Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/15532
DOI URL: http://dx.doi.org/10.21474/IJAR01/15532

RESEARCH ARTICLE

INFORMATION SECURITY POLICY: ESTABLISHING RULES AND STANDARDS OF USE AMONG EMPLOYEES

Felipe De Sousa Lopes, Mario Giovanne Marafigo Oliveira and Jean Mark Lobo De Oliveira

Manuscript Info

Manuscript History
Received: 19 August 2022
Final Accepted: 23 September 2022
Published: October 2022

Key words:-
Technology, Safety Polytic, PSI, Attacks On Security Assets

Abstract

Harmony between sectors of a company is something that adds a lot of value to the institution even more when it comes to the IT sector in relation to the others. Information security aims to adequately protect data from the various existing threats, and information security policy governs it. This is the basic theme of this article, in which the application proposal addressed aims to identify how it reflects in the area of information technology in relation to employees within a social concept of behavior in the face of some barriers imposed on sectors at the level of access. Within the context studied, the methodology applied to achieve the objective had a case study that provided the necessary data. Through the survey directly linked to the facts, the applied research raised the consequences of the theme. In addition to empirical and descriptive research, which through structured interviews used reports and documents, contributing to the understanding of the reflexes that occurred between the sectors related to the Security Policy.

Introduction:-

Traditionally, the "digital divide" has been understood as a socioeconomic perspective, dealing with access to information (communication technology), especially the Internet, and the ability to use this technology to participate fully in business, political and social life (Partridge, 2015). However, several authors argue that digital exclusion should also be understood in psychological, cultural and sociological terms. As an example: Warschauer (2016) stated that digital exclusion is not only about physical access to computers and connectivity, but also about people's ability to make full use of systems.

The network security policy is a set of standards that are applied to all users of a company's infrastructure. Its main objective is to reduce risks, avoid threats and problems related to data leakage and theft (CAMPOS, 2016). In addition, it guides teams to have a more robust pattern of actions to eliminate vulnerabilities and mitigate potential attacks.

According to kaspersky study about 30% of the main attacks on companies is of human origin, that is, at least 1/3 of the attacks were the result of human practices, becoming one of the main layers of attack in information security. With this many users feel uncomfortable working in an environment limited by security restrictions, other than that another part of users is afraid even for an oversight to perform some unauthorized procedure and suffer penalty imposed by the company's security policy. Causing a constant malaise between the company's collaborating users and the company's IT team.

Corresponding Author:- Felipe De Sousa Lopes

Information security awareness campaigns can be defined as an economic and sustainable practice to educate and change employees' relationship with IT staff.

Weighing this was developed this article in order to find an internal balance between the sectors of a company, creating a non-hostile work environment. It is important to inform users of the importance of company data and what is the collaboration in the security of these assets while respecting the company's security policy. The development of a balanced and thoughtful policy can be the solution of this obstacle among employees. Making them more aware of the whole process and redoubling the level of attention, thus avoiding the malaise exists between employees and THE IT team.

Theoretical Referecial

This chapter aims to present the theoretical framework of the research and to support the contributions to the study processes. Thus, the main references in the definition of the concept, dimensions and elements were sought in the field of knowledge, as well as the application of models or typologies related to culture and organizational values.

Information Security

According to Fontes (2016, p. 11), information security can be defined as a set of guidelines, standards, procedures, policies and other actions that aim to protect the information resource, enabling the organization's business to be carried out and its mission to be achieved.

From this, according to Laureano (2014), information security should be a process capable of providing organizations with more efficient to avoid possible risks related to the environment in which it is located.

Sources (2016) addresses that information security aims to provide the means to avoid risks and provide organizations with the possibility to reduce them, as they increasingly rely on processes that make use of information. This is explained, because by failing to obtain information or obtaining it in the wrong way, consequently, brings direct losses to the business that makes use of it.

Safety Standards

Standards and standards aim to define rules, principles and criteria, record best practices and provide uniformity and quality to processes, products or services, with a view to their efficiency and effectiveness (BEAL, 2015, p. 36). At the same time, Semola (2013) says that a standard has the purpose of defining rules, standards and control instruments that give uniformity to a process, product or service.

