/EO02_2016/pdf

[9] POSITIVE (2017). Information Security: Meet the 12 best practices. Accessed on 01 November 2018, available at Positive: https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/

[10] SANTO, adrielle FERNANDA SILVA SPIRIT. (2012). Information security. Accessed on November 5, 2018, available at ICE.EDU: http://www.ice.edu.br/TNX/encontrocomputacao/artigosinternos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf

[11] TCU (2018). 10 Steps for good risk management. Accessed on November 5, 2018, available at TCU: https://portal.tcu.gov.br/biblioteca-digital/10-passos-para-aboa-gestao-de-riscos.htm