Computer security, importance and scope in organizations

Lucio Garcia Choque[1] [0000-0002-6251-8169], Luis Jando Galindos Izaguirre[2] [0000-0003-1689-5438], Joel Arturo Flores Canterac[3] [0000-0002-5757-9610], José Antonio Ogosi Auqui[4] [0000-0002-4708-610X] and Jorge Cano Chuqui[5] [0000-0003-4809-6008]

[1] Universidad Privada San Juan Bautista, Lima, Perú, lucio.garcia@upsjb.edu.pe
[2] Universidad Privada San Juan Bautista, Chincha, Perú, luis.galindoz@upsjb.edu.pe
[3] Universidad Privada San Juan Bautista, Lima, Perú, joel.florez@upsjb.edu.pe
[4] Universidad Privada San Juan Bautista, Lima, Perú, jose.ogosi@upsjb.edu.pe
[5] Universidad Privada César Vallejo, Lima, Perú, ccanochu@ucvvirtual.edu.pe

Abstract. The globalization of the economy has required companies to implement technology platforms that support the new way of doing business. The use of the Internet for this purpose leads to the development of computer security projects that guarantee the integrity, availability, and accessibility of information. The creation of security policies is a fundamental task that involves the company's people, processes, and resources. Information security allows organizations to protect their financial resources, information systems, reputation, legal status, and other tangible and intangible assets. The main objective of this work is to develop a simulation model that allows evaluating the optimal level of security that society and organizations should have, considering aspects related to risk reduction and obtaining business benefits.

Keywords: Computer security, confidentiality, authentication, integrity, availability and audits.

1 Introduction

The issue of security and computer security is very important, currently there is a computer to carry out all kinds of procedures, because it serves us as a tool of daily life, the use of technology has spread and diversified to such degree that there are phones, tablets, laptops, etc., and it is at that moment where the dangers and risks appear. The age at which people choose to use technology is very early, currently from the age of 6 they already have control and management of information that is recorded on the internet and they do not take any care in its use, the most common activities They are access to emails, social networks, online shopping; thus generating password theft, which is one of the most common problems that can be found since not even the slightest care is taken, it is based on this that we continue to locate typi-cal pet names, surnames, first names, among others.

Nowadays, the use of computers and mobile devices with Internet access is in-creasing day by day to store information: documents, letters, spreadsheets, images, music, customer databases, payroll, orders, billing, bank accounts and else. Parallel to the growth in the use of information technology and communication networks, the number of security incidents has increased. The greater the volume of information processed and transferred electronically and telematically, the greater the risk derived from its loss, alteration or disclosure.

1.1 History of the problem

Currently, organizations do not have a strategy to identify vulnerabilities, risks that endanger information security, and there is no documentation that allows evidence of previous studies. It is of utmost importance to protect the system that is made up of Software, Hardware, the information that is handled and even the system operator itself, the principles of information security are to protect the Integrity, confidentiality and availability of information.

(Garcia, 2020) Information is a valuable asset for any organization, which serves as an input to achieve competitive levels, however, due to poor knowledge about how to safeguard, or due to the complexity in the implementation of security standards, many organizations, especially small and medium-sized companies jeopardize the continuity of their operations, since the difficulties in protecting their information, according to (Díaz-Batista and Blanco-Fernández, 2018) are due to insufficient fi-nancial resources, and the basic training of staff to perform complex functions.

Finally, it can be indicated that information security in any organization is constantly affected by security threats, cyber-attacks and computer fraud. In addition, they continually face sabotage or viruses with the consequent risk of deletion and loss of information.

The key is for the organization to invest resources in applying tools that improve security.

2 Theoretical framework

For the integration of an information security management system, we apply basic concepts that detail security and methodologies that provide ISMS security and pro-tection standards, such as ISO/IEC 27000 OSSTMM 3.0, of ethical hacking, which guarantees and certifies as a protected, safe and reliable system.

