Sistema de gestión de seguridad de la información SGSI

Gómez Orozco, Angélica.
anginza@gmail.com
Universidad Piloto de Colombia

Resumen— Un sistema de gestión es un conjunto de procesos que ayudan a lograr los objetivos de la organización mediante estrategias, optimización de procesos, operaciones y servicios. Un Sistema de Gestión de la seguridad de la Información (SGSI) es el conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos a los que están expuestos. En este documento haremos una breve descripción del estándar para la implementación de un SGSI y una forma de mejoramiento continuo al sistema como lo es la auditoria.

Abstract— A management system is a set of processes that help achieve organizational objectives through strategies, process optimization, operations and services. A Management System of Information Security (ISMS) is the set of processes to efficiently manage the accessibility of information, seeking to ensure the confidentiality, integrity and availability of information assets while minimizing the risks to which they are exposed. In this document we make a brief description of the standard for the implementation of an ISMS and a form of continuous improvement to the system as it is the audit.

Palabras clave— Activo, Auditoria, Información, Seguridad, Sistema de gestión.

Keywords— Active, Auditing, Information, Management System, Security.

I. INTRODUCCIÓN

Hoy en día, con el desarrollo acelerado que presentan las empresas en sus diferentes campos de acción, la información se ha transformado en el activo más valioso e importante para el desempeño adecuado de sus actividades diarias. Es tal su importancia que se recomienda establecer Sistemas de Gestión de Seguridad de la Información (SGSI) para su protección.

Este sistema facilita a la entidad la identificación de los factores que ponen en riesgo el ejercicio de su actividad y cómo pueden llegar a ocasionar traumatismos, pérdidas económicas, físicas y de imagen corporativa. Así mismo, permite tomar las medidas necesarias que la encaminen nuevamente en su misión para continuar con la meta financiera y de posicionamiento que toda empresa busca en el sector económico en el cual se encuentra ubicada.
Tomando como referencia lo anterior, una organización puede adaptar estándares que sirvan de guía para la gestión de la información. En este artículo hablaremos del estándar ISO 27001, el cual establece una metodología para planear, implementar, mantener y mejorar un sistema de gestión de seguridad de la información, así como también tendremos en cuenta los proceso de auditoría.

II. SEGURIDAD DE LA INFORMACIÓN

Cuando hablamos de seguridad de la información se piensa primero en qué pasaría, qué efecto o pérdidas causaría si la información que manipulamos a diario en nuestra organización cae en manos de personas malintencionadas, que nuestra infraestructura pueda sufrir algún tipo de ataque o daño o, simplemente, que perdiéramos nuestra información.
Es así como llegamos a considerar que si queremos que nuestra información esté protegida debemos garantizar su confiabilidad, integridad y disponibilidad, características esenciales de un SGSI que nos permitirá minimizar el riesgo. Para tener claro el tema se define cada una de estas características así:

- Confidencialidad: La propiedad para que la información esté disponible y no sea

divulgada a personas, entidades o procesos no autorizados.
- Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- Integridad: propiedad para guardar la exactitud e integridad de los activos.

Como se ha mencionado varias veces, la seguridad total no existe, sólo podemos minimizar los riesgos a los que están expuestas las organizaciones empleando metodologías de acuerdo a su estructura y negocio.

III. Sistema de gestión de seguridad de la información

La ISO/IEC 27000 es una serie de estándares que sirve para desarrollar, mantener e implementar un sistema de gestión de la seguridad de la información (SGSI) entre los cuales tenemos:

ISO/IEC 27000: contiene los términos y definiciones que se emplean en la serie 27000.
ISO/IEC 27001: norma principal de la serie y la que específica los requisitos necesarios para la implantación del SGSI. Está centrada en la mejora continua de los procesos y de la gestión de riesgos.
ISO/IEC 27002: guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información.
ISO/IEC 27003: guía de implementación de un SGSI e información acerca del uso del modelo PDCA y de los requerimientos en sus diferentes fases.
ISO/IEC 27004: específica las métricas y técnicas de medida aplicables al SGSI y de los controles relacionados.
ISO/IEC 27005: establece las directrices para la gestión del riesgo con relación a la seguridad de la información.
ISO/IEC 27006: especifica los requisitos para la acreditación de entidades de certificación de SGSI y auditoría.
ISO/IEC 27007: establece las directrices para la gestión de los sistemas de seguridad de la información de auditoria.

