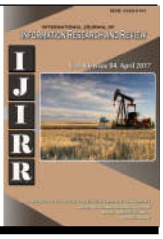


IJIRR

International Journal of Information Research and Review
Vol. 04, Issue, 04, pp.3981-3985, April, 2017

Research Article

INFORMATION SECURITY MODEL FOR HIGHER EDUCATION INSTITUTIONS IN ECUADOR

***[1]Navira Gissela Angulo Murillo, [2]Cevallos Gamboa Antonio and [3]Alex Alfonso Sánchez Arteaga**

[1]Magíster in Strategic Direction of the Technologies of the Information and Communication, National University of Piura, Peru, Systems Engineer, Universidad Laica Eloy Alfaro of Manabí, Ecuador
[2] Systems Engineer, Magíster in Systems of Managerial Information and Business administration, PhD candidate of the University Del Rosario in Bogota, Colombia. He is a dean of the Faculty of Engineering in Systems Telecommunications and Electronics (FISTE).Universidad Espíritu Santo, Guayaquil – Ecuador
[3]Lawyer of the Courts of the Ecuador, Universidad Laica Eloy Alfaro of Manabí, Ecuador

ARTICLE INFO

Article History:

Received 17th January, 2016
Received in revised form
25th Febuary, 2017
Accepted 29th March, 2017
Published online 30th April, 2017

Keywords:

Security, Information,
Deming, Magerit,
Higher Education Institutions.

ABSTRACT

This paper aims to present an evaluation of the most relevant processes in the analysis of risks and management of information systems, with the aim of proposing a model to reduce the probability of occurrence of hazards that affect higher education institutions. The proposal is based on the Deming and Magerit methodologies, which identify the threats, risks and vulnerabilities that the information faces. The results allowed to conclude that the presented proposal provides a guide that helps the universities to apply controls in order to generate important information to comply with each one of the indicators of the process of evaluation and accreditation of Ecuador.

INTRODUCTION

For Goñi (2008), this information is considered such as the most valuable assets today, since this resource allows organizations to raise their competitiveness levels, determine their economy, identify strengths and serve as support in making timely decisions in the organization. Also, emphasizes Pablos (2008) determined like the information generated through information systems is invaluable for companies, since it allows them to consolidate and have greater opportunities for development in the market. In this sense, it should be noted that an information system is a set of people, data, processes and information technology that interact to collect, store and provide the information necessary for the proper functioning of the organization (Fernández, 2006). For Goñi (2008), information is considered one of the most valuable assets today, since this resource allows organizations to raise their levels of competitiveness, determine their economy, identify strengths and serve as support in making timely decisions in the organization. Also, emphasizes Pablos (2008) that the information generated through information systems is invaluable for companies, since it allows them to consolidate and have greater opportunities for development in the market.

In this sense, it should be noted that an information system is a set of people, data, processes and information technology that interact to collect, store and provide information necessary for the proper functioning of the organization (Fernández, 2006). Aguilera (2011) stressed the importance of analyze the risks, vulnerabilities and threats presented by the information, since sometimes the loss or damages are usually presented in an unexpected or malicious that generates to the organization economic losses, delays and others. Chicano (2014) states that information must contain three properties: integrity, confidentiality and availability to meet the security appropriate standards. In support of this point, it is worth mentioning that one of the most frequently reported attacks is malicious codes or computer viruses that are "computer programs, (...) that carry out actions that are harmful to the computer system; (Mur, Nieto and Molina, 1990, Op. Cit. P.15) cited by Da Costa, 1992, p.127); many institutions have established control and monitoring to improve security incidents. Other

****Corresponding author: Navira Gissela Angulo Murillo,***
Magíster in Strategic Direction of the Technologies of the Information and Communication, National University of Piura, Peru, Systems Engineer, Universidad Laica Eloy Alfaro of Manabí, Ecuador.

organizations, Higher Education Institutions [IES] manage information at all levels, it's necessary to apply adequate techniques to infallibly protect this asset. This point support, Pires and Lemaitre (2008) concluded that the Latin America universities tendency is the development of institutional accreditation systems. Higher education institutions are generating, storing, sending and archiving information relevant to academic and administrative management, it is essential to apply techniques appropriate for the management analysis resources. Article purpose is to present a research perspective the information security subject in different Universities. To create a reference model that identifies and identifies the information assets, their risks and threats according to the current evaluating requirements in the agencies accreditation process, emphasizing the importance of applying the Magerit methodology to risks Carries the digital information by the use of Tic's.