2.1 Access controls

These provide us with access information and can be implemented at the level of the Operating System, of information systems, in databases, in a specific security pack-age or in any other reference utility. These controls are an important help in protect-ing the network operating system, information systems and additional software; that they may be used or modified without authorization; also, to maintain the integrity of the information (restricting the number of users and processes with access authori-zation) and to protect confidential information from unauthorized access. The con-siderations related to the procedure that is carried out to determine if an access per-mission requested by a user corresponds.

2.2 Identification and Authentication

It is the first line of defense for most computerized systems, preventing the entry of unauthorized persons and is the basis for almost all access controls, as well as allowing monitoring of user activities.

ID. It is when the user makes himself known in the system.

Authentication. It is the verification carried out by the identification system.

Roles. The use of roles is a fairly effective way of implementing access control, as long as the role definition process is based on a thorough analysis of how the organization operates. It is important to clarify that the use of roles is not the same as account sharing.

Transactions. Another approach to implementing access controls in an organization is transactions.

Limitations on services. The Limitations to the Services are controls that refer to the restrictions that de-pend on parameters specific to the use of the application or that have been pre-established by the system administrator.

Access mode. When an access can be allowed, it must also be taken into account what type of access or mode of access will be allowed. The concept of access mode is fundamental for the respective control, the access modes that can be used are:

- Reading.
- Writing.
- Execution.
- Erased.

Creation. Search These criteria can be used in conjunction with others.

Location and hours. Access to certain system resources may be based on the physical or logical loca-tion of data or people.

Internal Access Control. Internal access controls determine what a user or group of users can or cannot do with system resources using internal access control:

- Username.
- Keywords.
- Encryption.

ID. It is when the user makes himself known in the system.

2.3 Security Definition

Information security is the set of standards, processes, procedures, strategies, com-puter resources, educational resources and integrated human resources to propose all due and required protection to the information and computer resources of a company, institution or government agency

2.4 Network Security Planning

The security objectives must be created in accordance with the strategies of the organization, additionally these must be communicated to the entire organization, along with their importance of keeping the system safe, promoting a culture of security, security planning must take into account, in addition to its objectives, the people and entities that access the system, it must also tend so that all the participants are focused on maintaining a secure system, then it is not enough to define the security policies if the people involved do not appropriate them in a way intrinsic.

2.5 Security Politics

Security policies must respond to the need to maintain a secure environment. The policies must be able to be put into practice through procedures described in the ad-ministration of the system, that is, they must be able to be put into practice and force compliance with the related actions through security tools. Likewise, they must clear-ly define the areas of responsibility of the users, administrators and the management itself, having a person in charge for every possible situation.

2.6 Fraud around crypto assets will continue to increase

In addition to the challenges linked to remote work, it is worth mentioning that new technologies, especially those that are more fashionable, will undoubtedly be targeted for trickery. Such is the case of NFTs, also known as non-fungible tokens, which are non-exchangeable data units that are stored in the blockchain and that allow digital items to become unique and unrepeatable, whose ownership can be proven, trans-forming them into elements of value that they can be traded. These NFT tokens are already used in the art world, in collectibles and even in video games. Soon we will be seeing more and more scams associated with the buying and selling of these assets, as well as malicious software that seeks to obtain these digital assets.

2.7 Technological challenges for companies

In 2020 there was a lot of talk about the technological infrastructure needed to work remotely and securely since it has been complex for many organizations and with the adoption of a hybrid model it is even more so.

As the infrastructure grows and encompasses not only proprietary equipment but also cloud services, VPN networks, and more and more applications to communicate and access information, the number of potential security breaches grows. During the pandemic, significant Zero Day vulnerabilities were discovered in VPN services, platforms like Zoom, and other software and as-a-service applications that could have allowed attackers to remotely take control of user devices.

