Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI).

Raúl J. Martelo, Jhonny E. Madera y Andrés D. Betín

Universidad de Cartagena, Facultad de Ingeniería, Grupo de Investigación en Tecnologías de las Comunicaciones e Informática, GIMATICA, Avenida del Consulado, Calle 30, No. 48 – 152, Cartagena-Colombia. (e-mail: rmartelog1@unicartagena.edu.co , jmaderao@unicartagena.edu.co, abetinr@unicartagena.edu.co)

Recibido Jul. 20, 2014; Aceptado Oct. 2, 2014; Versión final recibida Dic. 4, 2014

Resumen

El objetivo principal de este trabajo consiste en desarrollar un software para contribuir al control de los documentos generados a partir del proceso de implantación de un Sistema de Gestión de Seguridad de la Información (SGSI). Dicho software permite recepcionar, administrar y organizar la documentación generada en el proceso de implantación del SGSI. Para soportar dicho software, se diseña e implementa un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI. Lo anterior, produjo como resultado un módulo para gestión documental que permite el control de documentos durante el proceso de implantación de un SGSI, trabajando bajo procedimientos del estándar ISO 27001.

Palabras clave: software, información, seguridad, ISO 27001, manejo de documentos

Software for Document Management, a Modular Component of the Information Security Management System (ISMS)

Abstract

The main objective of this paper was the development of software to contribute to the control of documents generated during the implantation process of an Information Security Management System (ISMS). The software allows receiving, managing and organizing the documents generated on the process of implantation of ISMS. To support this software, a model that defines the management actions that are necessary for approval, review, update, states and readability of documents through the life cycle of the ISMS was designed and implemented. As a result, a document management module that allows the control on documents during the implementation process, working under the standard ISO 27001 was developed.

Keywords: software, information, security, ISO 27001, document management

INTRODUCCIÓN

La información se ha convertido en activo importante de organizaciones (Piattini & Del Peso, 2001), toda vez cuando es completa, precisa y actualizada es fundamental en la toma de decisiones de las mismas. La importancia de la información se fundamenta en la teoría de la organización, la cual se define como un sistema conformado por personas, recursos materiales e información; existe una percepción sobre el concepto de información en la cual se indica que determina “*el ‘orden y el caos’ entre los individuos, los recursos y en la interrelación personas-recursos*” (Aja, 2002); por eso, debe considerarse a las organizaciones como sistemas de información.

Sin embargo dichos sistemas a medida que se consultan, almacenan y generan información, ponen en riesgo la integridad de la misma; riesgos, que no solo provienen del exterior sino también del interior de la organización (INTECO, 2010). Los virus, gusanos, hackers, phishing e ingenieros sociales, entre otras, son amenazas constantes que atentan contra la información de cualquier organización (Susanto et al, 2011a). Un Hacker, puede causar pérdidas considerables para una organización, tales como, robo de datos de clientes y espiar en la estrategia de negocio en beneficio de competidores (Susanto et al, 2011b).

Como consecuencia, la seguridad de la información no es sólo cuestión de tener nombres de usuario y contraseñas (Von, B. & Von, R. 2004), sino que requiere de reglamentos y diversas políticas de privacidad y protección de datos que imponen unas obligaciones para organizaciones (Susanto y Bin, 2010), igualmente debe ser integral y encajar en una empresa sin problemas, además de lo mencionado: seguridad del personal, control de acceso de usuarios, debe contener: seguridad de red y aspectos regulatorios. (Eloff y Eloff, 2005) Las anteriores obligaciones que se ejercen bajo la seguridad de la información, pueden ser solventadas con la ayuda de un SGSI que permite gestionar con eficacia los activos de información, minimizando posibles riesgos que atenten contra la misma (Broderick, 2006).