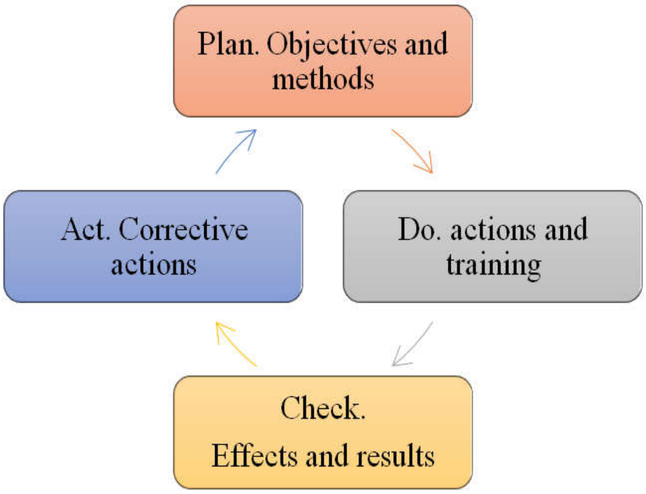
Importance of information security

Is common to speak about computer security in organizations, companies, public or private institutions, due to the amount of information that is generated in these entities; In this sense Diaz (2013) stressed that the information is the most important asset in organizations for the management that is given every time. Hence, Garcia, Hurtado, and Alegre (2011), indicate that the information in organizations can generate economic losses and time. On the other hand, López (2015) stressed that the information has become nomadic, since it is common for people to send files through the web, to support it in the cloud, to pass it to a storage device, to enter a program or any other form of mobility; making this resource increasingly vulnerable to different human or electronic threats. Aguilera (2011), information system is the main focus, although the field of information security has evolved constantly, however, the objective remains the same to protect the integrity, confidentiality and availability information, Prudente, Sánchez and Vásquez (2014), refer to the risks and threats that threaten the integrity of the information, which are only occurring in specific sectors such as: production, finance, administration; But also educational institutions are exposed to this type of logical or physical incidents. According to Symantec's (2015) annual report threats, computer education is one of the top 10 crime sectors (10%), 76 worldwide categories.

ISO 27000 safety regulations

ISO (International Organization Standardization) is an international standard-setting network in all industrial sectors. Its headquarters is located in Geneva and its offices are located in more than 160 countries. The ISO 2700 standards series is also called the Information Security Management System (ISMS), providing a standardization framework that manages information security regulations;

The most relevant in this family are: the ISO 27001 and ISO 27002 standards, the first contains the requirements that organizations must meet to comply with the code of good practices for information security management stipulated in the second rule. The ISO standard 27001 describe the requirements for the establishment and administration of an Information Security Management System ISMS in four cyclical stages, which contain a continuous evaluation of where we want to be? In front of where are we?, that is, what are the security requirements desired compared to existing ones (Giménez, 2014). The ISO 27001 standard specifies a set of requirements that allow: establishing, implementing, maintaining and improving an information security management system using the Deming or PDCA methodology, which consists with the author Cuatrecasas (2012), In a cycle that acts as a guide to good practices to achieve systematically the best continuity in the processes in the organization, consisting mainly of four basic activities: Plan, Do, Check and Act. Chicano (2014), ISO 27002 is a good practice guide, which includes 39 objectives and 133 controls to guard information in an optimal way. Figure 1 shows the Deming cycle processes to apply the analysis and management risk informations:



Information systems are exposed to threats such as: viruses, information theft, espionage, natural and / or technical accidents, malicious human damages, from which they take vulnerabilities advantage, which is why ISO 27001 describes a tools series to reduce the risk levels that affect information units. In order for this management to develop successfully, the so-called Information Security Management System (ISMS) has been established. "A management system generally encompasses a structure, resources, processes and procedures that tend to put into practice the objectives and organizations policies. The information management security requires technical, procedural, physical, logical, personnel and management security measures "(Areitio, 2008). Pablos, López, Romo, and Medina (2011), stressed the main security components: assets, threats, vulnerabilities, risks, impacts and safeguards. With regard to risk management, it is recommended to apply appropriate techniques to control these risks. Educational institutions, like other general purpose organizations, require in their academic management control to ensure information security, so that risk management is an essential part ISO 27001: 2007.

