GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: UN MARCO DE TRABAJO

Área de investigación: Administración de la Tecnología

Leidy Johanna Cárdenas Solano
Grupo de Investigación INNOTEC
Universidad Industrial de Santander
Colombia
leidy.cardenas2@correo.uis.edu.co

Luis Eduardo Becerra Ardila
Grupo de Investigación INNOTEC
Universidad Industrial de Santander
Colombia
lbecerra@uis.edu.co

Hugo Ernesto Martinez Ardila
Grupo de Investigación INNOTEC
Universidad Industrial de Santander
Colombia
hugo.martinez@correo.uis.edu.co

XVIII Congreso Internacional de Contaduría Administración e Informática

Octubre 2, 3 y 4 de 2013 ◆ Ciudad Universitaria ◆ México, D.F.

ANFECA Asociación Nacional de Facultades y Escuelas de Contaduría y Administración

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: UN MARCO DE TRABAJO

Resumen

En los últimos años, la seguridad de la información y los nuevos esquemas de gestión del conocimiento, han sido un tema de gran relevancia para la comunidad académica y las organizaciones empresariales que buscan ser más eficientes en la administración del capital intelectual. Para lograr lo anterior las entidades tienen que generar e implementar innovadores modelos, instrumentos o estrategias para el perfeccionamiento de esta gestión. Este trabajo tiene como objetivo consolidar el estado del arte sobre el tópico "information security" para el período 2001-2011 y, a partir de ello, proporcionar los factores claves para el diseño de un modelo de gestión de la seguridad de la información. La revisión de literatura se realizó en tres etapas: a) Revisión de información no estructurada, b) Análisis bibliométrico y c) Análisis, organización y síntesis del contenido. Como resultado se extrajo un amplio marco de trabajo multi-dimensional que relaciona gestión del conocimiento, gestión de riesgos, incidentes de seguridad, sistemas de información y redes, recursos humanos, aspectos económicos, gobernanza de seguridad de la información, políticas y buenas prácticas. De lo anterior, se concluye que en la literatura analizada existen espacios que permitirán direccionar las futuras líneas de investigación relacionadas.

Palabras claves: Buenas prácticas, Cultura de la seguridad de la información, Gestión del conocimiento

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: UN MARCO DE TRABAJO

1. INTRODUCCIÓN

Hace más de 20 años, algunos académicos como Drucker[1], Porter y Millar[2], fueron los primeros en reconocer que una "Revolución de la Información" estaba teniendo lugar, la cual tuvo un impacto inmediato, con efectos significativos en todos los aspectos de la vida organizacional[3]. A través de los años, la experiencia ha comprobado que una buena gestión de la información, no sólo puede mejorar significativamente el desempeño organizacional[4,5,6], sino que también puede transformar radicalmente los procesos, estructura y cultura de la organización[7,8].

Dada su creciente importancia, la información es a menudo vista como análoga a la "sangre" de la organización[9,10,11]. Por consiguiente, si el flujo de información es continuo, los procesos y tareas se ejecutarán de manera óptima; por el contrario, si este es restringido o seriamente perturbado, entonces la organización puede deteriorarse o incluso morir, lo cual se constituye en un riesgo de seguridad de la información. Acerca de cómo prevenir estos riesgos, Kevin Mitnick (2002) hizo la siguiente afirmación: "Nunca se confíe de los mecanismos de seguridad en la red para proteger su información. Revise su punto más vulnerable. En la mayoría de los casos descubrirá que este se encuentra en las personas".

Por lo anterior, se observa que el enfoque de seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de computadores y dispositivos de almacenamiento de información, pasando por la seguridad de sistemas y redes de

[1] DRUCKER, Peter. The coming of the new organization. En: Harvard Business Review. Vol. 66, No. 1 (1988); p. 47.
[2] PORTER, Michael y MILLAR, Victor. How information gives you competitive advantage. En: Harvard Business Review. Vol. 64, No. 4 (1985); p. 149.
[3] ZAMMUTO, Raymond, et al. Information technology and the changing fabric of organization. En: Organization Science. Vol. 18, No. 5 (Sep. 2007); p. 751.
[4] BRYNJOLFSSON, Erik y HITT, Lorin. Paradox lost? Firm-level evidence on the returns to information systems spending. En: Management science. Vol. 42, No. 4 (Abr. 1996). Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.
[5] SIRCAR, Sumit y CHOI, Jung. A study of the impact of information technology on firm performance: a flexible production function approach. En: Information Systems Journal. Vol. 19, No. 3 (2009). Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.
[6] WARD, Jhon y PEPPARD, Joe. Strategic planning for information systems. 3 ed. Chichester: Wiley Publishing, 2002. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.
[7] DOHERTY, Neil; KING, Malcolm y AL-MUSHAYT, Omar. The impact of inadequacies in the treatment of organizational issues on information systems development projects. En: Information & Management. Vol. 41, No. 1 (Oct. 2003); p. 50.
[8] MARKUS, Lynne. Technochange management: using IT to drive organizational change. En: Journal of Information Technology. Vol. 19, No. 1 (2004); p. 4.
[9] HALLIDAY, S., BADENHORST, K. y VON SOLMS, R.A business approach to effective information technology risk analysis and management. En: LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Vol. 2006, No. 12 (Dic. 2006); p. 17
[10] WILLS M. Personal communication. En: GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. Vol. 24 (2005); p. 17.
[11] PEPPARD, Joe. The conundrum of IT management. En: European Journal of Information Systems. Vol. 16, No. 1 (2007); p. 339.

tecnologías de información, a concentrarse en la gestión de alto nivel mediante políticas, procedimientos y controles basados en las personas[12].

A pesar de la evolución exponencial y relevancia del tema, no existen directrices que proporcionen la base teórica necesaria para un marco y una metodología para la gestión de la seguridad[13]. Algunos autores, como Hong et al. (2003) sugieren que la ausencia de un marco y una metodología para la gestión de la seguridad han contribuido a la falta de teoría en gestión de la seguridad.

En este contexto, el propósito de este trabajo es comprender la evolución de la gestión de la seguridad de la información en la literatura de investigación, la investigación no será delimitada a un cierto nivel (es decir, macro o micro). De la misma manera los términos de búsqueda se mantienen amplios a fin de no limitar la investigación a un área determinada dentro de la temática.