El SGSI consiste básicamente en un conjunto de políticas para definir, construir, desarrollar y mantener la seguridad del equipo basado en hardware y recursos de software (ISO/IEC 27001, 2005); estas políticas, muestran la manera en que los recursos del computador pueden ser utilizados (INTECO, 2010). Adicionalmente, el proceso de implantación de un SGSI opera a través de proceso de cinco etapas, establecimiento de políticas de seguridad de la información, alcance del Sistema de Gestión, control de riesgos, realización de medidas y control de seguimiento (Hangbae, 2013), bajo un modelo PHVA (Planear-Hacer-Verificar-Actuar). Es importante definir el enfoque que se tiene para la evaluación del estado de seguridad de información en una organización, de ahí la razón de definir un marco jerárquico para priorizar lo que se tiene (Eloff y von Solms, 2000). Además que los procesos de los SGSI conlleva a dificultades tales como: falta de documentación, administración y organización de la misma, ausencia de roles y responsabilidades, para llevar a cabo las actividades pertinentes para dar cumplimiento a objetivos y alcances del SGSI (Del Rio, 2013).

En este orden de ideas, abordar el proceso de forma tradicional y, las dificultades evidenciadas en cuanto a la documentación que se genera durante este proceso, sugiere la necesidad de buscar una pronta solución, lo cual se constituye en el objetivo principal de este trabajo. Para alcanzar el objetivo mencionado anteriormente, se desarrolló un software que enmarca la consecución de los requerimientos y actividades que conforman la debida documentación del SGSI. Como principal resultado, se obtiene un módulo de gestión documental que permite ejercer un control de documentos y asignación de actividades para miembros del grupo de implantación del SGSI, que facilita la recepción, administración, mantenimiento y estado de la documentación obtenida en el desarrollo del mismo.

Los Sistemas de Gestión de la Seguridad de la Información bajo los requerimientos que exige la norma ISO 27001, constituyen la base para la gestión de la seguridad de la información; dicha norma, define un SGSI que garantiza el conocimiento, apropiación, gestión y disminución de riesgos de seguridad de la información para la organización, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cambios que se produzcan en los riesgos, entorno y tecnologías (Calder, 2006). La implantación de un SGSI implica adaptarse a un nuevo paradigma definido como enfoque de gestión, desde la implementación de controles que figuran en la norma ISO 27002 hasta incluir productos certificados, manteniendo la combinación inteligente de aspectos tales como las políticas, normas, directrices, códigos de la práctica, la tecnología, asuntos humanos, asuntos legales y éticos hacen parte de este nuevo enfoque (Eloff y Eloff, 2003). Para habilitar dicho enfoque, el proceso de seguridad comprende la seguridad lógica y física de la organización, de esta forma establecer una estructura de seguridad a partir de canales de comunicación entre áreas de la organización, facilitando el cumplimiento de las políticas o normas de seguridad aplicables. (Peciña et al, 2011).

Ahora bien, la necesidad que se ha generado para implantar un SGSI (Cano y Saucedo, 2013), la problemática que ejerce el proceso tradicional, así como la descentralización y desorganización de la información generada, más la complejidad del desarrollo del SGSI, ha permitido innovar, construir, validar herramientas y modelos que aborden el proceso de implantación del SGSI de principio a fin, bajo el cumplimiento de actividades que lo requieren y la gestión documental de la misma.

De esta forma propuestas como e-PULPO, plataforma que integra un módulo SGSI, enfocado a la primera fase de planificación del mismo, permite el manejo de activos, documentación, incidencias, formación, indicadores y auditorías establecidas por la norma ISO 27001, además de la implementación de controles basado en la norma ISO 27002; e-PULPO se concentra en la gestión documental, la revisión, control y administración de ésta, de manera que la facilidad, interactividad y los componentes distribuidos de su interfaz gráfica del módulo gestión documental, la hace ser una plataforma eficiente, eficaz y regulada en el cumplimiento de sus funciones. (Ingenia, 2010).

