https://dx.doi.org/10.22161/ijaers.5.11.20 ISSN: 2349-6495(P) | 2456-1908(O)

The security of information and the risks associated with its use, a model for its implementation

Ricardo Ramírez Véliz[1], Marlon Altamirano Di Luca[2], Neilys González Benítez[3]

[1]Department of Computer Security, Guayaquil University, Guayaquil - Ecuador
Email: ricardo.ramirezv@ug.edu.ec
[2]Department of Computer Security, Santa Elena University, Santa Elena - Ecuador
Email: maltamirano@ncsa.ec
[3] Scientific group of the Meteorological Center of Pinar del Río, Pinard el Río Meteorological Center, Pinar del Río - Cuba
Email: neilysgonzalezbenitez@gmail.com

Abstract**—** *To assess whether the management of information security and the risks associated with its use, through computer networks, at the Peninsula State University of Santa Elena, is effective, it is proposed to implement a model that establishes the goals to achieve to advance through the different levels that make up the rating scale.*

To evaluate the management of information security and the risks associated with its use, it is necessary to have a maturity model that not only allows evaluating the processes involved in the management of information security, but also those associated with the management of the risks linked to the processing of information in all its phases, since an adequate information security plan depends on it.

Based on the aforementioned, the objective of this paper is to propose a model for the management of information security and the risks associated with its use, in computer networks.

Keywords**— Information security management, information processing, risks associated with the use of information, computer networks**

I. INTRODUCTION

The information systems that in educational institutions are manipulated, sometimes, are directed towards the mission of the organization which usually have a hostile environment, that is why the security of information is a discipline that integrates a set of policies, processes, procedures, organizational structures and software and hardware functions to help protect the confidentiality, integrity, availability and traceability of resources managed by IS in organizations (Achiary, 2005).

- Confidentiality: it is guaranteed that the information is accessible only by authorized persons.
- Integrity: safeguard the accuracy and completeness of the information and processing methods.
- Availability: it is guaranteed that authorized users have access to the information and resources related to it, whenever they require it.
- Traceability: make the IS auditable through a history that allows knowing the location and trajectory of a resource.

From these fundamental objectives of safety derive others such as:

- Authenticity: seeks to ensure the validity of information in time, form and distribution. Likewise, the origin of the information is guaranteed, validating the issuer to avoid identity theft.
- Non-repudiation: avoid that an entity that has sent or received information alleges to third parties that it did not do so.

In order to regulate aspects related to security in information systems (IS), standards have been developed that propose a set of policies and good practices, which help to strengthen the security of information. Computer security is commonly associated with a small group of technical measures such as antivirus and firewalls, the controls to be established are many and varied (Montesino, 2009).

Computer security as a concept has been evolving over time. Initially it was a discipline dominated by the elite of professionals specialized in the subject, but since the beginning of this century a more encompassing vision of information security has been proposed, which formally

https://dx.doi.org/10.22161/ijaers.5.11.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

links elements such as technology, the individual and the organization, emphasizing in the study of these and their relationships, to rethink computer security beyond the traditional technological experience (Cano, 2005).

According to Solms (2006), computer security has gone through history through four stages. The first stage was characterized by the technical aspect, the second was related to the management approach, where aspects such as policies and processes began to be considered. The third stage became standardized and documents of good practices and certifications began to appear.

Topics such as computer security culture, evaluation and monitoring began to be important. The fourth stage has been driven by regulations, where computer security has become a key aspect for the managers of the organizations and therefore is addressed from the first level of management.

The process of information security management is described in the ISO / IEC 27001 standard, which is an internationally certifiable standard. This standard offers a model for the establishment, implementation, operation, monitoring, review, maintenance and improvement of an information security management system (ISMS) (ISO / IEC, 2005).

The standard proposes a process approach where information security is not a state that is reached in a certain moment of time and remains unchanged, but is a continuous process that needs to be managed. Several actions are proposed that form a closed cycle for the continuous improvement of the system.

The ISM3 consortium, made up of several companies and organizations, has developed the Maturity Model of Information Security Management (ISM3). This model aims to extend the quality principles established in ISO 9001 to an ISMS. Instead of being oriented to controls, it focuses on computer security processes that may be common to all organizations (Aceituno, 2007).

Five basic configurations for an ISMS are described, equivalent to levels of maturity, which allows organizations to scale up levels depending on their needs. There are three categories of management: strategic, tactical and operational, for which 45 processes are defined that must be considered.

