SCIENTIAMERICANA, Revista Multidisciplinaria
Volumen 5 Número 2, 2018

Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001

Analysis of an Information Security methodology based on ISO 27001 standards

Oscar Duarte Burgos[1]
Mario Roberto Monges Olmedo[2]

Artículo Recibido: 31/07/2018.
Aceptado para Publicación: 25/10/2018.

Resumen: La norma ISO/IEC 27001 se desarrolló con el objetivo de brindar asistencia con los requisitos de implementación para los Sistemas de Gestión de Seguridad de la Información (SGSI) de una organización determinada. El SGSI es una visión sistemática para el manejo de información en las organizaciones con el fin de que está permanezca segura y se mantenga dentro de un ambiente que respete la Confidencialidad, Integridad y Disponibilidad de la información. La información es el activo más valioso para las organizaciones, y la protección de esta es un objetivo primario para la operación del negocio. La falta de protección de la información ha provocado la fuga de datos sumamente importantes dentro de muchas organizaciones a nivel global, lo que ha provocado pérdidas irreparables en las organizaciones debido a las filtraciones que se han dado. En este trabajo se presenta una revisión bibliográfica del estándar ISO/IEC 27001/2/5, para el diseño de un sistema para la gestión de la seguridad de la información en empresas.
Palabras clave: Seguridad de Información, protección de información, ISO/IEC 27001, incidentes, riesgos.

Abstract: The ISO / IEC 27001 standard was developed with the aim of providing assistance with the implementation requirements for the Information Security Management Systems (ISMS) of a given organization. The ISMS is a systematic vision for the management of information in organizations so that it remains safe and is maintained in an environment that respects the confidentiality, integrity and availability of information. Information is the most valuable asset for organizations, and the protection of this is a primary objective for the operation of the business. The lack of information protection has led to the leakage of extremely important data within many organizations at a global level, which has caused irreparable losses in organizations due to leaks that have occurred. This paper presents a bibliographic review of the ISO / IEC 27001/2/5 standard for the design of a system for the management of information security in companies.
Keywords: Information Security, information protection, ISO / IEC 27001, incidents, risks.

INTRODUCCIÓN

El estándar ISO/IEC 27001 es una norma que se desarrolló para ayudar a definir los requisitos que permitirán establecer, implementar, mantener y mejorar continuamente la gestión de seguridad de una empresa, mediante el Sistema de Gestión de Seguridad de la Información (SGSI). El estándar ISO/IEC 27001 se puede implementar dentro de una organización para evaluar el estado de la organización en cuanto a seguridad de la información se refiere, ayudarlos a saber si los mismos podrían cumplir con sus propios requisitos en materia de seguridad de la información.

[1] Estudiante de Maestría en Tecnologías de la Información y Comunicación Facultad Politécnica de la Universidad Nacional de Asunción. San Lorenzo, Paraguay. E-mail: oduarteburgos@gmail.com
[2] Docente de la Facultad Politécnica de la Universidad Nacional de Asunción. San Lorenzo, Paraguay. E-mail: mario.monges@gmail.com

El objetivo primario que tiene un SGSI es brindar conocimientos acerca de cómo dar un correcto tratamiento a la información circundante dentro de la organización, manteniendo los principios de Confidencialidad, Integridad y Disponibilidad, para que todo activo digital se mantenga seguro apoyado en una normativa estándar de seguridad y por supuesto gestionado por personal calificado en materia de seguridad de la información y utilizando herramientas que ayuden a la gestión antes mencionada.

Dentro de toda organización es prioritario el mantener toda información circundante dentro de la misma, enmarcada con los estándares de calidad referentes a seguridad de la información, con el fin que dicho activo (la información) se mantenga dentro del Confidencialidad, Integridad y Disponibilidad. Así mismo es de saberse que muchas organizaciones (sean grandes, medias o pequeñas) no están conscientes de los riesgos que corren al no tener los controles de seguridad definidos y aplicados.