Por otro lado, Gesconsultor herramienta que integra elementos necesarios para la implantación y gestión completa del ciclo de vida de un SGSI, así como otros requisitos de cumplimiento de aspectos legales, normativos, contractuales y con terceras partes, que sean de aplicación al alcance del sistema de gestión (Gesconsultor, 2013). En el mismo sentido, la plataforma GlobalSGSI permite la gestión integral de la norma 27001 y cumple con el ciclo completo de la misma, desde las fases de inicio y planificación del proyecto hasta el mantenimiento y mejora continua, pasando por el análisis de riesgos, el cuadro de mandos e implantación de procedimientos (GlobalSGSI, 2013).

Respecto a metodologías que no han sido materializadas en software, pero que aportan debido a su aplicación en pequeñas y medianas empresas (PYMES), Linares y Paredes (2007), publican Metodología en español para implantación de seguridad de la información para este tipo de empresas, la cual surge como solución y aproximación para el camino a seguir hacia la implementación de la seguridad de la información, en empresas cuyo modelo de seguridad aún no es maduro y desean acometer la labor de implantación de la seguridad de la información y de su sistema de gestión, asociado de una forma eficiente, eficaz y práctica, de forma que permita disminuir el riesgo de la organización a corto plazo, a la vez que se inicie el camino hacia el cumplimiento de los estándares deseados. Por otro lado, María Eugenia Corti (2010) propuso una metodología que permite la disminución de tiempo y costos de implementación de un sistema de gestión para estas empresas en el mediano plazo, en conformidad con la norma ISO 27001 dando cumplimiento a las buenas prácticas según lo establecido en la norma ISO 27002.

MODELO PLANTEADO

En esta sección, se presenta el modelo propuesto para contribuir a solucionar los problemas efectuados durante el proceso de implantación de un SGSI, que pueden ser generados por la poca gestión documental. La siguiente figura presenta el modelo de procesos planteado:

Fig. 1: Modelo planteado. Fuente: Grupo de trabajo.

Para el inicio del control de documento y su debida gestión, el modelo enmarca la disposición de un módulo gestión de usuarios, de modo que el encargado pueda realizar el seguimiento de determinado documento y otro módulo de actividades el cual genera como producto un documento a gestionar.

El modelo abarca tres pasos esenciales: i) Asignar encargado; ii) Realización de Actividad;y iii) Control documental.

i) *Asignar encargado* (Gestión de roles o usuarios): Permite la selección del encargado a realizar la actividad cuyo objetivo es generar alguna documentación; ii) *Realización de Actividad*: (Gestión de actividades): El usuario asignado para determinada actividad debe subir el documento entrega;y iii) *Control documental* (Gestión Documental): Permite la disponibilidad, seguimiento y versionamiento de los documentos referentes a actividades agregadas. Para este paso el documento cumple un proceso cíclico, pasando por distintos estados cumpliendo con el ciclo PDCA del proceso de implantación de un SGSI. El flujo de estado de los documentos: (a) Borrador > Revisión > Verificación > Aprobado > Publicado (Flujo base); (b) Verificación > Borrador (Cuando se atiende las observaciones por el administrador o encargado de auditar el documento); (c) Publicado > Borrador (Cuando el documento se encuentra en un estado “Actuar” del proceso de implantación se debe atender observaciones e incidencias, generando nueva versión del documento).

Características Modelo Planteado:

Almacenamiento: La personalización respecto al almacenamiento y persistencia de los documentos teniendo en cuenta principios de seguridad de la información: disponibilidad, integridad y confidencialidad, el modelo de control de documentos permite elegir entre un almacenamiento por defecto referente a un componente Google Engine en la nube, enfocado a organizaciones con bajo presupuesto; y la configuración de almacenamiento personalizada para alojar los documentos según los parámetros dados por la organización que utilice el software.

Notificaciones: La constante comunicación entre el Administrador y el encargado de las actividades las cuales generan algún documento es de manera intensiva, para evitar atrasos y cumplimiento de metas en cuanto a documentación. Todo es notificado.

