**COMUNICACIÓN CORTA**

Altamirano, M.
Vol.21 No. 2, abril-junio, 2019 p. 248-263.
ISSN 1562-3297

Avances@ciget.vega.inf.cu

Avances

Centro de Información y Gestión Tecnológica

# Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso

## *Model for the management of information security and the risks associated with its use*

**Marlon Altamirano Di Luca**

Magister in Computer Security, Auditor Interno. Universidad Península de Santa Elena, Santa Elena, Ecuador, maltamirano@ncsa.ec ; ORCID: http://0000-0002-2456-3372

**Para citar este artículo / to reference this article / para citar este artigo**

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*, 21(2), 248-263. Recuperado de http:// www.ciget.pinar.cu/ojs/index.php/publicaciones/article/view/440/1426

Recibido: diciembre 2018
Aceptado: marzo 2019

**RESUMEN**

Para evaluar la efectividad de la gestión de la seguridad de la información y los riesgos asociados a su uso, en redes de computadoras, en la Universidad Estatal Península de Santa Elena, se propuso la implementación de un modelo que establece las metas a lograr para avanzar a través de los diferentes niveles que conforman la escala de valoración. El modelo se encuentra formalizado con los principales

estándares, recomendaciones y regulaciones existentes, tanto a nivel internacional como nacional, sobre gestión de la seguridad de la información y ofrece una visión integral de controles de seguridad de la información, considerando todos los controles automatizables y no automatizables y define las acciones a realizar en cada uno de los casos. El modelo no constituye una nueva propuesta de controles y procesos de gestión, sino que brinda un enfoque de automatización, integración y síntesis a las propuestas existentes, para disminuir la complejidad de la gestión y aumentar la efectividad de los controles de seguridad de la información en redes de computación.

**Palabras Clave:** Gestión de seguridad de la información, tratamiento de la información, riesgos asociados al uso de la información, redes de computadoras.

**ABSTRACT**

In order to evaluate the effectiveness of information security management and the risks associated with its use, in computer networks, at the Santa Elena Peninsula State University, the implementation of a model that establishes the goals to be achieved to advance was proposed, through the different levels that make up the rating scale. The model is formalized with the main standards, recommendations and existing regulations, both at an international and national level, on information security management and offers a comprehensive vision of information security controls, considering all the automated controls and not automatable and defines the actions to be carried out in each of the cases. The model does not constitute a new proposal of controls and management processes, but rather provides an automation, integration and synthesis approach to existing proposals, to reduce the complexity of management and increase the effectiveness of information security controls in computer networks.

**Keywords**: Information security management, treatment of information, risks associated with the use of information, computer networks.

## INTRODUCCIÓN

La seguridad de la información aprueba asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización. Es un concepto amplio que no se centra en la protección de las Tecnologías de la Información y las Comunicaciones (TIC) sino en todos los activos de información que son de un alto valor para la institución.

Por tal motivo, se entiende la seguridad de la información como un proceso integrado con un conjunto de estrategias, medidas preventivas y medidas reactivas que se ponen en práctica en las instituciones para proteger la información y mantener su confidencialidad, disponibilidad e integridad de la misma.

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) ha traído el surgimiento de los sistemas de información digital, unido a un exceso de información que conlleva a la necesidad de identificar los flujos de información útiles que favorezcan la toma de decisiones y aún más, eliminen las duplicidades innecesarias (Franganillo, 2009; Castillo, 2017).

"Una de las principales funciones que debe realizar el sistema de información de una organización es proporcionar la información necesaria a la alta dirección para la adecuada toma de decisiones". (Solana-Álvarez, 2014:473).

En el mundo académico existen publicaciones que plantean modelos relacionados con la seguridad informática (Eloff, 2000; Tashi and Ghernouti-Hélie, 2009), pero en la práctica no son muy utilizados.

Los estándares sobre gestión de la seguridad de la información son complementados con otros que tratan el tema de la gestión de riesgos. Entre los más conocidos están OCTAVE (Alberts, Dorofee, Stevens y Woody, 2003), MAGERIT (Minhap, 2012), ISO/IEC 27005 (ISO/IEC, 2008) y NIST SP 800-30 (NIST, 2012).

El cambio social producido por Internet y la rapidez en el intercambio de información, ha ocasionado que las empresas y organizaciones empiecen a tomar conciencia del valor que tiene la información y se preocupen por proteger sus datos. Con la creciente dependencia que la sociedad de la información tiene de las TIC, la necesidad de proteger la información está creciendo enormemente (Sanchez & Piattini, 2015).