Risk Analysis and Management

Requirements standars established in the ISO 27001: 2005 the analysis and risk management, where it analyzes, classifies and evaluates the information that is stored in the organizations. Risk has been defined as "an event or set of events that may endanger an organization's project or that may prevent its success" (Chicano, 2014). In this sense, Pablos et al. (2008) points out that risk analysis and management determines the information systems weakness, identifies threats and evaluates the impact that the organization would have if they affected the information. Similarly, Gaspar (2004) adds that the purpose of risk analysis is prevent, reduce and control the risks investigated to recommend measures to know. To better understand the role played by components in the analysis and risk information systems management, the table shows the description and example of its components:

Figure 1. Risk analysis descriptions and management components

Elements	Description	Types
Actives	Resources necessary for the operation and organization continuity.	Information, computers, storage devices, applications, communications networks, facilities to manage information, human talent.
Menace	An event that has detrimental effects on information assets.	Menaces, electric failures, information theft, espionage, fraud, information disclosure, information modification, among others.
Vulnerabilities	Probability of the threat running on an asset.	Intrinsic (comes from asset and threat), effective (generated from existing safeguard), residual (safeguards application).
Risks	Risks Probability that the threat materializes. High, medium, low adapted from (Alexander, 2010)	High ,medium, down
Safeguards Defense	Mechanisms so that threats do not cause damage.	Active (eliminate risk); Passive (reduce impact); Physical (protect physical access to assets); (Protecting assets through computer tools). Source: Own elaboration,

Source: Own elaboration, adapted from (Alexander, 2010)

Magerit and its components

Is necessary to mention the differentiation made by Giménez (2014) about the two components of information security: risk analysis and management; The first is to analyze threats and risk management is the process that will help identify, control and eliminate uncertain events that affect information. In the web portal of ISO 27000 (2012), several methodologies for performing risk analysis are described, in this case the Magerit methodology is chosen, which is defined as "a systematic process to estimate the magnitude of the risks to which it is exposed An organization "(Giménez, 2014). This methodology details important processes that help the analysis and management of risks in information systems, their initial appearance was presented in 2005 and the last version was published in 2012. The main methodology objectives are analyze and minimize. The risks of assets and consists of two phases: risk analysis and risk management.

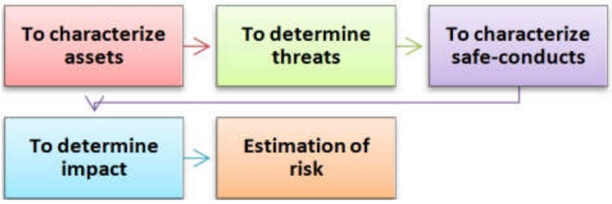


Figure 2. Processes for the analysis of risks as methodology Magerit

DISCUSSION

The model proposed is based with the continuous improvement stages cycle Deming and the Magerit methodology, to guarantee the academic information in higher education institutions security, the proposed strategy allows the protection and monitoring some flow channels and Sensitive information circulating between departments, it is important to identify what information is vital for the institution, before adequately protecting it. Also, important to be clear about the different states of information depending on their location. This model is based on a process approach that will help managers in Universities, make timely decisions regarding information quality and security, which involves the stages of the Deming cycle: planning, doing, verifying and acting, and phases Magerit methodology: including within it the security policy, assets, threats, vulnerabilities, risks, safeguards and impact identifications , whose purpose is to ensure that information systems in higher education institutions are available, up-to-date and reliable. The components of the model are detailed in figure 2.

Management Strategic

Are managers made up, committee chairs, among others.

Information

Corresponds to the data collection process carried out in the University Academy, these are: reports, Subjects, manuals, physical and digital documents, practices, follow up to graduates, projects, among others.

Responsible commissions

They are responsible for the information collection to evidence the full compliance of the indicators through reports or others.

External Evaluation

Conformed by the team of evaluators

Evidence

Information support that guarantees a process.

Deming Cycle

Systematic methodology for the continuous improvement cycle. It consists with four important processes: Planning, setting objectives, security policy, distributing activities, creating commissions and other work groups. Doing, in this process is where the proposed model is implemented, for this the Magerit methodology is applied in each one of the stages and it is continued until the fulfillment of each one of the carried out tasks is verified satisfactorily. In the Verification stage, the managers will carry out a periodic revision through the model to the processes, verifying the results obtained through the evidences;in the stage of acting it is verified if the results are satisfactory, in case they are not they will be implemented an improvement to try to obtain clear, truthful and organized results.

