estud.gerenc. 28 (2012) 87-95

ESTUDIOS GERENCIALES

www.elsevier.es/estudios_gerenciales

Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional

Marlene Lucila Guerrero Julio [a,*] y Luis Carlos Gómez Flórez [b]

[a]*Decana, Facultad de Ingeniería, Universidad Cooperativa de Colombia, Bucaramanga, Colombia*
[b]*Profesor Titular, Universidad Industrial de Santander, Colombia*

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:
Recibido el 27 de mayo de 2011
Aceptado el 13 de diciembre de 2012

Códigos JEL:
M15
M42

Palabras clave:
Gestión de riesgos y controles
Aprendizaje
Pensamiento de sistemas blandos
Sistemas de información
Transformación organizacional

RESUMEN

La gestión de riesgos y controles en sistemas de información (GRCSI) comúnmente se ve como una función técnica encomendada a expertos en tecnologías de la información, ingenieros de *software* o programadores de sistemas de información. No obstante, esta labor requiere una perspectiva más amplia que aporte al aprendizaje de su sentido y a la apropiación de los procesos de cambio organizacional que ella requiere. Este artículo presenta el resultado de un proceso de investigación, abordado desde la perspectiva del pensamiento de sistemas blandos para apoyar la GRCSI en las organizaciones, mostrando el sistema de actividad humana de la dirección estratégica de tecnologías de información, la transformación organizacional necesaria y la descripción de las actividades y métodos propuestos.

JEL classification:
M15
M42

Keywords:
Risk management and controls
Learning
Information systems
Soft system thinking
Organizational transformation

Risk management and controls in information systems: from the learning to organizational transformation

ABSTRACT

Risk management and controls for information systems (RMCIS) is commonly seen as a technical function used by experts in information technology, software engineers, or information systems programmers. . However, this task requires a much broader perspective that helps the learner have better comprehension of its meaning and the processes of organizational change that it requires. This article shows the results of a research process, approached from the perspective of soft systems thinking, to support RMCIS in organizations, showing the human activity system of the strategic management of information technology, the organizational changes necessary, and a description of the activities and methods proposed.

Classificação JEL:
M15
M42

Palavras-chave:
Gestão de riscos e controlos
Aprendizagem
Pensamento de sistemas moles
Sistemas de informação
Transformação organizacional

Gestão de riscos e controlos em sistemas de informação: da aprendizagem à transformação organizacional

RESUMO

A gestão de riscos e controlos em sistemas de informação (GRCSI) é habitualmente vista como uma função técnica encomendada a especialistas em tecnologias da informação, engenheiros de software ou programadores de sistemas de informação. No entanto, este trabalho necessita de uma perspectiva mais larga que dê sentido à aprendizagem e à adequação dos processos à mudança organizacional que ela necessita. Este artigo apresenta o resultado de um processo de investigação, abordado da perspectiva do pensamento de sistemas moles para apoiar a GRCSI nas organizações, mostrando o sistema de actividade humana da direcção estratégica de tecnologias de informação, a transformação organizacional necessária e a descrição das actividades e métodos propostos.

*Autor para correspondencia: Universidad Cooperativa de Colombia, Calle 30.ª N.º 33-51 Piso 6 Oficina 605, Bucaramanga, Colombia.
Correo electrónico: marlene.guerrero@ucc.edu.co (M.L. Guerrero Julio).

0123-5923/$ see front matter

1. Introducción

Actualmente, según Laudon y Laudon (2008), el auge en el desarrollo de los sistemas de información ha generado mayor crecimiento y competitividad en las organizaciones al apoyar los procesos de negocio, las actividades de procesamiento de la información y las actividades de administración, lo que abre un sinnúmero de posibilidades para ampliar las relaciones entre clientes, proveedores y empleados, y posibilita la rapidez en las respuestas a los cambios en el entorno (Aguilera y Riascos, 2009).

