Contribución de la norma ISO/IEC 27000 en la gestión de seguridad de la información, por Ana Chacón

Volumen: Número 69

ESPOL • FCSH • CIEC

FENOpina online

Escuela Superior Politécnica del Litoral.
Facultad de Ciencias Sociales y Humanísticas.
Revista FENopina.
Número 69
15 de Diciembre de 2014.
Administración.

Contribución de la norma ISO/IEC 27000 en la gestión de seguridad de la información

Por Ana Eva Chacón Luna, Mgti.
Docente de la UNEMI
evitachacon@gmail.com

Fecha de recepción: 11/septiembre/2014
Fecha de aprobación: 13/diciembre/2014

Resumen.- *Con el auge de las tecnologías de la información se han desarrollado grandes avances en diferentes áreas, siendo una de las beneficiadas las organizaciones, cambiando incluso hasta su forma de realizar negocios, migrando al comercio electrónico; sin embargo, detrás de todos estos beneficios existe la necesidad urgente de adoptar medidas de seguridad de la información, pues es de conocimiento general las prácticas fraudulentas y ataques a los sistemas de TI que han tenido que enfrentar algunas organizaciones. Las Normas ISO/IEC 27000, 27001 y 27002 son normas internacionales que cada vez tienen mayor aceptación debido a la colaboración que estas proporcionan en cuanto a la seguridad de la información, posibilitando que las organizaciones obtengan certificaciones de sus sistema de gestión de seguridad de la información (SGSI), lo que favorecerá a la percepción de sus clientes por las medidas de seguridad adoptadas por la Organización.*

Palabras Claves: *Seguridad de la Información, ataques a los sistemas de TI, Normas ISO/IEC 27000, sistema de gestión de seguridad de la información*

Abstract: *With the rise of the information technologies have been developed breakthroughs in different areas, one of the beneficiary are the organizations, even changing their way of doing business migrating to electronic commerce; However, behind all these benefits there is an urgent need for measures of information security, because it is generally known fraudulent practices and attacks on IT systems that have had to face some organizations. The ISO / IEC 27000, 27001 and 27002 standards are international standards that are becoming more widely accepted because of the collaboration that they provide in terms of information security, enabling organizations to obtain certification of their management system security information (ISMS), which favor the perception of your customers for the security measures adopted by the Organization.*

Keywords: *Information Security, attacks on IT systems, ISO / IEC 27000 standards, system security management information.*

La información es el activo más valioso dentro de una empresa, por ello se emplean mecanismos de control para salvaguardar dicho activo, para así evitar el hurto y manipulación maliciosa, asegurando la integridad, disponibilidad, confidencialidad de la misma; lo que contribuirá para alcanzar los objetivos organizacionales.

Ilustración 1: Características de la Información
Fuente:(TÜV SÜD Iberia, 2010)

Las nuevas tecnologías utilizadas han dado un giro radical de cómo hacer negocio, dando lugar a nuevas oportunidades de expansión a las empresas; sin embargo, dichas tecnologías también conllevan a nuevas amenazas, posibilitando que personas maliciosas con conocimientos avanzados (crackers) puedan encontrar vulnerabilidades en los equipos, sistemas o redes informáticas violentando su seguridad, con el objetivo de causar daños. Cabe indicar que la información no solo se enfrenta a daños físicos sino también a daños lógicos; físicos como incendios, vandalismos, etc. que podrían afectar la disponibilidad de recursos e información; y como ya habíamos mencionado también riesgos lógicos relacionados con la propia tecnología, enfrentándose día a día a hackers, robos de identidad, spam, virus, espionaje industrial, hurto de información, los que podrían poner en peligro la continuidad de las operaciones de las empresas; si no están preparadas para afrontarlos.

