UNIVERSIDAD SIMÓN BOLÍVAR | INSTITUTO DE POSGRADOS

MODELO DE CIBERSEGURIDAD PARA LA UNIVERSIDAD DE CARTAGENA

JOSÉ DAVID PÉREZ GONZÁLEZ

Trabajo de Investigación o Tesis Doctoral como requisito para optar el título de Magister en Ingeniería de Sistemas y Computación

Tutores

PAUL SANMARTÍN MENDOZA PHD.

RESUMEN

El avance de las nuevas tecnologías ha traído consigo nuevos retos en materia de seguridad, es importante que se mantengan los principios de confidencialidad, integridad y disponibilidad para mantener los procesos en la organización, una cosa es clara y es que algunas características comunes, entre ellas el que no es necesario tener recursos para cometer ciertos delitos; la posibilidad de anonimato que ofrece internet y la dificultad técnica que requiere rastrear un ataque ha hecho que estas modalidades sean atractivas. Con la revisión de la literatura y desde la perspectiva de diferentes estudio se determinó que es fundamental mantener la confidencialidad, la integridad, la disponibilidad y la usabilidad autorizada de la información cobra especial relevancia y plantea la necesidad de disponer de profesionales idóneos y capaces de asegurar, gestionar y mantener la seguridad de los datos en sus sistemas ante amenazas presentes y futuras**.** De igual manera existen estándares que sirven como modelos referentes para hacer frente a las nuevas exigencias de las tecnologías en cuanto a seguridad, un modelo de seguridad sirve como apoyo para lograr mitigar las amenazas y vulnerabilidades. El objetivo de esta investigación radico en proponer un modelo de seguridad informática para mitigar posibles ataques cibernéticos en los sistemas de información de la Universidad de Cartagena UdeC. Se optó por hacer uso de la investigación en sitio. El modelo de investigación utilizado fue el sistémico estructural y a su vez un enfoque holístico en investigación que surge como respuesta a la necesidad integradora delos diversos enfoques, métodos y técnicas, inicialmente se acudió a las técnicas de observaciones (recolección de datos) que permitan formar una idea sólida del estudio de la investigación que se está planteando, de allí la necesidad de utilizar la técnica de clasificación que permitió agrupar las políticas que mejor se amolden a nuestros objetivos y por último la técnica de definiciones, ésta no proporcionara las estructuras finales de nuestro

objetivo principal. Con el diagnóstico realizado en la UdeC, se logra obtener una perspectiva o evaluación de cómo estaban funcionando los procesos relacionados con las tecnologías de la información y la seguridad de la información, permitiendo tomar decisiones para el desarrollo de la investigación, al comprender desde el reconocimiento, análisis y evaluación, las tendencias de uso de la red y de esa manera solucionar un problema o remediar una dificultad. De igual manera determinar cuáles son los puntos fuertes y los puntos débiles y comprender con que elementos se contaba y las posibles vulnerabilidades a las que se podría estar expuesto. Se definen teóricamente las categorías seleccionadas evidenciando la importancia que tienen los estándares escogidos, en ese sentido COBIT 5, NIST y la ISO 27002 en conjunto con los cuales se permiten mantener niveles óptimos de confidencialidad, integridad y disponibilidad de la información debido a su complementariedad. El modelo permite evidenciar que las categorías escogidas se complementan de tal manera que brindan las herramientas necesarias para mitigar y/o contrarrestar vulnerabilidades y amenazas, debido a que, con ellas, se encuentra un apoyo en el uso de las normativas al comprender que herramienta o estrategia usar para cada caso en específico, teniendo en cuenta cada fase presente dentro de una posible materialización de algún ataque.

Palabras clave: Ciberseguridad, vulnerabilidades, COBIT 5, NIST, ISO 27002, buenas prácticas

ABSTRACT

The advance of new technologies has brought with it new challenges in terms of security, it is important that the principles of confidentiality, integrity and availability are maintained in order to maintain the processes in the organization. One thing is clear and that is that some common characteristics, among them the fact that it is not necessary to have resources to commit certain crimes; the possibility of anonymity offered by the Internet and the technical difficulty required to track an attack has made these modalities attractive. With the review of the literature and from the perspective of different studies, it was determined that it is fundamental to maintain the confidentiality, integrity, availability and authorized usability of the information, which takes on special relevance and raises the need for suitable professionals capable of ensuring, managing and maintaining the security of the data in their systems in the face of present and future threats. Similarly, there are standards that serve as reference models to meet the new demands of technologies in terms of security, a security model serves as a support to mitigate threats and vulnerabilities. The objective of this research is to propose a model of computer security to mitigate possible cyber attacks on information systems at the University of Cartagena UdeC. It was decided to make use of on-site research. The research model used was the structural systemic one and at the same time a holistic approach in research that emerges as a response to the need to integrate the various approaches, methods and techniques. Initially, we resorted to observation techniques (data collection) that