Information Security Policy

It is possible to define information security policy, as instructions to be followed to have a good management of security, as Semola describes (2014, p. 105), "politics has a fundamental role and, in the proper proportions, has similar importance to the federal constitution of a country". Thus we can observe such the importance of a very precise and impeccable security policy, to ensure the preservation of information against future eventualities.

The objective of an information security policy in accordance with ABNT ISO/IEC 27002 (2013, p.02). Provide guidance from the Board and support for information security in accordance with business requirements and relevant laws and regulations. Its definition must be approved by the strategic layer of the corporation, and then passed on to the other relevant employees and external parties.

Information Assets

In relation to information assets Semola (2014, p. 43) describes how, "It is every element that composes the processes that manipulate and process the information, from the information itself". Thus, any component that interacts with information directly can be considered an asset of information.

For example, a server that stores the organization's data is an information asset, just as a fingerprint reader, which serves to free access to a particular location is also considered an asset of the information.

Methodology:-

The article is a case study that will be presented below conducts the research among the 5 members of the IT team of the company targeted by this study. This research was conducted through interviews and investigations of daily

routines. These employees perform technical and specific functions in the technological area. Being an IT Manager, a Networks Analyst, a Support Analyst, a Jr Support Analyst, a Hardware Technician. In an applied manner, the reactions of the Information Security Policy in the IT team will be examined quantitatively and qualitatively across the interviews and observations raised.

Quantitative Analyses

The quantitative research methodology aims to explain through a systemic investigation of observable phenomena through data collection, analyzed using methods based on mathematical, statistical and computational techniques.

All quantitative data are numerical data, such as statistics, percentages, etc., obtained through surveys, questionnaires or by manipulating pre-existing statistical data.

Results:-

It is essential that companies implement educational strategies for their employees making awareness part of the organization's safety culture. Being implemented in hiring the employee to become part of the organizational culture of the company involved.

The steps implemented in the process are expressed in Figure 1 where it shows sequentially the correct order of implementation applied.

Figura 1:- Organizational awareness cycle.

Source: Good management, (2021).

All these steps were inserted through lectures, examples of organizations successful in their security policies, showing the positive results that brought awareness and adoption of these changes.

Process Steps

» **Deconstruction:**

The idea of deconstruction is based on the organizational culture of employees, on how they treat information security, which can be changed to a better use respecting the limits of the structure, and without facing existing standards of protection. It's not talking about who's wrong, it's showing another way to do it.

» **Scope Definition:**

At this stage, it is critical to identify what the needs of the company are or the security-related problems, what needs to be resolved, and then develop the planning. The idea is to create action plans, metrics and objectives for the cycle to start.

» **Strategy elaboration:**
It is the process in which to elaborate a strategy of an organization and define how it can be achieved, aiming at a good planning of the future implementation.