La estructura de este trabajo es la siguiente. En primer lugar, se discuten cuestiones metodológicas. Luego se consideran las características de la investigación existente sobre gestión de seguridad de la información, con respecto a las temáticas tratadas y la relación entre ellas. La última sección presenta las conclusiones y se discuten las implicaciones para futuras investigaciones.

2. METODOLOGÍA

Con el fin de obtener información reciente, relevante y relacionada con el problema de investigación, se utilizaron varias bases de datos a las cuáles se tiene suscripción con acceso desde el campus universitario como: ISI Web of Science, Ebsco Host, ScienceDirect, Scopus, ProQuest, y Springerlink.

La revisión de la literatura partió de una búsqueda realizada en ISIWOS, utilizando el campo "tópico" con la frase "Information Security", entre comillas para asegurar que las dos palabras aparecieran juntas, y con un horizonte de tiempo de 2001 – 2011. El principal foco de esta revisión fue investigar lo que se ha dicho acerca de la gestión de seguridad de la información en las organizaciones.

Primeramente, se examinaron los títulos de los artículos, con el fin de excluir aquellos que no estuvieran directamente relacionados con el foco de la revisión. Luego, se realizó un segundo filtro por el contenido y temática tratada en el resumen, para finalmente organizar las publicaciones de acuerdo a las palabras claves en nueve categorías, que dieron origen al desarrollo de un marco de trabajo, o framework, sobre gestión de seguridad de la información (ver Figura 1).
Adicionalmente, se incluyeron en la revisión artículos de los autores más relevantes en el tema, y documentos relacionados, utilizando el método "bola de nieve", que consiste en descubrir otros documentos de interés mediante la revisión de la bibliografía citada en los

[12] NNOLIM, Anene. A framework and methodology for information security management. Southfield, 2007. Dissertation (Doctor of Management in Information Technology). Lawrence Technological University. Graduate Faculty of the College of Management. p.2
[13] NNOLIM, Op. Cit., p. 5.

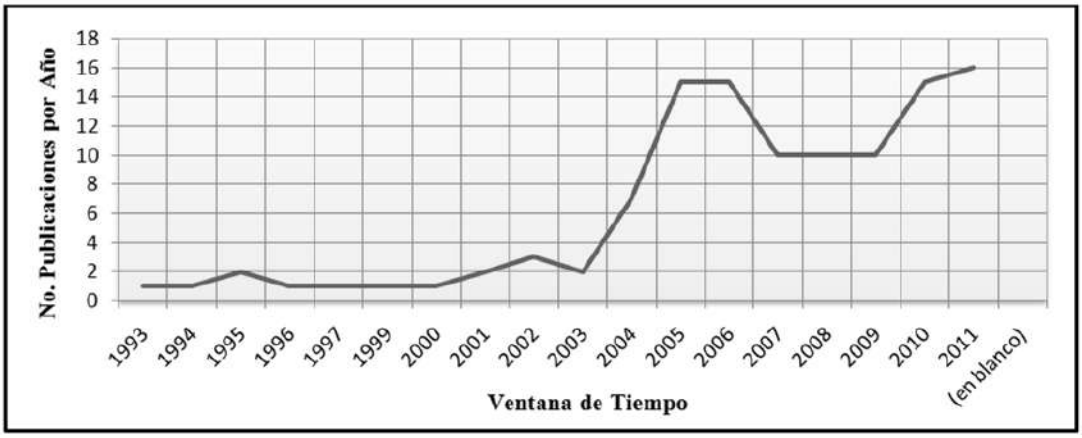
documentos iniciales. Como consecuencia, se encontraron documentos de años anteriores al 2001, y se pudo identificar algunos autores relevantes sobre los cuales se profundizó la búsqueda.

Además para complementar los resultados, se realizó una búsqueda utilizando las mismas palabras claves ("Information Security"), en la herramienta Google Académico, incluyendo los documentos relevantes diferentes a los que ya se tenían. Finalmente se obtuvieron más de 100 publicaciones para el análisis. A continuación se presenta una breve reseña de los artículos consultados.

3. RESULTADOS

De acuerdo con la literatura evaluada, la seguridad de la información es una temática con un rápido crecimiento, cuyo número de artículos por año en 2011 fue 3.3 veces los del año 2001, pero que aún no llega a su etapa de madurez, lo cual se refleja en los incrementos porcentuales positivos y da la oportunidad de seguir explorando en la temática y enriquecerla a futuro. Además, este reporte de publicaciones también muestra que dentro del rango de años estudiado, la mayor cantidad de publicaciones se encuentra después del año 2000 (ver Figura 1).

Figura 1. Tendencia de publicaciones por año



Fuente. Los Autores

Como principal resultado de esta revisión de literatura, se desarrollo un marco de trabajo, en el cual se agruparon las temáticas tratadas en las publicaciones en nueve categorías relacionadas entre sí como se muestra en la Figura 2, con el fin de entender la estructura de conocimiento de las investigaciones en "information security, sus patrones y tendencias asociadas.

Entiéndase por Marco de trabajo o *Framework*, según El diccionario Oxford, una estructura básica que subyace a un sistema, un concepto o texto. En términos más prácticos, puede considerarse como una aplicación genérica, incompleta y configurable a la que se le pueden

añadir piezas adicionales para construir una aplicación concreta[14]. En este sentido, un "Framework" también puede ser visto como un estándar que, tomado como base o referencia, es útil para enfrentar y resolver nuevos problemas de índole similar. Los objetivos principales que persigue un Framework se relacionan con el hecho de acelerar el proceso de desarrollo, reutilizar creaciones ya existentes y promover buenas prácticas de desarrollo como el uso de patrones[15].

En este *Framework*, el elemento de mayor nivel jerárquico es la gobernanza de seguridad de la información, en donde se toman las decisiones de carácter estratégico que afectan directamente el desarrollo de políticas. Es normal que exista una política general de seguridad de la información, y a partir de ella se pueden desencadenar políticas específicas para distintas áreas de la organización. En la política, también se establecen lineamientos sobre cómo, cuándo y quién lleva a cabo la evaluación y tratamiento de riesgos, actividades que constituyen la gestión de riesgos. Esta última es alimentada por los incidentes de seguridad que brindan alertas sobre riesgos no identificados o no controlados.

Como base de todas las actividades realizadas, se encuentran siempre los estándares, lineamientos o guías de buenas prácticas, los cuales permiten a las organizaciones conocer los requisitos mínimos para gestionar la seguridad de la información.

