Dom. Cien., ISSN: 2477-8818
Vol. 3, núm 4, octubre, 2017, pp. 284-295

Número Publicado el 23 de octubre de 2017

http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.4.oct.284-295
URL:http://dominiodelasciencias.com/ojs/index.php/es/index

Ciencias Informática

Artículo corto

Apuntes teóricos introductorios sobre la seguridad de la información

Introductory theoretical notes on information security

Notas teóricas introdutórias sobre segurança da informação

Efraín I. Chilán-Santana [I]
efra1783@hotmail.com
Willians F. Pionce-Pico [II]
wfpp1@hotmail.com

Recibido: 31 de mayo de 2017 * **Corregido:** 19 de julio de 2017 * **Aceptado:** 27 de septiembre 2017

[I] Ingeniero en Sistemas, Programa de Revalidación de la Maestría de Gestión Estratégica de Tecnologías de la Información, Facultad de Ingeniería; Universidad de Cuenca, Campus Central, Cuenca, Azuay

[II] Ingeniero en Sistemas Informáticos, Docente Universidad Técnica de Manabí, Portoviejo, Ecuador.

Resumen

La información como uno de los principales recursos de las organizaciones, debe protegerse de todas las amenazas que pueden poner en peligro a la empresa. Es por eso que se hace imprescindible lograr la confidencialidad, integridad y disponibilidad de esta información. Este trabajo tiene como objetivo exponer los referentes teóricos conceptuales, que aparecen en la literatura consultada sobre la seguridad de la información. Para ello se aborda, que se entiende por seguridad de la información y qué comprende un sistema de gestión de seguridad de la información; qué papel juega el Comité de Seguridad de la Información y qué significan las políticas de seguridad de la información. Se muestran esquemas conceptuales y bibliografía.

Palabras clave: seguridad de la información; protección de la información; sistema de gestión de la seguridad de la información; comité de seguridad de la información; políticas de seguridad de la información.

Abstract

Information as one of the main resources of organizations, should be protected from all threats that may endanger the company. That is why it is essential to achieve confidentiality, integrity and availability of this information. The objective of this work is to expose the conceptual theoretical referents, which appear in the consulted literature on information security. To this end, it is addressed, what is meant by information security and what comprises an information security management system; what role does the Information Security Committee play and what does information security policy mean? Conceptual schemes and bibliography are shown.

Keywords: information security; protection of information; information security management system; information security committee; information security policies.

Resumo

A informação como um dos principais recursos das organizações, deve ser protegida de todas as ameaças que possam pôr em perigo a empresa. É por isso que é essencial alcançar a confidencialidade, integridade e disponibilidade desta informação. O objetivo deste trabalho é expor os referentes teóricos conceituais, que aparecem na literatura consultada sobre segurança da informação. Para este

fim, é abordado, o que se entende por segurança da informação e o que compreende um sistema de gerenciamento de segurança da informação; Qual o papel desempenhado pelo Comitê de Segurança da Informação e o que significa política de segurança da informação? Esquemas conceptuais e bibliografia são mostrados.

Palavras chave: segurança da informação; proteção de informações; sistema de gerenciamento de segurança da informação; comitê de segurança da informação; políticas de segurança da informação.

Introducción

La información es un activo fundamental, para el desarrollo de cualquier organización. Los sistemas de información forman parte de todos los procesos, sin excepción.

La seguridad de esta información que se maneja en la organización es una prioridad, pues estos sistemas de información, deben estar protegidos contra amenazas de rápida evolución y con potencial, para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno, para garantizar la prestación continua de los servicios.

La información, es como el aparato circulatorio para las organizaciones y requiere que se proteja ante cualquier amenaza que pueda poner en peligro las empresas, tanto públicas como privadas, pues en otro caso podría dañarse la salud empresarial. La realidad nos muestra, que las organizaciones empresariales se enfrentan en la actualidad con un alto número de riesgos e inseguridades procedentes de una amplia variedad de fuentes. (Fernández C.M., 2012).

La información, como uno de los principales recursos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía.

Este trabajo tiene como objetivo, exponer los referentes teóricos conceptuales que aparecen en la literatura consultada, sobre la seguridad de la información.

Desarrollo

La seguridad de la información, tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, disrupción o destrucción no autorizada.

Los términos seguridad de información, seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información, independientemente de la forma que los datos puedan tener: electrónicos, impresos, audio u otras formas. (Guindel Sánchez, 2009).