The need for remote access boosted the use of web applications, which led to an increase in attacks on these platforms and, according to a Verizon report, 20% of information leaks were due to attacks on web applications. In addition, attacks on remote access protocols such as SMB and RDP grew; in fact, ESET reported a 768% increase in attacks targeting RDP in Q3 2020.

3 Method

In the study of art, there is a series of investigations related to information security and vulnerabilities, which are treated in order to understand their importance in the current environment of computer systems. The objective of this study is to identify and analyze common cybersecurity vulnerabilities. The results show that the security approaches mentioned so far only focus on security in general, and the solutions provided in these studies need further empirical validation and actual implementa-tion. Instead, his codification of what organizations need to consider when develop-ing PSI fell into three broad areas:

- Security Policy Drivers.
- Security Policy Guidance.
- Existing theories.

Security policy drivers refer to what puts pressure on organizations to design PSIs, and according to the authors, such pressure can come from both external and inter-nal sources. The security policy guidance refers to the use of information security standards, such as the ISO-27000 series, to support when designing ISPs. Finally, existing theories deal with the use of theories to understand the information security behavior of employees, arguing that these theories should have an impact on design work.

3.1 Secure networks

We must know that if we do not use any encryption protocol in our connection, anyone within the range of our network can connect and use a sniffer to see the traffic, in addition to using our connection for criminal purposes through the Internet.

There are a series of previous steps to know the type of encryption that we use in the wireless connection to which we connect. When we click on the icon to see the available networks, passing the mouse over any of them shows relevant information.

3.2 Biometric indicators

- For access control with biometric technology to be reliable, it must be created around human characteristics that have the following indicators:
- Universality. All individuals possess that characteristic.
- Uniqueness. The characteristic is different in each individual.
- Permanence. It does not change over time, neither in the short nor in the long term.
- Quantification. It can be measured with any system (numerical, physical, mathematical...).
- Characteristics required of a biometric system
- Effectiveness. Its use must be made comfortable and fast for users.
- Acceptability. It must not cause people to refuse to submit to the exami-nation, nor can it be dangerous to health or physical integrity.
- Reliability. It must be robust, in the sense that its results are as reliable as possible and that it cannot be tampered with or used fraudulently.

4 Results

The research was carried out to propose security measures for different types of organizations. In this proposal, two forms of information security protection have been integrated: logical (Software) and physical (Hardware).

Basic security measures must be studied in depth, such as identification, authentication, authorization, integrity, confidentiality and availability of information. Currently, there must be a specialized and direct look at social networks, because through them thousands of computer virus attacks are allowed, spies for copies of credentials, user passwords, different codes, which allows them to be sent to an external computer and, therefore, Thus, granting the Crackers to commit the crime.

It is noteworthy that, although it is something that has already been widely studied and disseminated in the literature, the constant research and study on the subject of information security helps prevention, thus reducing unnecessary economic investment expenses based on measures safety precautions, which are precautionary measures. from computer attacks, for example, on servers, it is advisable to install firewall, antimalware, antispyware and use cryptographic techniques, put a strong password, create backups or redundant backups.

We can understand through a survey that many organizations do not have their employees trained on what information security is, therefore, we can define that audit at the organizational level are necessary for different types of companies for the management and good use of confidentiality of information (see Fig. 1).

Are the employees of the organizations trained in computer security (prevention and protection of data and/or equipment)?