Finalmente como tema transversal se encuentra la gestión del conocimiento, ya que cualquier esfuerzo realizado en la organización se convierte en conocimiento y experiencia que debe ser apropiado por los individuos. Asimismo, no solo la información debe ser protegida sino también el conocimiento existente en las personas, es allí donde surgen nuevos riesgos que deben evaluarse y tratarse.

[14] GUTIÉRREZ, Javier J. ¿Qué es un framework web?. Universidad de Sevilla. [En Línea]. [Citado 28 julio, 2012]. Disponible en internet: <http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf>
[15] Ibid.

Figura 2. Marco de trabajo de seguridad de la información

Fuente. Autores.

3.1 Gestión del conocimiento

Según una definición propuesta por William Wallace (1999), la gestión del conocimiento es una nueva disciplina que permite habilitar personas, equipos y organizaciones completas en la creación, compartición y aplicación del conocimiento, colectiva y sistemáticamente, para mejorar la consecución de los objetivos de negocio. Actualmente el interés por este campo sigue creciendo a un ritmo asombroso, aunque son escasos los estudios cómo proteger los activos basados en conocimiento[16]; por tanto, existe un gran interés en el diseño y desarrollo de marcos de trabajo (frameworks) de gestión de seguridad de la información[17], que proporcionen una guía en la protección de la información y conocimiento generado, gestionado y transferido en las organizaciones.

3.2 Gestión de riesgos

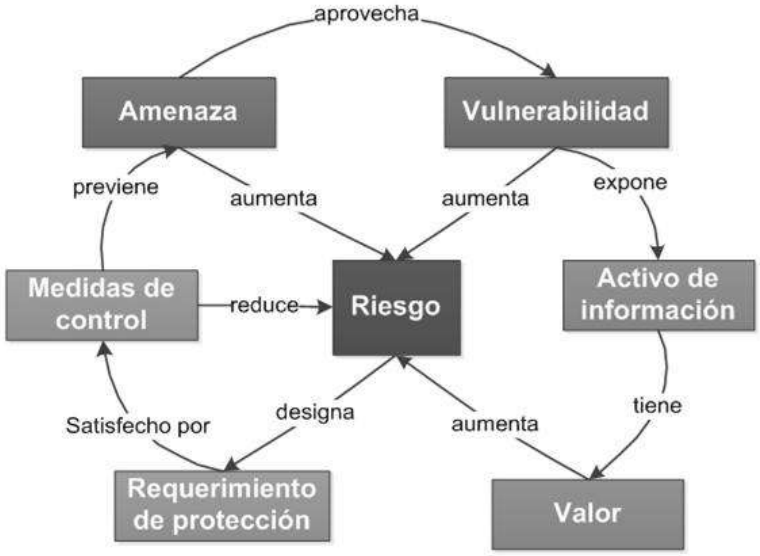
Gerber y von Solms (2005) proponen adoptar un enfoque alternativo al análisis de riesgos tradicional, en el cual se analicen no solamente los riesgos de los activos tangibles, sino también los riesgos de los intangibles como la información; además, consideran relevantes los riesgos causados por asuntos culturales, legislativos, sociológicos, entre otros.

Asimismo, Lategan y von Solms (2006), enfatizan en que las empresas hoy en día deben asegurar que los riesgos sean gestionados holísticamente y que la terminología y prácticas de riesgo relacionadas con TICs estén congruentemente alineadas con la terminología y prácticas de la empresa. Es decir, las TICs no pueden ser vistas como un componente independiente en cuanto a la gestión de riesgos se refiere.

[16] DESOUZA, Kevin y VANAPALLI, Ganesh. Securing knowledge in organizations: lessons from the defense and intelligence sectors. En: International Journal of Information Management. Vol. 25, No. 1 (Feb. 2005); p. 85.
[17] NNOLIM, Op. cit., p. 13.

De acuerdo con Layton (2007), un **riesgo** está constituido por la probabilidad, impacto y consecuencia de eventos negativos que la organización debe considerar como parte de sus operaciones; mientras que una **vulnerabilidad** consiste en un defecto o debilidad en un sistema de información, procedimiento asociado, o **control** existente que tiene el potencial de ser ejercido (accidental o intencionalmente) y resultar en un incumplimiento o violación de la política de seguridad de la información. Por ende, las vulnerabilidades no tienen ningún impacto si una amenaza en cuestión no está presente. Por otra parte, la **amenaza** se refiere a un posible peligro del sistema o atacante que aprovecha las debilidades (vulnerabilidades del sistema). En la Figura 3, se observan las múltiples relaciones existentes entre los conceptos anteriores.

Figura 3. Relaciones entre los componentes del riesgo



Fuente. Autores. Adaptado de FARN, Kwo-Jean, LIN, Shu-Kuo y FUNG, Andrew Ren-Wei (2004)

En este sentido, como uno de los primeros pasos en la implantación de un protocolo de seguridad de la información, se debe llevar a cabo una evaluación del riesgo (en inglés risk assessment), el cual consiste en el proceso de identificar los riesgos de seguridad de un sistema y determinar su probabilidad de ocurrencia, su impacto, y los mecanismos que mitiguen ese impacto[18].

Según la US General Accounting Office, la mayoría de las metodologías de evaluación de riesgos utilizadas incluyen los siguientes elementos básicos:

- Identificación de las amenazas.
- Estimación de la probabilidad de que dichas amenazas ocurran.
- Identificación y valoración de los activos que podrían estar en riesgo.

[18] SYALIM, Amril, HORI, Yoshiaki y SAKURAI, Kouichi. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, En: International Conference on Availability, Reliability and Security.2009, p. 726.

- Cuantificación del impacto.
- Recomendación de controles: Identificar las acciones costo-efectivas que podrían mitigar el riesgo.
- Determinación del riesgo: es el resultado de combinar la probabilidad de ocurrencia y el impacto de la amenaza, junto con la vulnerabilidad existente.
- Documentación de los resultados y elaboración de un plan de acción.

En particular, existen diferentes metodologías de evaluación del riesgo, entre las cuales se encuentran:

3.2.1 Magerit

Es una metodología abierta para análisis y gestión del riesgo, desarrollada por el Ministerio Español de Administración Pública, ofrecida como un marco de trabajo y guía para la Administración Pública. Dada su naturaleza abierta, también es usado fuera de la Administración[19]. Esta metodología es de interés para cualquiera que trabaje con información estructurada y sistemas de computación. Si esta información, o los servicios que son provistos a través de ella, son de valor, esta metodología permitirá conocer que tanto de ese valor está en riesgo y ayudará a protegerlo.