Hoy en día, las amenazas en las TIC son globales y están repartidas en

distintos niveles de criticidad según sea la orientación y el ámbito de su utilización, múltiples los riesgos asociados a que los equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Preocupante es para las organizaciones a todos los niveles y tamaños el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información.

Cada día, se desarrollan nuevos métodos que afectan a la seguridad de la información de las organizaciones, es por ello la necesidad de trazar estrategias confiables de seguridad, de manera de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de los usuarios, clientes y socios de negocios (Burgos & Campos, 2013).

Con el fin de conducir a las organizaciones actuales a una adecuada gestión de la misma, se propone adoptar el modelo de gestión propuesto en las normas de la serie ISO 9000, que permitirá identificar los principales procesos que realiza la organización y orientarla hacia ellos, de este modo se conseguirá un funcionamiento adaptado de ella y sus sistemas informáticos (Solana-Álvarez, 2014).

La seguridad Informática se ocupa de la salvaguarda de la tecnología y de la información contenida en ella, mientras que la seguridad de la información se ocupa de los riesgos, beneficios y procesos involucrados en la manipulación de la información dentro de la organización, independientemente de cómo sea creada, manejada, transportada, o almacenada (Espinoza, 2013). Además, se encarga de minimizar los riesgos asociados con el acceso y utilización de los sistemas de forma malintencionada, esto implica, que se debe tener una visión general de los bienes a los cuales se necesita proteger, los cuales deben ser analizados para poder reducir al mínimo los riegos, con esto se logra tener un control en la utilización de medidas preventivas y correctivas en la seguridad (Balarezo & Poveda, 2015).

Un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados. Evidentemente, el nivel de seguridad establecido tendrá que ser consecuente con un análisis previo de

los riesgos, considerando el impacto de dicho acceso no deseado contra las posibilidades de que este se produzca (Ferrer & Fernández, 2012).

Los sistemas de información (SI) que en las instituciones educacionales se manipulan, en ocasiones están encaminados hacia la misión de la organización, las que por lo general poseen un entorno hostil, es por esto que la seguridad de la información es una disciplina que integra un conjunto de políticas, procesos, procedimientos, estructuras organizacionales y funciones para ayudar a proteger la confidencialidad, integridad, disponibilidad de los recursos gestionados por los SI independientemente del formato que tengan sean electrónicos o papel. (Achiary, 2005).

El consorcio ISM3, compuesto por varias empresas y organizaciones, ha desarrollado el Modelo de Madurez de Gestión de la Seguridad de la Información (ISM3 por sus siglas en inglés). Este modelo pretende extender los principios de calidad establecidos en ISO 9001 a un Sistema de Gestión de Seguridad de la Información (SGSI). En lugar de estar orientado a controles, se enfoca en los procesos de seguridad de la información que pueden ser comunes a todas las organizaciones (Aceituno, 2007).

Se describen cinco configuraciones básicas para un SGSI, equivalentes a niveles de madurez, lo cual permite a las organizaciones ir escalando los niveles en dependencia de sus necesidades. Se plantean tres categorías de gestión: estratégica, táctica y operacional, para las cuales se definen 45 procesos que deben ser tenidos en cuenta.

En ISM3 los procesos relacionados con la seguridad de la información son descritos detalladamente, estableciendo objetivos y métricas que permitan establecer un sistema de calidad. El enfoque práctico y de medición, así como la orientación hacia los objetivos de negocio de la organización, es lo que diferencia este modelo del resto de los estándares relacionados con la seguridad de la información.

A pesar de que ISM3 plantea un enfoque novedoso, su publicación es relativamente reciente y tiene competidores muy fuertes como ISO/IEC, COBIT e ITIL, por lo que en general todavía no posee un amplio reconocimiento a nivel internacional. Existen un grupo de recomendaciones y mejores prácticas sobre gestión de las Tecnologías de la Información (TI),

que abordan de alguna manera la temática de la seguridad de la información como parte del proceso, por lo que constituyen también un referente en este sentido.

Por otra parte, la Biblioteca de Infraestructura de Tecnologías de Información (ITIL por sus siglas en inglés) es un conjunto de buenas prácticas para la gestión de servicios de TI, desarrollado por el gobierno británico. ITIL ofrece descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI, contribuyendo de esta manera a una mayor efectividad del negocio (OGC, 2007).

