METODOLOGÍA ÁGIL DE ESTABLECIMIENTO DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADOS EN ISO/IEC27001

J. S. Borbón Sanabria, Ingeniero de sistemas Universidad Distrital Francisco José de Caldas
Recibido Noviembre 10, 2011- Aceptado Febrero 23, 2012
http://dx.doi.org/10.18566/puente.v6n1.a03

***Resumen*— La conformación de sistemas de gestión de seguridad de la información es un procedimiento complejo y extenso al interior de toda organización. Ajustarse a la guía de estándares tales como ISO 27000 ya no es suficiente, es por ello que se propone complementar dicha metodología con manuales, guías y certificaciones con el fin de estructurar de forma eficaz, eficiente y ágil políticas y planes de seguridad de la información.**

***Palabras clave*— Seguridad de la información, política, plan, control, seguridad, metodología, ISO/IEC 27001, riesgos.**

***Abstract*— Create an information security management system is a complex and extensive procedure inside of an organization. Use only ISO/IEC 27001 standard to create a management system is not enough. Because of that this work takes advantage of some others methodologies, manuals, guidelines and certifications to create a new effective, efficient and agile methodology to design information security politics and plans.**

***Keywords*—Information security, politic, plan, control, security, methodology, ISO/IEC 27001, risk.**

I. INTRODUCCIÓN

Los tres objetivos fundamentales de la seguridad de la información permiten establecer un marco de referencia a través del cual se puede identificar el grado de aseguramiento de los activos de una organización, siendo la información el activo más valioso. El lograr niveles altos o en su defecto aceptables para confidencialidad, integridad y disponibilidad requieren la implementación de controles, medidas y acciones de tipo disuasivo, preventivo y correctivo en caso de ocurrencia de eventos o actividades que puedan afectar la seguridad de la información, por otra parte, subsanando la necesidad de reducir niveles de riesgo llegando a un punto aceptable para la organización.

El proceso asociado a la conformación de un sistema de gestión de seguridad de la información (SGSI), implica la realización de revisiones de procesos por área, establecimiento del panorama de riesgos, creación de políticas para su cumplimiento y educación hacia el recurso humano, aplicación de controles físicos y lógicos, el establecimiento de una política general para la seguridad de la información y finalmente su cumplimiento a través de planes de seguridad y ejecución de los controles asociados.

El anterior proceso se encuentra basado en el cumplimiento del estándar internacional ISO/IEC 27001[1], a través del cual una organización puede certificar sus procesos relacionados con la seguridad de la información y asociado al cumplimiento de los objetivos y controles propuestos por este estándar.

A pesar de la claridad del estándar ISO/IEC 27001 acerca de los objetivos y tipos de controles que deben cumplirse al interior del SGSI, no se estipula el como deben establecerse los controles, dejando un vacío que puede conducir a una implementación que descuide puntos cruciales en virtud de la seguridad de la información.

A partir de lo anterior en el trabajo desarrollado al interior de la Universidad Distrital Francisco José de Caldas[2], se diseñó y construyó una metodología ágil para la conformación de planes de seguridad estableciendo a través del uso de guías, metodologías, estándares y certificaciones un marco de referencia complementario que permite a una organización, la conformación de su SGSI, asegurando fortaleza sobre aquellos puntos que el estándar ISO/IEC 27001 no aborda a fondo, como lo son el manejo del riesgo, clasificación de la información, comercio electrónico, criptografía y hacking ético.

[1] J. Borbón Sanabria Ingeniero de Sistemas de la Universidad Distrital Francisco José de Caldas 2011. e-mail: jeffto@eljeffto.com.

II. UNA NUEVA METODOLOGÍA

La metodología diseñada cuenta con una estructura creada a partir de la experiencia en procesos de auditorías a organizaciones. Estas auditorías han sido orientadas a normas tales como ITIL [3] y la misma ISO/IEC 27001 en conjunto con un proceso de auditoría desarrollado con la Red de datos de la Universidad Distrital Francisco José de Caldas entre el año 2008 y 2009. Las dificultades de la implementación de un SGSI se ven representadas en la falta de profundidad o recomendación de actividades a realizar dentro de cada control, haciendo referencia al numeral A del estándar ISO/IEC 27001.