RESULTADOS

Con el fin de dar cumplimiento al objetivo principal de este artículo, se desarrolló un módulo de gestión documental para control de documentos generados durante el proceso de implantación de un SGSI. Este módulo garantiza la organización, versión, apoyo y accesibilidad al material documental para procesos de auditorías y certificación del sistema de gestión. Además, permite un seguimiento exhaustivo para cada documento, creado a partir de actividades asignadas a usuarios partícipes de este proceso. Estos documentos pasan por distintos estados que definen el ciclo PDCA y un proceso secuencial, que continúa de un estado borrador, revisión, verificación, aprobado, hasta que sea publicado para un grupo seleccionado por el administrador del sistema o, en su defecto, el encargado del desarrollo del SGSI.

Este módulo es innovador y presenta como valor agregado varias características: 1) La integración de los módulos de roles (usuarios), documental, actividades y comunicaciones (notificaciones) permiten el seguimiento continuo de documentos del encargado y establecer compromiso en los partícipes en el proceso de implantación; 2) Modulo documental bajo el marco PDCA para un mejoramiento continuo, versionamiento y la no utilización de archivos o documentos obsoletos, además de las disponibilidad, integración y confiabilidad del mismo; 3) Para cualquier organización dicho software establece un almacenamiento en la nube para configurar un entorno PYME, debido que los aplicativos o software están enfocados a grandes organizaciones donde su infraestructura es fuerte en cuanto a seguridad de información. Por lo tanto configurar el almacenamiento para PYMES con un servicio en la nube de Google (Blobstore: Google Cloud Platform) y la configuración dada por la propia organización; y 4) La instalación del software se realiza para la organización solicitante, no se maneja como SaaS (Software como servicio) para evitar la responsabilidad de mantener los principios de seguridad de la información como disponibilidad, integridad y confidencialidad, debido que la documentación generada es única y confidencial para la organización.

Una forma de visualizar los estados del documento y las características que permiten una gestión eficiente en cuanto a seguimiento, mantenimiento, facilidad y control documental durante todo el proceso, se muestra en la figura 3. En la anterior figura, se presenta las características para los documentos gestionados: título, nombre del documento personalizado por el usuario asignado; tipo, hace referencia la clase de documento (Documento requerido por la ISO 27001, Informe u otro), versión, la parte decimal representa las

modificaciones hechas al documento, la entera evidencia el número de publicaciones del documento; estado; inicio, fecha de creación del documento; fin, fecha de finalización del documento; actualización, fecha de última modificación del documento; observaciones, comentarios hechos para el documento; y acción, son opciones para cambiar el estado del documento.

Título	Tipo	Versión	Estado	Inicio	Fin	Actualización	Observaciones	Acción
Atenas-49-BG	Documento	1.0	Publicado	26 de Noviembre 2013	5 de Diciembre 2013	5 de Diciembre 2013	Documento publicado	
Lista de propiedades de activos	Documento	0.1	Aprobado	29 de Noviembre 2013	8 de Diciembre 2013	2 de Diciembre 2013	El documento ha sido aprobado para su publicación	
Lista de propiedades de activos	Documento	0.1	Verificar	27 de Noviembre 2013	2 de Diciembre 2013	29 de Noviembre 2013	Los activos del subdepartamento de sistema	
Publica de clasificación de activos	Documento	1.0	Eliminar	28 de Noviembre 2013	5 de Diciembre 2013	10 de Noviembre 2013	Faltan objetivos	

Fig. 2: Gestión Documental

CONCLUSIONES

De los resultados obtenidos, se pueden anunciar las siguientes conclusiones sobre el modelo y la herramienta que lo soporta: 1) Permite identificar el estado de los documentos; 2) Previene la utilización de documentos obsoletos; 3) Compromiso bajo la gestión de roles y asignación de actividades; 4) Garantiza la disponibilidad, accesibilidad y seguimiento a documentos asignados; 5) Permite trabajar bajo procedimientos estrictamente del estándar ISO 27001; y 6) Modelo de trabajo cíclico.