De ahí que, para minimizar los riesgos de la información, existen los Sistemas de Gestión de Seguridad de la Información, que no son más que estudios y análisis de la situación actual de la organización aplicados dentro de un marco normativo que trabaja sobre entre otros puntos con la gestión de riesgos de la institución, cuya finalidad es la de verificar el nivel de seguridad de dicha organización y proponer controles para mitigar los riesgos a los que está expuesto dicha organización.

La frecuente ocurrencia de eventos con relación a riesgo operacional hace que dichos eventos generen pérdidas económicas, daño de imagen a las organizaciones, los cuales muestran cuan desprotegidas están las instituciones en cuanto a la efectividad de las actividades de control que se realizan en las mismas. Para paliar las constantes vulnerabilidades que existen en el medio empresarial, al no aplicar correctamente una gestión de riesgos, la norma ISO brinda las orientaciones para una correcta implementación del SGSI organizacional y por consiguiente para el correcto manejo de la seguridad de la información.

TEORÍA DE ESTÁNDARES APLICADOS

Los estándares utilizados para la realización del presente trabajo están basados en estándares ISO, más específicamente estándares de la familia ISO/IEC 27000 (www.iso.org)

A continuación, se expondrán las ISO que se utilizaron en este trabajo:

NP ISO/IEC 27001

Este es el estándar internacional propuesto por la International Organization for Standarization (ISO) que proporciona el modelo para establecer, implementar, monitorear, revisar, mantener y mejorar un SGSI dentro de cualquier organización (Information technology - Security techniques). Este estándar indica las acciones que se tienen que llevar a cabo dentro de la organización para poder alinearse a los requerimientos que tiene un SGSI, esta norma fue nacionalizada en nuestro país por la INTN en el año 2014 pasando a ser la Norma Paraguaya ISO 27001:2014

En la norma de NP ISO/IEC 27001 se utiliza el modelo de PDCA (Plan-Do-Check-Act), lo que sería lo mismo decir Planear-Realizar-Chequear-Actuar) como base para la mejora continua en todo lo referente al SGSI a implementar que habla este estándar. Podemos enfatizar que este modelo de PDCA toma como entradas las expectativas de las partes interesadas de la organización en materia de seguridad de la información y produce una salida de seguridad de la información que satisfaga a las partes interesadas (Figura 1).

Figura 1. Ciclo de PDCA (Corvo, Teofilo Sy, 2018).

FASE DE LA NORMA INP SO/IEC 27001

La norma ISO/IEC 27001 establece los lineamientos para la correcta administración, comprensión y uso de las tecnologías de la información como un método para facilitar el poder alcanzar los objetivos del negocio de manera eficiente, lo que conlleva el requerimiento de conocer los riesgos actuales, emergentes y el impacto que tendría en la organización el impacto de dichos riesgos (Norma Paraguaya ISO 27001, 2013). La implementación de los Sistemas de Gestión de la Seguridad de la Información en las organizaciones está basada en las necesidades, objetivos, procesos, tamaño, estructura y requerimiento de seguridad únicos de cada organización (Shojaie, 2014).

La norma ISO/IEC 27001 se divide en siete fragmentos o fases para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) siguiendo sus controles, tal como se demuestra a continuación en la figura 2.

Figura 2. Fases del SGSI (Normativa Técnica de Colombia ISO 27001, 2006).

NP ISO/IEC 27002

Este es el estándar internacional que establece los lineamientos generales y principios para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización (Norma Paraguaya ISO 27001, 2013). Esta norma nos brinda un marco de control necesarios para la implementación de un sistema de gestión de seguridad de la información (SGSI), además posee 14 cláusulas de control de seguridad y cada una posee un número determinado de categorías de seguridad principales, así mismo cada una de las categorías de seguridad tiene un objetivo de control que demuestra cual es la finalidad que quiere alcanzar y los controles que se pueden aplicar para lograr dicho objetivo. Las cláusulas de controles junto a la Introducción se desglosan en la figura 3:

1. Política de Seguridad
2. Organización de la Seguridad de la Información
3. Seguridad de RRHH
4. Gestión de Activos
5. Control de accesos
6. Cifrado
7. Seguridad Física y ambiental
8. Seguridad en la operativa
9. Seguridad en las Telecomunicaciones
10. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
11. Relaciones con suministradores
12. Gestión de incidentes en la seguridad de la información.
13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14. Cumplimiento

Figura 3. Secciones de la ISO 27001 (Norma Paraguaya ISO 27001, 2013).