• La confidencialidad (asegurando que sólo quienes estén autorizados, pueden acceder a la información), es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

• La integridad (garantizando que la información es fiable y exacta) es la propiedad, que busca mantener a los datos libres de modificaciones no autorizadas.

• La disponibilidad (asegurando que los usuarios autorizados tienen el acceso debido a la información) es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En lo que respecta a la seguridad de la información, uno de los aspectos más importantes es comprender que esta debe ser gestionada. La correcta gestión de la seguridad de la información, busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es, tal como su nombre lo indica, un elemento para administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información. (Pacheco, 2010).

La idea fundamental que se persigue, es la gestión de la seguridad de la información para conseguir unos niveles de seguridad mínimos, y para ello es imprescindible contar con un Sistema de Gestión de la Seguridad de la Información (SGSI), mediante un proceso sistemático, documentado y conocido por toda la organización, de forma similar a como se desarrollan los sistemas de gestión de la calidad basados en la norma ISO 9001/ISO 14001, etc. La función que tiene un SGSI consiste en garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, actualizándose constantemente y mejorando continuamente los sistemas y la gestión de la seguridad de la información. (Diaz A., 2010).

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Entre las actividades propias a desarrollar al abordar una implantación a ISO27001 se encuentran: (GESCONSULTOR, 2017)

• Definición del alcance del SGSI.

• Definición de una política de seguridad.

• Definición de una metodología y criterios para el análisis y gestión del riesgo.

• Identificación de riesgos.

• Evaluación de los posibles tratamientos del riesgo.

• Elaboración de una declaración de aplicabilidad de controles y requisitos.

• Desarrollo de un plan de tratamiento de riesgos.

• Definición de métricas e indicadores de la eficiencia de los controles.

• Desarrollo de programas de formación y concienciación en seguridad de la información.

• Gestión de recursos y operaciones.

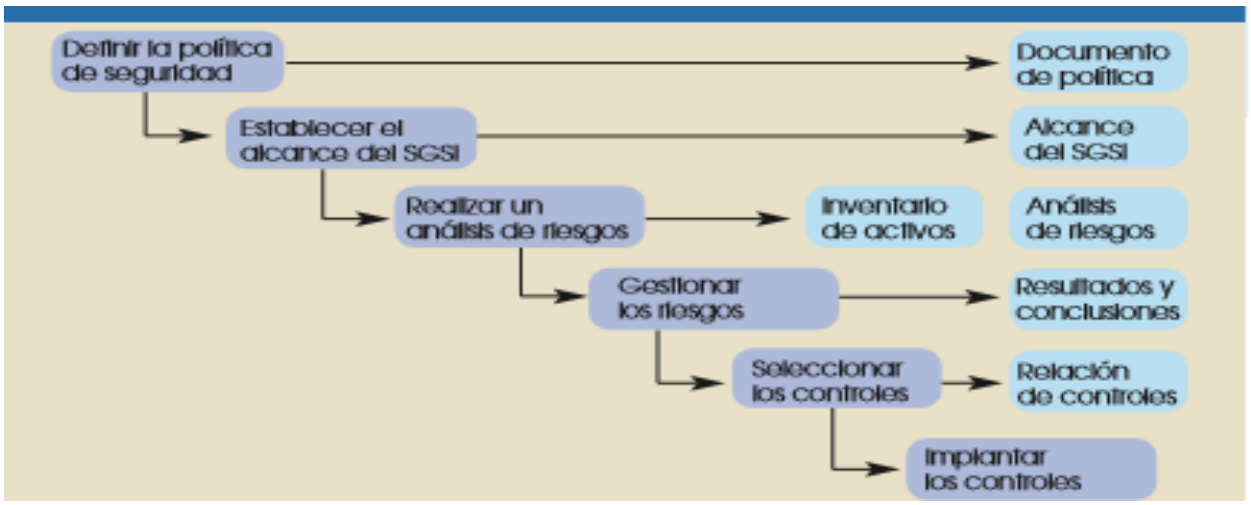
• Gestión de incidencias.

• Elaboración de procedimientos y documentación asociada.

