ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 39 (Nº 18) Año 2018 • Pág. 5

Gestión de seguridad de la información con la norma ISO 27001:2013

Information security management with ISO 27001: 2013 standard

Aníbal Rubén MANTILLA Guerra 1

Recibido: 29/12/2017 • Aprobado: 15/01/2018

Contenido

RESUMEN:
Este artículo presenta un marco de trabajo para diseñar, establecer y operar un sistema de gestión de seguridad de la información, basado en las características de la organización, que permita alcanzar confidencialidad, integridad, disponibilidad y el no repudio, aportando de esta manera a la organización a alcanzar sus metas manteniendo continuidad en sus operaciones aún ante la ocurrencia de eventos catastróficos. Se tomó el estándar ISO 27001:2013 para SGSI (Sistemas de Gestión de la Seguridad de la Información) como base para la evaluación del riesgo y la aplicación de los controles necesarios para tratarlos, por cuanto es de uso global, enfocada a los procesos, y además es certificable.
Palabras-Clave: seguridad de la información, ISO 27001, gestión del riesgo

ABSTRACT:
This article presents a framework for designing, establishing and operating an information security management system, based on the characteristics of the organization, which allows to achieve confidentiality, integrity, availability and non-repudiation, thereby contributing to the organization to reach its goals maintaining continuity in its operations even before the occurrence of catastrophic events. The ISO 27001: 2013 standard for ISMS (Information Security Management Systems) was taken as a basis for risk assessment and the application of the necessary controls to deal with them, as it is of global use, focused on the processes, and it is also certifiable.
Keywords: security information systems, ISO 27001, risk management

1. Introducción

La información es un activo que como otros es esencial para la operación y negocio de una organización, por tanto debe ser protegido adecuadamente. El riesgo es la medida de la probabilidad de que una amenazada aproveche una vulnerabilidad y consiga afectar a un activo de información.

La seguridad informática se enfoca en la protección de la infraestructura de las *TIC*

(Tecnologías de Información y Comunicación) como por ejemplo: redes, impresoras, computadoras, servidores, estaciones de trabajo; mientras que la seguridad de la información se concentra en la protección de los activos de información críticos para la organización como por ejemplo: bases de datos, correos electrónicos, contratos, páginas web, documentos. Se puede manifestar que la información está asegurada cuando posee las siguientes propiedades: **confidencialidad** (la información no será conocida por individuos, entidades o procesos no autorizados), **integridad** (la información será confiable, completa, no alterada), **disponibilidad** (la información estará al alcance en el momento en que es requerida por una entidad autorizada), **no repudiación** (garantiza que quien genere un evento de forma válida no pueda retractarse, pues se puede probar la ocurrencia de un evento y quien lo origina). (Lohse, 1985)