ITIL, en su tercera versión, consta de cinco libros basados en el ciclo de vida del servicio. Se plantean las fases de estrategia, diseño, transición, operación y mejora continua del servicio; especificando 86 tópicos fundamentales a tener en cuenta en la gestión de TI. Esta guía de buenas prácticas también es muy utilizada a nivel internacional.

Existen también otras guías y regulaciones que tienen un carácter regional. En general la mayoría de los países poseen regulaciones relacionadas con la seguridad de la información. Algunas recomendaciones son conocidas fuera de sus fronteras porque constituyen guías de buenas prácticas aplicables a diferentes organizaciones. Cabe mencionar aquí al IT Baseline Protection Catalog (IT-Grundschutz) de Alemania (BSI, 2005) y el Manual de Seguridad de la Información (ISM) de Australia (DSD, 2012).

Gestionar la seguridad de la información es un proceso que las organizaciones deben llevar con respecto a las amenazas que puedan existir contra sus activos de información y que se puedan materializar como riesgos de consideración.

La única manera de manejar un porcentaje mayor de las medidas de seguridad será establecer los procesos de seguridad y determinar las responsabilidades, esto sería un enfoque basado en procesos dentro de los estándares de gestión descrito en el estándar ISO/IEC 27001. Esta norma ofrece un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI) (ISO/IEC, 2016). Esta norma ayuda a fortalecer la seguridad de la información, introduce buenas prácticas acoplables a cualquier tipo de organización, para

gestionar la seguridad de la información y medir la eficacia del sistema. (Montesino, 2009).

Se debe tener en cuenta que los controles de seguridad de la información no son sólo técnicas implementadas, son controles que deben estar relacionados con la tecnología de la información. Se pueden tener diferentes tipos de controles, por ejemplo la documentación de un procedimiento es un control de la organización y la implantación de una herramienta de software será un control de tecnología de la información.

El SGSI es un conjunto de procesos relacionados entre sí basado en un enfoque hacia los riesgos de una organización, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información (ISO/IEC, 2016)

La identificación de amenazas y vulnerabilidades hacia los activos más críticos de una entidad (tangibles o intangibles, conformados por los datos, software, hatware, imagen de la organización, etc.), a través de la implementación de la norma ISO 27001:2016 permite la recomendación de controles adecuados, de tal manera, que la organización pueda minimizar los riesgos de los activos de información, una vez identificados y tratados. Para los usuarios y clientes esto constituye una garantía de calidad y confidencialidad y para la propia organización la posibilidad de certificar el sistema ofrece una imagen favorable tanto nacional e internacional, al implementar en sus procesos las normas de buenas prácticas reconocidas internacionalmente.

Las universidades en sentido general demandan muchos productos, sistemas y servicios para gestionar y mantener la información, y no es suficiente con realizar unos controles de seguridad superficiales. Además, es necesario aplicar un enfoque riguroso para evaluar y mejorar la seguridad de los productos y también de los procesos que se llevan a cabo en el contexto de las Tecnologías de la Información y las Comunicaciones (Sanchez & Piattini, 2015).

Actualmente en las universidades ecuatorianas los SI aún presentan insuficiencias en su desempeño integral para contribuir a un Control de Gestión para la toma de decisiones, que responda a las Normas Técnicas Ecuatorianas (NTE) vigentes en el país.

La Secretaría Nacional de la Administración Pública de Ecuador

(2016) establece el Esquema Gubernamental de Seguridad de la Información (EGSI) y exige a través de sus acuerdos el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información para las entidades de la Administración Pública Central e Institucional.

En apoyo a lo anterior, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (2016) establece la política de seguridad de la información de obligatorio cumplimiento con la creación de un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI y cuya designación deberá ser comunicada a la Secretaría Nacional de la Administración Pública.

Por todo lo hasta aquí expresado, se define como objetivo diseñar un modelo para la gestión de la seguridad de la información y los riesgos asociados en la Universidad Península de Santa Elena para favorecer las decisiones que responda a las NTE.

## MATERIALES Y METODOS

En la investigación se emplearon tanto métodos empíricos como teóricos, entre ellos: Histórico-lógico que posibilitó analizar diferentes criterios y profundizar en la evolución, tendencias y generalizaciones del desarrollo de los sistemas de gestión de seguridad de la información.

Método sociológico o empírico a través de la observación, la revisión de documentos, encaminados a encontrar la mejor opción para el diseño del modelo previsto. La observación participante, entrevistas semi-estructuradas, estos, con el objetivo de entrar en mayor profundidad en las potencialidades y debilidades que subyacen en el objeto de estudio y las encuestas, las cuales permitieron identificar los controles puestos en práctica por la universidad anteriormente, así como recolectar y analizar los activos de información en el desarrollo del proceso de gestión de la seguridad de la información en dicha entidad de estudio.