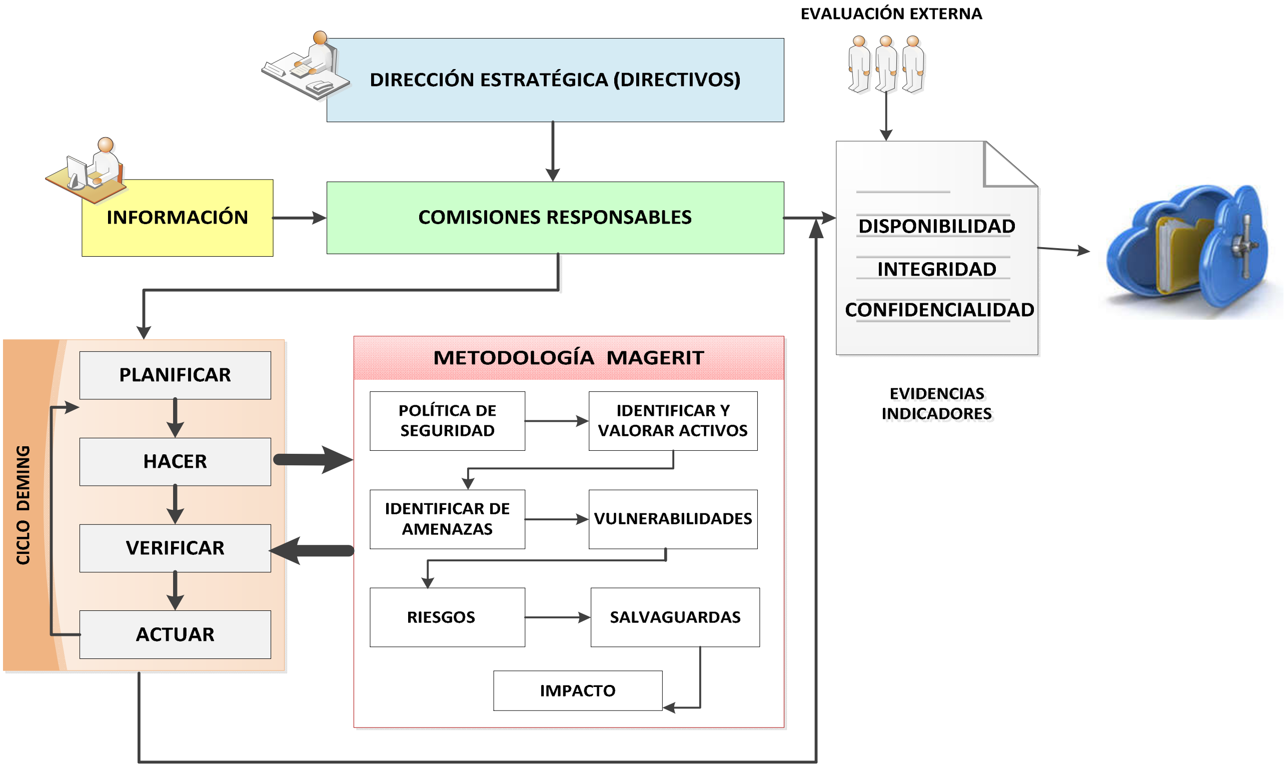


Figure 3. I shape safety information in universities

Magerit Methodology

The first phase consists identifying the existing assets in the Higher Educations Institution, such as: storage devices, computer equipment, communications networks, people, and applications. The assets are organized according to the order of dependence and valuation of the assets. Phase 2 involve identifying and analyzing threats; the degradation consists in characterizing the damage that can cause the threat in an asset. Phase 4 has to do with measuring the damage by the materialization of the threat. Phase 5 is measuringresponsible for the level risk for each asset, threat and size. Evidence and indicators: Wheneverinformation is generated correctly, the information assistant is stored in a physical, digital way.

Conclusion

Deming cycle and Magerit methodology are quality tools that merge appropriately to identify issues that break into information security and proposes activities that ensure that the assets of the organization are reliable, sound and available.

The information issue security is pertinent in any institution that manages assets, however, the emphasis of this theme is general and not particular; Therefore, the proposed model raises important activities that can be carried out in areas of the university where controls are required to protect the information that is frequently stored, migrated, shared, modified, eliminated with the full possible guarantee. It proposed as a model future work application in other institutions that handle sensitive information assets, in order to provide greater document management control in order to achieve confidentiality, integrity and availability of information.