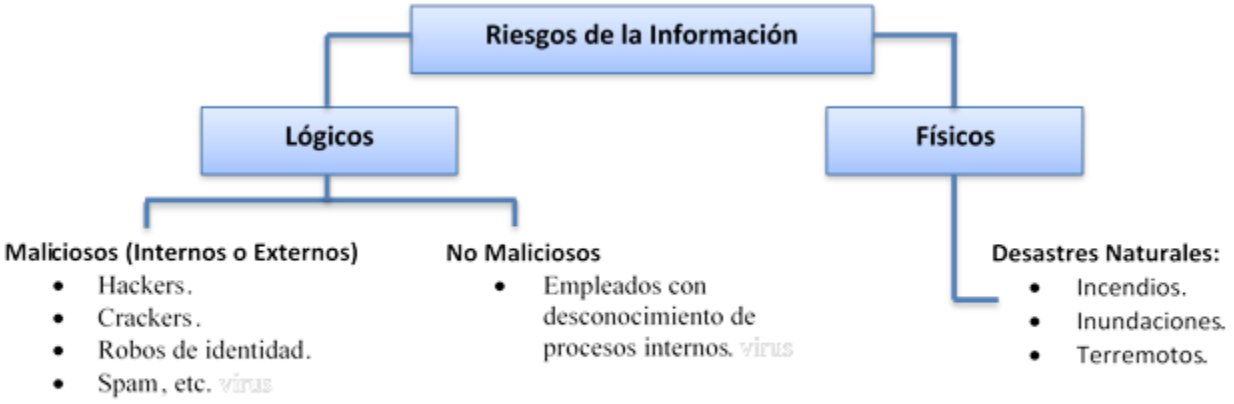

Ilustración 1: Riesgos de la Información
Fuente: Elaboración Propia

Para salvaguardar a las organizaciones de estas debilidades y amenazas que enfrentan, es ineludible conocer los riesgos para poder afrontarlos de una manera adecuada; lo que permitirá mantener el riesgo de la información en un porcentaje asumible. Además, es necesario considerar el ciclo de vida de la información, ya que lo que hoy puede ser crítico para nuestro negocio puede dejar de tener importancia con el tiempo o viceversa. (Instituto Nacional de Tecnologías de la Comunicación, 2008)

Como se ha manifestado la Seguridad de la Información incluye la tecnología. La misma que se preocupa por la seguridad de los sistemas y los datos almacenados en los mismos, así como la gestión de todos los procesos relacionados. (TÜV SÜD Iberia, 2010) Sin embargo; únicamente con la compra de firewalls o antivirus no será suficiente para salvaguardar la información de la organización, sino más bien se necesita *una planificación estructurada, y un control de todas las medidas de seguridad.*

Ilustración 3: Esfuerzos para Salvaguardar la Información
Fuente:(TÜV SÜD Iberia, 2010)

Por lo expuesto, indicamos que para custodiar este valioso activo se deberá establecer procedimientos e implementar controles de seguridad fundamentados en la evaluación de riesgos, mediante la implementación de un Sistema de Gestión de Seguridad de la Información.

Un sistema de gestión de seguridad de la información SGSI o conocido por sus siglas en inglés como ISMS (Information Security Management System), es un conjunto de políticas que definen el camino a seguir en la administración de la información permitiendo la construcción, implementación y mantenimiento de procesos que permitan gestionar eficientemente la accesibilidad a la información, optimizando los controles implementados para la seguridad.

En este punto, cabe mencionar que la gestión de riesgos y controles en sistemas de información, tiene un papel esencial, al proporcionar a las organizaciones capacidades para: alinear los niveles de riesgo con su impacto organizacional, el retorno de la inversión, optimizar la toma de decisiones y minimizar las pérdidas.(Guerrero Julio & Gómez Flórez, 2012)

La implementación de un sistema de gestión de seguridad de la información contribuye a:

- Analizar y ordenar la estructura de los sistemas de información.
- Facilitar la definición de procedimientos de trabajo para mantener su seguridad.
- Disponer de controles que permitan medir la eficacia de las medidas tomadas. Asegurar la confidencialidad, integridad y disponibilidad de la información
    - La confidencialidad, es dar acceso a la información exclusivamente por parte de quienes están autorizados.
    - La integridad de la información presume la exactitud y completitud.
    - La disponibilidad, es dar acceso a la información en el momento que lo requieran los usuarios autorizados y los sistemas de información.
- Obtener reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos.
- Reducir las amenazas hasta alcanzar un nivel asumible por la organización.
- Asegurar la continuidad del negocio, si se produce una incidencia, los daños se minimizan.
- Eliminar inversiones innecesarias e ineficientes por desestimar o sobrestimar riesgos.
- Asegurar el cumplimiento del marco legal de la legislación vigente evitando riesgos y costes innecesarios.
- Obtener la certificación del Sistema de Gestión de Seguridad de la Información contribuyendo a mejorar la competitividad en el mercado. (Instituto Nacional de Tecnologías de la Comunicación, 2008)

Por los beneficios enunciados se considera que la implementación de un sistema de gestión de seguridad de la información es una disposición estratégica para una organización. Siendo necesario que el SGSI se integre con los procesos de la organización, sistemas de información, controles implementados y estructura de gestión global.

NORMAS ISO/IEC 27000

Con el objetivo de proporcionar protección a los sistemas de información y a la información que estos manejan, las normas ISO/IEC 27000, relacionando los modelos publicados por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) han creado estándares que facilitan la implantación de controles específicos, los que permiten la evaluación y el tratamiento de los riesgos de seguridad de información, estos principios pueden ser adaptados a cualquier tipo, tamaño o naturaleza de la organización.

El Sistema de Gestión de la Seguridad de la Información se fundamenta en la norma UNE-ISO/IEC 27001:2007, esta sigue un enfoque basado en procesos utilizando el ciclo de mejora continua o de Deming, que consiste en Panificar- Hacer-Verificar-Actuar, más conocido con el acrónimo en inglés PDCA (Plan-Do-Check-Act) *similar a la más extendida y reconocida norma ISO 9001*. De la misma manera se fundamenta en la norma UNE–ISO/IEC 27002:2009, que recoge una lista de objetivos de control y controles necesarios para lograr los objetivos de seguridad de la información.(Fernández, 2010)
Las norma ISO 27000 realmente es una serie de estándares, los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.(“Iso 27000,” 2010).
A continuación mencionaremos las más utilizadas: (César, 2014).

ISO 27000.
Contiene términos y definiciones empleadas en todas las serie 27000 con el objetivo de evitar diferentes interpretaciones en los términos utilizados.
ISO 27001.
Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información y es la norma que permite obtener la certificación por auditores externos sobre los SGSI de las organizaciones.
ISO 27002.
Es una guía de buenas prácticas que recoge las recomendaciones sobre las medidas a tomar para asegurar los sistemas de información de una organización. Para ello describe 11 dominios, es decir áreas de actuación, 39 objetivos de control o aspectos a asegurar dentro de cada área, y 133 controles o mecanismos para asegurar los distintos objetivos de control.
(Instituto Nacional de Tecnologías de la Comunicación, 2008).
ISO 27003.
Es una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
ISO 27004.
Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.
ISO 27005.

Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO 27006.

Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO 27007.

Es una guía de auditoría de un SGSI.

ISO 27011.

Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031.

Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032.

Consiste en una guía relativa a la ciberseguridad.

ISO 27033:

Esta norma se encarga de la gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.

ISO 27034:

Consiste en una guía de seguridad en aplicaciones.

De entre todas las normas mencionadas una de las más importantes es la norma ISO 27001, la misma que contempla once dominios: (Hernando, 2008).

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos.
4. Seguridad de Recursos Humanos.
5. Seguridad Física y del Entorno.
6. Gestión de Comunicaciones y Operaciones.
7. Control de Acceso.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes de la Seguridad de la Información.
10. Gestión de la Continuidad del Negocio.
11. Cumplimiento.

Sistema de Gestión de la Seguridad de la Información fundamentado en ISO 27001

Ilustración 4: Sistema de Gestión de Seguridad de la Información fundamentado en ISO 27001
Fuente: AENOR

A continuación se describen las fases del ciclo PDCA. (Audisec, 2010).