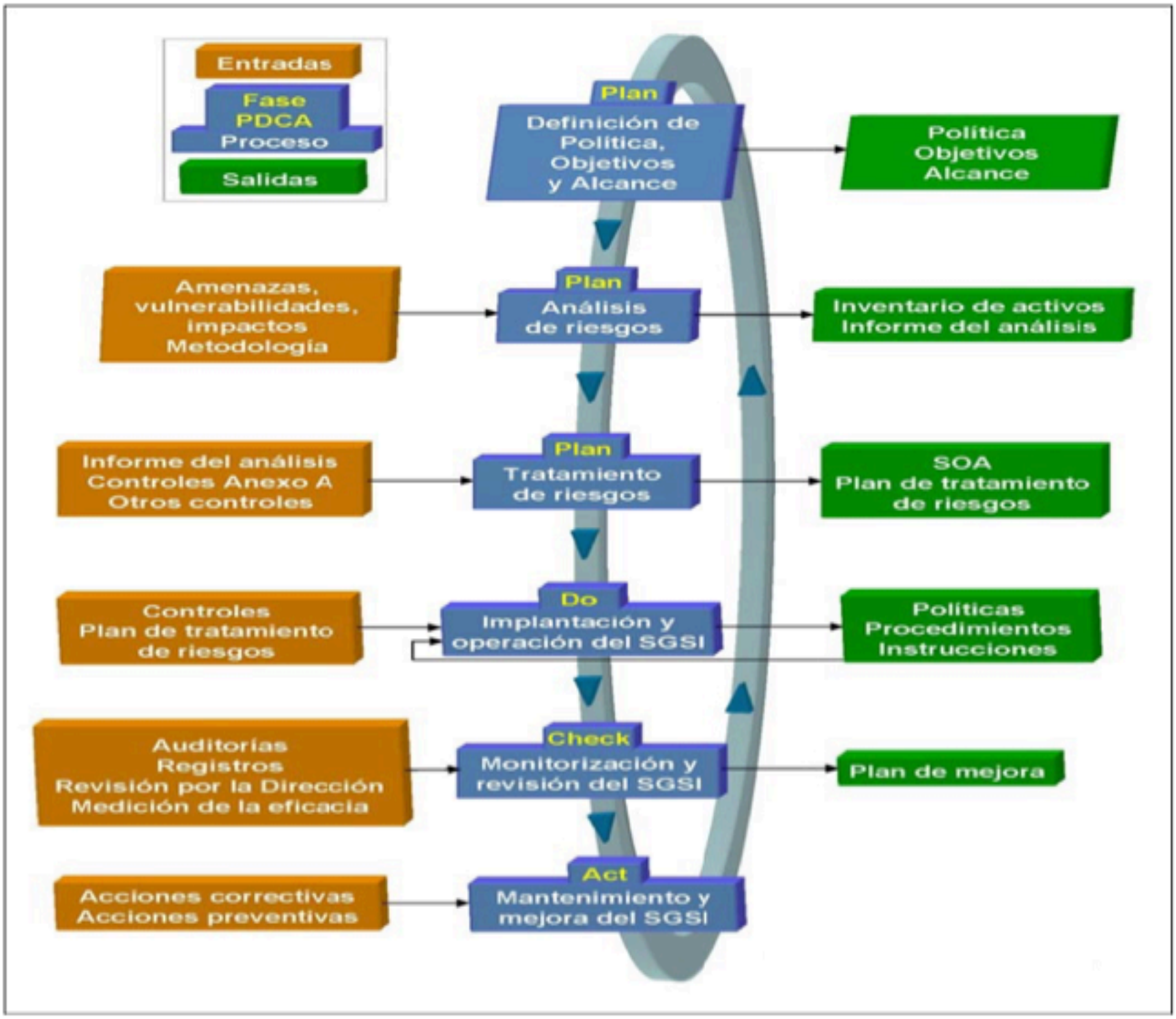
Como puede verse, el manejo de la seguridad de la información requiere una gestión integral por procesos, de los recursos humanos, recursos tecnológicos, leyes y reglamentos, en concordancia con las metas de la organización. Un sistema que realiza esto se denomina Sistema De Gestión De Seguridad De La Información, conocido por sus siglas como SGSI. (Carlo 2017).

1.1. Norma ISO 27001:2013

Es una norma desarrollada como modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un *SGSI* para cualquier tipo de organización. Permite diseñar e implantar un *SGSI*, en base a las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la organización. Esta norma ha sido estructurada metodológicamente para adaptarse al modelo "Planificar, Hacer, Verificar, Actuar" (Plan Do Check Act), el cual se aplica para estructurar todos los procesos del SGSI y tiene por objeto: establecer, gestionar y documentar el SGSI, responsabilizando a la Dirección, incluso en el monitoreo, auditoría y mejoramiento continuo. Dado que la norma ISO 27001:2013 trabaja sobre un enfoque a procesos, una aplicación detallada y puntual de la misma, requiere de un manual de procesos, completa y debidamente establecidos, definidos, documentados y validados. El correcto diseño, establecimiento y operación de un SGSI permite a la organización realizar más eficientemente sus actividades, sin embargo, si no se ha aplicado una reingeniería de procesos a la organización previa al establecimiento del SGSI, esta ralentiza sus operaciones. Esta norma tiene un total de 14 Dominios, 35 Objetivos de Control y 114 Controles. (Aginsa 2016)

La figura 1 representa el proceso de planificación, ejecución, monitoreo y control, al que el *SGSI* es llevado por el estándar ISO 27001, especificando el insumo y el producto en cada una de las etapas. ISO 27001 (2017)