El análisis documental se utilizó para obtener información acerca de cómo se comporta el proceso de la gestión de la seguridad de la información dentro del sistema de información, en la universidad y cómo se planificaron y organizaron acciones para el mejoramiento del mismo. Se consultaron los documentos que rigen la política de información y las normas vigentes.

De manera general se utilizó la técnica de modelación para diseñar la

propuesta de sistema de gestión de seguridad de la información teniendo en cuenta las exigencias actuales de Ecuador para el sistema de información de entidades de la Administración Pública Central e Institucional.

El procesamiento de la encuesta se realizó a través del software informático estadístico SPSS.

## RESULTADOS Y DISCUSIÓN

A través de una encuesta aplicada a directivos y especialistas de la Universidad Estatal Península de Santa Elena, la cual tuvo como objetivo evaluar los factores que contribuyen a aumentar la efectividad de la gestión de la seguridad de la información y a disminuir la complejidad de la gestión de la seguridad informática se constató el efecto positivo que tiene la automatización y la gestión integrada de los controles, a la vez que se reconoce la importancia de medir la eficacia del sistema, de manera que se pueda corregir a tiempo y disminuir los riesgos de la información. Con respecto al empleo de algún sistema de indicadores para evaluar la efectividad de los controles de seguridad informática, el 75 % de los encuestados respondió afirmativamente su uso.

Se constata, además que con la aplicación del modelo (*figura 1*) se alcanza la máxima automatización en la operación de los controles, y además se automatizan los procesos de monitorización y revisión de los mismos, lo cual se traduce en una mayor efectividad de los controles de seguridad informática dentro de la gestión de la seguridad de la información y los riesgos asociados a su uso de la información en redes de computadoras.

En la presente investigación se realiza un análisis integrador, donde se tienen en cuenta todos los controles de seguridad de la información propuestos por las principales guías y estándares internacionales (ISO/IEC 27001:2016 y NIST SP 800-53), puestos en práctica en la Universidad Estatal península de Santa Elena en el Ecuador.

Para la gestión de la seguridad de la información y los riesgos asociados a su uso en las redes de computadoras, se propone el modelo que se muestra en la *figura 1.*

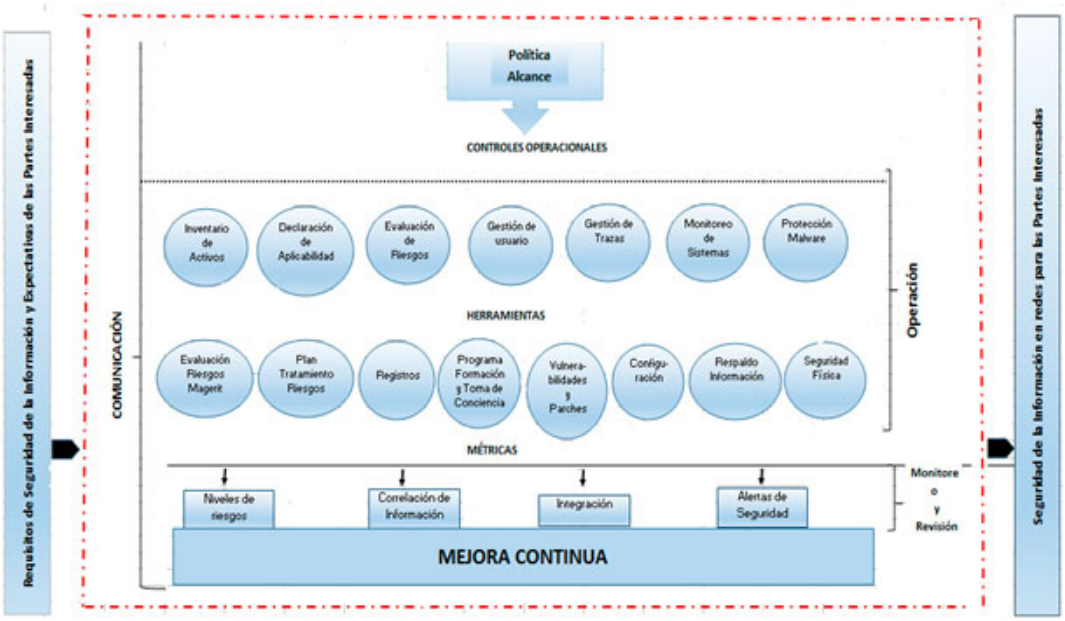


**Figura**. Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso en redes de computadoras. **Fuente**: Elaboración propia.