1. **Planificar**

Esta fase se encarga de la creación del SGSI, con la definición del alcance y las Políticas de Seguridad. El objetivo principal de esta fase es la realización de un análisis de riesgos que refleje la situación actual de la organización. Tomando como base el resultado de este análisis se definirá un plan de tratamiento de riesgos que conlleva la implantación en la organización de una serie de controles de seguridad con el objetivo de mitigar los riesgos no asumidos por la Dirección.

2. **Hacer**

Esta fase cubre la implantación del plan de tratamiento de riesgos, su ejecución. Incluye también la formación y concienciación de los empleados en materia de seguridad y la definición de métricas e indicadores que sirvan para evaluar la eficacia de los controles implantados.

3. **Comprobar**

Durante esta fase se realizan diferentes tipos de revisiones para comprobar la correcta implantación del sistema. Entre ellos: Ejecutar procedimientos y controles de monitoreo y revisión, medir la eficacia de los controles implementados, revisar regularmente la evaluación de riesgos y la eficacia del SGSI, realizar regularmente auditorías internas, actualizar planes de seguridad.

4. **Mejorar**

El resultado de las revisiones debe reflejarse en la definición e implantación de acciones correctivas, preventivas y de mejora para avanzar en la consecución de un SGSI eficaz y eficiente.

Con la Implementación de un SGSI apoyado en la norma ISO 27001 las compañías se habilitan para certificarse con normas reconocidas internacionalmente, ocasionando mayor credibilidad, responsabilidad, confianza y comodidad en los clientes en cuanto a seguridad de la información se refiere; además asevera el cumplimiento de normas legales, reduciendo el riesgo de multas o pagos de compensaciones por violaciones de las normativas existentes.

Implementación de las Normas ISO 27001 a nivel mundial.

Haciendo referencia a un estudio realizado por (Disterer, 2013) en la Ilustración **5** se muestra la evolución desde el año 2006 al 2010 en base al número de certificados de acuerdo con la Norma ISO 27001, se evidencia la aceptación por parte de las organizaciones debido a los grandes beneficios que esta Norma conlleva.

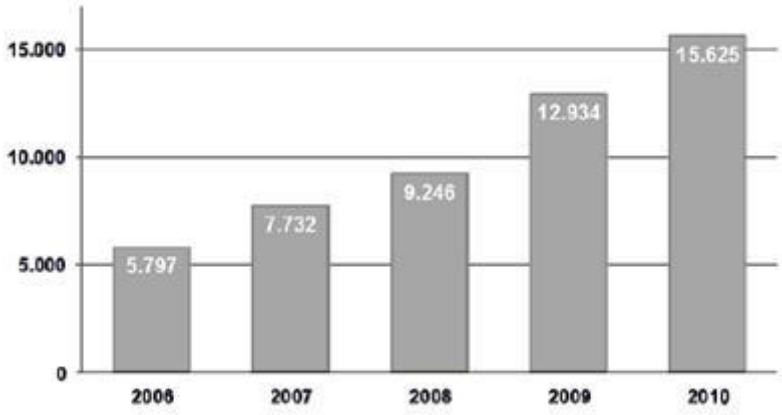

Ilustración 5 : Number of certificates accord. ISO 27001
Fuente: (Disterer, 2013)

Top Countries in 2010	
Japan	6.264
India	1.281
United Kingdom	1.157
Taipei	1.028
China	957
Spain	711
Czech Republic	529
Italy	374
Germany	357
Romania	350

Ilustración 6: Number of certificates

Fuente: (Disterer, 2013)

En la Ilustración 6, se muestra que los países que mayormente han obtenido las certificaciones ISO 27001 fueron los países Asiáticos, el autor indica que esta particularidad se evidencia debido a que la mayoría de los países Asiáticos son proveedor de servicios de externalización de TI y en el afán de brindar confianza y profesionalismo a sus mayores consumidores empresas de Europa y América del Norte, vieron la necesidad de implementar las Normas ISO 27001 obteniendo con ello documentación de conformidad con sus procesos de seguridad amparados en un estándar reconocido. Una vez más se muestra el impacto y la aceptación que ha generado la implementación de estas Normas.