ISO/IEC 27005

Este estándar internacional provee las directrices para la gestión de los riesgos de la seguridad de la información de acuerdo con la norma ISO/IEC 27001.

Es compatible con los conceptos generales especificados en ISO / IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminologías descriptos en ISO/IEC 27001/2 es sumamente importante para una correcta comprensión de la ISO/IEC 27005.

La normativa estándar ISO/IEC 27005 es aplicable a todo tipo de organizaciones (por ej. Empresas pequeñas, medias o grandes, así como instituciones gubernamentales, entre otras) que pretendan gestionar los riesgos que podrían comprometer la seguridad de la información de la organización (Norma Paraguaya ISO 27001, 2013).

La norma ISO/IEC 27005 se compone de 12 ítems que son:

- Alcance
- Referencias normativas
- Términos y definiciones
- Estructura de la norma
- Background
- Resumen del proceso de la gestión de riesgos de SI
- Establecimiento del contexto
- Evaluación de riesgos
- Tratamiento de riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo del riesgo

Esta norma suministra directrices para la gestión del riesgo en la seguridad de la información y brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

Es necesario un enfoque sistemático para la gestión del riesgo en la seguridad de la información para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información y para crear un sistema de gestión de la seguridad de la información (SGSI) eficaz según a figura 4.

Figura 4. Proceso de la gestión de riesgos de seguridad de información (Normativa Técnica de Colombia ISO 27005, 2006).

MARCO DE EVALUACIÓN

El estándar normativo de la ISO/IEC 27001 es quien nos proporciona una orientación acerca de la elaboración y uso de las medias para evaluar la eficacia de un Sistema de Gestión de la Seguridad de la Información (SGSI), siendo las mismas aplicadas a la medición de controles o conjuntos de controles para llevar a cabo la correcta implementación y medición del SGSI, sin embargo en la normativa, no se describen ni se especifican las maneras para medir o evaluar la efectividad de los controles implementados dentro de la organización, solo se limitan a exigir el cumplimiento y la posterior evaluación de los controles del Sistema de Gestión de la Seguridad de la Información.

El modelo que proponemos para este trabajo es definir correctamente el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) con las autoridades de la organización, una vez definido correctamente el alcance, procederíamos a realizar los relevamientos necesarios utilizando los métodos de observación, encuesta, entrevistas entre otros métodos para elaborar un bosquejo de la situación actual de la organización y su estado en cuanto a seguridad de la información.

Definido lo citado líneas atrás, realizaremos las tareas necesarias para ejecutar el trabajo de diseño de la metodología para la organización.

IMPLANTACIÓN DE LA NORMA NP ISO/IEC 27001

A la hora de implantar el Sistema de Gestión de Seguridad de la Información (SGSI), debemos de tener en cuenta y considerar como eje principal el sistema de Gestión de Riesgos, que es quien nos indicará el estado en que se encuentra la organización.

La acción de tener una evaluación de riesgos permitirá a la alta dirección de la organización tener la visión necesaria para definir el alcance y el ámbito de aplicación de la norma

ISO/IEC 27001, así como la facilidad para definir las políticas y medidas a implementar en la organización, que a su vez se verá beneficiada con la integración del sistema de mejora continua que promulga esta normativa estándar.

El primer paso, es elegir una metodología para evaluar el riesgo de la organización de forma apropiada según los requerimientos de misma organización.

Si bien es cierto existen numerosas metodologías estandarizadas para la evaluación de riesgos, nosotros nos centraremos en la normativa estándar de la ISO/IEC 27005, y cuyas fases explicaremos a continuación (Figura 5).

Figura 5. Método de Evaluación y Tratamiento de Riesgos (Trujillo, 2013).

Fase 1. Identificación de activos y de sus responsables, es entendiendo a todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificio, servidores, equipos de comunicación, etc.) así como material a fin al negocio (como ser informes, software, proyectos, diseño, etc.) así como la reputación y la marca por citar algunas.