No obstante, en un estudio realizado por Piattini (2007), basado en la denominada crisis de la ingeniería del *software*, se logró determinar que el 23% de los desarrollos de sistemas de información fallan, en contraste con un 49% cuyo desarrollo es cuestionado y con sólo un 28% entregado satisfactoriamente. Lo anterior ha llevado a las organizaciones a preocuparse cada vez más por las pérdidas económicas acarreadas por los riesgos ocasionados tanto por la propia naturaleza de los sistemas de información como por la falta de calidad en su desarrollo.

En este punto, la gestión de riesgos y controles en sistemas de información (GRCSI) tiene un papel esencial en la protección de los riesgos relacionados con los sistemas de información, al proporcionar a las organizaciones capacidades para: alinear los niveles de riesgo con su impacto organizacional y el retorno de la inversión, optimizar la toma de decisiones y minimizar las pérdidas.

El objetivo principal de la GRCSI en una organización es proteger sus procesos de negocio y su capacidad para cumplir su misión. Por lo tanto, la GRCSI no debe ser tratada solamente como una función técnica realizada por los expertos de tecnologías de información que manejan los sistemas de información, sino como una labor organizacional que requiere una perspectiva mucho más compleja que la que se da desde el pensamiento duro (Adams, 2005) y que incluye los sistemas de actividad humana (SAH) encargados de su utilización y su desarrollo durante todo el ciclo de vida.

En este artículo, se presenta una propuesta para la GRCSI, desde la perspectiva de pensamiento blando, partiendo desde los diagnósticos exploratorios acerca de los estándares y la literatura relevante para la GRCSI planteado por Guerrero y Gómez (2011), hasta llegar al diseño de los SAH (Checkland, 2000a; Checkland y Scholes, 1999a; Checkland y Scholes, 1999b) encargados de dicha labor en las organizaciones.

En la primera sección del documento se presentará una descripción del aporte de la metodología de los sistemas blandos al proceso de investigación desarrollado. En la segunda sección se analizará y describirá el sistema de actividad humana pertinente para la gestión de riesgos y controles en sistemas de información. Finalmente, en la tercera sección se plantearán las conclusiones obtenidas a partir de las reflexiones realizadas y las recomendaciones para futuras investigaciones.

2. La metodología de los sistemas blandos y su aporte al proceso de investigación

La metodología de los sistemas blandos (MSB) ha sido involucrada en estudios de sistemas de información a través del proceso de investigación-acción en las organizaciones en los últimos años, con el fin de apoyar a la disciplina desde la perspectiva organizacional (Checkland y Poulter, 2006). Lo anterior implica tener en cuenta los factores sociocultural, político y administrativo que en muchas ocasiones se tiende a minimizar o excluir (Checkland, 2000b; Checkland y Holwell, 1998).

La idea central detrás de la labor descrita por Checkland y Holwell es que los modelos conceptuales desarrollados en la MSB puedan ser utilizados para iniciar y estructurar discusiones sobre la información soportada por las actividades que las personas realizan en el mundo real, proceso que normalmente se conoce como análisis de requerimientos. Durante el desarrollo de la MSB, Checkland y Griffin (1970) diseñaron el primer modelo conceptual para determinar las necesidades de información de una empresa textil de mediano tamaño. Desde entonces, estudios como el de Gómez y Olave (2007) han permitido relacionar el pensamiento de sistemas en general y la MSB en particular con el campo de los sistemas de información (Checkland y Scholes, 1999a).

Por su parte, autores contemporáneos como Cater-Steel y Ka-Wai-Lai, entre otros (Cater-Steel y Al-Hakim, 2009), proveen una mirada a la aplicación de la MSB al mantenimiento y el desarrollo de sistemas de información. La mayoría de estas perspectivas señalan que en los últimos años el desarrollo de sistemas de información se ha ido incrementando, de tal manera que han apoyado el cambio organizacional desde el punto de vista de la funcionalidad, la flexibilidad y la disponibilidad de la información. Sin embargo, los sistemas de información no están exentos de errores y/o cambios en el entorno operativo al que brindan servicio, por lo cual es necesario realizar periódicamente estudios de evaluación de los riesgos a que se exponen, con el fin de generar controles que permitan disminuir el costo asociado a la pérdida de información y recursos informáticos.