In ISM3 the processes related to computer security are described in detail, establishing objectives and metrics that allow establishing a quality system. The practical and measurement approach, as well as the orientation towards the business objectives of the organization, is what differentiates this model from the rest of the related standards.

II. MATERIALS AND METHODS

In this research, an integrative analysis is carried out, considering all computer security controls proposed by the main international guidelines and standards (ISO / IEC 27002 and NIST SP 800-53), implemented in the Peninsular State University of Santa Elena in Ecuador. For the management of information security and the risks associated with its use in computer networks, the model shown in Figure 1 is proposed.

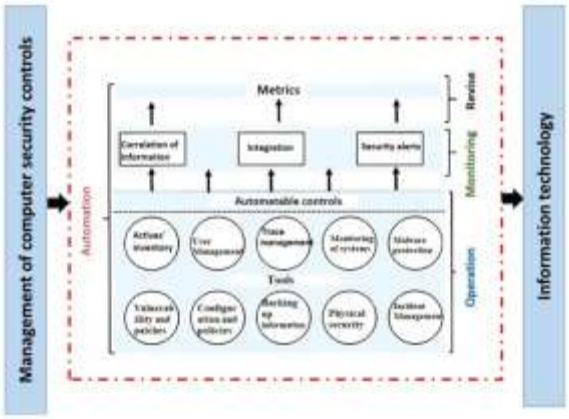

Fig. 1: Model for the management of information security and the risks associated with its use in computer networks. Source: self-made.

The model is based on the following principles:

1. Maximum automation: all automatable computer security controls must be considered.
2. Integration: the management of computer security controls must be done from a centralized system that allows the monitoring and review of them.
3. Synthesis: an adequate process of grouping and synthesis of the automatable controls must be carried out to manage a relatively small number of controls.
4. Objective measurement: the effectiveness of the controls must be evaluated and measured by means of objective indicators obtained automatically from the data provided by the different IT security tools.
5. Continuous improvement: the management of controls must be seen as a dynamic process consisting of several actions, which form a closed cycle for the continuous improvement of computer security controls.
6. Generality: the model must be applicable to a wide variety of organizations.

Based on the description of the principles of the model, which is proposed for the management of information security and the risks associated with its use in the computer networks of the Peninsula State University of Santa Elena, Ecuador, the automation for the automatable controls identified, defining the main computer security controls that must be automated for the protection of information security and the risks associated with their use through the computer networks of the Península de Santa Elena State University, Ecuador. Automated computer security controls represent a grouping and synthesis of the automatable controls identified in the ISO / IEC 27002 and NIST SP 800-53

https://dx.doi.org/10.22161/ijaers.5.11.20 ISSN: 2349-6495(P) | 2456-1908(O)

standards. Automation is applied to the actions of operation, monitoring and review of computer security automation controls for the protection of information security and the risks associated with their use through the computer networks of Santa Peninsula State University Elena, Ecuador.

The central component of the model allows the integration of different IT security tools, the correlation of information and the generation of security reports in an automated way. Computer security controls are implemented and operated by different tools, but their monitoring is done centrally in the central component of the model.

The central component of the model receives the information through the traces generated by the different systems, for which it is necessary to define connectors that allow interpreting the different formats of existing traces. The review of the controls is done through a group of computer security metrics, also defined as part of the model, which are calculated and reported in an automated way.

The model developed for the management of information security and the risks associated with its use in computer networks of the Peninsula de Santa Elena State University, offers a comprehensive vision of the automation of computer security controls, considering all the automatable controls and defining the actions to be carried out automatically in each of the cases. The model also proposes an automation of the actions of operation, monitoring and review of computer security automation controls for the protection of information security and the risks associated with its use through computer networks, which is intended for Trace management and security event detection. This presupposes that a deep process of personalization and adaptation of the operation, monitoring and revision actions must be carried out to apply the proposed model, through the definition of connectors, policies, correlation rules and computer security reports.

It is important to note that through the application of the model the operation, monitoring and review of a group of computer security controls is automated, which represents an important part of the process of managing computer security in its entirety. However, it should not be interpreted that the model solves all problems in an automated way. For an adequate management of information security, it is necessary to implement the rest of the controls proposed by the existing standards and regulations, which are not contemplated in this model. In addition, the model addresses the automation of the do and verify phases, so it is necessary to complete the management cycle even for automated controls. The automatically calculated indicators should be adequately reviewed by computer security specialists to take corrective actions on the security controls implemented.