Fases para la implementación de la norma ISO 27001

Para la implantación de un SGSI se van a utilizar dos normas, la UNE ISO/IEC 27001:2007 que describe, el ciclo PDCA de gestión del sistema; y la norma ISO/IEC 27002:2005 que es un guía de implantación de controles de seguridad (Audisec, 2010).

Las seis fases necesarias para la implementación de un Sistema de Gestión de Seguridad de la Información conforme a la ISO/IEC 27001 son: (Instituto Nacional de Tecnologías de la Comunicación, 2008).

1. Definir el alcance del modelo

En esta fase se establece en que campos se aplica el SGSI. Además se deberá determinar los procesos críticos para la organización decidiendo qué es lo que quiere proteger y cuál es el camino a seguir para realizar esta actividad.

Ilustración 1: Fases en la Implementación de la Norma ISO 27001
Fuente: Elaboración Propia

2. Definir una política de seguridad de la información

Su principal objetivo es recoger las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la organización y a la legislación vigente.

3. Efectuar un análisis y evaluación del riesgo

Para realizar esta tarea se deberá tener en cuenta:

- Identificación de activos y evaluación de los mismos.
- Identificación de las debilidades.
- Identificación de las amenazas.
- Valorar las consecuencias.

4. Definir opciones de tratamiento del riesgo

Gracias al análisis de riesgos conoceremos el impacto económico de un fallo de seguridad y la probabilidad realista de que ocurra ese fallo, el análisis de riesgos tiene que cubrir las necesidades de seguridad de la organización teniendo siempre en cuenta los recursos económicos y humanos con los que ésta cuenta*. **La inversión en seguridad tiene que ser proporcional al riesgo.***

5. Seleccionar controles a implementar

Los controles pueden ser seleccionados de esta norma o de otros conjuntos de control, o nuevos controles pueden ser diseñados para satisfacer necesidades específicas, según corresponda. Dependerá de las decisiones de la organización sobre la base de los criterios de aceptación del riesgo.

6. Prepara un enunciado de aplicabilidad

Consiste en un resumen de las decisiones tomadas en relación al tratamiento de los riesgos

Conclusiones

- Hay que tener claro que los riesgos de seguridad de la información están siempre presentes, lo que se pretende con la implementación de un SGSI es reducir estos riesgos mediante la implementación de un conjunto propicio de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware para reducir el impacto que podría provocar una amenaza o vulnerabilidad en la organización.
- Las políticas de seguridad de la información creadas en la organización deben estar orientadas a los objetivos de la organización.
- Los controles se deben construir, implementar, supervisar, revisar y mejorar, cuando sea necesario, es decir, deberán realizar un feedback continuo, para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización.
- Para asegurar éxito en la implementación de un SGSI se requiere el apoyo de todos los empleados en la organización. Así como de los accionistas, proveedores u otras partes externas, se deberá crear conciencia de los problemas de TI que enfrenta la organización.

Referencias Bibliográficas.

Audisec, P. B. Y. (2010). SEGURIDAD DE LA INFORMACIÓN UNE – ISO / IEC 27001 : 2007.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. doi:10.4236/jis.2013.42011

Fernández, C. M. (2010). La norma ISO 27001 del Sistema de Gestión de la Garantía de confidencialidad , integridad y Seguridad de la Información disponibilidad de la información.

Guerrero Julio, M. L., & Gómez Flórez, L. C. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. *Estudios Gerenciales*, *28*(125), 87–95. doi:10.1016/S0123-5923(12)70011-6

Hernando, V. M. A. (2008). El Derecho Informático y la gestión de la Seguridad de la Información, *29*.

Instituto Nacional de Tecnologías de la Comunicación. (2008). Implantación de un SGSI en la empresa.

Iso 27000. (2010).

TÜV SÜD Iberia, S. L. U. (2010). Iso/iec 27001.