3.2.2 Operationally Critical Threat, Asset, and Vulnerability Evaluation

Desarrollada por el Carnegie Mellon Software Engineering Institute[20], consiste en una serie de herramientas, técnicas, y métodos para el proceso de planeación estratégica y evaluación basada en riesgos de seguridad de la información, los cuales se caracterizan por ser auto-dirigidos, flexibles y evolucionados[21].

3.2.3 Global Information Security Assessment Methodology

Este tipo de evaluación tiene como propósito cuantificar y calificar los riesgos de seguridad de la información de manera holística a nivel organizacional. GISAM aprovecha los dos tipos de evaluación (cuantitativa y cualitativa) dentro de la metodología y se considera que es un tipo de modo mixto de evaluación, razones por las que será la metodología a utilizar en el presente proyecto.

Este tipo de evaluación brinda una perspectiva integral de seguridad de la información a nivel institucional, ya que considera los aspectos operativos y de gestión de seguridad de la información, así como la aplicación y uso de la tecnología. Además, es muy escalable ya que se puede aplicar tanto en pequeñas empresas como en organizaciones mundiales.

[19] *ENISA - Agencia Europea de Seguridad de las Redes y de la Información (n.d). RiskManagement - RiskAssessmentMethods: Magerit. [en línea]. [Consultado el 10 de Octubre de 2011]. Disponible en: <http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html>*

[20] El Carnegie Mellon Software Engineering Institute es un centro de investigación y desarrollo financiado con fondos federales. Sitio web: http://www.sei.cmu.edu

[21] Características y ventajas de OCTAVE. [en línea]. [consultado el 10 de agosto de 2011] Disponible en: <http://www.cert.org/octave/>

Según Layton (2007), la metodología contempla los siguientes componentes del análisis y evaluación de riesgo:

- Determinación de los activos dentro del alcance
- Identificación de amenazas
- Caracterización de las amenazas.
- Identificación de vulnerabilidades.
- Análisis de controles.
- Determinación de la probabilidad de ocurrencia.
- Análisis de impactos.
- Determinación del riesgo.

3.3 Incidentes de seguridad

En comparación con otras áreas del framework, los incidentes de seguridad son poco mencionados en la literatura, y en su mayoría corresponden a aspectos técnicos de seguridad como violaciones a los sistemas de información y redes[22].

Como objetivo general, los autores que han tratado el tema, se han enfocado en mejorar el entendimiento de las amenazas a la seguridad de la información a fin de que los profesionales en el área puedan tomar mejores decisiones sobre cómo hacer frente a estas amenazas[23] [24] [25]. Algunos tipos de incidentes (o brechas) de seguridad de la información incluyen:

- Negación del servicio
- Acceso desautorizado a información de clientes
- Acceso desautorizado a información de empleados
- Alteración del sitio web
- Acceso desautorizado a información de la compañía

En cuanto a las causas que originan los incidentes de seguridad en las organizaciones. Beautement y Sasse (2008) afirman que un gran número de incidentes ocurren como resultado de los fracasos de los empleados para cumplir con las políticas de seguridad. La causa más común son los errores no intencionales; pero, existe evidencia de que en algunos casos los empleados eligen no esforzarse por cumplir con las tareas de gestión de seguridad. Al indagar sobre las razones de este no cumplimiento, la mayoría lo justifica con el impacto que estas medidas tienen en la productividad personal y organizativa, la

[22] KRAEMER, S., CARAYON, P. y CLEM, J.F. Characterizing violations in computer and information security systems. En: Proceedings of the 16th Triennial World Congress of the International Ergonomics Association (IEA). 2006.
[23] Ibid.
[24] WEI, June y LI, Yi. Computer information systems threat analysis on security. En: 2004 IRMA International Conference. 2004, p. 952.
[25] GOODALL, John, LUTTERS, Wayne y KOMLODI, Anita. Developing expertise for network intrusion detection.En: Information Technology & People. Vol. 22, No. 2 (2009); p. 7.

percepción de ausencia de riesgo y el hecho de que otros compañeros de trabajo tampoco las cumplan[26,27].

3.4 Sistemas de información y redes

Dentro de la investigación sobre seguridad de la información, los sistemas de información y las redes de telecomunicaciones hacen parte del común denominador en los análisis de riesgos. Son estos los principales objetivos de los ataques por parte de los criminales informáticos.

3.5 Recursos humanos

El rol de las personas es vital para el éxito de cualquier organización, sin embargo estas constituyen el eslabón más débil cuando se habla de seguridad de la información[28,29]. Esto explica porque gran parte de la literatura se ha dedicado a temáticas relacionadas con el comportamiento de los usuarios de la información. Thomson, von Solms y Louw (2006), enfatizan que los empleados pueden volverse conscientes y estar entrenados en las habilidades correctas necesarias para proteger los activos de información, y estas habilidades pueden convertirse en parte de las prácticas diarias de los empleados.

Para asegurar el éxito, las organizaciones deben tratar de maximizar el nivel de conocimiento exclusivo utilizable dentro de sí mismas. Actualmente, este objetivo se aborda desde dos campos de actividad principales: Gestión del Conocimiento y Gestión de la Seguridad de la Información. El triunfo de ambas disciplinas depende fuertemente de las personas.

En la Gestión del Conocimiento, las personas tienen que compartir su conocimiento individual – tanto tácito como explícito – con otros para formar y establecer un cuerpo de conocimiento comprensible que pueda ser usado (y aprovechado) por toda la organización. Lo mismo es cierto acerca de la Seguridad de la Información. Después de décadas de acercamientos meramente técnicos, ahora es ampliamente aceptado que "las personas son la piedra angular de la seguridad de la información"[30].

Varios autores confirman la importancia de convertir las políticas de seguridad de la información en comportamientos cotidianos de los empleados, es decir, trabajar en la construcción de una cultura organizativa de seguridad de la información[31,32]. Además, la

[26] WEIRICH, Dirk. Persuasive password security.Londres, 2005.Tesis para optar al título de doctor en filosofía. University of London.Department of Computer Science. p. 51.

[27] BEAUTEMENT, Adam, et al. Modelling human and technological costs and benefits of USB memory stick security. En: Workshop on economics in information security 2008. (2008); p. 1.

[28] VROOM, Cheryl y VON SOLMS, Rossouw. Towards information security behavioural compliance. En: Computers & Security. Vol. 23, No. 3 (May. 2004); p. 193.