Figura 1
Proceso de planificación, ejecución, monitoreo y control con ISO 27001



2. Metodología

2.1. Métodos de aplicación de la norma

Para establecer un sistema de gestión de seguridad de la información efectivo y eficiente, es necesario tener un conocimiento correcto sobre el alcance y los límites que debe poseer, en concordancia con la política de seguridad y el tamaño de la organización. De esta manera es posible realizar correctamente la identificación, análisis, evaluación y tratamiento del riesgo. (Lontsikh, 2016) El plan para el tratamiento del riesgo debe ser aprobado por la dirección de la organización, que además debe autorizar su implementación y operación con monitoreo y control permanentes. Las opciones para el tratamiento del riesgo son: mitigar, evitar, transferir, aceptar, o una combinación de estas alternativas.(Fu-Tung Wang, 2010)

Un sistema de gestión de seguridad de la información debería ser capaz de garantizar que la organización mantenga sus operaciones vitales aun en caso de siniestros y eventos de gran magnitud como por ejemplo sismos, terremotos, incendios, atentados. Para esto es necesario contar con un Plan de Continuidad del Negocio, que puede ser generado siguiendo 5 fases secuenciales tal como se presenta en la tabla 1.

Tabla 1
Fases para generar un Plan de Continuidad del negocio

FASE	ACTIVIDAD	INFORME DOCUMENTAL EN CADA FASE

I	Gestionar el riesgo	Amenazas, vulnerabilidades, niveles de riesgo y controles.
II	Analizar el impacto al negocio	Impacto al Negocio. Procesos críticos, operacionales y financieros. Requerimientos para superarlo.
III	Desarrollar el plan de reanudación de operaciones	Estrategia de Continuidad. Recursos críticos
IV	Desarrollar un Plan de Continuidad del Negocio	Plan de Continuidad del Negocio
v	Ensayar el Plan de Continuidad de Negocio	Informe de ensayo del Plan de Continuidad del Negocio

3. Resultados y Análisis

Es común que al aplicar los métodos descritos, se encuentren amenazas, vulnerabilidades y riesgos como los que se presentan en la tabla 2. Son clasificadas por áreas.

Tabla 2
Amenazas, riesgos y vulnerabilidades más comunes

TECNOLOGICA	**PROCESOS ORGANIZACIONALES**
• Computadores personales con virus • Correo electrónico usado indebidamente • Conexión a Internet para actividad no organizacional • Fuga de información estratégica de computadoras en sistemas inalámbricos	• Pérdida de información producto de infección por virus informático • Fuga de información a través del personal que ingresa en forma temporal • Gestión de Tecnologías de la Información y Comunicación • Fuga de información estratégica mediante la sustracción de computadoras • División inadecuada de espacios de trabajo • Medio de comunicación • Inexistencia de manual de procesos • Inexistencia en el organigrama a, de un departamento o persona destinado a la Gestión de la Seguridad Informática • Inexistencia de una clasificación de la información en términos de su uso • Asalto o robo • Riesgo de incendio
TALENTO HUMANO	
• Interés en obtener información estratégica de la Cooperativa, con fines políticos y económicos • Interés en obtener beneficios económicos mediante actividades fraudulentas. • Actividad Vandálica • Falta de conciencia en seguridad de la información por parte del personal de la Cooperativa • Fuga de información a través del personal • Controles inadecuados para información almacenada en computadores personales	
LEGAL	
• Existen aplicaciones sin las debidas licencias • No se cumplen normas de seguridad en la prevención y control de incendios. • No existe política de seguridad, documentada y llevada a norma.	

Una vez que ha sido determinada la capacidad del sistema para gestionar la seguridad de la información, es conveniente contrastarla con los requerimientos de la norma ISO 27001: 2013 en sus 14 dominios de control. El resultado de este proceso se representaría como se presenta en la tabla 3. (Hajdarevic 2016).

Tabla 3

Diagnóstico de la situación de la gestión de seguridad de la información en la organización

Nº	DOMINIOS DEL ESTÁNDAR IS0 27001	ALCANCE DE LA SEGURIDAD	
		Representación gráfica	Medida porcentual
1	Políticas de seguridad de la información		10%
2	Organización de la seguridad de la información		20%
3	Seguridad de los recursos humanos		60%
4	Gestión de los activos		20%
5	Control de accesos		60%
6	Criptografía		60%
7	Seguridad física y medioambiental		20%
8	Seguridad de las operaciones		60%
9	Seguridad de las comunicaciones		60%
10	Adquisición, desarrollo y mantenimiento del sistema		60%
11	Relación con proveedores		60%
12	Gestión de los incidentes de seguridad de la información		10%
13	Gestión delos aspectos de la seguridad de la información para la continuidad del negocio		20%
14	Cumplimiento		10%