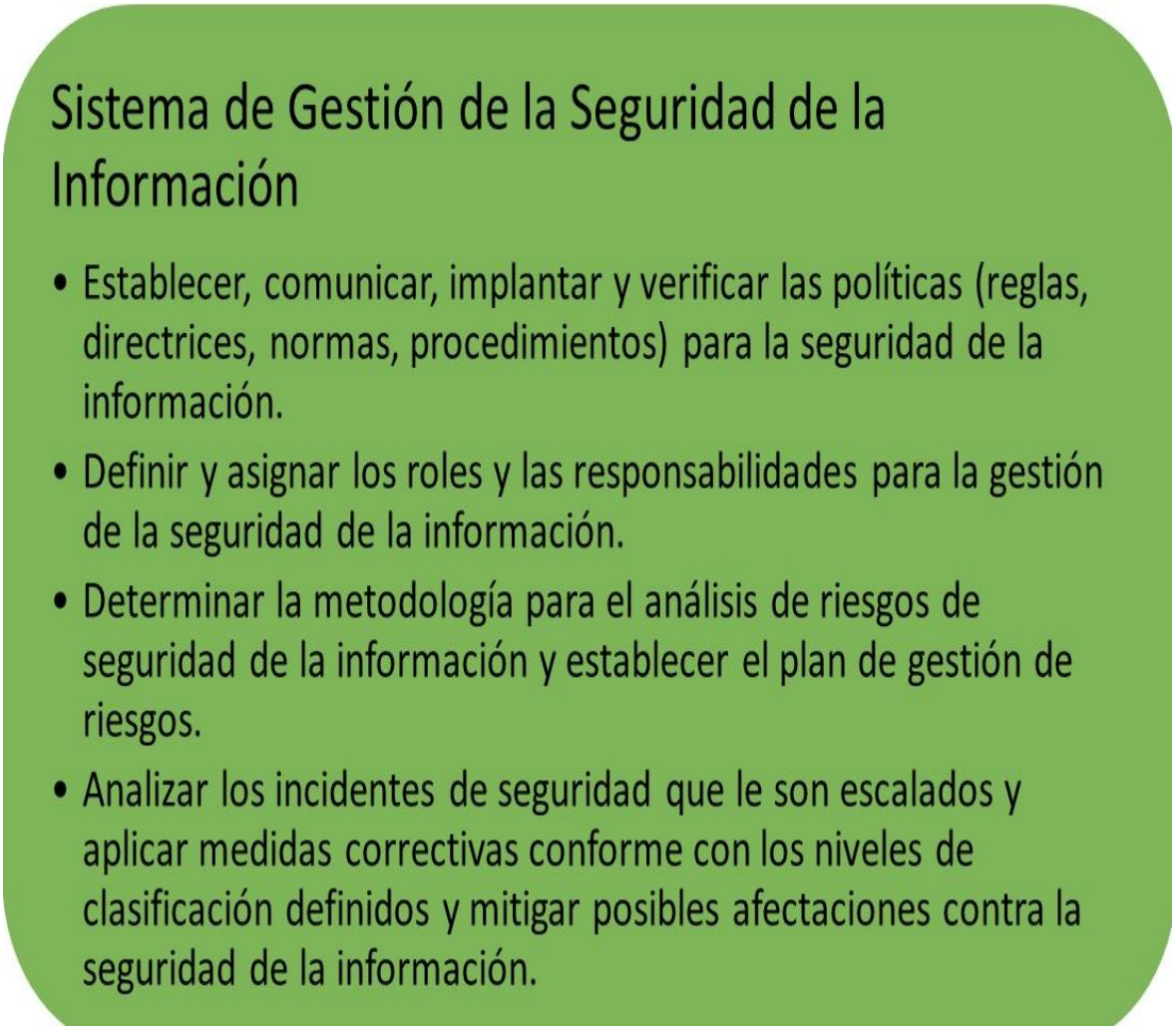
Como otras Normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad. Asimismo, está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización.

La norma ISO 27001, específica los requisitos necesarios para establecer un SGSI, que incluye las etapas que muestra el esquema 1 confeccionado por Díaz (2010).

El Esquema 2, de elaboración propia resume los aspectos que incluye un SGSI.