Para efectos específicos de la investigación presentada en este artículo, la MSB permitió abordar el tema de la apropiación sobre el sentido y el propósito de la GRCSI en las organizaciones, desde el punto de vista de la definición de los procesos y las responsabilidades de cada uno de los actores que intervienen. Esto posibilitó establecer la definición de la transformación organizacional necesaria para llevar a cabo las actividades de GRCSI y la elaboración de casos de estudio para el aprendizaje de los diversos niveles de riesgo. En la figura 1 se presenta la aplicación de la metodología al contexto de la investigación mencionada anteriormente.

3. Hacia una comprensión del SAH para la GRCSI

La elaboración de la definición raíz del SAH pertinente para llevar a cabo la GRCSI en la organizaciones está basada en la revisión de la literatura y los estándares relevantes para la GRCSI; se presenta un estudio sobre los niveles de riesgo y los controles que podrían mitigarlos y una propuesta de integración de las actividades que las organizaciones deben desarrollar.

3.1. Transformación organizacional

La siguiente transformación organizacional corresponde al sistema planteado para la GRCSI para la cual se enuncian sus elementos CATWOE (abreviatura utilizada por Peter Checkland para elaborar la transformación organizacional. C: clientes; A: actores; T: transformación; W: *weltanschauung* —cosmovisión o perspectiva que da origen a la transformación organizacional—; O: *owners* —propietarios—, y E: restricciones del entorno).

«La GRCSI es un sistema que hace parte del sistema de gestión de seguridad de la información de una organización, el cual es desarrollado por la dirección estratégica de tecnologías de información y de responsabilidad de todos los miembros de la organización mediante el alineamiento con los estándares de seguridad de sistemas de información que permitan el establecimiento del contexto organizacional, la identificación de los activos críticos en los diferentes espacios de la organización, la identificación y evaluación de las amenazas y vulnerabilidades de los activos, el diseño de escenarios de riesgo de acuerdo con su impacto organizacional, el diseño de estrategias de tratamiento y protección basados en estándares y buenas prácticas, la documentación de los resultados y revisión de casos y la implementación de procesos de monitoreo y control; con el fin de proteger la misión y los activos de la organización y apoyar a los administradores de tecnologías de la información a equilibrar los costos económicos y operacionales de las medidas de seguridad utilizadas para proteger los Sistemas de Información que apoyan los procesos de negocio de la organización.» (Guerrero, 2010, p. 88.)

