International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 3 ǁ March 2023 ǁ PP. 235-238

Basic security policies in Information Technology

Enrique Ramírez-Méndez, David Asael Gutiérrez-Hernández
Tecnológico Nacional de México campus León, León, Guanajuato, México. CorrespondingAuthor:Enrique Ramírez-Méndez (Enrique.ramirez@leon.tecnm.mx)

Abstract
This article presents an overview that justifies why basic Security Policies in Information Technology should be implemented within companies, based on the mention of one of the international standards that in the field of computer security represents a proven and recognized option, In order to have controls in organizations that help us deal with situations of insecurity in the fields of Information Technology (IT), a series of proposed internal policies are listed within the document, which can serve as the basis for the construction of a document that gives certainty and supports organizations in a practical way in the location of risks, threats and care that in IT matters the company can review and implement, and know the important contribution of IT areas, in the difficult task of taking advantage of the investments that are made in terms of Technology and that are so necessary for the performance of the productive activities.

Keywords: *information technology, security policies, computer security*

Date of Submission: 03-03-2023 Date of acceptance: 15-03-2023

I. INTRODUCTION

CSecurity in any of its facets represents an ideal that is difficult to achieve, especially if what is sought is proactive and preventive security, as is the case with computer security.

Over time, efforts have been made to find and, where appropriate, to standardize the processes or tasks that guarantee computer security, as a result of this we find initiatives such as the standard issued by the International Organization for Standardization (ISO) in conjunction with the Commission International Electrotechnical (IEC), ISO/IEC 17799, currently known as ISO/IEC 27001, which is the section that most interests us for the purposes of this article, this section defines information security with three fundamental aspects called CIA (Confidentiality, Integrity, Availability), ISO (2022).

The three aspects of CIA security, according to Katz (2013), are explained below.

Confidentiality; This aspect refers to the fact that all information stored and transmitted by computer means can only be read by the recipient, in case it falls into the hands of unauthorized persons, the document cannot be read or accessed in its content except by authorized entities.

Integrity; guarantees that the information has not been subject to modifications, either since its creation or in the process of electronic transmission in any telecommunications network, it can only be modified by authorized entities and using authorized methods.

Availability; It consists of guaranteeing the permanent availability of the information, of course this implies that the information will be accessed only by authorized users, it is worth mentioning that its availability must contemplate disaster recovery, so that the information is always available.

Regarding the ISO/IEC 27000 standard, it is worth mentioning that it is made up of a whole family of norms and standards that ranges from 27000 to 27019 and from 27030 to 27044, and that it proposes the implementation of an Information Security Management System (ISMS).

When implementing an ISMS and in order to protect IT resources, such as information, technology and business processes, within the ISO/IEC 27001 section, controls are established to analyze the risks of the organization, policies and standards of security in the organization and legal, regulatory and contractual obligations, in this article we will mainly address the establishment of security policies and standards in the organization, without overlooking the fact that for this we need to internally analyze the risks and review the legal and contractual obligations of the organization.

Computer security arises in both internal and external environments, according to the Defense in Depth Principle, mentioned by Gómez (2011), the most external levels can be reinforced or implemented by firewalls, then going to the level of Network Segmentation using ACL's (Access Control List), VLAN's (Virtual Local Area Networks), then there will be the level of Robust Configuration of equipment, implementing patches and controlling ports, the next level corresponds to User Management and the deepest level corresponds to Data Encryption, as shown in Figure 1.

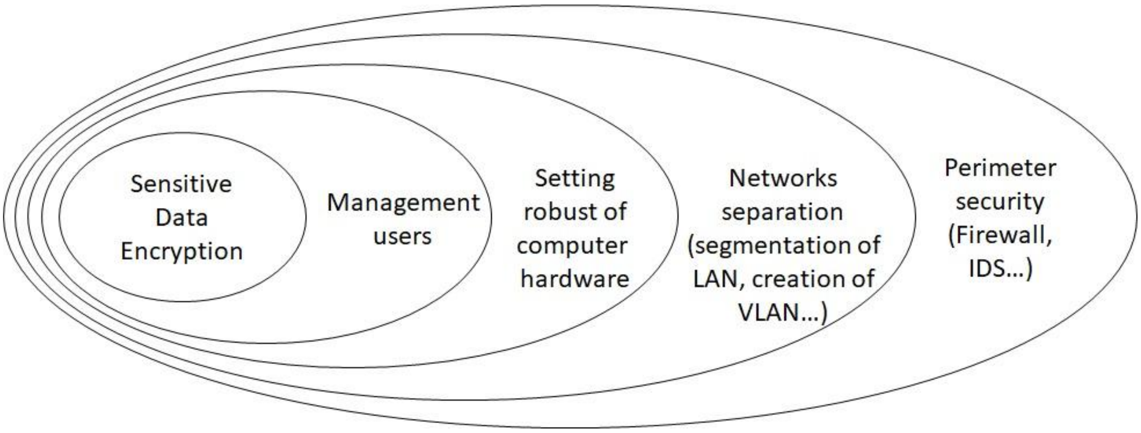
Sensitive Data Encryption
Management users
Setting robust of computer hardware
Networks separation (segmentation of LAN, creation of VLAN...)
Perimeter security (Firewall, IDS...)