33.3 % of the total sample responded that employees are trained in computer security. This allows users to carry out best physical and logical security practices framed on it. Also, on topics related to crimes, legislation, threats, risk factors, incidents and security policies, among others. All the appropriation of knowledge that they may have and be applied, will allow obtaining a high level of computer security

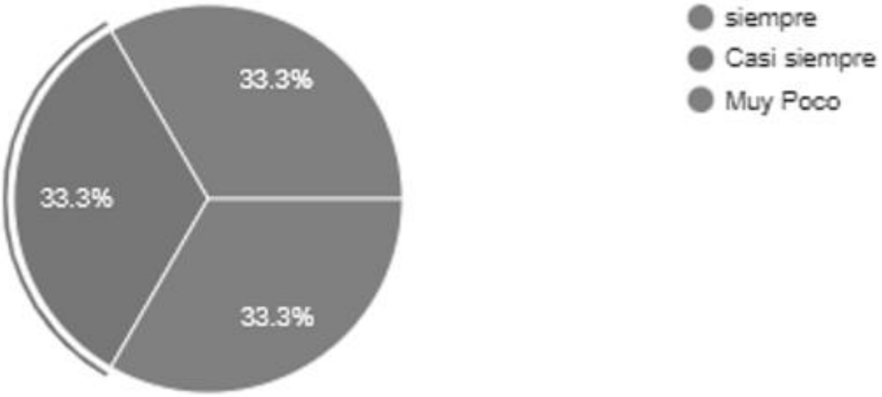

Fig. 1. A figure caption is always placed below the illustration. Short captions are centered, while long ones are justified. The macro button chooses the correct format automatically.

66.7% agree that there are policies and regulations that safeguard the security of their information, information systems (IS) and technological resources, benefiting from making better use of in-formation technologies (IT) based on the (SI) of the companys.

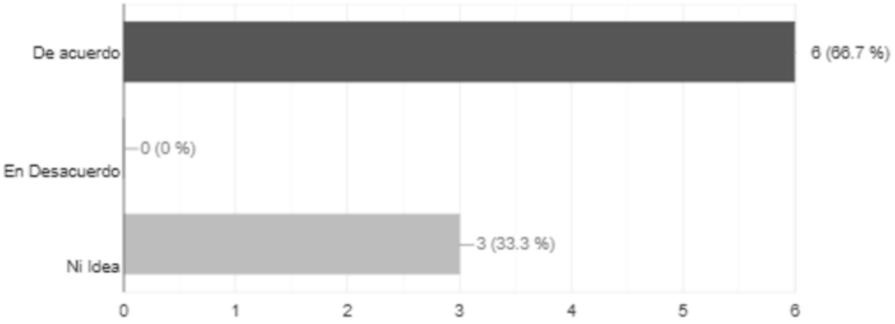

Fig. 2. Are there regulations (policies and standards) for the use of software or programs in organiza-tions?