A su vez y siguiendo el marco de referencia estipulado por el estándar ISO/IEC 27001, la metodología se aborda a través de la aplicación del ciclo Deming [4] o también conocido como PHVA (Planificar, Hacer, Verificar, Actuar) el cual es aplicado de la siguiente forma:

"*PLANEAR:* Diseñar o revisar procesos que soportan servicios de tecnologías de la información.

HACER: Implementación del plan y gestión de los procesos.

VERIFICAR: Medición de los procesos y de los servicios de tecnologías de la información, comparación con los objetivos marcados y generación de informes.

ACTUAR: Planificación e implementación de cambios para la mejora de los procesos." [5]

Sin embargo, dada la finalidad de la metodología desarrollada, la organización aún no cuenta con un SGSI, por consiguiente los procedimientos y pasos a seguir se orientan hacia la creación del mismo y no a su manutención y mejora continua, como ocurre con ISO/IEC 27001. Es por ello que se plantea una modificación para ser abordado de la siguiente forma:

PLANEAR: Identificar y seleccionar las áreas a analizar y que serán incluidas dentro de los dominios de los procesos parte del SGSI.

HACER: Desarrollar actividades de peritaje, análisis y evaluación a nivel de amenazas, vulnerabilidades y riesgos a nivel de recursos humanos, físicos, lógicos y activos de la organización

VERIFICAR: Aplicar correctivos de fallas, amenazas y vulnerabilidades identificadas a nivel físico y lógico.

ACTUAR: Establecer la política de seguridad y los planes de seguridad a través de los cuales se busca el cumplimiento de la política que debe estar alineada con la norma ISO/IEC 27001.

De esta manera una vez establecida la política y planes de seguridad se puede continuar a la implementación de ISO/IEC 27001 y sus procesos asociados en torno al SGSI.

III. DEFINICIÓN DE ETAPAS DE LA METODOLOGÍA

Cada uno de los pasos del ciclo Deming implica a su vez la ejecución de diversas actividades en pos de la adquisición, recolección, estudio y análisis de información que permita constituir un estado del arte en cuanto a la seguridad de la información dentro de la organización, además de permitir definir las actividades a desarrollar para la construcción de las políticas y los planes de seguridad. A continuación el listado de pasos seguidos en la metodología.

- *Identificar el estado del arte en seguridad de la información*
- *Definir procesos a incluir en el SGSI*
- *Definición y evaluación de riesgos*
- *Generación de la política y planes de seguridad*

En la Fig. 1. se explica mejor el flujo que sigue esta metodología propuesta:

A. Análisis de recursos humanos

Por medio de entrevistas y encuestas aplicadas al personal de las áreas involucradas en procesos seleccionados a incluir en el SGSI, se establece un marco de referencia que permitirá identificar el estado del arte de la organización frente a la seguridad de la información desde las perspectivas de sus trabajadores además de las competencias de estos en dichos temas.

B. Análisis de recursos físicos

A través de peritaje y reconocimiento físico se establece la memoria fotográfica que da soporte a los informes de estado actual de la organización en cuanto a su infraestructura física evaluando temas como controles de acceso y continuidad del servicio.

C. Análisis de recursos lógicos

Uno de los procedimientos más críticos se aborda en este punto, dado que para lograr determinar el estado en cuanto a seguridad de la información de los recursos lógicos es necesario realizar detección de vulnerabilidades, test de penetración, entre otros, en ambientes controlados con el fin de detectar vulnerabilidades tales como el acceso no autorizado.