Esquema 1. (Diaz A., 2010)

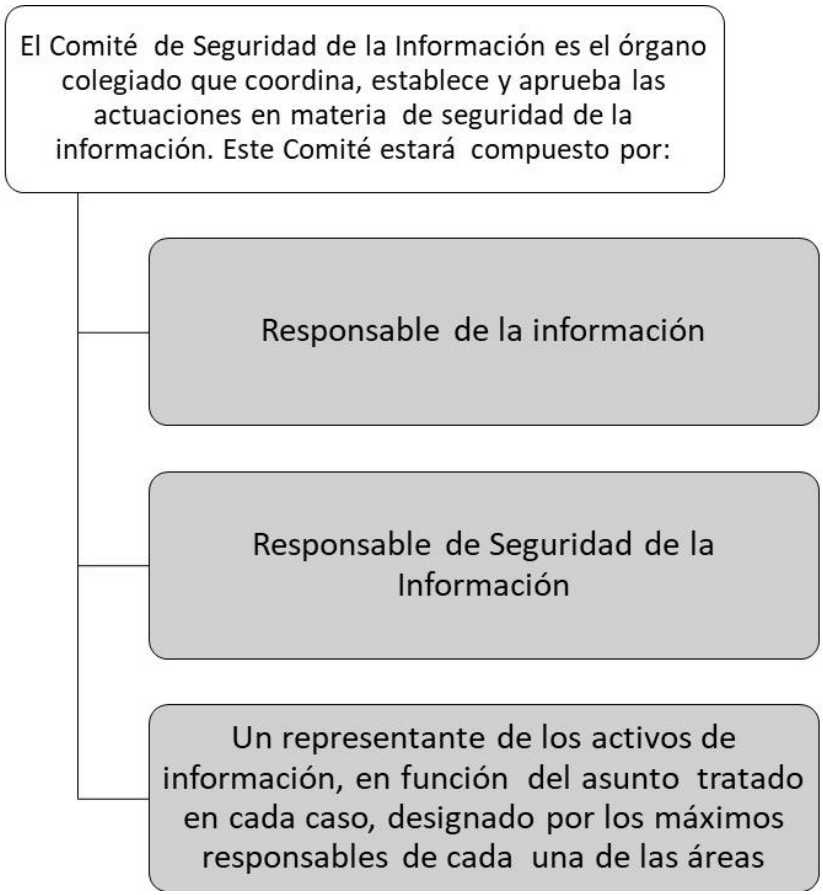


Esquema 2. Elaboración propia

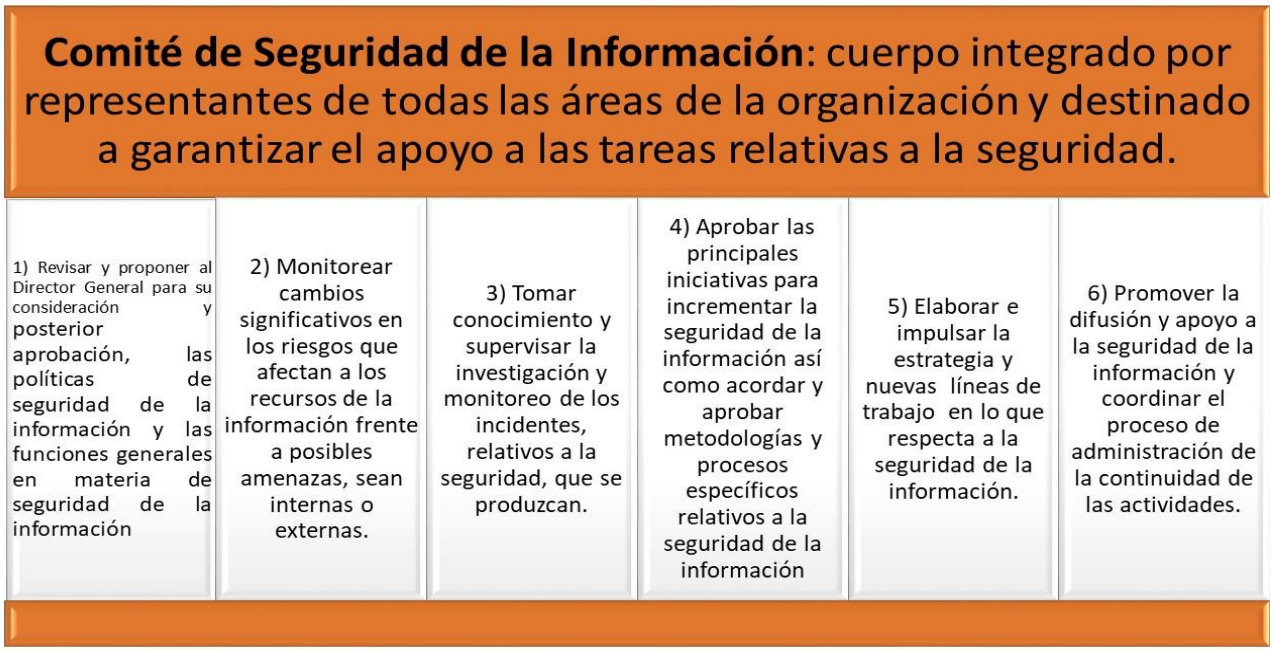
Para poder implementar un SGSI, es importante crear un Comité de Seguridad de la Información (CSI), que sería un grupo de trabajo donde se compromete directamente a las áreas que sustentan la razón de ser de la organización (áreas/gerencias de negocios); y esto traería como consecuencias que las áreas de apoyo, deberán ajustarse a los lineamientos generados por el CSI. (Solis C., 2012).