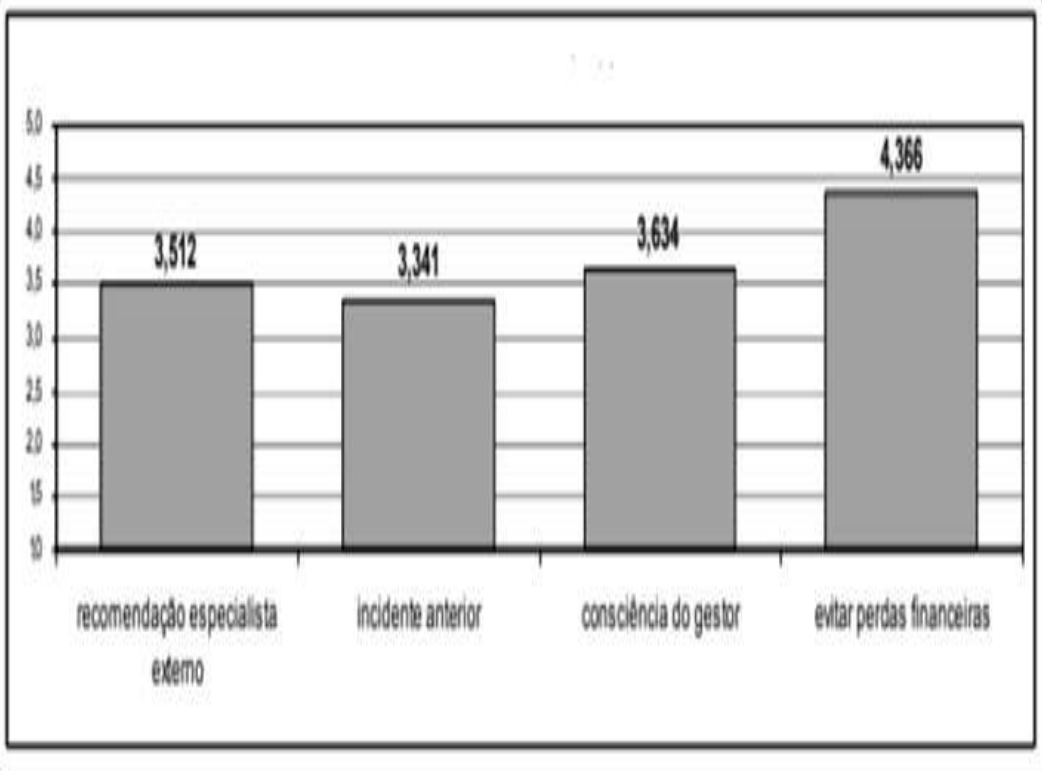
» **The campaign begins:**
At this stage begins awareness campaigns regarding the security policy that the company adopts. Showing the positives of your deployment. Campaigns can't be immediate impositions, but awareness.

» **Note the results** :
Step in which all possible indicators are collected for decision-making regarding the policy to be implemented.

» **Continuous improvement administration:**
Main stage of the process, where the policy is managed, verifying some flexibilities or snare the existing policy is a stage of great evolution of the course of its management.

Positive And Negative Factors On Security Policy
Information security policy is the security that no one has access to restricted information. We consider that this information is restricted to the data of the company itself, its partners and its users. But if on the one hand the explanation is simple, implementation, on the other, requires constant care.

Gráfico 1:- Positive factors.

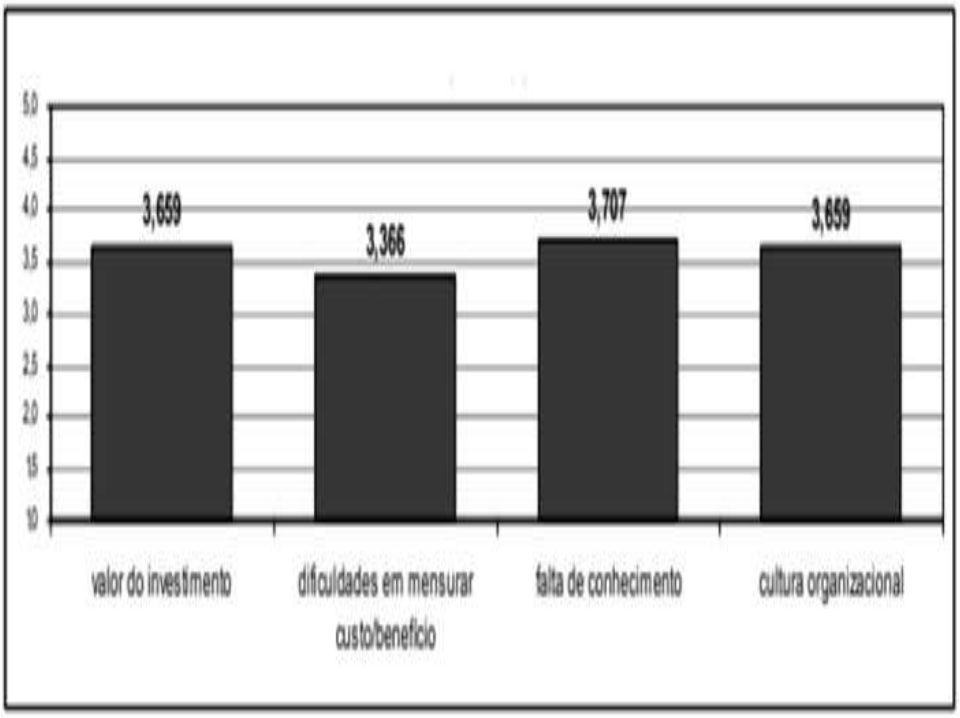


Source: Own Authorship, (2021).