REFERENCES

Aguilera, P. 2011. Introduction to computer security. Spain: Editex.

Alexander, A. 2010. Risk Analysis and Information Security Management System: The ISO 27001: 2005 approach. Managerial efficiency and productivity.

Areitio, J. 2008. Information security: networks, computers and information systems. Madrid - Spain: Paraninfo.

Arévalo, J., Bayona, R., Rico, D. 2015. Implementation of an information security management system under ISO 27001: information risk analysis. *Tecnura*, 19 (46), 4-10.

Chicano, E. 2014. Computer security management audit. IFCT0109.

Corletti, A. 2011. Security Levels. Madrid.

Cuatrecasas, L. 2012. Organization of the production and management of operations: Current systems of efficient and competitive management. Madrid: Díaz de Santos.

Da Costa, C. M. 1992. Fundamentals of Documentary Technology. Madrid: Cumplutense.

De Freitas, V. Abril de 2009. Analysis and evaluation of information risk: case study Universidad Simón Bolívar. Technology and Knowledge.(1), 43-55.

Díaz, D. 2013. Public libraries, new information technologies. Impact on library staff. Spain: Palibrio.

Díaz, G., Alzórriz, I., Sancristóbal, E., and Castro, M. 2014. Processes and tools for network security. Madrid: National University of Distance Education.

Fernández, V. 2006. Development of Information Systems: A Methodology based on modeling. Barcelona: UPC.

Funivcyl, 2012. University training module for the creation of technology-based companies. Spain: University Foundation Castilla y León (Funivcyl).

García, A., Hurtado, C., and Alegre, M. D. 2011. Informatic security. Spain: Paraninfo.

García-Cuevas, E. 2007. Basic Principles of Informatics. Madrid: Dykinson S.L.

Gaspar, J. 2004. Contingency plans. Business continuity in organizations. Barcelona: Díaz de Santos.

Giménez, J. F. 2014. Security in computer equipment (First ed.) Málaga - Spain: IC.

Giménez, V. July - December 2014. ISO criteria for the digital preservation of archival documents. CÓDICES, 10(2), 135-150.

González, L. 2005. The impact of the Evaluation and Accreditation process in Latin American universities. CINDA.

Goñi, J. J. 2008. Talent, Technology and Time. The pillars of conscious progress to choose a future. Spain: Díaz de Santos.

Guaglianone, A. 2013. Evaluation and accreditation policies in Argentine universities. Buenos Aires: Teseo.

Guerrero, M., and Gómez, L. October - December 2011. Review of relevant standards and literature on risk management and controls in information systems. Management Studies, 27(121), 195-215.

ISO 27000. 2012. Iso27000.es. Recovered el 21 de January de 2016, de http://www.iso27000.es/

Lackerbauer, I. 2000. All about internet. Barcelona: Marcombo.

López, J. August - September 2015. Protection of data in movement. Security. Prevention culture for ICT. 25).

Mur, A., Nieto, P., and Molina, J. 1990. Computer viruses. Madrid: Anaya Multimedia.

Pablos, C., López, J., Agius, H., Martín, S., Salgado, S., Montero, A., and Nájera, J. 2008. Management and management of information systems in the company. Second Edition. Madrid: ESIC.

Pablos, C., López, J., Romo, S., & Medina, S. 2011. Organization and transformation of information systems in the company. (First edition. Madrid: ESIC.

Pires, S., and Lemaitre, M. 2008. Accreditation and Evaluation Systems of Higher Education in Latin America and the Caribbean.Venezuela: UNESCO.

Prudente, L., Sánchez, G., and Vásquez, J. L. 2014. Information security management based on MAAGTICSI for academic programs in Higher Education Institutions. Security. Prevention culture for ICT (24), 4-9.

Sánchez, J., andMora, J. L. s.f.. Handling and interpreting the package SPPSS/PC+. México: UNAM.

Valdivia, C. 2014. Telematic networks. Spain: Paraninfo. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-ecurity-threat-report-volume-20-2015-social_v2.pdf

UNESCO. 2016. UNESCO IESALC. Retrieved on February 02, 2016, de http://www.iesalc.unesco.org.ve/index.php?option=com_fabrik&view=details&formid=1&rowid=19&lang=es

****