[29] BULGURCU, Burcu, CAVUSOGLU, Hasan y BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. En: Mis Quarterly. Vol. 34, No. 3 (Sep. 2010); p. 523.

[30] BISHOP, Matt y FRINCKE, Deborah. A human endeavor: lessons from Shakespeare and beyond. En: IEEE Security & Privacy Magazine. Vol. 3, No. 4 (Jul. 2005); p. 49.

[31] VON SOLMS, Rossouw y VON SOLMS, Bassie. From policies to culture. En: Computers & Security. Vol. 23, No. 4 (Jun. 2004); p. 279.

[32] VON SOLMS, Bassie. Information Security: the third wave? En: Computers & Security. Vol. 19 (2000); p. 618.

necesidad de cambiar el enfoque en tecnología por un enfoque en las personas[33,34]. De los diferentes enfoques del cumplimiento de políticas de seguridad de la información, la formación es el más comúnmente sugerido en la literatura[35,36].

Otro aspecto que se ha profundizado, es la relación entre la cultura de seguridad de la información y la cultura corporativa, resaltando que estas dos deberían estar alineadas y como se influencian mutuamente[37,38].

3.6 Aspectos económicos

Bojanc y JermanJerman-Blažič (2008), analizan varios enfoques que permitan evaluar las inversiones necesarias en tecnología de seguridad desde el punto de vista económico. Además presenta los métodos para la identificación de los activos, las amenazas, las vulnerabilidades de los sistemas de TIC y propone un procedimiento que permite la selección de la inversión óptima de tecnología de seguridad necesaria basada en la cuantificación de los valores de los sistemas protegidos.

Salmela (2007) examina el uso de análisis de procesos de negocio como un método para asociar los riesgos de los sistemas de información con las pérdidas potenciales del negocio.

3.7 Gobernanza de seguridad de la información

La gobernanza como concepto aislado representa: "el proceso de toma de decisiones y el proceso por el que las decisiones son implementadas"[39]. Al hablar de gobernanza corporativa se hace referencia al compromiso de la dirección ejecutiva de una compañía y consiste en "un conjunto de políticas y controles internos por los cuales las organizaciones, sin importar su tamaño, son dirigidas y gestionadas"[40]. Del mismo modo, la gobernanza de seguridad de la información describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización.

Al respecto, varios autores[41,42], muestran que la seguridad de la información debe ser una prioridad de la dirección ejecutiva, incluida la Junta Directiva, y por lo tanto, debe comenzar como una responsabilidad de gobierno corporativo. Esto establece la necesidad

[33] KAYWORTH, Tim y WHITTEN, Dwayne. Effective information security requires a balance of social and technology factors. En: MIS Quarterly Executive. Vol. 9, No. 3 (Sep. 2010); p.164.

[34] JOHNSON, M. Eric y GOETZ, Eric. Embedding information security into the organization. En: IEEE Security & Privacy Magazine. Vol. 5, No. 3 (May. 2007); p. 16.

[35] PUHAKAINEN, Petri y SIPONEN, Mikko. Improving employees' compliance through information systems security training: an action research study. En: Mis Quarterly. Vol. 34, No. 4 (Dic. 2010); p. 758.

[36] VON SOLMS y VON SOLMS (2004), Op. cit., p. 279.

[37] CHANG, Shuchih y LIN, Chin-Shien.Exploring organizational culture for information security management. En: Industrial Management & Data Systems. Vol. 107, No. 3 (2007); p. 438.

[38] LIM, Joo, et al. Exploring the relationship between organizational culture and information security culture. En: Proceedings of the 7th Australian information security management conference. (2009); p. 8-9.

[39] COMISIÓN ECONÓMICA Y SOCIAL DE LAS NACIONES UNIDAS. ¿Qué es gobernanza? ¿y buen gobierno? [en línea]. [consultado el 8 de mayo de 2012]. Disponible en <http://www.casaasia.es/governasia/boletin2/3.pdf>

[40] NATIONAL CYBER SECURITY SUMMIT TASK FORCE. Information security governance: a call to action. [en línea]. [consultado el 15 de septiembre de 2012]. Disponible en <http://www.cyberpartnership.org/InfoSecGov4_04.pdf>

[41] POSTHUMUS, Shaun y von Solms, Rossouw. A framework for the governance of information security. En: Computers & Security. Vol. 23, No. 8 (2004); p. 638.

[42] VON SOLMS, Bassie y VON SOLMS, Rossouw. From information security to… business security? En: Computers & Security. Vol. 24, No. 4 (Jun. 2005); p. 271.

de integrar la seguridad de la información en la dirección corporativa a través del desarrollo de un marco de gobierno de la seguridad de la información.

De acuerdo con von Solms (2006), la gobernanza de seguridad de la información hace parte integral de la gobernanza corporativa, y consiste en:

- El compromiso y conciencia de la alta dirección en cuanto a la gestión y liderazgo de una buena seguridad de la información.
- Las estructuras organizativas apropiadas para reforzar la buena seguridad de la información.
- Conocimiento de requisitos legales y reglamentarios, en cuanto a privacidad de los datos y la información se refiere.
- Óptimas implementaciones de políticas, procedimientos, procesos, tecnologías y mecanismos de cumplimiento necesarios, que mejoren falencias o eviten consecuencias nefastas debido a negligencia en una buena seguridad de la información.

Por otra parte, Knapp et al. (2009) presenta la "gobernanza de seguridad de la información", como un componente general que afecta directamente a todas las etapas del proceso de gestión de política de seguridad de la información, insistiendo en que la gobernanza no es solamente un proceso interno de la organización, sino que también puede incluir la participación de entes externos tales como el comité directivo.

3.8 Políticas

En la literatura, hay amplio acuerdo en que una buena política de seguridad de información es la base de la seguridad de la información en las organizaciones[43,44,45,46]. Según David[47], "sin políticas de seguridad formales, la seguridad es arbitraria, sujeta a los caprichos de aquellos que la administran".

Los resultados de la evaluación y análisis de riesgos, deben conducir a la elaboración de la política de seguridad, la cual consiste en un documento que indica el compromiso y apoyo de la dirección, así como la definición del papel que debe jugar la seguridad de la información en la consecución de la misión y visión de la organización. En esencia, la política de seguridad se documenta para explicar la necesidad de seguridad de la información - y sus principios - a todos los usuarios de los recursos de información[48].