Cobertura alcanzada en gestión de la seguridad de la información en el caso de estudio

Medida de la brecha existente con relación al requerimiento de la norma ISO 27001:2013

Las actividades que generalmente deberían realizarse para el tratamiento inmediato del riesgo se presentan en la tabla 4. (Nurbojatmiko, 2016)

Tabla 4

Actividades para el tratamiento del riesgo

TECNOLOGICA	PROCESOS ORGANIZACIONALES

• Adaptar la configuración de los sistemas de comunicación • Adaptar la arquitectura de red • Estandarizar y actualizar el software	• Definir políticas de seguridad • Clasificar la información • Incorporar un departamento de seguridad informática • Registrar e inventariar los accesos a los sistemas informáticos • Adaptar contratos con proveedores • Elaborar un manual de seguridad • Contratar seguros • Gestionar incidentes de seguridad • Plan de contingencias: actividades contra incendios
TALENTO HUMANO	
• Concientizar a los funcionarios y empleados de la cooperativa • Capacitar al personal en uso seguro de los servicios de internet	
LEGAL	
• Verificar el cumplimiento legal	

Resulta conveniente primero establecer planes para el tratamiento del riesgo en los procesos críticos o activos severamente amenazados, antes de iniciar una amplia reingeniería de procesos en la organización, actividad en la que se requiere la participación de muchísimas personas. (Sihwi, 2016)

---

4. Conclusiones

La norma ISO27001:2013 es una herramienta efectiva para manejar un Sistema de Gestión de Seguridad de la Información en cualquier organización, sin importar a que se dedique esta, debido a que es un tema de extrema trascendencia y permanente actualidad. Es de uso global y además es certificable.

La seguridad de la información es un aspecto, que debe ser parte de la cultura organizacional, inherente a toda actividad humana; cursos, seminarios, y talleres no bastan, hay que interiorizar en las personas de la organización, la necesidad y beneficios de dicha cultura, así como los riesgos de no tenerla.

Referencias bibliográficas

Aginsa A., Matheus I.(2016). "*Enhanced Information Security Management System Framework Design Using ISO 27001 And Zachman Framework A Study Case of XYZ Company* " in 2nd International Conference Wireless and Telematics (ICWT), Yogyakarta, Indonesia

Carlo Di Giulio C., Sprabery R. Kamhoua Ch., (2017). "*Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?* " in IEEE 10th International Conference on Cloud Computing (CLOUD). Honolulu, CA, USA.

Fu-Tung Wang F., Yun Ch., (2010). "*Information Security on RFID Based Power Meter System*"*. in* The 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010. Chengdu, China

Hajdarevic K., Allen P., and Spremic M. (2016). "Proactive *Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments*". Telecommunications Forum (TELFOR). Belgrade, Serbia.

Lohse E. (1985). "*The role of the ISO in telecommunications and information systems standardization*". IEEE Communications Magazine .Volume: 23, Issue: 1, January 18 – 24.

Lontsikh P., Karaseva V., and. Nikiforova K. (2016). "Implementation *of Information Security and Data Processing Center Protection Standards*". in IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS),. Nalchik, Russia.

Nurbojatmiko, Susanto A.,Shobariah E.(2016) . "*Assessment of ISMS Based On Standard ISO/IEC27001:2013 at DISKOMINFO Depok City*"*.* in International Conference on Cyber and IT Service Management. Bandung, Indonesia.

Sihwi S., Andriyanto F., and Anggrainingsih R. (2016). "*An expert system for risk assessment of information system security based on ISO 27002*". In IEEE International Conference on Knowledge Engineering and Applications (ICKEA), Singapore, Singapore.

-

ISO 27001 (2017). El portal de ISO 27001 en Español. Recuperado de http://www.iso27000.es/. Accedido Diciembre 2017.

---

1. Universidad Central del Ecuador, Quito – Ecuador (armantilla@uce.edu.ec)

Revista ESPACIOS. ISSN 0798 1015
Vol. 39 (Nº 18) Año 2018

[Índice]

[En caso de encontrar un error en esta página notificar a webmaster]