allow us to form a solid idea of the study of the research that is being proposed, hence the need to use the classification technique that allowed us to group the policies that best fit our objectives and finally the technique of definitions, which will not provide the final structures of our main objective. With the diagnosis carried out at the UdeC, it is possible to obtain a perspective or evaluation of how the processes related to information technologies and information security were working, allowing decisions to be made for the development of the research, by understanding from the recognition, analysis and evaluation, the trends in the use of the network and thus solve a problem or remedy a difficulty. Likewise, determining the strengths and weaknesses and understanding what elements were available and the possible vulnerabilities to which one could be exposed.

The selected categories are theoretically defined, highlighting the importance of the standards chosen, such as COBIT 5, NIST and ISO 27002, which together allow optimal levels of confidentiality, integrity and availability of information due to their complementarity.

The model shows that the selected categories complement each other in such a way that they provide the necessary tools to mitigate and/or counteract vulnerabilities and threats, since they support the use of regulations by understanding which tool or strategy to use in each specific case, taking into account each phase of a possible attack.

KeyWords: Cybersecurity, vulnerabilities, COBIT 5, NIST, ISO 27002, good practices.

REFERENCIAS

Andrés, p. S. P. (2018). *"equipo de respuesta ante incidentes de seguridad informática para la universidad regional autónoma de los andes "uniandes"*. Universidad regional autónoma de los andes -uniandes-, ambato-ecuador. Retrieved from http://dspace.uniandes.edu.ec/bitstream/123456789/8158/1/piuasis011-2018.pdf

Diseñar los controles de acceso aplicables a la empresa Spytech S.A.S para su posterior implementación, de acuerdo con el dominio A9 de la norma ISO 27001:2013.

Agudelo, S. F. (1997). Violencia y salud en Colombia. *Pan American Journal of Public Health*, *1*, 93-103

Armendáriz, D. N. L. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica-ESPOL*, *30*(1).

Arquitectura TI Colombia. G.INF.06 Guía Técnica - Gobierno del dato, Versión 1.0, 30 de diciembre de 2014

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*: Editorial Paraninfo.

Betancourt, C. E. A. (22 de agosto de 2017). Ciberseguridad en los sistemas de información de las universidades. In (Vol. 3, pp. 200-217).

Betancourt, C. E. A. (2017). Ciberseguridad en los sistemas de información de las universidades. In (Vol. 3, pp. 200-217).

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *bie3: Boletín ieee* (2), 950-966.

Benavides Gaviria, D. F., & Flor García, G. A. (2019). *Pilares estratégicos en la transición de la banca tradicional a la banca digital en una filial del Banco de Occidente y una filial del Banco BBVA Colombia* (Master's thesis, Universidad EAFIT).

Center, P. M. (2017). Los mayores ciberataques de 2017 hasta la fecha. Retrieved from https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/

Chicharro Lázaro, A. (2009). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. *IDP. Revista de Internet, Derecho y Política* (9).

CONPES 3854, (2016).

de Barrera, J. H., & Morales, M. F. B. (2000). *Metodología de la investigación holística*: Instituto Universitario de Tecnología Caripito.

DigiNews's. ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital? Retrieved from http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

DigiNews's. (2018). ¿A qué amenazas cibernéticas se enfrentará el sector educativo con la transformación digital? Retrieved from http://www.digiware.net/?q=es/blog/a-que-amenazas-ciberneticas-se-enfrentara-el-sector-educativo-con-la-transformacion-digital

Díaz, F. J., Molinari, L. H., Venosa, P., Macia, N., Lanfranco, E. F., & Sabolansky, A. J. (2018). *Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización.* Paper presented at the XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste).

FBI. (2016, 2016/05/03 -). Delito cibernético - FBI. Retrieved from https://www.fbi.gov/investigate/cyber

Galán, C. M., & Cordero, C. G. La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad* (47), 293-306.

Galán, C. M., & Cordero, C. G. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho & Sociedad* (47), 293-306.

Gamon, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO: Revista Latinoamericana de Estudios de Seguridad* (20), 80-93.

GARCÍA, D. (2017). 7 herramientas para la evaluación de riesgos. Retrieved from https://www.ealde.es/herramientas-evaluacion-de-riesgos/

García, J. A. (2015). *Derecho penal y redes sociales*: Aranzadi-Thomson Reuters.