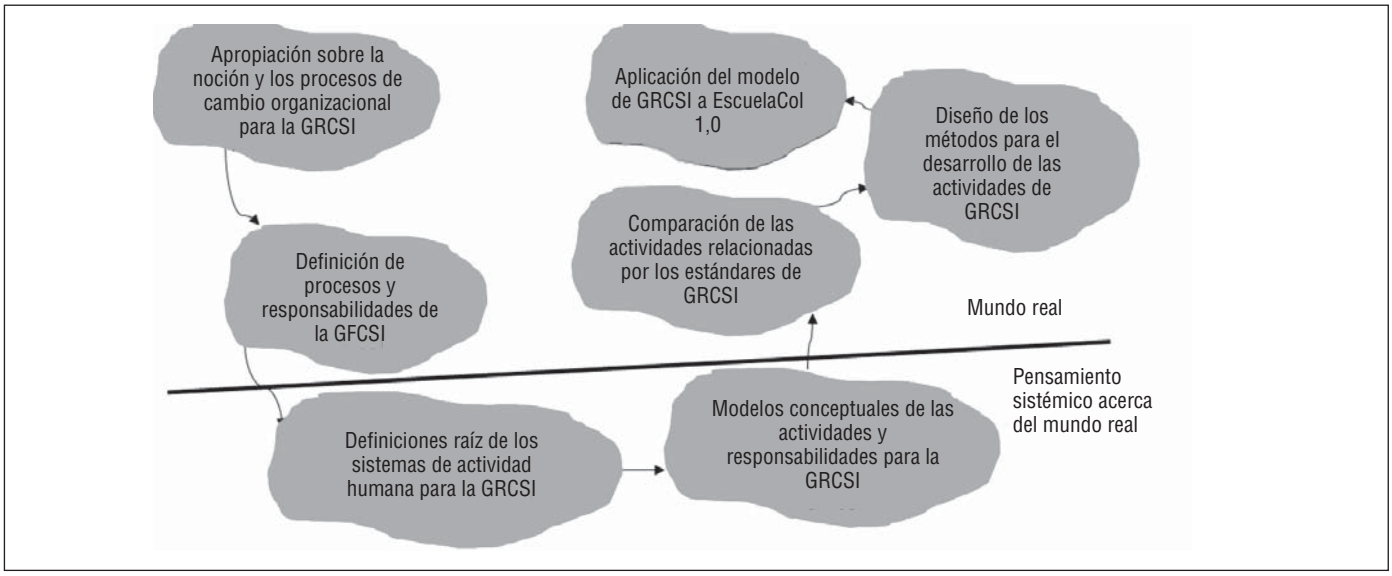

Figura 1. Aplicación de la metodología al contexto de la investigación.
GRCSI: gestión de riesgos y controles en sistemas de información.
Fuente. Adaptado de Checkland y Scholes (1999b). pp. 77-105.

3.2. Elementos CATWOE

Los elementos CATWOE para la transformación organizacional planteada, posibilitarán la selección de una perspectiva particular y la realización de un estructurado y riguroso proceso de desarrollo de los modelos. El punto de partida es una transformación para la perspectiva seleccionada y a partir de allí se identifican los otros elementos clave del sistema para la GRCSI (tabla 1).

En la transformación organizacional planteada se utilizarán los conceptos de amenaza, vulnerabilidad y riesgo, en el sentido planteado por Silberfich (2009), que explica que la amenaza es una condición del entorno del sistema de información, que ante determinada circunstancia podría ser una fuente de desastre informático y afectar a los activos de la compañía. Por su parte, la vulnerabilidad es una situación generada por la falta de controles que permite concretar una amenaza, y el riesgo es la posibilidad que una amenaza se materialice y produzca un impacto en la organización.

3.3. Descripción de las actividades propuestas para la GRCSI

Teniendo en cuenta la transformación organizacional construida, se planteó el sistema de actividades (fig.2) que permita a la dirección de tecnologías de información definir los niveles de riesgo de los sistemas de información en su contexto organizacional propio y que la organización pueda identificar los activos relacionados con los sistemas de información que, por su propia vulnerabilidad o por factores externos, están expuestos a amenazas. De igual manera, se busca que los miembros de la organización conozcan su función y su responsabilidad dentro de la GRCSI y que aprendan de los incidentes en la organización para evitar la repetición de esfuerzos y el desgaste organizacional.

3.3.1. Actividad A1. Establecer el contexto organizacional

Establecer el contexto organizacional es la actividad primaria que la empresa ha de llevar a cabo, dado que esto permite identificar las

Tabla 1
Elementos CATWOE de la transformación organizacional para la GRCSI

Elemento	Descripción
Clientes	Miembros de la organización y clientes de la organización
Actores	Dirección estratégica de tecnologías de información
Transformación	Dirección de tecnologías de información con necesidad de definir los niveles de riesgo de los sistemas de información en su contexto organizacional → contexto organizacional identificado y establecido
	Organización con necesidad de identificar los activos expuestos a amenazas y el impacto organizacional ocasionado por la vulnerabilidad de los sistemas de información → organización con elementos de acción para identificar los activos expuestos a amenazas y con conocimiento de los niveles de riesgo de los sistemas de información
	Entes organizacionales con necesidad de conocer su función y su responsabilidad dentro de la GRCSI → funciones y responsabilidades definidas
	Organización con necesidades de aprendizaje sobre los casos de riesgo ocurridos en la organización → organización con documentación de resultados sobre las estrategias de mitigación implantadas, monitoreo y control
Cosmovisión	La GRCSI ayuda a proteger los activos de la organización y ayuda a los administradores de tecnologías de la información a equilibrar los costos administrativos y operacionales de las medidas de seguridad utilizadas para proteger los sistemas de información que sustentan los procesos de negocio de las organizaciones, mediante el alineamiento con los estándares de seguridad de sistemas de información
Propietarios	Administración
Restricciones del entorno	Recursos, estándares utilizados