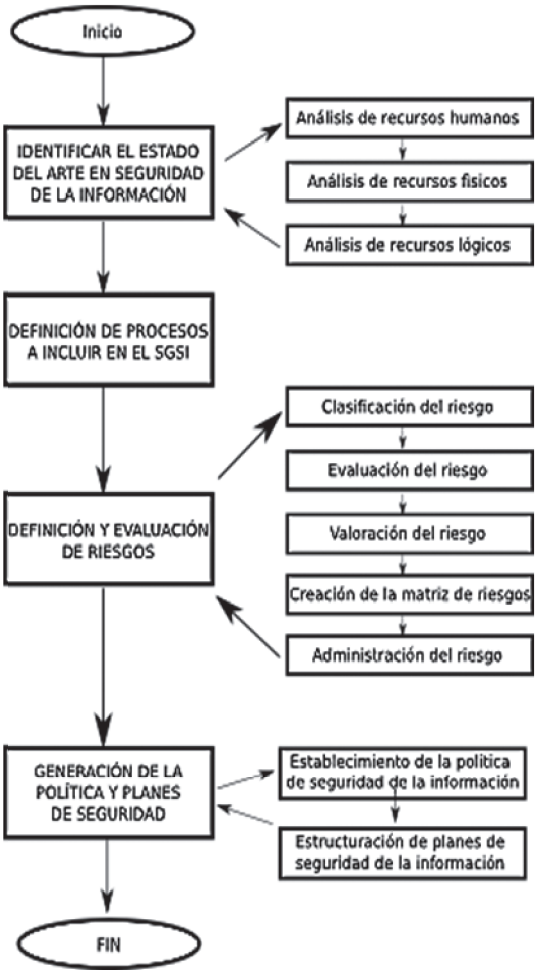

Fig. 1. Diagrama de metodología ágil de implementación de SGSI

IV. DEFINICIÓN DE PROCESOS A INCLUIR EN EL SGSI

La dirección de la organización es parte fundamental para la creación e implementación del SGSI, es por ello, que hace parte de esta fase inicial en la cual se deben establecer que procesos y áreas involucradas van a hacer parte del SGSI. Para ello se define el documento "declaración de aplicabilidad del estándar ISO/IEC 27001".

V. DEFINICIÓN Y EVALUACIÓN DE RIESGOS

De acuerdo a los requerimientos del estándar ISO/IEC 27001 es necesario establecer actividades y generación de documentación en torno a la gestión del riesgo. A través de la metodología desarrollada se establece un modelo para la gestión del riesgo que permite agilizar uno de los procesos más complejos y extensos de la creación de un SGSI y así generar de manera satisfactoria políticas y planes de seguridad.

Este proceso debe realizarse en conjunto con la dirección, la cual define su apetito de riesgo, estableciendo los niveles de riesgo aceptables para la organización.

Para la realización de actividades relacionadas a clasificación, evaluación y tratamiento del riesgo, es necesario el desarrollo de análisis que implican dos perspectivas para abordar la gestión del riesgo, el primer enfoque consiste en definir riesgos, las amenazas y vulnerabilidades asociadas a través del listado general de procesos de la organización, específicamente de aquellos procesos a incluir al interior del SGSI. El segundo enfoque consiste en la definición antes mencionada orientada a los activos de la organización que se desean proteger.

En ambos esquemas de análisis es necesario realizar una clasificación ya sea de procesos o activos a través de su incidencia/impacto en la organización y posteriormente evaluarlo de tal manera que se establezca por parte de la dirección una posición frente al riesgo, de acuerdo con el apetito de riesgos y oportunidades/amenazas de estos para la organización.

Se recomienda a lo largo de este proceso, emplear como guía dos estándares internacionales para la gestión y tratamiento de riesgos: ISO27005:2009 y NIST SP 800-30

A. Clasificación del riesgo

A través de este proceso se establece una categorización para los riesgos de acuerdo con su naturaleza a nivel de la organización:

- Riesgo estratégico
- Riesgo operacional
- Riesgo financiero
- Riesgo legal
- Riesgo tecnológico
- Riesgo de imagen

Siendo esta una clasificación sugerida de acuerdo con el trabajo realizado.

B. Evaluación del riesgo

A través de listas de chequeo y los resultados obtenidos en los análisis de recursos humanos, lógicos y físicos, se establece un listado de riesgos existentes contrastados con los objetivos de control del estándar ISO/IEC 27001.

C. Valoración del riesgo

La valoración del riesgo consiste en definir la relación impacto versus ocurrencia de los riesgos evaluados en el proceso anterior. Estos valores conformarán la matriz de riesgos de la organización.