Gil, M. A. M. (2018). La amenaza de los Rootkits. Retrieved from http://www.bvs.hn/cu-2007/ponencias/SEG/seg021.pdf

Gómez Fernando, S. E. (2007). *Seguridad de la información.* Retrieved from http://cybertesis.uni.edu.pe/handle/uni/9764

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de ingeniería* (31), 109-118.

Institute, I. G. (2007). *COBIT Mapping: Mapping of TOGAF 8. 1 with COBIT 4. 0*: ISACA.

Sistema de Gestión de la Seguridad de la Información, (2013).

ItSMF, U. (2012). *ITIL foundation handbook*: The Stationery Office.

Isootols, (2019). *ISO 27002. La importancia de las buenas prácticas en los Sistemas de Seguridad de la Información*. https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

ITU. ICT FACTS AND FIGURES 2017. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

ITU. (2010). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación*. Paper presented at the Actas finales de la Conferencia de Plenipotenciarios, Guadalajara. http://handle.itu.int/11.1002/pub/80366152-en

ITU. (2017). ICT FACTS AND FIGURES 2017. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

kaspersky. (2013). ¿Qué es un botnet? Retrieved from https://www.kaspersky.es/blog/que-es-un-botnet/755/

KasperskyLab. (2018a). ¿Qué es la ciberseguridad en internet? Retrieved from https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KasperskyLab. (2018b). ¿Qué es el spam? Retrieved from https://encyclopedia.kaspersky.com/knowledge/what-is-spam/

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software*, *3*(4), 161-176.

Martínez, J. (2012). Seis pasos para el Gobierno de Datos ¿Qué es y cómo se implementa un programa de Gobierno de Datos? *IBM DeveloperWorks*, 1-5.

Morales, S. D. T. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. *Revista Icade. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales* (92), 13-47.

Mosso, J. M. R. (2015). Ciberseguridad Inteligente. *arXiv preprint arXiv:1506.03830*.

Orr, A. T., & Britain, G. (2011). *Introduction to the ITIL service lifecycle*: The Stationery Office.

pandasecurity. (2007). ¿Qué es IP Spoofing? Retrieved from https://encyclopedia.kaspersky.com/glossary/spoofing/

Recio, j. (2012). de la seguridad informática a la seguridad de la información. *asociación española para la calidad*, 14-19.

Rodríguez, C. H., Flores, M. C., López, &, T. G. la universidad y su relación con la ciberseguridad. *Memorias del Coloquio: "Ciberseguridad desde el ámbito legal, empresarial y tecnológico"*, 94.

Schjølberg, C. J. S. (2008). ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG). *Report of the Chairman of HLEG. Genf: ITU. Online verfügbar unter https://www. itu. int/en/action/cybersecurity/Documents/gca-chairman-report. pdf, zuletzt geprüft am*, *1*, 2016.

Subijana Zunzunegui, I. J. (2008). El ciberterrorismo: Una perspectiva legal y judicial.

Symantec. (2018). ¿Qué es un troyano? Retrieved from https://co.norton.com/internetsecurity-malware-what-is-a-trojan.html

Urueña Centeno, F. J. (2015). Ciberataques, la mayor amenaza actual. *Documento de Opinión*, *9*(2015), 16.

Van Dalen, D. B., & Meyer, W. J. (2006). Síntesis de" Estrategia de la investigación descriptiva. *Manual de técnica de la investigación educacional*.

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems, 66*, 1-12. doi:https://doi.org/10.1016/j.knosys.2014.02.018

Villanueva Méndez, J. C. (2015). *La ciberdefensa en Colombia.* Universidad Piloto de Colombia. Retrieved from f?sequence=1

Organization for Economic Co-operation and Development (OECD). Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy (2012).http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Informe Estado de la Unión 2017. Cybersecurity. Resilience, Deterrence and Defence. Building strong cybersecurity in Europe. http://europa.eu/rapid/attachment/IP-17-3193/en/Cybersecurity.

en.pdf (consultado en agosto de 2018). [En línea] [Citadoel: 25 de agosto de 2018.] http://europa.eu/rapid/attachment/ P-17-3193/en/Cybersecurity.en.pdf.

Reyna, D., & Olivera, D. (2016). Las Amenazas Cibernéticas. Revista electrónica de investigación de la universidad de Xalapa. Ciberseguridad. Desde el ámbito legal, empresarial y tecnológico. 35 - 55.

Raudales, C. (2017). La brecha existente en la ciberseguridad en honduras. Innovare Ciencia y Tecnología, 58 - 73.

REPUBLICA DE COLOMBIA, departamento Nacional de planeación, consejo nacional de política económica y social-COMPES 3701, Bogotá 14 de Julio del 2011.