Fase 2 Identificación de Vulnerabilidades de cada activo de información que posee la organización, que no es más que identificar aquellas debilidades propias de dichos activos que pueden subir algún ataque o daño.

Fase 3 Identificación de las amenazas de los activos, que no son más que las acciones que puede suceder y dañar el activo de la organización provocando por ende un impacto negativo en la misma.

Fase 4 Identificación de los requisitos legales y contractuales en los que la organización está enmarcada para con sus clientes, socios o proveedores de servicios.

Fase 5 Identificación del impacto o identificación de riesgos, que no es más que la definición por cada activo, la probabilidad de que las amenazas o vulnerabilidades se concreten y de esta manera dañar dicho activo de información perjudicando a la organización.

Fase 6 Seleccionar e implementar controles, en esta fase se realiza después de contar con la probabilidad de ocurrencia del riesgo y el impacto que tendrá una vulnerabilidad explotada en la organización.

Fase 7 Tratamiento de riesgos, en este punto estamos preparados para definir las acciones de tratamiento de los riesgos en función de los puntos anteriormente citados y acompañado por la política que la alta dirección de la organización ha aprobado. En el tratamiento de los riesgos se puede asumir el riesgo, reducir el riesgo, eliminar el riesgo o transferir el riesgo de cada activo de información de la organización.

BENEFICIOS DE IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE UNA ORGANIZACIÓN

El principal beneficio que se logra al implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) es estar preparados para mejorar la gestión de seguridad de la información en la organización.

Es por esto por lo que debemos estar conscientes que con una buena gestión de riesgos lograríamos el conocimiento preciso para poder manejar los riesgos, las amenazas y las vulnerabilidades para dotar a la organización de los recursos necesarios para salvaguardar sus activos de información.

Dicho de otra manera, podríamos ver a un sistema de gestión de la seguridad de la información (SGSI) como un enfoque sistemático para la gestión de información de carácter confidencial en la organización para que la misma siga siendo segura, la cual abarca personas, procesos y activos de TI.

El implementar un SGSI con la ayuda del estándar ISO/IEC 27001 dará confianza a clientes internos y externo en cuanto a lo referente de la seguridad de la información y mostrará un compromiso con la seguridad, mostrando estar a la vanguardia en la aplicación de la técnica de procesos para hacer frente a las amenazas de la información y problemas de seguridad.

CONCLUSIÓN

El modelo de trabajo propuesto nos permite recopilar la información necesaria para disminuir la valoración subjetiva de la que es vulnerable el sistema de gestión de seguridad de la información (SGSI) y sus posteriores auditorias.

Además, este modelo de Sistema de Gestión de la Seguridad de la Información (SGSI) se apoya para su implementación en las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, donde gracias a estos estándares es posible identificar controles claves para una pronta y correcta implementación del SGSI.

Adicionalmente a esto, una de las grandes ventajas de tener un sistema apoyado en estándares internacionales es que dicho modelo de base de conocimiento puede crecer exponencialmente y de esta manera logramos mantener la calidad del sistema de gestión de seguridad de la información (SGSI) mediante la mejora continua de los controles aplicados.

REFERENCIAS BIBLIOGRÁFICAS

Calder, A. (2003) Implementing Information Security based on ISO 27001/27002

Normativa Técnica de Colombia ISO 27001. 2006.

Norma Paraguaya ISO 27001. 2013.

ISO/IEC 27001:2005 Information technology - Security techniques

Corvo, T. (2018). Círculo de deming: Etapas, ventajas, desventajas y ejemplo. Recuperado de: https://www.lifeder.com/circulo-deming/

Trujillo, L.M. (2013). Guía de aplicación de la ISO 27001. Recuperado de: https://ofiseg.wordpress.com/tag/guia-de-aplicacion-de-la-iso-27001/

Susanto, H., Almunawar, M., Tuan, Y. Information Security Management System Standards.

Shojaie, B., Federrath, H., Saberi, I. (2014). Evaluating the effectiveness of ISO 27001:2013.

Hajdarevic, K., Allen, P. (2015). A new method for the identification of proactive information security management system metrics.