Fuente: tomado de Guerrero (2010), p. 89.

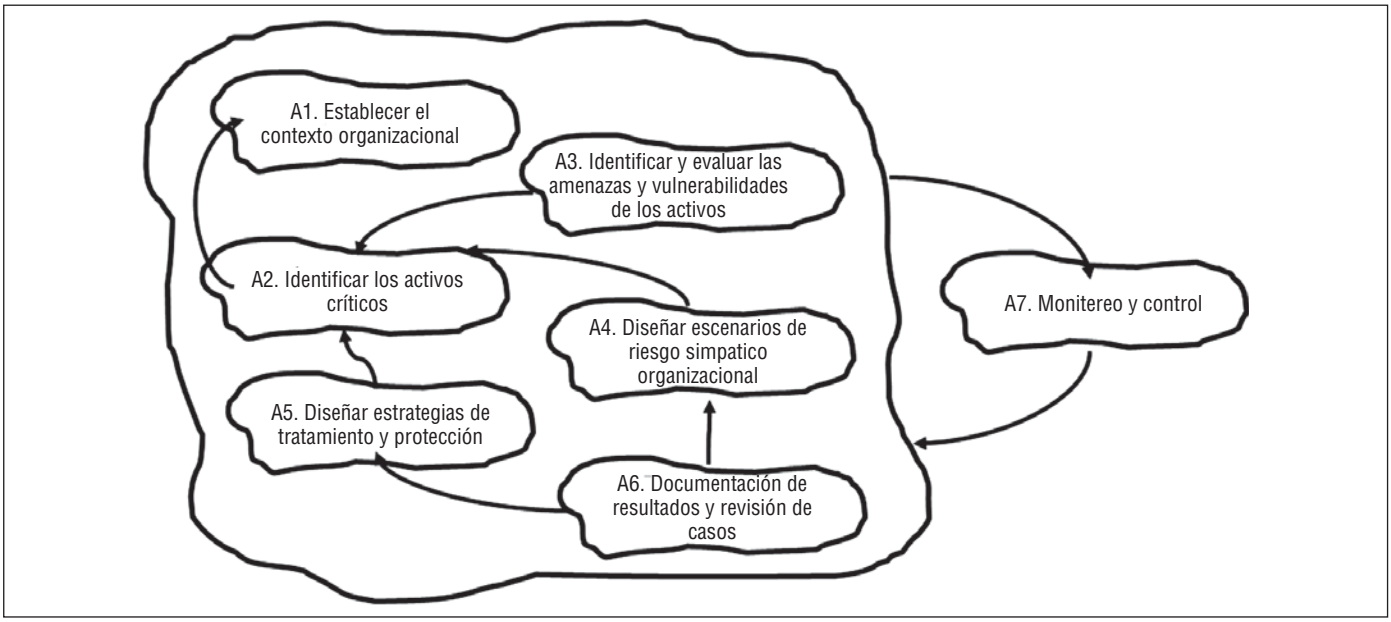

Figura 2. Sistema de actividades para la dirección de tecnologías de información.
Fuente: tomado de Guerrero (2010), p.90.

funciones y sus responsabilidades frente a la GRCSI. Como se ha expresado anteriormente, cada organización tiene una cultura particular, por lo cual la aplicación de esta actividad requiere repensar la organización en cuanto a sus necesidades, características, sistemas de información que apoyan los procesos de negocio, funciones y responsabilidades de los actores vinculados con los sistemas de información y la caracterización de la información que estos manejan.