REFERENCIAS

- Aja Quiroga, L. (2002). Gestión de información, gestión del conocimiento y gestión de la calidad en las organizaciones. *Acimed*, 10(5), 7-8.
- Broderick, J. S. (2006). ISMS, security standards and security regulations. *information security technical report*, 11(1), 26-31.
- Calder, A. (2006). Implementing information security based on ISO 27001/ISO 17799: a management guide. J. Van Bon (Ed.). Van Haren Publishing.
- Cano, J. y Saucedo, G. M. (2013) Encuesta Latinoamericana de Seguridad de la Información 2013. ACIS.
- Corti, M. E. (2009). *Metodología de Implantación de un SGSI*. Uruguay. Tesis de Maestría: Universidad de la República.
- Del Rio, M. (2011). Deficiencias más comunes en los SGSI basados en la ISO 27001. Recuperado el 20 de septiembre de 2013, <http://www.securitybydefault.com/2011/08/deficiencias-mas-comunes-en-los-sgsi.html>
- Eloff, J. H., y Eloff, M., Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130-136). South African Institute for Computer Scientists and Information Technologists, September (2003).

Eloff, J.H. y Eloff, M., Information security architecture, Computer Fraud & Security, Volume 2005, Issue 11, November 2005, Pages 10-16, ISSN 1361-3723 (en línea), [http://dx.doi.org/10.1016/S1361-3723\(05\)70275-X](http://dx.doi.org/10.1016/S1361-3723(05)70275-X). Acceso: 21 Octubre (2014).

Eloff, M.M y von Solms, S.H, Information Security Management: A Hierarchical Framework for Various Approaches, Computers & Security, Volume 19, Issue 3, 1 March 2000, Pages 243-256, ISSN 0167-4048 (en línea), [http://dx.doi.org/10.1016/S0167-4048\(00\)88613-7](http://dx.doi.org/10.1016/S0167-4048(00)88613-7). Acceso: 20 Octubre (2014).

GesConsultor., Recuperado el 25 de Noviembre de 2013 de <http://www.gesconsultor.com/> (2013).

GlobalSGSI., Recuperado el 12 de Noviembre de 2013 de <http://www.globalsgsi.com/> (2013).

Hangbae C., Is ISMS for financial organizations effective on their business?, Mathematical and Computer Modelling, Volume 58, Issues 1–2, July 2013, Pages 79-84, ISSN 0895-7177, (en línea), <http://dx.doi.org/10.1016/j.mcm.2012.07.018>. Acceso: 5 Noviembre (2014).

Ingenia. Recuperado el 28 de Abril de 2013 de <https://www.e-pulpo.es/> (2010).

INTECO. Sistema de gestión de la seguridad informática. Obtenido de INTECO. Recuperado el 12 de Noviembre de 2013. <http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/index.html>.

ISO/IEC 27001:2005. Information technology – Security techniques - Information security management system implementation guidance. Recuperado el 20 de septiembre de 2013, <http://web.bryant.edu/~commtech/guidelines/iso27001.pdf>. (2005).

Linares, S., y Paredes, I. IS2ME Seguridad de la Información a la Mediana Empresa. (2007).

Peciña, K., Estremera, R., Bilbao, A., y Bilbao, E., Physical and Logical Security management organization model based on ISO 31000 and ISO 27001. In Security Technology (ICCST), 2011 IEEE International Carnahan Conference on (pp. 1-5). IEEE. October (2011)

Piattini, M., y Del Peso, E. Auditoría Informática. Un enfoque práctico. RA-MA, Madrid, 245.
Susanto, H. & Bin, F. Multimedia Information Security Architecture. @ IEEE. 2010. (2001).

Susanto, H., Almunawar, M. N. y Chee, Y. I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution's Six Domains. Journal of Computer, Asian Transaction. July (2011).

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five.

Von, B. y Von, R.. The 10 deadly sins of Information Security Management. Computer & Security 23(2004) 371- 376. Elsevier Science Ltd. (2004).