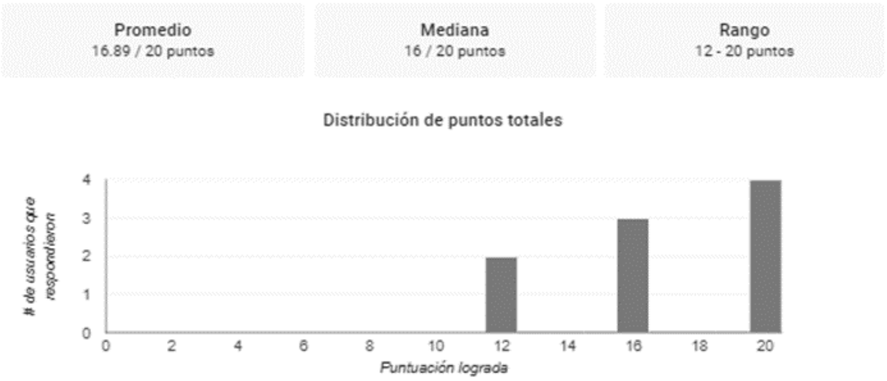

Fig. 3. Number of participants

References

1. Flores, J., Guarda, T., & Molina, L. (2019). Computer security in the use of new technological equipment. Iberian Journal of Information Systems and Technologies, (e 17), 32-38.
2. Peg, c. AD (2006). Computer security policies. Lattice, 2(1), 86-92.
3. VD Gil Vera and JC Gil Vera, "Organizational Information Security: A Simulation Model Based on System Dynamics", Sienta et technica, vol. 22, no. 2, p. 196, June 2017. Accessed June 6, 2022. [Online]. Available: https://doi.org/10.22517/23447214.11371
4. Rivers, no. RT, Álvarez Morales, e. L., & Sandoya, s. DC (2017). Computer security, a mechanism to safeguard company information. Publishing Magazine, 4(10 (2)), 462-473.
5. Vieites Gomez, Alvaro (2022). Computer security audit, chapter 3 (3.1), 41-44.
6. Maria Augustina Sisti (2019). Computer security: the protection of information In a wine company in Mendoza, chapter 2(2.1), 28-33.
7. Vanessa Michelle s (2020), computer security policies and vulnerabilities in the system to generate appointments and billing payments for the Ambacar dealership, chapter 1 (1-20).
8. MI Romero Castro et al., Introduction to computer security and vulnerability analysis. Editorial Científica 3Ciencias, 2018. Accessed June 6, 2022. [Online]. Available: https://doi.org/10.17993/ingytec.2018.46
9. Espinel, strategy to implement an information security management system based on the iso 27001 standard, 2017, p. 13.
10. Grenache, a. R. (2008). Personal data protection and information security. Legal Rev. Castilla & León, 16, 373.
11. Garcia, S. B. (2020). Factors that contribute to the loss of information in organizations. Cuban Journal of Computer Sciences, 10-12.
12. Diaz-batista, J. Y Blanco-Fernández, y., Adoption and use of information technologies in Cuban organizations. Industrial Engineering, 2018. Vol. 39, no. 2, p. 273-282.
13. Aguilera, purification. Computer security (2017), unit. 3, ch. 64.
14. Gomez, a. (2022). Computer security audit. Editions of the u.

15. JA Figueroa-Suárez, RF Rodríguez-Andrade, CC Bone-Obando and JA Saltos-Gómez, "Computer security and information security", Pole of Knowledge, vol. 2, no. 12, p. 145, March 2018. Accessed June 6, 2022. [Online]. Available: https://doi.org/10.23857/pc.v2i12.420Postigo Palacios, a. (2020). Computer security (2020 edition). Paraninfo editions, Sa.
16. Zambrano, S. MQ, & valence, d. GM (2017). Computer security: considerations. Mastery of the Sciences, 3(3), 676-688.
17. Zambrano, S. MQ, & valence, d. GM (2017). Computer security: considerations. Mastery of the Sciences, 3(3), 676-688.
18. MI Romero Castro et al., Introduction to computer security and vulnerability analysis. Editorial Científica 3Ciencias, 2018. Accessed June 6, 2022. [Online]. Available: https://doi.org/10.17993/ingytec.2018.46
19. Lopez, R. A. (2017). Computer security management systems.
20. Imbaquingo, d. E., herrera-granda, e. P., herrera-granda, i. D., Arciniega, s. R., Guamán, v. L., & Ortega-Bustamante, m. C. (2019). Evaluation of university computer security systems case study: teacher evaluation system. Iberian magazine of information systems and technologies, (e22), 349-362.
21. Giraldo , m. CB, arias, a. V., Giraldo, I. FG, & Arango, d. AG (2020). Main research trends in computer network security from the bibliometric study of the literature from 1973 to 2019. Evolution and research trends, 52.
22. Zuña Macancela, e. R., arce Ramírez, a. A., rosemary Berrones, w. J., & lonely baque, c. J. (2019). Analysis of information security in SMEs in the city of miracle. University and society magazine, 11(4), 487-492.
23. Álvarez, e., Carreño, s., Tirado, n., & Ramos, d. (2017). Computer security, a mechanism to safeguard company information. Publishing Magazine, 4(10), 2.
24. Briceño Huaygua Christian (2019). Application of the magerit methodology for the preparation of a plan to improve the security of information assets in the special development zone – zed paita chapter 4.3.2. (57-58)