A nivel metodológico el modelo cuenta con varias guías anexas que ayudaran a la entidad seguir detalladamente las fases del modelo, y poder comprender a su vez los resultados obtenidos por cada etapa desarrollada.

- Guía 1- Política del SGSI
- Guía 2- Procedimientos y registros de Seguridad de la Información
- Guía 3- Roles y responsabilidades
- Guía 4- Gestión y clasificación de activos (Identificar Activos de información, amenazas, vulnerabilidades)
- Guía 5- Metodología para evaluar los riesgos del sistema (análisis y evaluación de riesgos)
- Guía 6- Indicadores de gestión (Objetivos y control y controles para el tratamiento, aprobación de riesgos residuales)
- Guía 7- Declaración de aplicabilidad
- Guía 8- Plan de tratamiento a los riesgos
- Guía 9- Plan de comunicación, sensibilización, capacitación

- Guía 10- Auditoría interna (Seguimiento y revisión)
- Guía 11- Evaluación de Desempeño
- Guía 12- Mantenimiento y mejora continua

El modelo se apoya en los siguientes principios:

1. Automatización: se deben tener en cuenta todos los controles de seguridad de la información automatizables.
2. Integración: la gestión de los controles de seguridad de la información debe realizarse desde un sistema centralizado que permita la monitorización y revisión de los mismos.
3. Síntesis: debe realizarse un adecuado proceso de agrupación y síntesis de los controles automatizables y no automatizables para gestionar un número relativamente pequeño de controles.
4. Medición objetiva: se debe evaluar y medir la efectividad de los controles mediante indicadores objetivos obtenidos a partir de los datos suministrados por las diferentes herramientas de seguridad de la información.
5. Mejora continua: la gestión de los controles debe verse como un proceso dinámico que consta de varias acciones, las cuales conforman un ciclo cerrado para la mejora continua de los controles de seguridad de la información.
6. Generalidad: el modelo debe ser aplicable a una gran variedad de organizaciones.

Basado en la descripción de los principios del modelo que se propone para la gestión de la seguridad de la información y los riesgos asociados a su uso en las redes de computadoras de la Universidad Estatal Península de Santa Elena, Ecuador, se tuvo en cuenta la automatización para los controles automatizables aplicados a las acciones de operación, monitorización y revisión identificados, definiendo los

principales controles de seguridad informática que deben ser automatizados para la protección de la seguridad de la información y los riesgos asociados a su uso, así como los controles identificados en los estándares ISO/IEC 27001:2016 y NIST SP 800-53 a través de las redes de computadoras de la Universidad Estatal Península de Santa Elena, Ecuador.

El modelo permite la integración de diferentes herramientas de seguridad informática, la correlación de información y la generación de reportes de seguridad de forma automatizada y no automatizada. Los controles de seguridad de la información son implementados y operados por diferentes herramientas, para su monitorización de forma centralizada en el componente central del modelo.

El componente central del modelo recibe la información mediante el inventario de activos, objetivos de controles y controles donde se encuentran las trazas generadas por los diferentes sistemas para los que se definieron los conectores que permiten interpretar los diferentes formatos de trazas existentes.

La revisión de los controles se realiza mediante un grupo de métricas de seguridad, definidas también como parte del modelo, que son calculadas y reportadas de forma automatizada.

El modelo desarrollado para la gestión de la seguridad de la información y los riesgos asociados a su uso en redes de computadoras de la Universidad Estatal Península de Santa Elena, ofrece una visión integral de controles de seguridad de la información, considerando todos los controles automatizables y no automatizables y definiendo las acciones a realizar en cada uno de los casos.

El modelo propone además una automatización de las acciones de operación, monitorización y revisión de los controles automatizables de seguridad informática para la protección de la seguridad de la información y los riesgos asociados a su uso a través de las redes de computadoras, que está destinado a la gestión de trazas y detección de eventos de seguridad. Esto presupone que se debe realizar un proceso profundo de personalización y adaptación de las acciones de operación, monitorización y revisión para aplicar el modelo propuesto, mediante la definición de conectores, políticas, reglas de correlación y reportes de seguridad informática.

