Polo del Conocimiento

Pol. Con. (Edición núm. 14) Vol. 2 No 12
Diciembre 2017, pp. 145-155
ISSN: 2550 - 682X
DOI: 10.23857/pc.v2i12.420

Recepción: 25 / 10 / 2017
Aceptación: 28 / 11 / 2017
Publicación: 15/ 12/ 2017

Ciencias de la computación

Artículo de investigación

La seguridad informática y la seguridad de la información

Information security and information security

Segurança da informação e segurança da informação

Juan A. Figueroa-Suárez [I]
juan.figueroa@uleam.edu.ec

Richard F. Rodríguez-Andrade [II]
richardrodand@hotmail.com

Cristóbal C. Bone-Obando [III]
colonboneo@gmail.com

Jazmín A. Saltos-Gómez [IV]
ing.jasycar@gmail.com

Correspondencia: juan.figueroa@uleam.edu.ec

[I] Magister en Gerencia Educativa, Especialista en Diseño Curricular por Competencias, Analista de Sistemas, Contador Público, Ingeniero en Contabilidad y Auditoría, Docente de la Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador.

[II] Magister en Gerencia Educativa, Analista de Sistemas, Licenciado en Ciencias de la Educación Especialización Docencia Técnica en Informática, Profesor de Educación Pre-Primaria - Nivel Técnico Superior, Docente de la Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador.

[III] Magister en Gerencia de Proyectos Educativos y Sociales, Magister en Docencia Mención Gestión en Desarrollo del Currículo, Doctor en Ciencias de la Educación Mención Investigación Educativa, Licenciado en Ciencias de la Educación Profesor de Segunda Enseñanza en la Especialización de Física y Matemática, Docente Universidad Técnica Luis Vargas Torres de Esmeraldas, Esmeraldas, Ecuador.

[IV] Ingeniera en Sistemas y Tecnologías de la Información, Docente de la Universidad Luis Vargas Torres de Esmeraldas, Esmeraldas, Ecuador.

Resumen

Muchos profesionales hablan indistintamente de la seguridad informática y la seguridad de la información. Sin embargo, cada disciplina tiene su particularidad aun cuando están estrechamente relacionadas. Este trabajo tiene como objetivo mostrar la distinción y relación entre estos dos temas. Para ello se realiza un análisis documental.

Palabras clave: seguridad de la información; seguridad informática.

Abstract

Many professionals speak indiscriminately of computer security and information security. However, each discipline has its particularity even though they are closely related. This paper aims to show the distinction and relationship between these two themes. For this, a documentary analysis is carried out.

Keywords: information security; computer security.

Resumo

Muchos profesionales hablan indistintamente de la seguridad informática y la seguridad de la información. Sin embargo, cada disciplina tiene su particularidad aun cuando están estrechamente relacionadas. Este trabajo tiene como objetivo mostrar la distinción y relación entre estos de los temas. Para ello se realiza un análisis documental.

Palavras chave: seguridad de la informação; segurança informática.

Introducción

Es frecuente que el público en general -nos referimos a personas que no están ligadas profesionalmente a la informática- entienda Seguridad informática, seguridad de la información como sinónimos entre sí. De hecho, hasta el momento no ha sido sencillo lograr un consenso en relación con estas definiciones, de tal manera que sean aceptadas por la mayoría de profesionales de la seguridad de las tecnologías de información y comunicación. (Rojas Valduciel, 2016)

Este trabajo tiene como objetivo exponer la distinción y relación que existe entre la seguridad informática y la seguridad de la información.

Para ello se realiza un análisis documental a partir de las fuentes que aparecen en internet, evaluación la autoridad y calidad de los documentos encontrados.

Desarrollo

La Seguridad Informática

Según ISOTools Excellece la seguridad informática, con sus siglas en inglés IT security, es la disciplina que se encarga de llevar a cabo las soluciones técnicas de protección de la información. "La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa". (ISOTools Excellence, 2017)

Los Consultores en Seguridad de la Información (2016) hablan de la seguridad informática o también llamada seguridad de tecnologías de la información, definiéndola como "el área de la informática que consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización, sean utilizados de manera correcta". (Consultores en Seguridad de la Información, 2016)

En este sentido, González (2011) plantea que la Seguridad Informática, es la "disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que-articulados con prácticas de gobierno de tecnología de información-establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo". (Gonzalez, 2011)

Y Rojas Valduciel (2006), considera que la seguridad informática es el conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen. Y expone que "Dentro de esta categoría, se

puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos". (Rojas Valduciel, 2016)

Las prácticas de este tipo de seguridad son diversas, y consiste en lo general en la restricción del acceso al sistema o parte del sistema. El acceso solo es permitido a ciertas personas que se encuentren acreditadas, así como su modificación dentro de los límites de su autorización. Las amenazas que se encuentran, son debido a que el propio usuario no tiene en cuenta las vulnerabilidades que existen al hacer un mal uso del sistema. Por ejemplo, al descargar archivos peligrosos o borrar archivos importantes para el sistema. Al mismo tiempo, programas maliciosos como virus o malware.