Figure 1. Principle in Defense of Depth, Gomez (2011).

At all levels of defense, professionals in the IT area can implement technological tools designed to have defense mechanisms, ranging from firewall to establish access controls between the LAN (Local Area Network) and the WAN (Wide Area Network), Manageable Switches that allow us to separate networks, updated operating systems, drivers and secure applications, data encryption systems using algorithms such as RSA (Rivest, Shamir, Adleman), DSS (Digital Signature Standard), DES (Data Encryption Standard) and many other mechanisms and versions for hiding information; At the end, I mention User Management, which requires an analysis that involves those who use IT in the organization and where not only technology will provide defense mechanisms, but user participation becomes essential to achieve better results in computer security. .

The scope of this article focuses on actions that we can carry out to apply the recommendations and have practical examples of internal computer security policies, which will help us in the most sensitive part of security failures and that has to do with the User Management.

II. CONSIDERATIONS FOR IT SECURIRY POLICIES

Within the company it is necessary to locate each person in their specific role, each associate or employee is responsible for carrying out certain activities and in case of carrying out other activities there must be a specific authorization with time and access restrictions, these same policies must be applied in the case of computer security, assigning roles and access to systems, databases or equipment that each user requires to perform their task, Shimean & Spring (2014).

Of course, this implies not only unique passwords and preferably with two or three levels of verification, it also involves keeping access control systems up to date, for example Windows Active Directory, RADIUS servers, Wireless access, ERP ´s, and in general any access to software systems or databases, certainly this task can be tedious and exhausting, but it is a very important measure to guarantee user access to the appropriate sites.

In the creation of information security policies we can start with a plan as Firtman (2005) proposes, in said plan we must include the premises of: what is it that you want to protect? from whom do you have to protect yourself?, how can we protect ourselves?, What restrictions and procedures are we going to establish? and what will be the consequences if users do not comply with the policies and guidelines.

According to Cisco (2005), people from the company itself can cause most of the damage and unconsciously or consciously disable security schemes, sometimes being victims of social engineering, others out of resentment or simply carelessness.

Despite the experiences and the large number of testimonies due to failures in computer security, it is still a problem for IT experts to determine the budget allocated to computer security. Given this problem, I agree with Winkler (2008), when pointing out that a good determination of the security budget would have to do with determining the vulnerabilities and what their probable losses would be, then defining the countermeasures, their cost and, if possible, their return on investment, always with the clarity that the most valuable thing in organizations is the information above the computer systems, this is where the design of IT security policies can support us.

IT security policies require an inventory that contains not only the technical data of the equipment and software, but also the explicit names of the people to whom the IT resources are assigned, all of this reflected in a document that shows that the person will have the resources under their protection and that they will be responsible for their use and conservation, of course said document must have the electronic or autograph signature of both the user, the immediate boss, the person in charge of the IT area and without forgetting the resource staff or human capital.

Below are some examples of the content to generate a Basic IT Security Policies document. Clarifying firstly that: IT resources comprise any hardware and software component, including specialized printing, telecommunications, storage, processing, robotics and any other equipment that includes electronic features or components, after clarification, the policies are listed:

1. The user is responsible for the good use of the IT resources that have been assigned to them to carry out the tasks for which they have been hired by the company.
2. The user is responsible for the care, conservation, availability and integrity of the information contained in the IT resources, assigned to fulfill their tasks.
3. The user is not allowed to open, disassemble or tamper with the internal components of company-owned IT equipment.
4. The user is not allowed either by himself or by third parties to make repairs or modifications to the IT resources.
5. The user must immediately report to the IT department any failure or problem in the IT resources that have been assigned.
6. The user may not introduce IT resources that are not owned by the company to the company's facilities.
7. The user may not introduce any electronic storage device into the company's facilities, nor connect it to the company's IT equipment.
8. The user may not move, transport, connect, disconnect or exchange IT resources.
9. User may not install software to IT equipment.
10. The user may not transfer, lend or allow the use of IT resources by other users or personnel who do not belong to the company.
11. The user will be solely responsible for the use of their access credentials to IT resources.
12. The user must keep their access credentials to IT resources out of the reach and knowledge of other people.
13. The user will keep the assigned IT resources under their protection, until their superiors on behalf of the company release them from the corresponding protection.
14. The user will use external connection resources such as the Internet only through the company's telecommunications equipment, no other connectivity that does not belong to the company or that has not been assigned to the user will be allowed.
15. The user will use the email account provided by the company and it will be for the exclusive use of information management and communication related to their role in the company.
16. The user may not use personal email accounts in the company's IT resources.
17. All information generated or acquired by either the users or the company will be stored in the IT resources designated by the company.
18. The company undertakes to safeguard the personal information of users under the guidelines of the current Federal Law on Protection of Personal Data Held by Individuals.
19. In case of loss or damage to IT resources, the IT department will prepare an opinion determining the cost that the user must cover to the company.
20. The Human or Financial Resources Department will determine how to cover the costs determined by the IT Department, in relation to policy number 19.
21. The user will be responsible for making a complaint to the corresponding authorities in cases of theft or loss of the IT resources under their protection.
22. The user will not be able to use IT resources for games, music and consultation of sites that are not part of their assigned role in the company.
23. The cases not contemplated in this document will be reviewed and, where appropriate, sanctioned by the IT Department together with the General Management or with whomever it delegates.

The document presents some examples and is not intended to be implemented to the letter or limit the scope that the IT professionals of each company or organization determine, of course, the document must contain information on the person or user that makes it valid before administrative or legal, having to capture the autograph signature or, where appropriate, be endorsed with the electronic signature, specifying the date and place where it was accepted or signed by the user.

Depending on the company, its turn and magnitude, we must couple or generate the appropriate IT security policies, surely in the eyes of users, it is a restrictive document, but necessary to safeguard the confidentiality, integrity and availability of IT resources.

“Once a security policy has been created, the next step is to put the policy rules into practice. This step includes the training of employees and the addition of new pieces of hardware and software programs that are needed to enforce the rules”, IBM (2015). It will then be necessary to implement controls and rules, such as, and just to mention a few; how to form a secure password, from its content, length and encryption, implement tokens or identification devices, mechanisms such as ticket systems, to meet user requests and needs and other controls and rules, but above all generate training spaces and awareness so that users feel an important part in the care and management of IT and thus understand the importance of their role and interaction with IT resources for the productive processes of the organization.

III. CONCLUSION

BWe must implement computer security policies that are easy for the user to identify, the more specific and technical we are, the more confusion we could generate in the personnel regarding their compliance and we could fall into the paradigm that dictates that what is not prohibited is permitted, placing us in a defenseless position in cases not contemplated in our information security policy document.

Responsibility for security issues must always be shared by all the actors involved in the use of information technology, it would not be correct to delegate all responsibility to system administrators, since the interaction of users with the data is Being the most critical link in the security implementation, therefore it is important to know who will be able to access the network resources, to determine the limits and exclusion areas, Cisco (2005).

IT security policy documents must be subject to constant review, since if the organization undergoes changes, the policies must be adapted, modified, added or eliminated according to the needs of the company, we must not assume that our established policies will be functional forever.

The success or failure of any security policy will depend, in most cases, on the support and dissemination of the top management of the company, so it is our task to convince the management teams or owners of the company of the benefits or in your case, the situations that will be avoided thanks to the implementation and compliance with information security policies.

REFERENCES

[1]. Cisco, Academia de Networking de Cisco Systems (2005), Fundamentos de Seguridad en Redes, Especialista en Firewall Cisco, Editorial PEARSON EDUCACIÓN, Madrid, España.

[2]. Firtman Sebastián (2005), Seguridad Informática, Editorial MP Ediciones, Buenos Aires, Argentina.

[3]. Gómez Alvaro (2011), Enciclopedia de la Seguridad Informática, segunda edición, Alfaomega Grupo Editorial, México.

[4]. IBM (2015), Política y objetivos de seguridad, recuperado el 25 de enero de 2023 de: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

[5]. Kats Matías (2013), Redes y seguridad, Alfa Omega grupo Editor, Argentina.

[6]. ISO (2022), ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management systems – Requirements, disponible el 24 de enero de 2023 en: https://www.iso.org/standards.html

[7]. Shimeall Timothy, Spring Jonathan (2014), Introduction to Information Security a Strategic-based Approach, Elsevier Inc., Waltham, USA.

[8]. Winkler Ira (2008), El Zen y el Arte de la Seguridad de la Información. Grupo Editorial Patria, México.