Es importante señalar que mediante la aplicación del modelo se automatiza la operación, monitorización y revisión de un grupo de controles de seguridad informática, lo cual representa una parte importante del proceso de gestión de la seguridad de la información en todo su conjunto.

Además, el modelo aborda la automatización de las fases de hacer y verificar del ciclo de gestión para los controles automatizados y no automatizados. Los indicadores calculados automáticamente deben ser adecuadamente revisados por los especialistas de seguridad informática para tomar acciones correctivas sobre los controles de seguridad implementados.

El modelo se encuentra formalizado con los principales estándares, recomendaciones y regulaciones existentes, tanto a nivel internacional como nacional, sobre gestión de la seguridad de la información. En este sentido no constituye una nueva propuesta de controles y procesos de gestión, sino que brinda un enfoque de automatización, integración y síntesis a las propuestas existentes, para disminuir la complejidad de la gestión y aumentar la efectividad de los controles de seguridad de la información en redes de computación.

## CONCLUSIONES

Después de haber valorado los controles propuestos por los principales estándares internacionales, se puede concluir que alrededor del 40 % de los controles de seguridad de la información son automatizables.

Para la gestión integrada de los controles de seguridad de la información se propone el modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso en redes de computadoras en la Universidad Estatal Península de Santa Elena, modelo que posee las siguientes características generales:

- Se definen controles de seguridad de la información los cuales representan una agrupación y síntesis de los controles automatizables identificados.
- La automatización es aplicada a las acciones de operación, monitorización y revisión de los controles.
- La correlación de información y la generación de reportes de seguridad de forma automatizada es el componente central del modelo, permitiendo

la gestión integrada de los controles de seguridad informática.

- La revisión de los controles se realiza mediante un grupo de métricas de seguridad, definidas también como parte del modelo, que son calculadas y reportadas de forma automatizada.

El modelo desarrollado ofrece una visión integral de la automatización de controles de seguridad, considerando todos los controles automatizables y definiendo las acciones a realizar de forma automática en cada uno de los casos.

La implementación del modelo se realiza mediante la instalación, configuración y personalización de aplicaciones de seguridad informática existentes, así como la complementación de las mismas a través de pequeños desarrollos que posibilitan su adaptación al modelo propuesto.

**REFERENCIAS BIBLIOGRÁFICAS**

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

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, pp. 7-16. Recuperado de http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf*

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

Balarezo, A., & Poveda, D. (2015). *Propuesta de mejoramiento de la herramienta OSSIM SIEM (Open Source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en Cloud Computing.* Quito: Universidad Politécnica Saleciana.

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

Burgos, J. & Campos, P. (2013). *Modelo para seguridad de la información en TIC.* Chile: Departamento de tecnologías y sistemas de información. p. 234-253.

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.*

Castillo, G. y Pérez, E.M. (2017). Diagnóstico de los sistemas de información en las empresas priorizadas según los requerimientos actuales. *Revista de la FAHCE. Palabra clave,* 6(2), 1-11. Recuperado de https://www.palabraclave.fahce.unlp.edu.ar/article/view/PCe022/8122

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

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

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC/27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Perú: Pontificia Universidad Católica del Perú.

Ferrer, J., & Fernández, J. (2012). Seguridad Informática y Software Libre. *Hispanolinux*.

Franganillo, J. (2009). Gestión de información personal: elementos, actividades e integración. *El profesional de la información*, *18*(4), 399-406. Recuperado de http://www.elprofesionaldelainformacion.com/contenidos/2009/julio/06.pdf

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

ISO/IEC. (2016). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. *International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).*

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.*

Ministerio de Telecomunicaciones y de la Sociedad de la Información

(2016). Política de Seguridad de Información en el MIN de Telecomunicaciones. (Acuerdo Ministerial 005). Ecuador. 6 p.

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.*

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

Nof, S. Y. (2009). Springer Handbook of Automation. *Springer*

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

Sanchez, L. & Piattini, M. (2015). *Hacia un método para la construcción de cuadros de mando de la seguridad en TI para PYMES.* España: Departamento de tecnologías y sistemas de información.

Secretaría Nacional de la Administración Pública (2016). *Esquema gubernamental de seguridad de la Información, EGSI* (modificado 15-jun.-2016). Ecuador. 47 p.

Solana-Álvarez, J. M. (2014). El sistema de información de una organización. Necesidad de implicación de la dirección. En: *Anuario Jurídico y Económico Escurialense*, *XLVII*. Recuperado de http://www.rcumariacristina.net:8080/ojs/index.php/AJEE/article/view/202/169

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).*