"La totalidad de los especialistas en seguridad basan sus conocimientos y experticias sobre el aspecto técnico tradicional de la seguridad, esto es en las áreas IT, aunque bastantes de ellos consideran las cuestiones propias como el nuevo aspecto en las comunicaciones y que hace que actualmente se hable de TIC. Además de tener un enfoque técnico prácticamente, los especialistas únicamente se manejan con las vulnerabilidades y en parte con amenazas en forma de ataques (…) Con el fin de establecer una evaluación de riesgos, se necesita realizar una evaluación a los activos, además de identificar cualquier amenaza que pueda aprovechar y explotar las vulnerabilidades de estos activos". (ISOTools, 2015)

La Seguridad de la Información

Para ISOTools Excellence (2017), la definición de la seguridad de la información tributa a una disciplina "que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo (…) es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información". (ISOTools Excellence, 2017)

Information Security es la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo la normativa o las buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos.

La seguridad de la información es la disciplina que se encarga de garantizar la:

- confidencialidad,
- integridad y
- disponibilidad de la información.

Es habitual que la seguridad de la información se apoye en la política de seguridad que se desarrolla mediante la elaboración de un plan director de seguridad. La dirección será la encargada de marcar todas las líneas de actuación en materia de seguridad y mediante el plan director para determinar las medidas tanto técnicas como procedimentales que garantice los objetivos marcados por la política de seguridad.

Las medidas técnicas serán llevadas a cabo por el equipo de seguridad informática, administradores de sistemas y seguridad, los roles de seguridad, que implantan las medidas necesarias para el cumplimiento de la política de seguridad y el análisis de riesgos en el que se debería basar la política.

La implementación de la norma ISO 27001 de seguridad de la información, además de reducir el impacto de los riesgos y amenazas, entre otros beneficios, mejora la planificación y la gestión de la seguridad de la empresa. Establece garantías de continuidad del negocio en caso de contingencia, proporciona una imagen de prestigio frente a terceros y da cumplimiento de normativas nacionales.

"Esto va enfocado no solo al cuidado de la información, también a la mejora de los procesos de la empresa, agregando más medidas de seguridad como es la organización y las cuestiones legales conforme a las normas que rige ISO/IEC 27001, esto aumentando que sea aún más sólido, confiable, íntegro y mucho más fácil la disposición de su sistema de la información". (Consultores en Seguridad de la Información, 2016)

González (2011), concibe la seguridad de la Información como la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

Y Rojas Valduciel (2016), enfoca la seguridad de la información como las medidas y actividades que procuran proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.

"La Seguridad de la Información es muy extensa, por lo que no es sólo una cuestión técnica sino que supone una responsabilidad de la alta dirección de la empresa, así como de sus directivos (…) En el caso de no involucrarse las unidades activas y los líderes de negocio, como podrían ser, ejecutivos, directivos, etc. de las entidades, no podrá existir un plan de Seguridad de la Información, a partir de todos los riesgos determinados. Todo ello se lleva a cabo en el seno del sistema de dirección y control propio del gobierno corporativo. Se tiene que considerar los sujetos, los procesos y las funciones de negocio, además de la protección de todos los activos/recursos de la entidad impulsora, propietaria y beneficiaria de la Seguridad de la Información, dentro de un marco de responsabilidades compartidas. Se tienen que considerar la totalidad de los riesgos técnicos de TIC, además de que la seguridad se desarrolle por toda la empresa, es decir, son riesgos organizacionales, operacionales y físicos. Los riesgos operacionales son hoy en día más cruciales en lo referente a Seguridad de la Información. Las vulnerabilidades de este tipo de riesgo se expanden durante una amplia gama de grises, en conexión con el comportamiento humano y los juicios subjetivos de las personas, la resistencia al cambio, la cultura empresarial, la forma de comunicarse, etc.". (ISOTools, 2015)

"La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas. Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la

presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan". (Tarazona, s/f)

Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías:

- ✓ Factores Humanos (accidentales, errores)
- ✓ Fallas en los sistemas de procesamiento de información;
- ✓ Desastres naturales y;
- ✓ Actos maliciosos o malintencionados.

Algunas de estas amenazas son:

- ✓ Virus informáticos o código malicioso
- ✓ Uso no autorizado de Sistemas Informáticos
- ✓ Robo de Información
- ✓ Fraudes basados en el uso de computadores
- ✓ Suplantación de identidad
- ✓ Denegación de Servicios (DoS)
- ✓ Ataques de Fuerza Bruta
- ✓ Alteración de la Información
- ✓ Divulgación de Información
- ✓ Desastres Naturales
- ✓ Sabotaje, vandalismo
- ✓ Espionaje

Conclusiones

Es evidente la diferencia entre seguridad informática y seguridad de la información, pero también es indiscutible que ambos temas se encuentran muy ligados entre sí. A pesar de ser disciplinas diferentes, la una no puede ir sin la otra.