IV. ISO/ IEC 27001

El estándar para la gestión de seguridad de la información ISO/IEC27001 (Information technology - Security techniques - Information security management systems - Requirements) específica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) según el Ciclo de Deming – PDCA. Fig.1

Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Fig. 1 Esquema del Ciclo PDCA

Pero, ¿qué entendemos por PDCA? Esta es una metodología para realizar actividades de mejora continua aplicable a cualquier actividad que se realice en la organización.

El ciclo consta de 4 fases: planificar, hacer, verificar y actuar. Estas etapas son también aplicables a cada una de las fases de desarrollo del Sistema de Gestión de Seguridad de la Información de la siguiente manera:

- PLAN (Planificar): Establecer los objetivos y procesos necesarios para obtener los resultados. Se traduce en instaurar el SGSI.
- DO (Hacer): Implementar los nuevos procesos. Es la ejecución del SGSI.
- CHECK (Verificar): Recopilar de nuevo datos de control y analizarlos para evaluar si se ha producido el cambio esperado. Es verificar y evaluar el SGSI.
- ACT (Actuar): Tomar las acciones correctivas

y documentar el ciclo. Es mantener y mejorar el SGSI.

El objetivo de esta norma, como ya se mencionó, es establecer las especificaciones para que una organización desarrolle e implemente un SGSI y así obtenga la certificación en Gestión de la seguridad de la información, permitiendo constituir una confianza frente a terceros llámense estos clientes proveedores o usuarios que entienden la importancia de su información y que establece controles y medidas para mantener su confidencialidad, integridad y disponibilidad. *[1]*

A. Establecer el SGSI

De acuerdo a la norma, debemos definir los alcances de nuestro sistema partiendo de las características del negocio, objetivo y organización, entre otros. Además, definir una política de seguridad clara, práctica, general sin comprometerse con tecnologías específicas, que atiendan los requerimientos legales o reguladores. Es de aclarar que esta política debe ser aprobada por los directivos o alta gerencia antes de iniciar la implementación del sistema. En este punto también se define la gestión de riesgos, teniendo en cuenta que la metodología de valoración que utilicemos nos produzca resultados medibles para gestionar los controles necesarios y así minimizar el riesgo al que la organización está expuesta.

En el marco de la gestión de riesgos tenemos que:

- Identificar los activos a proteger.
- Identificar sus amenazas, vulnerabilidades y el impacto que tengan frente a la organización.
- Calcular el impacto, la probabilidad de ocurrencia y el nivel de riesgo.
- Identificar y evaluar las opciones para el tratamiento del riesgo, aquí la norma ISO/IEC 27001 nos presenta 4 opciones; aplicar los controles apropiados, aceptar el riesgo, evitar los riesgos y transferir el riesgo.
- Seleccionar los controles a aplicar.

Una vez realizadas las actividades descritas anteriormente tenemos que contar con la aprobación y autorización de la alta gerencia para seguir con la implementación del SGSI.

B. Implementar y operar el SGSI

Para la implementación del SGSI la norma ISO/IEC 27001 nos pide un plan de gestión del riesgo que tendrá en cuenta la acción de la gerencia, los recursos disponibles para el desarrollo de las actividades requeridas, las responsabilidades y prioridades para el manejo de los riesgos. Para ello, nos da, en el numeral 5.0, unas acciones que se deben ejecutar las cuales van desde el compromiso que tiene la alta gerencia hasta el usuario final, quien puede ser empleado, cliente o proveedor. *[1]*

Aquí quiero detenerme y resaltar que en el SGSI no solamente se están protegiendo los sistemas de los delincuentes sino de simples fallas producidas por el mismo personal de la empresa. Fallas que pueden ocasionar un gran caos o pérdidas a gran escala. A pesar del esfuerzo que realizan las empresas con sus empleados con capacitaciones, charlas de seguridad, informándolos sobre el sistema que se va a implementar, esto para ellos pasa como si nada pues no aplican lo aprendido y más se demoran en salir a continuar con su trabajo del día a día que producir una falla de seguridad. Puede ser negligencia del personal, resistencia al cambio o, simplemente, que no ‘tienen la camiseta puesta’ y de esta manera ponen en peligro tanto la seguridad de la empresa como la de los clientes pues la información confidencial anda desprotegida.