III. RESULTS

Through a survey applied to managers and specialists of the Santa Elena Peninsula State University, which aimed to evaluate the factors that contribute to increase the effectiveness of the controls and to reduce the complexity of the computer security management, the positive effect of automation and integrated management of controls, while recognizing the importance of other factors that are also key in the management of information security in computer networks. With respect to the use of some system of indicators to evaluate the effectiveness of computer security controls, 75% of the respondents answered affirmatively their use.

It is also noted that the application of the model achieves maximum automation in the operation of the controls, and also automates the processes of monitoring and review thereof, which translates into greater effectiveness of computer security controls on the management of information security and the risks associated with its use in computer networks.

IV. CONCLUSION

After having assessed the controls proposed by the main international standards, it can be concluded that around 40% of computer security controls are automatable. For the automated and integrated management of computer security controls, we propose the model for the management of information security and the risks associated with its use in computer networks at the Peninsula de Santa Elena State University, a model that has the following general characteristics:

- Computer security controls are defined which represent a grouping and synthesis of the automatable controls identified.
- Automation is applied to the actions of operation, monitoring and review of controls.
- The correlation of information and the generation of security reports in an automated way is the central component of the model, allowing the integrated management of computer security controls.
- The controls are reviewed through a group of computer security metrics, also defined as part of the model, which are calculated and reported automatically.

The model developed offers a comprehensive vision of the automation of computer security controls, considering all the automatable controls and defining the actions to be carried out automatically in each case.

The implementation of the model is carried out through the installation, configuration and personalization of existing IT security applications, as well as the complementation of them through small developments

https://dx.doi.org/10.22161/ijaers.5.11.20 *ISSN: 2349-6495(P) | 2456-1908(O)*

that enable their adaptation to the proposed model.

REFERENCES

[1] Aceituno, V. (2007). ISM3: Information security management maturity model v2.0. ISM3 Consortium.

[2] Achiary, C. (2005). Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. E. Oficina Nacional de Tecnologías de Información (ONTI). SGP Nº 45/2005, pp: 7-16. Disponible en: http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pDF, [Consultado 15/05/2011]. 2005.

[3] Agoulmine, N. (2010). Autonomic network management principles: from concepts to applications. London: Academic, 2010.

[4] Alberts, C., Dorofee, A., Stevens, J. y Woody, C. (2003). Introduction to the OCTAVE® Approach. Carnegie Mellon University.

[5] BSI (2005). IT Baseline Protection Catalog. German Federal Office for Security in Information Technology (BSI).

[6] Cano, J. (2005). Un concepto extendido de la mente segura: pensamiento sistémico en seguridad informática, Criptored.

[7] Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. y Robinson, W. (2008). NIST SP 800-55: Performance measurement guide for information security." National Institute of Standards and Technology, 2008.

[8] DSD (2012). Australian Government Information Security Manual (ISM). Department of Defense. Australian Government, Sep-2012.

[9] Eloff, M. M. (2000). A Multi- Dimensional Model for Information Security Management, PhD Thesis.

[10] ISO/IEC (2008). ISO/IEC 27005: Information technology - Security techniques - Information security risk management. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

[11] ISO/IEC. (2005). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

[12] Martin, R. A. (2009). Making security measurable and manageable. In Military Communications Conference, 2008. MILCOM 2008. IEEE, 2009, pp. 1–9.

[13] Masera, M. y Fovino, I.N. (2010). Security metrics for cyber security assessment and testing. Joint Research Centre of the European Commission, Aug-2010.

[14] MINHAP (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, Gobierno de España, Oct-2012.

[15] Montesino, R. (2009). Gestión de la seguridad informática: de la teoría a la práctica. IX Seminario Iberoamericano de Seguridad en las Tecnologías de la Información, La Habana, Cuba.

[16] NIST (2012). NIST SP 800-30 rev1: Guide for Conducting Risk Assessments. National Institute of Standards and Technology, Sep-2012.

[17] Nof, S. Y. (2009). Springer Handbook of Automation. Springer

[18] OGC (2007). Information Technology Infrastructure Library (ITIL v3). Office of Government Commerce UK (OGC).

[19] Schmidt, D. (2010). Security automation: a new approach to managing and protecting critical information. IA newsletter, vol. 13, no. 1, 2010.

[20] Solms, von B. (2006). Information Security – The Fourth Wave," Computers & Security, vol. 25, no. 3, pp. 165-168, May. 2006.

[21] Tashi, I. y Ghernouti-Hélie, S. (2009). A Security Management Assurance Model to holistically assess the Information Security posture. Presented at the International Conference on Availability, Reliability and Security (ARES).