El CSI se encarga de establecer un marco normativo consistente, que sirva como base y referencia para los temas de seguridad de información dentro de la organización.

A partir de la literatura sobre el CSI, se han elaborado dos esquemas. El Esquema 3, muestra quienes deben conformar dicho Comité y en el Esquema 4, se exponen las funciones que debe ejercer.



Esquema 3 Elaboración propia



Esquema 4 Elaboración propia

Esquema 5 Elaboración propia

La política de seguridad de la información, reconoce la importancia de proteger los activos de información, evitando el acceso, uso, divulgación, modificación y destrucción no autorizada de toda información relacionada con empleados, clientes, productos, servicios, precios, bases de conocimiento, manuales, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

El jefe de seguridad de la información es responsable directo, sobre el mantenimiento de esta política por brindar consejo y guía para su implementación, así como también investigar toda violación reportada por el personal.

En el Esquema 5, refleja todas aquellas políticas que integra la seguridad de la información.

La norma ISO 27001 plantea: (ISOTools Excellence, 2016).

• La política tiene que adaptarse a la empresa, esto significa que no puede simplemente copiar la política de una gran organización y utilizarlo en una pequeña organización de TI.

• Es necesario definir un marco, para establecer todos los objetivos de seguridad de la información, la política debe definir cómo se proponen los objetivos, la forma en la que se encuentran aprobados y la manera en la que se revisan.

• La política tiene que mostrar el compromiso de la alta dirección, para cumplir con los requisitos de todas las partes interesadas y mejorar de forma continua el sistema de gestión de seguridad de la información, eso se hace normalmente mediante un tipo de declaración dentro de la política.

• La política se debe comunicar dentro de la organización y a todas las partes interesadas, la mejor práctica es definir quién es el responsable de tal comunicación, y entonces esa persona es responsable de hacerlo de forma continua.

• La política debe ser revisada de forma continua, por parte del propietario de una política que debe ser definida. Dicha persona será la responsable de mantener la política hasta la fecha.

Por lo tanto, como se puede ver, la política no tiene por qué ser un documento muy largo. Y no tiene por qué incluir todas las reglas de seguridad de la información, dentro de este documento a tal fin de escribir las políticas detalladas, como políticas de control de acceso, política de clasificación, política de utilización aceptable, etc.

Hay que tener un par de cosas en cuenta a la hora de escribir la política de seguridad de la información:

• Las intenciones de la alta dirección en cuanto a la seguridad de la información.

• La legislación y todos los requisitos.

• El sistema existente para establecer los objetivos.

Conclusiones

La seguridad de la información en una empresa se consigue implantando un sistema de gestión, que establezca la forma más adecuada de tratar los aspectos de seguridad, mediante la conjugación de los recursos humanos y técnicos, respaldados por medidas administrativas, que garanticen la instauración de controles efectivos, para lograr el nivel de seguridad necesario en correspondencia con los objetivos de la organización, de manera que se mantenga siempre el riesgo por debajo del nivel asumible por la propia entidad.

Bibliografía

Diaz A. (2010). Sistema de gestión de la seguridad de la información UNE-ISO/IEC 27001

Fernández C.M. (2012). La norma ISO 27001 del sistema de gestión de la seguridad de la información. Calidad.

Gesconsultor. (2017). ISO 27001 – sistema de gestión de la seguridad de la información. Obtenido de http://www.gesconsultor.com/iso-27001.html

Guindel Sánchez, E. (2009). Calidad y seguridad de la información y auditoría informática. Proyecto de Fin de Carrera

ISOTools Excellence. (2016). Qué debe incluir en su política de seguridad de la información basado en la norma ISO 27001?

Pacheco, F. (2010). La importancia de un SGSI. Obtenido de https://www.welivesecurity.com/

Solis C. (2012). ¿Qué es el Comité de Seguridad de la Información? Obtenido de www.segu-info.com.ar