Algunas características de una política eficaz, son:

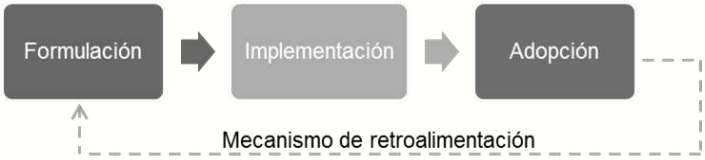
[43] BASKERVILLE, Richard y SIPONEN, Mikko. An information security meta-policy for emergent organizations. En: Logistics Information Management. Vol. 15, No. 5/6 (2002); p. 337.
[44] KNAPP, Kenneth, et al. Information security policy: an organizational-level process model. En: Computers & Security. Vol. 28, No. 7 (Oct. 2009): p. 493.
[45] VON SOLMS y VON SOLMS (2004). Op. cit., p. 372
[46] DAVID, Jon. Policy enforcement in the workplace. En: Computers & Security. Vol. 21, No. 6 (2002); p. 506.
[47] Ibid. p. 506.
[48] HÖNE, Karin y ELOFF, J.H.P. Information security policy – what do international information security standards say? En: Computers & Security. Vol. 21, No. 5 (2002); p. 402.

- Ser relevante, accesible, y comprensible para todos los usuarios previstos de la organización.
- Especificar su frecuencia de revisión y las formas en que será comunicada a toda la organización.

Entre los aspectos que debería contener el documento sobre políticas de seguridad se encuentran[49,50,51]: definición de seguridad para los activos de información, responsabilidades, planes de contingencia, gestión de contraseñas, sistema de control de acceso, respaldo de datos, y manejo de virus e intrusos. Además se debe incluir el tema del reporte de incidentes de seguridad, sobre el cual se deben establecer lineamientos claros dentro de la política de seguridad de la compañía[52].

Para la creación de las políticas, se debe tener la participación activa de los colaboradores, o miembros de la organización, donde al mismo tiempo se involucran las actividades de éstos y el entorno de trabajo. Según Karyda, Kiiountouzis y Kokolakis[53], los tres procesos involucrados en la adopción de una política de seguridad son: formulación, implementación y adopción. Ver Figura 4.

Figura 4. Proceso de aplicación de una política de seguridad



Fuente. Autores a partir de KARYDA, Maria, KIOUNTOUZIS, Evangelos y KOKOLAKIS, Spyros. Information systems security policies: a contextual perspective. En: Computers & Security. Vol. 24, No. 3 (2005); p. 248.

3.9 Buenas prácticas

Las buenas prácticas (*bestpractices)* "definen prácticas y procedimientos que permitan crear un ambiente consistente que sea seguro mientras siga siendo útil"[54]. En casi todas las áreas del conocimiento y del mundo económico se requieren estándares que permitan establecer bases y criterios para la excelencia. El campo de la seguridad de la información no ha sido la excepción.

Según Von Solms (2000), las buenas prácticas internacionales, para la gestión de la seguridad de la información, son la compilación de experiencias combinadas de muchas

[49] DOHERTY, Neil y FULFORD, Heather. Aligning the information security policy with the strategic information systems. En: Computers & Security. Vol. 25, No.1 (2006); p. 57.
[50] HÖNE y ELOFF. Op. cit., p. 403-404.
[51] LINDUP, KENNETH. A new model for information security policies. En: Computers & Security. Vol. 14, No. 8 (1995); p. 694.
[52] WIANT, Terry. Information security policy's impact on reporting security incidents. En: Computers& Security. Vol. 24, No. 6 (Sep. 2005); p. 449.
[53] KARYDA, Maria, KIOUNTOUZIS, Evangelos y KOKOLAKIS, Spyros. Information systems security policies: a contextual perspective. En: Computers & Security. Vol. 24, No. 3 (2005); p. 248.
[54] Information Security Best Practices. [En línea]. [Consultado 16 febrero 2012]. Disponible en: <http://networking.lamar.edu/files/LU%20Best%20Practices%20Final.pdf>

compañías internacionales influyentes, acerca de la forma en que ellos gestionan la seguridad de la información. Estas prácticas reflejan la experiencia de dichas empresas sobre las medidas de control relevantes, procedimientos y técnicas, que proporcionan un nivel adecuado o aceptable de seguridad de la información.

Además, las buenas prácticas proveen un marco de trabajo como referencia para asegurar que las organizaciones cubran todas las bases de seguridad de la información. Uno de los documentos más conocidos de este tipo, es el código de buenas prácticas para la gestión de la seguridad, ISO/IEC 27002[55]. Este estándar establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización. Además, tiene 133 medidas de control de alto nivel que abarcan tanto las amenazas externas como internas, las cuales se agrupan en 11 dimensiones (cláusulas). La consideración de otros controles de seguridad, no incluidos en ISO/IEC 27002, podría ser requerida para proveer mayor protección especialmente para activos de gran valor o para contrarrestar los niveles excepcionalmente altos de las amenazas de seguridad[56]. De igual forma, la norma ISO/IEC 27001, es el único esquema de aceptación internacional que permite certificación.

Finalmente, es importante mencionar el concepto de conformidad, que es el proceso práctico de comparar los controles aplicados en una organización con aquellos propuestos en ISO/IEC 27002. Es básicamente un análisis de brechas en el cual se descubren las diferencias entre la situación de la organización y el estándar. Al respecto, Karabacak y Sogukpinar (2006), proponen un método cuantitativo basado en una encuesta que evalúa la conformidad de ISO/IEC 27002. Este tiene cualidades únicas como su facilidad de uso y flexibilidad. Se pueden cambiar fácilmente el número de preguntas, opciones de respuesta y ajustar los valores numéricos para las mismas.

4. CONCLUSIONES

En este trabajo se ha analizado elementos relacionados con la base teórica necesaria para un marco de trabajo en la gestión de la seguridad de la información. Al respecto, algunos autores como Hong et al. (2003) sugieren que la ausencia de un marco y una metodología en el tema han contribuido a la falta de teoría en gestión de la seguridad de la información. De lo anterior, el aporte significativo de este documento es la clasificación de las variables estratégicas del sistema de investigación en el área de seguridad de la información y el desarrollo de un lenguaje común para ello. Por supuesto, este marco debe integrarse con otros puntos de vista a fin de logran una comprensión holística del tema.