La seguridad informática se describe como la distinción táctica y operacional de la seguridad, mientras que la seguridad de la información es la línea estratégica de la seguridad.

La seguridad informática atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales mientras que la seguridad de la información integra toda la información independientemente del medio en el que esté.

La seguridad de la información, para conseguir el objetivo se apoya a la seguridad informática, es decir, la seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información.

La seguridad de la información va mucho más allá de la seguridad informática, puesto que intenta proveer de medidas de seguridad a otros medios donde se localiza la información como:

- Impresos en papel
- Discos duros
- Medidas de seguridad respecto de las personas que la conocen

Mientras la seguridad de la información integra toda la información independientemente del estado en el que se encuentre, la seguridad informática se enfoca en la protección de infraestructura (redes, sistemas operativos, ordenadores.

La Seguridad Informática se encarga de la parte operativa de la Seguridad, es decir, las medidas técnicas que aseguran la Seguridad de la Información.

Rojas Valduciel (2016) establece algunas diferencias:

- La seguridad de la información se orienta a proteger los activos de información sin importar su forma o estado, valiéndose de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, para la aplicación y gestión de las medidas de seguridad apropiadas en cada caso. Por tanto abarca a la seguridad informática.
- La seguridad informática, se limita a proteger activos de información en formato digital y los sistemas informáticos que los procesan y almacenan, indistintamente si están interconectados o no.

El desarrollo que se ha experimentado en cuanto a seguridad informática al de seguridad de la información, implica incrementar el campo de visión del marco de riesgos de negocio respectos a la perspectiva tradicional de seguridad técnica, fundamentada en las vulnerabilidades.

En el entorno de la seguridad de la información los riesgos de negocio incluyen, no sólo las vulnerabilidades y las amenazas, sino que incluyen también el conjunto de factores que determinan los riesgos:

- Activos
- Vulnerabilidades
- Amenazas

Los riesgos de negocio que incluyen los riesgos organizacionales, operacionales, físicos y de sistemas TIC.

Podemos conseguir un enfoque completo de seguridad de la información en la parte en la cual se considera los recursos necesarios para minimizar los riesgos dentro de un plan de seguridad, no se puede considerar un gasto sino una inversión para la empresa. Solicita de un análisis y determinar de una manera cuantificable el retorno de las inversiones en seguridad.

Es importante establecer en las organizaciones un sistema de Gestión de la Seguridad de la Información con vistas a la protección de la confidencialidad, integridad y disponibilidad de la información y de los bienes que la contienen o procesan. De esta manera, las organizaciones y personas se pueden proteger de: (Tarazona, s/f)

- Divulgación indebida de información sensible o confidencial, de forma accidental o bien, sin autorización.
- Modificación sin autorización o bien, de forma accidental, de información crítica, sin conocimiento de los propietarios.
- Pérdida de información importante sin posibilidad de recuperarla.
- No tener acceso o disponibilidad de la información cuando sea necesaria

La información debe ser manejada y protegida adecuadamente de los riesgos o amenazas que enfrente. La información valiosa se puede encontrar en diferentes formas: impresa, almacenada electrónicamente, transmitida por diferentes medios de comunicación o de transporte, divulgada por medios audiovisuales, en el conocimiento de las personas, etc.

Los estándares ISO 17799 e ISO 27001 le dan a una organización las bases para desarrollar un marco efectivo de gestión de la seguridad de la información, que le permita proteger sus activos de información importantes, minimizando sus riesgos y optimizando las inversiones y esfuerzos necesarios para su protección.

Una de las formas de protección consiste en la aplicación de controles, que en la práctica pueden ser políticas, procesos, procedimientos, organización (definición de una estructura organizacional de seguridad), elementos de software y hardware, mecanismos de protección de la infraestructura física y de seguridad, así como la adecuada selección y entrenamiento del personal que opera y utiliza los recursos de información o informáticos.

La norma ISO 17799 presenta una serie de áreas para ser gestionadas, mediante la aplicación de controles o mecanismos de protección, las cuales van desde la seguridad en los sistemas, pasando por los aspectos de seguridad física, recursos humanos y aspectos generales de la organización interna en las organizaciones. (Tarazona, s/f)

Referencias Bibliográficas

Consultores en Seguridad de la Información. (2016). Seguridad Informática vs Seguridad de la Información. Recuperado el 03 de marzo de 2017, de https://www.maestrodelacomputacion.net/seguridad-informatica-seguridad-de-la-informacion/

Gonzalez, J. (2011). ¿Seguridad Informática o Seguridad de la Información? Recuperado el 02 de febrero de 2016, de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

ISOTools Excellence. (2017) ¿Seguridad informática o seguridad de la información? Recuperado el 05 de marzo de 2017, de http://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Rojas Valduciel, H. (2016). Seguridad de la Información, Seguridad Informática y Ciberseguridad: ¿Son sinónimos? Recuperado el 20 de febrero de 2017, de https://infobyteabyte.wordpress.com/2016/04/20/seguridad-de-la-informacion-seguridad-informatica-y-ciberseguridad-son-sinonimos/