Graph 1 illustrates the positive points in our research on information security policy. Where the former refers to financial losses with breach of security or a failure in the process. The second positive point that we can highlight is a better awareness of managers about the security policy implemented in the organization. The third positive point is the notoriety that the company gains by having an information security policy. And finally and no less important the end of incidents that happened for lack of limit imposed on employees. There are other positive points that did not stand out in our study, but are gained with the implementation of the policy such as: Process Optimization, Competitive Differential, Improved Communication and Value Generation.

Information security policy can both bring some positives and negative points. So next, let's look at some of the downsides that the topic may have on business.

Graphic 2:- Negative factors.



Source: Own Authorship, (2021).

Graph 2 shows the indexes of some negative points, which can hinderthe need for a good information security policy. The first highlight is the lack of knowledge of its employees the degree of importance of the policy for the company's business. The second is organizational culture, where employees insist on not changing. The third and fourth well say tied is the value of the investment with awareness lectures and the last is the difficulty in measuring the cost benefit of the policy. However, we can point out other negative points in the use of information security policy such as: crisis in the company's image, customer dissatisfaction and financial losses.

Results Discussion:-

Regardless of the size of the company has defined a set of standards and guidelines for the use of IT resources as a basis for gaining competitive advantage and understanding of all, it can be the differential between successful and stagnant companies, since the policy, when well used, guarantees four main points.

» Resource Savings
» Increased Productivity
» Greater Market Power
» Better understanding of employees

It's not enough to implement a plethora of network monitoring systems, Big Data Analytics capabilities for algorithmic scanning of potential threats, firewalls, and Cloud Security services.

For its effective functioning, the information security policy must be simple, true, understandable written in a clear and concise manner and aligned with the company's business strategies. With these measures, key vulnerabilities will be quickly identified and the organization will be more able to keep its devices safe. Trying to implement a policy that clashes head-on with the way you work in the company is not easy. It is necessary a mild approach without mandatory imposition at first, educational lectures, examples of successes obtained in regional, national and international companies, with the purpose of a better awareness and without conflict between sectors.

Conclusion:-

The lack of direct obedience to information security among employees may be because, when they were hired, information security was not such an important issue. Whatever the reason, whenever there is an information security policy, the role and importance of information security should be rewritten and updated as an integral part of the duty of all employees of the company, whatever the hierarchy occupied by that person within the company.

From the above discussion, we have no doubt that information security should be addressed directly, and by name, in all documents describing good corporate practices. This will clearly indicate the role that senior management and the Council have to play, and will greatly simplify the information efforts of security managers.

References:-

1. ALBRECHTSEN, E. A qualitative study of users' view on information security. Computers & Security 2017; 26(4):276–89.
2. BEAL, Adriana. Information Security: principles and best practices for the protection of information assets in organizations - São Paulo: Atlas, 2015.
3. CAMPOS, André L. N. Information Security System: Controlling Risks. Florianópolis: Visual Books, 2016. SOURCES, E. Information security: the user makes a difference. São Paulo: Saraiva, 2016.
4. HAIR, J.R. Joseph F.; BABIN, Barry; MONEY Arthur H.; SAMOUEL, Phillip. Fundamentals of Research Methods in Administration - Porto Alegre: Bookman, 2015.
5. ISO 17799. ABNT NBR ISO/IEC 17799:2005 - Information Technology - Security techniques - Code of practice for information security management. Brazilian Association of Technical Standards - Rio de Janeiro: ABNT, 2005.
6. LAUREANO, M.A.P. Information security. Curitiba: Technical Book, 2014.
7. SÊMOLA, M. Information Security Management - An Executive Vision - 2 ed. São Paulo: Elsevier, 2014
8. Semola, Mark. Information Security Management: an executive vision - Rio de Janeiro: Campus, 2013.