Teniendo en cuenta que la información (y el conocimiento) se ha convertido en una fuente de riqueza y de riesgo para las compañías (sea que decidan protegerla activamente o no), aquellos involucrados en la gestión de información necesitan entender la complejidad e

[55] INTERNATIONAL STANDARDS ORGANIZATION. ISO/IEC 27002:2005. Código para la práctica de la gestión de la seguridad de la información. 2005, p 7.*Sistemas de Gestión de la Seguridad de la Información (SGSI) – Requisitos

[56] VON SOLMS, Basie. Information security: a multidimensional discipline. En: Computers & Security. Vol. 20, No. 6 (2001); p. 505.

importancia de su aseguramiento. Se puede argumentar entonces, que las organizaciones deben utilizar el marco presentado en este documento con el fin de poner un poco de estructura en un área intrínsecamente no estructurada como lo es la gestión de seguridad de la información. Además, se logró identificar que en una organización donde el conocimiento es el activo más importante, no puede abordarse asuntos específicos de seguridad de la información sin antes implementar una política que ayude a escoger los controles adecuados para disminuir los riesgos que se identifiquen, y tener una priorización clara de los asuntos de seguridad a tratar para que los controles implementados sean coherentes con los requerimientos de seguridad de la organización.

Además, cabe destacar que a pesar de que se ha hecho esfuerzo por cambiar el enfoque técnico por un enfoque de gestión. Aún las evaluaciones de riesgo están encaminadas a la identificación de amenazas técnicas, por lo cual es necesario profundizar en la identificación de amenazas y vulnerabilidades provenientes del eslabón más débil: el recurso humano.

Al respecto, existe alguna preocupación de profesionales y académicos por la ausencia de una base teórica y un acercamiento formal a la gestión de seguridad de la información, Herath (2008) advierte que la investigación empírica sobre las conductas en los usuarios de la información y los factores que influyen en ellas apenas ha comenzado. Se concluye finalmente, que futuras investigaciones podrían estar encaminadas hacia los riesgos correspondientes al capital intelectual más allá de la misma información.

REFERENCIAS

BASKERVILLE, Richard y SIPONEN, Mikko. An information security meta-policy for emergent organizations. En: Logistics Information Management. Vol. 15, No. 5/6 (2002); p. 337-346.

BEAUTEMENT, Adam, et al. Modelling human and technological costs and benefits of USB memory stick security. En: Workshop on economics in information security 2008. (2008); p. 1.

BISHOP, Matt y FRINCKE, Deborah. A human endeavor: lessons from Shakespeare and beyond. En: IEEE Security & Privacy Magazine. Vol. 3, No. 4 (Jul. 2005); p. 49.

BOJANC, Rok y JERMAN-BLAŽIČ, Borka. An economic modeling approach to information security risk management. En: International Journal of Information Management. Vol. 28, No. 5 (2008); p. 413-422.

BRYNJOLFSSON, Erik y HITT, Lorin. Paradox lost? Firm-level evidence on the returns to information systems spending. En: Management science. Vol. 42, No. 4 (Abr. 1996). Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

BULGURCU, Burcu, CAVUSOGLU, Hasan y BENBASAT, Izak. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. En: Mis Quarterly. Vol. 34, No. 3 (Sep. 2010); p. 523.

CHANG, Shuchih y LIN, Chin-Shien. Exploring organizational culture for information security management. En: Industrial Management & Data Systems. Vol. 107, No. 3 (2007); p. 438.

COMISIÓN ECONÓMICA Y SOCIAL DE LAS NACIONES UNIDAS. ¿Qué es gobernanza? ¿y buen gobierno? [en línea]. [consultado el 8 de mayo de 2012]. Disponible en http://www.casaasia.es/governasia/boletin2/3.pdf

DAVID, Jon. Policy enforcement in the workplace. En: Computers & Security. Vol. 21, No. 6 (2002); p. 506-513.

DESOUZA, Kevin y VANAPALLI, Ganesh. Securing knowledge in organizations: lessons from the defense and intelligence sectors. En: International Journal of Information Management. Vol. 25, No. 1 (Feb. 2005); p. 85-98.

DOHERTY, Neil y FULFORD, Heather. Aligning the information security policy with the strategic information systems. En: Computers & Security. Vol. 25, No.1 (2006); p. 55-63.

DOHERTY, Neil; KING, Malcolm y AL-MUSHAYT, Omar. The impact of inadequacies in the treatment of organizational issues on information systems development projects. En: Information & Management. Vol. 41, No. 1 (Oct. 2003); p. 50.

DRUCKER, Peter. The coming of the new organization. En: Harvard Business Review. Vol. 66, No. 1 (1988); p. 47.

ENISA - Agencia Europea de Seguridad de las Redes y de la Información (n.d). RiskManagement - RiskAssessmentMethods: Magerit. [en línea]. [Consultado el 10 de Octubre de 2011]. Disponible en: http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html

FARN, Kwo-Jean, LIN, Shu-Kuo y FUNG, Andrew Ren-Wei. A study on information security management system evaluation: assents, threat and vulnerability. En: Computer Standards& Interfaces. Vol. 26, No. 6 (2004); p. 507.

GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age. En: Computers & Security. Vol. 24, No. 1 (Ene. 2005); p. 28.

GLASER, Timo y PALLAS, Frank. Information security and knowledge management: solutions through analogies?Berlin: Universidad Técnica de Berlín, 2007, p. 17.

GOODALL, John, LUTTERS, Wayne y KOMLODI, Anita. Developing expertise for network intrusion detection.En: Information Technology & People. Vol. 22, No. 2 (2009); p. 7.

GUTIÉRREZ, Javier J. ¿Qué es un framework web? Universidad de Sevilla. [En Línea]. [Citado 28 julio, 2012]. Disponible en internet: http://www.lsi.us.es/~javierj/investigacion_ficheros/Framework.pdf

HERATH, Tejaswini. Essays on information security practices in organizations. Buffalo, 2008. Dissertation (Doctor of Philosophy).University of New York. Faculty of the graduate school. p. 9.

HÖNE, Karin y ELOFF, J.H.P. Information security policy – what do international information security standards say? En: Computers & Security. Vol. 21, No. 5 (2002); p. 402-409.

HONG, Kwo-Shing, et al. An integrated system theory of information security management. En: Information Management & Computer Security. Vol. 11, No. 5 (2003); p. 243-244.