D. Creación de la matriz de riesgos

En la matriz de riesgos permite ilustrar a la dirección y líderes en las áreas de la organización acerca del panorama de riesgos que enfrenta la organización. La generación de la matriz es un proceso complejo y puede crecer en la medida que las escalas de valoración son más descriptivas y/o especializadas. Es una herramienta de toma de decisiones para la dirección de la organización.

E. Administración del riesgo

La dirección de la organización indica que niveles de riesgo son aceptables o con cuales puede convivir la organización. Las acciones preventivas y correctivas, además de los controles deben guiar hacia la minimización del riesgo existente.

VI. GENERACIÓN DE LA POLÍTICA Y PLANES DE SEGURIDAD

La política de seguridad de la información es el marco que establece los alcances y objetivos del SGSI. Por su parte, los planes de seguridad son documentos de tipo ejecutivo que aplican controles, acciones preventivas y correctivas establecidas a través del tratamiento del riesgo y complementado con buenas prácticas para el cumplimiento por parte del personal de la organización y terceras partes.

Una vez finalizados estos documentos, deben contar con el aval de la dirección de la organización y deben establecer el inicio del SGSI. Sigue a este proceso la educación en seguridad de la información a todo el personal y el establecimiento de auditorías y mejoramiento continuo.

Cada cierto tiempo, como lo establece el estándar ISO/IEC 27001, deben realizarse actualizaciones y mejoras a los planes, adecuándolos según la introducción de nuevos procesos y tecnologías.

A. Establecimiento de la política de seguridad de la información

La construcción de la política de seguridad de la información para la organización es un proceso en conjunto con todas las áreas de la organización involucradas con las tecnologías de la información y cuyos procesos hacen parte del SGSI. Esta política establece el lineamiento de la organización frente a la seguridad de la información y es la hoja de ruta que deben cumplir los objetivos del SGSI.

B. Estructuración de planes de seguridad de la información

Finalmente, se realiza el establecimiento de los planes de seguridad a través de los cuales la organización implementará los controles establecidos para sus procesos. Para el establecimiento de los planes de seguridad se hará uso de estándares internacionales, guías y librerías de buenas prácticas en tecnologías de la información y seguridad, certificaciones internacionales de seguridad de la información, normas y/o leyes nacionales aplicables.

VII. APLICABILIDAD DE ESTÁNDARES, GUÍAS Y CERTIFICACIONES INTERNACIONALES

Como se indicó anteriormente, al dar cumplimiento a los controles establecidos por el estándar ISO/IEC 27001, existen puntos que no son cubiertos, para ello se sugiere emplear las siguientes guías, estándares y certificaciones como marco de complemento o de apoyo para alcanzar niveles de control aceptables para el SGSI.

A. Estándares

ISO/IEC 27002

A través del estándar ISO 27002 (el cual no es certificable), se puede establecer una guía de buenas prácticas aplicables a los controles de seguridad para el SGSI. Además de sugerir controles no abordados por ISO/IEC 27001.

ISO 31000:2009

Estándar internacional ISO 31000:2009, Risk Management – Principles and guidelines. Creado en 2009, provee principios, un marco de trabajo y un proceso para gestionar cualquier forma de riesgo de forma transparente, sistemática y creíble dentro del alcance del contexto.

ISO 27005:2008
Estándar internacional ISO 27005:2008, Information technology – Security Techniques – Information Security Risk Management. Este estándar proporciona pautas a nivel de la gestión de los riesgos a la seguridad de la información. Fue creado con la intención de ser apoyo a la implementación del SGSI a través de ISO/IEC27001.

B. Guías
MAGERIT
Esta metodología española establece un marco de referencia para el análisis e identificación de riesgos a nivel de los sistemas de información, complementando los controles relacionados con sistemas de información al interior del estándar ISO/IEC 27001.[6]

IT BASELINE PROTECTION MANUAL
Documento alemán que establece métricas y controles de seguridad empleados a nivel de creación de campañas de educación en seguridad de la información para usuarios y terceras partes. Además de proveer recomendaciones para establecimiento de controles de cifrado y uso de contraseñas. [7]

NIST SP 800-30
Guía desarrollada por el National Institute of Standards and Technology (NIST). "Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of standards and Technology". Establece controles y recomendaciones para evaluación, tratamiento y gestión del riesgo.