Esto es una invitación a que si en su empresa implementaron o van a implementar este tipo de sistemas hay que sensibilizarse y colaborar con todas las medidas adoptadas, por el bienestar propio y el de la empresa logrando así un objetivo común: nuestra seguridad.

C. Monitorear y revisar el SGSI

En esta etapa se evalúa que las gestiones realizadas en los pasos anteriores sean las correctas. Es decir, que en caso de que suceda algo los controles y medidas adoptadas surtan el efecto esperado. Hay que tener en cuenta que cada vez que

se produzca un cambio en la organización ya sea a nivel de estructura, tecnológico, de eventos externos, entre otros, debemos revisar nuevamente el nivel de riesgo y, de ser posible, implementar nuevos controles o medidas de seguridad.

Una manera de evaluar esta gestión es realizar auditorías al SGSI que nos permita conocer si el sistema implementado se está ejecutando de manera correcta o, si por el contrario, requiere de ajustes.

D. Mantener y mejorar el SGSI

Finalmente, tenemos el proceso de mantener y mejorar el SGSI que es aplicar las mejoras a nuestro sistema, realizar las acciones correctivas y preventivas asegurando que estas nos conlleven a alcanzar los objetivos para los cuales se diseñó el plan de gestión de seguridad.

Hay que tener en cuenta que estos procedimientos deben estar debidamente documentados, registrados, según los dispone la norma ISO/IEC 27001 en su numeral 4.3.3. *[1]*

Cabe resaltar que se debe estar siempre a la vanguardia y buscar los métodos de prevenir los riesgos pues los delincuentes están al acecho mejorando su modus operandi, buscando actualizarse en cómo ingresar, vulnerar un sistema, sacar provecho de la información bien sea para ganar retos propuestos entre ellos mismos o para causar daño a las personas u organizaciones.

Como reza la frase aquella de que ‘la cadena se rompe por el eslabón más débil’, en seguridad de la información se puede aplicar haciendo referencia al personal de la organización. Por eso es importante recalcar que la efectividad del SGSI comienza por ellos mismos debido a que por más tecnología que se adopte y programas de seguridad que se implementen si ellos no tienen una cultura de seguridad, no conocen los riesgos a los que está expuesta su actividad y el impacto que pueda tener, todo esfuerzo será en vano permitiendo que poco a poco se destruya la confianza que depositamos en los sistemas de información. *[2], [3]*

V. AUDITORIAS

Como apoyo a la implementación de este sistema, la norma ISO/IEC 27001, en su numeral 6, nos brinda orientación acerca de la realización de auditorías planeadas con el fin de determinar si los procesos, procedimientos y controles establecidos cumplen con los objetivos propuestos, si son efectivos o requieren de acciones de mejora. Esta auditoria bien puede ser interna que son las realizadas por la propia organización con propósitos internos o externas también llamadas auditoría de tercera parte que son las que realizan las organizaciones auditoras externas, bien sea porque ofrecen un registro o certificación de conformidad con los requisitos de la norma.

Las auditorias se componen de 4 fases

- Planeación: conocimiento y entendimiento de los procesos de la organización.
- Análisis: analizar y evaluar los procesos y controles establecidos para determinar su efectividad.
- Informe: informan de resultados, conclusiones y recomendaciones como oportunidad de mejora al sistema auditado.
- Seguimiento: se realiza para evaluar el nivel del cumplimiento y el impacto de las recomendaciones hechas.

En la fase *planeación* se debe tener en cuenta la estructura organizacional, normas y políticas, disposiciones legales, controles internos y toda la información requerida para conocer el estado de la organización, criterios de evaluación. Así mismo se decide el alcance de la auditoria, que se va a hacer, cuantos procedimientos se van a realizar, en que tiempo y se asignan los responsables y recursos de cada proceso con el fin de lograr el objetivo de la auditoria que para nuestro caso se trata de asegurar la confiabilidad, disponibilidad e integridad de la información.