Establecer el contexto organizacional es una actividad incluida directamente en los modelos planteados por AS/NZS (2004) *(Estándar Australiano para la Administración de Riesgos),* SP800-30 *(Guía para la Gestión de Riesgos en Tecnologías de la Información),* presentada por Stonebumer (2002), y SP800-39 *(Guía para la Gestión de Riesgos en Sistemas de Información),* los cuales posibilitaron plantear comparaciones que tienden a detectar la integración de las subactividades y diseñar los métodos para establecer el contexto organizacional para el desarrollo de la GRCSI (fig.3).

Las subactividades A1.1, A1.2 y A1.3 que se presentan a continuación y su alineamiento con los sistemas de información y los procesos de negocio deberán ser responsabilidad inicialmente de los administradores de la organización y del comité de seguridad encargado específicamente para esta labor.

3.3.1.1. Subactividad A1.1. Identificar la estrategia de la organización en torno a los sistemas de información

Las organizaciones efectivas deben ser capaces de clarificar las estrategias asociadas a los sistemas de información, las cuales deben

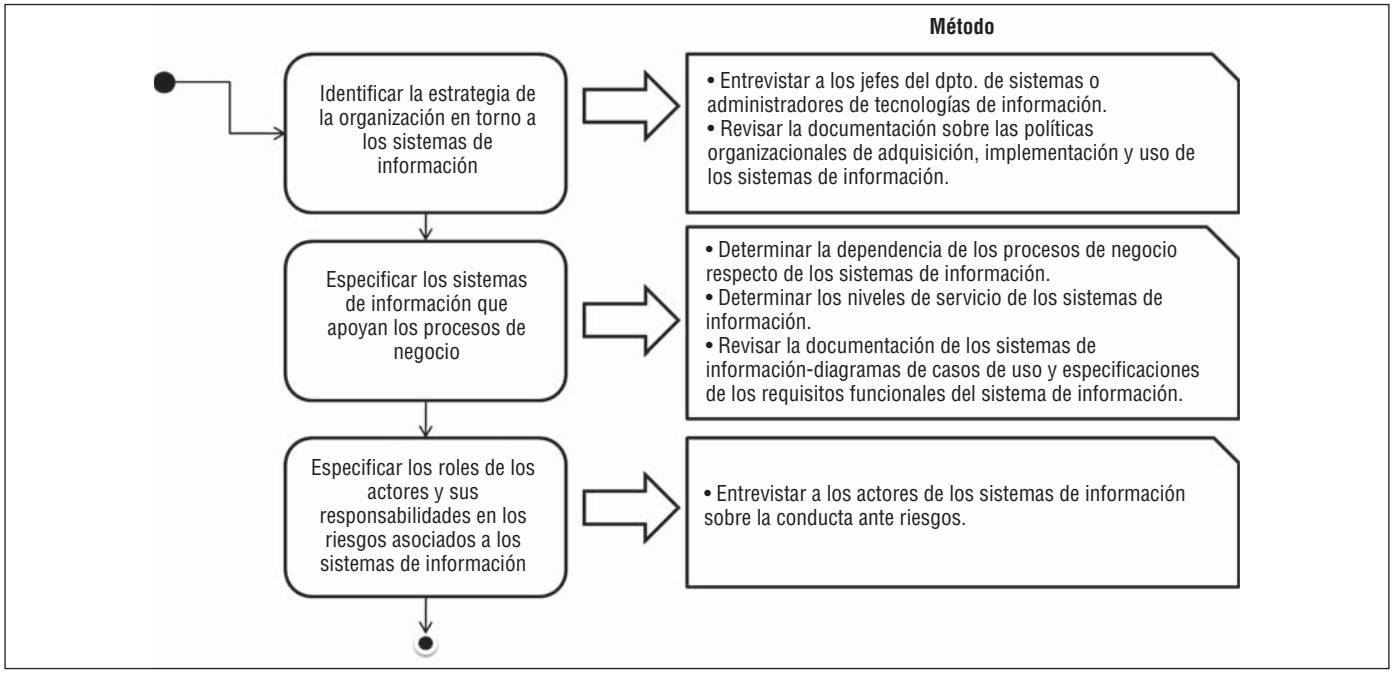

Figura 3. Métodos definidos para la actividad A1.
Fuente: tomado de Guerrero (2010), p.92.