INFORMATION SECURITY BEST PRACTICES. [En línea]. [Consultado 16 febrero 2012]. Disponible en: http://networking.lamar.edu/files/LU%20Best%20Practices%20Final.pdf

INTERNATIONAL STANDARDS ORGANIZATION. ISO/IEC 27002:2005. Código para la práctica de la gestión de la seguridad de la información. 2005, p 7.*Sistemas de Gestión de la Seguridad de la Información (SGSI) – Requisitos

JOHNSON, M. Eric y GOETZ, Eric. Embedding information security into the organization. En: IEEE Security & Privacy Magazine. Vol. 5, No. 3 (May. 2007); p. 16-24.

KARABACAK, Bilge y SOGUKPINAR, Ibrahim. A quantitative method for ISO 17799 gap analysis. En: Computers& Security. Vol. 25 (2006); p. 419.

KARYDA, Maria, KIOUNTOUZIS, Evangelos y KOKOLAKIS, Spyros. Information systems security policies: a contextual perspective. En: Computers & Security. Vol. 24, No. 3 (2005); p. 248.

KAYWORTH, Tim y WHITTEN, Dwayne. Effective information security requires a balance of social and technology factors. En: MIS Quarterly Executive. Vol. 9, No. 3 (Sep. 2010); p. 163-175.

KNAPP, Kenneth, et al. Information security policy: an organizational-level process model. En: Computers & Security. Vol. 28, No. 7 (Oct. 2009): p. 493-508.

KRAEMER, S., CARAYON, P. y CLEM, J.F. Characterizing violations in computer and information security systems.En: Proceedings of the 16th Triennial World Congress of the International Ergonomics Association (IEA). 2006.

LATEGAN, Neil y VON SOLMS, Rossouw. Towards enterprise information risk management: a body analogy. En: Computer Fraud & Security. Vol. 2006, No. 12 (Dic. 2006); p. 17

LAYTON, T. Information Security: Design, implementation, measurement and compliance. Boca Raton: Auerbach Publications, 2007, p. 23 – 40.

LIM, Joo, et al. Exploring the relationship between organizational culture and information security culture. En: Proceedings of the 7th Australian information security management conference. (2009); p. 8-9.

LINDUP, KENNETH. A new model for information security policies. En: Computers & Security. Vol. 14, No. 8 (1995); p. 694.

MARKUS, Lynne. Technochange management: using IT to drive organizational change. En: Journal of Information Technology. Vol. 19, No. 1 (2004); p. 4.

MITNICK, Kevin y SIMON, William. The art of deception: controlling the human element of security. Indianapolis: Wiley Publishing, 2002, p. 79.

NNOLIM, Anene. A framework and methodology for information security management. Southfield, 2007. Dissertation (Doctor of Management in Information Technology). Lawrence Technological University. Graduate Faculty of the College of Management. p.2-13.

PEPPARD, Joe. The conundrum of IT management. En: European Journal of Information Systems. Vol. 16, No. 1 (2007); p. 339.

PORTER, Michael y MILLAR, Victor. How information gives you competitive advantage. En: Harvard Business Review. Vol. 64, No. 4 (1985); p. 149.

POSTHUMUS, Shaun y von Solms, Rossouw. A framework for the governance of information security. En: Computers & Security. Vol. 23, No. 8 (2004); p. 638-646.

PUHAKAINEN, Petri y SIPONEN, Mikko. Improving employees' compliance through information systems security training: an action research study.En: Mis Quarterly. Vol. 34, No. 4 (Dic. 2010); p. 757-778.

SALMELA, Hannu. Analysing business losses caused by information systems risk: a business process analysis approach. En: Journal of Information Technology. Vol. 23, No. 3 (2007); p. 185-202.

SIRCAR, Sumit y CHOI, Jung. A study of the impact of information technology on firm performance: a flexible production function approach. En: Information Systems Journal. Vol. 19, No. 3 (2009). Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

SYALIM, Amril, HORI, Yoshiaki y SAKURAI, Kouichi. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide, En: International Conference on Availability, Reliability and Security. 2009, p. 726.

VON SOLMS, Basie. Information security: a multidimensional discipline. En: Computers & Security. Vol. 20, No. 6 (2001); p. 505.

VON SOLMS, Bassie y VON SOLMS, Rossouw. From information security to… business security? En: Computers & Security. Vol. 24, No. 4 (Jun. 2005); p. 271-273.

VON SOLMS, Bassie y VON SOLMS, Russouw. The 10 deadly sins of information security management. En: Computers & Security. Vol. 23, No. 5 (Jul. 2004); p. 371-376.

VON SOLMS, Bassie. Information Security: the fourth wave. En: Computers & Security. Vol. 25, No. 3 (May. 2006); p. 165-168.

VON SOLMS, Bassie. Information Security: the third wave? En: Computers & Security. Vol. 19 (2000); p. 615-620.

VON SOLMS, Rossouw y VON SOLMS, Bassie. From policies to culture. En: Computers & Security. Vol. 23, No. 4 (Jun. 2004); p. 275-279.

VROOM, Cheryl y VON SOLMS, Rossouw. Towards information security behavioural compliance. En: Computers & Security. Vol. 23, No. 3 (May. 2004); p. 193.

WALLACE, William. La Gestión del Conocimiento. En: Knowledge Management Today. Sevilla, Diciembre 1999. Citado por http://www.a3net.net/es/gescon/definiciones.htm

WADLOW, Thomas. The process of network security: designing and managing a safe network. Reading: Addison-Wesley Professional, 2000, p. 304.

WARD, Jhon y PEPPARD, Joe. Strategic planning for information systems. 3 ed. Chichester: Wiley Publishing, 2002. Citado por DOHERTY, Neil; ANASTASAKIS, Leonidas y FULFORD, Heather. The information security policy unpacked: a critical study of the content of university policies. En: International Journal of Information Management. Vol. 29, No. 6 (Dic. 2009); p. 449.

WEI, June y LI, Yi. Computer information systems threat analysis on security. En: 2004 IRMA International Conference. 2004, p. 951-953.

WEIRICH, Dirk. Persuasive password security. Londres, 2005.Tesis para optar al título de doctor en filosofía. University of London. Department of Computer Science. p. 51.

WHITMAN, Michael. In defense of the realm: understanding threats to information security. En: International Journal of Information Management. Vol. 24 (2004); p. 51-52

WILLS M. Personal communication. En: GERBER, Mariana y VON SOLMS, Rossouw. Management of risk in the information age.En: Computers & Security. Vol. 24 (2005); p. 17.

ZAMMUTO, Raymond, et al. Information technology and the changing fabric of organization. En: Organization Science. Vol. 18, No. 5 (Sep. 2007); p. 751.