Durante el *análisis* de los procesos se debe tener en cuenta aspectos administrativos, legales, económicos y tecnológicos permitiendo identificar en todos los aspectos las falencias que pueda tener la organización que ha implementado un sistema de gestiona de seguridad de la información.

Existen diferentes técnicas a aplicar en una auditoria entre las que podemos mencionar las

entrevistas, observación, muestreo, registros y revisión, en este punto es importante resaltar que el auditor debe tener ciertas características de manera que cuando esté realizando la auditoria sus actitudes o palabras no interfieran en las respuestas o posibles hallazgos y así se pueda perder la tarea realizada. Una vez obtenida todas las evidencias se compararan con los criterios seleccionados y de esta manera obtener los hallazgos los cuales nos dirán que está cumpliendo la organización frente a la gestión y objetivos propuestos en nuestro SGSI.

Estos hallazgos se pueden clasificar como Conformidad, No conformidad y observación.

- Una conformidad: es cuando el control auditado cumple con el propósito para el cual fue establecido.
- No conformidad: Se presenta cuando no hay cumplimiento del control, la norma u objetivo que se estableció.
- Observación: es lo que el auditor plasma en el documento para indicar una oportunidad de mejora y evitar que se produzca a futuro una no conformidad.

Informe aquí es donde se reúnen los responsables de realizar la auditoria para recopilar los hallazgos obtenidos, evaluar esta información y definir las no conformidades que serán informadas a la alta dirección, este debe ser de manera clara, entendible, no debe contener vocabulario técnico, críticas hacia la organización ni información confidencial. Debe indicar la metodología para obtener y analizar la evidencia, resultado de dichos análisis, los hallazgos, conclusiones y recomendaciones y finalmente la firma de quien realiza la auditoria.

Seguimiento, estas son auditorias que se realizan para verificar que las recomendaciones dadas en la auditoria inicial se aplicaron correctamente y el sistema funciona de manera eficiente y eficaz. *[4], [5]*

VI. Conclusiones

Las organizaciones al tener identificada la información más relevante de su negocio ha buscado mecanismos que le ayuden a la administración adecuada de la misma, adoptando métodos como la norma ISO/IEC 27001 en la cual encontramos lineamientos que facilitan la aplicación de políticas, procesos y procedimientos de seguridad de la información.

Por ello es sumamente importante que a pesar del fenómeno de globalización y avance de las diferentes tecnologías y el afán de las compañías en solo obtener una rentabilidad a los accionistas, se miren los diferentes escenarios a los cuales se puede exponer y concientizar al público en general que la seguridad de la información en lugar de ser un gasto es una inversión para proteger el patrimonio de la organización.

Reconocimiento

La autora agradece al Ingeniero Álvaro Escobar Director de la Especialización en Seguridad Informática por la colaboración para la presentación de este documento.

Referencias

[1] Instituto Colombiano de Normalización y Certificación. *Sistemas de gestión de seguridad de la información. NTC-ISO/IEC 27001:2005*. Bogotá D.C

[2] Jesús Sánchez Echeverría, (2005) *Gestión de la seguridad de la información*. [En línea]. Disponible en: http://www.degerencia.com/articulo/gestion_de_la_seguridad_de_la_informacion

[3] Álvarez Marañón Gonzalo; Pérez Pedro Pablo, "*Seguridad informática para empresas y particulares.*", Editorial McGraw-Hill Interamericana, p. 29 – 38, 2004.

[4] Nubia Fernández Grajales, (2005), *Importancia de la auditoría informática en las organizaciones*. [En línea]. Disponible en: http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.html

[5] *Information Systems Audit and Control Association*. [En línea]. Disponible en: http://www.isaca.org.mx/

Autor

Angélica Gómez Orozco, Ingeniera de sistemas de la Escuela Colombiana de Carrera Industriales, estudiante de Especialización de Seguridad Informática de la Universidad Piloto de Colombia. Actualmente se desempeña en el cargo de analista en la Equidad Seguros.

Áreas de interés: Sistemas de gestión, Seguridad informática, y seguros.

E-mail: anginza@yahoo.es