ITIL
A partir de la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) se pueden establecer controles para emplear a nivel de acuerdos de servicio, gestión de sistemas de mesa de ayuda y el tema crítico de gestión de cambios al interior del SGSI.

C. Certificaciones

CISSP (Certified Information Systems Security Professional)
Certificación internacional que a través de sus 10 dominios ofrece recomendaciones en su material de estudio para controles relacionados con criptografía, continuidad del negocio (BCP/DRP), seguridad en telecomunicaciones y seguridad física y del entorno. [8]
CEH (Certified Ethical Hacker)
Certificación orientada a realización de pruebas de hacking ético. A través de las diversas técnicas, metodologías y actividades propuestas al interior de esta certificación, es posible desarrollar pruebas de penetración, acceso no autorizado a plataformas y otro tipo de ataques controlados que permitan evaluar los controles de seguridad lógicos en sistemas de hardware y software al interior de la organización.[9]

VIII. CONCLUSIONES

La eficacia y eficiencia de la construcción del SGSI, las políticas y planes de seguridad de la información a través del uso de la metodología sugerida comprueban la agilidad del proceso y los beneficios para la organización.

En promedio este proceso de establecimiento de un SGSI toma para una organización entre un año y dos años debido a la dificultad de la limitación de procesos, aseguramiento de plataformas tecnológicas y educación del personal.

La metodología desarrollada permite realizar el procedimiento de una manera ágil y segura, tomando de otros dominios y puntos de vista, elementos que permiten el establecimiento de planes de seguridad más robustos y que además de evaluar procesos, tengan presente la importancia del aspecto técnico al interior del SGSI.

En el caso de la Universidad Distrital Francisco José de Caldas, actualmente se encuentra en proceso de estandarización y mejoramiento de las políticas y planes desarrollados para la implementación de medidas de seguridad y controles que permitan en cuanto sea necesario el establecimiento de un SGSI.

REFERENCIAS

[1] ISO (International Standard Organization). "Estándar de Seguridad ISO 27001. Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos", 2005

[2] E.T. Luque Melo., Borbón Sanabria, Jeffrey Steve. 2009 "Análisis y diseño del plan y políticas de seguridad para la Red de Datos de la Universidad Distrital Francisco José de Caldas". Dic. 2009.

[3] A. Cartlidge, H. Ashley 2007, An Introductory Overview of ITIL® V3, The UK Chapter of the itSMF. 2009

[4] E. Demings. 1989 Calidad, productividad y competitividad: la salida de la crisis, Madrid, Ediciones Díaz de Santos, 1989

[5] Office of Government Commerce, "ITIL V3" Glossary, The Stationery Office 2007

[6] Ministerio de administraciones públicas, "MAGERIT - Metodología de análisis y gestión de riesgos de los sistemas de información" versión 2, España, 2006.

[7] Federal Agency for Security in Information Technology, “IT Baseline Protection Manual”, Octubre 2000

[8] Harris, Shon, "CISSP Certification Exam Guide" Third Edition, McGr.aw-Hill, 2005

[9] R. L. Krutz, R. D. Vines, “The CEH Prep Guide: The Comprehensive Guide to Certified Ethical Hacking”, Wiley, 2007

BIOGRAFÍA

Jeffrey Steve Borbón Sanabria, Lugar de nacimiento Bogotá, Ingeniero de sistemas egresado de la Universidad Distrital Francisco José de Caldas. Actualmente estudiante de máster de seguridad Informática de la Universidad Oberta de Catalunya. Ha realizado varios diplomados y cursos especializados (Sistemas operativos, Bases de datos, Telecomunicaciones, Desarrollo Web y Seguridad Informática). Se ha desempeñado como oficial de seguridad, hacker ético, administrador de sistemas, servidores y comunicaciones en varias organizaciones del mercado financiero, empresas desarrolladoras de software y ONG’s. Certificado: CISSP - E|CSA - CEH - A.I. ISO 27001 - ITIL V3