estar enmarcadas dentro de la estrategia organizacional, de manera que los proyectos y las inversiones relacionadas con sistemas de información sean especificadas a los distintos actores de la organización y administradas de manera adecuada. Las tareas que la organización podría utilizar para llevar a cabo esta actividad se describen a continuación:

- Entrevistar a los jefes del departamento de sistemas o administradores de tecnologías de información. Esta tarea es desarrollada por los líderes de seguridad de la información en la organización. Uno de los métodos que se podría utilizar para esta actividad son las listas de verificación con preguntas orientadas a descubrir los intereses y/o necesidades organizacionales en términos de la estrategia asociada a los sistemas de información.
- Revisar la documentación sobre las políticas organizacionales de adquisición, implementación y uso de los sistemas de información. Esta tarea es desarrollada por el grupo de trabajo encargado del gobierno de tecnologías de información y sistemas de información con el fin de esclarecer si la organización tiene un nivel de madurez asociado con la adquisición, implementación y uso de los sistemas de información. La definición de estos niveles de madurez se sustenta en los estándares COBIT *(Control Objectives for Information and Related Technologies)* (ISACA, 2007) y CMM *(Capability Madurability Model)* (Paulk, Weber, Curtis y Chissis, 2001).

3.3.1.2. Subactividad A1.2. Especificar los sistemas de información que apoyan los procesos de negocio

Actualmente muchas organizaciones dan soporte a sus procesos de negocio con sistemas de información. Por lo tanto, un reconocimiento del contexto organizacional implica especificar los sistemas de información que apoyan a los procesos de negocio, de manera que se clarifique la dependencia de la ejecución de los procesos con respecto a la disponibilidad de los sistemas de información. Esta actividad es desarrollada por el grupo de trabajo encargado del gobierno de tecnologías de información. Las tareas que la organización podría utilizar para llevar a cabo esta actividad se describen a continuación.

- Determinar la dependencia de los procesos de negocio respecto de los sistemas de información. Dentro de las organizaciones, no todos los procesos de negocio se apoyan en sistemas de información, y en otros casos, aunque así sea, la dependencia de la continuidad del servicio de aquellos no es demasiado alta. Por lo tanto, una organización efectiva debe medir qué tanto depende de los sistemas de información la disponibilidad de sus procesos de negocio. La jerarquización de estos niveles de dependencia se basó en la propuesta de ISM3 (modelo de madurez para la seguridad de la información).
- Determinar los niveles de servicio de los sistemas de información. Esta tarea está orientada a establecer los servicios prestados por el sistema de información a los diferentes actores, que se podrá clasificar en niveles según su relevancia. Los niveles de servicio se clasificaron en «alto», «medio» o «bajo», de acuerdo con su relación con los requisitos funcionales del sistema de información.
- Revisar la documentación de los sistemas de información. La revisión de los manuales de usuario, administración, configuración e instalación del sistema de información es de vital importancia para establecer los riesgos asociados con los cambios realizados a los programas. De igual manera, la revisión de los diagramas de casos de uso del sistema implantado y de las especificaciones de los requisitos realizadas por la organización permitirá detectar el grado de cumplimiento de los requisitos contractuales del sistema de información.

3.3.1.3. Subactividad A1.3. Especificar las funciones de los actores y sus responsabilidades en la GRCSI

Los actores de los sistemas de información cumplen con una función de acuerdo con sus necesidades y los servicios prestados por el sistema de información. De acuerdo con esto, surgen responsabilidades en términos de la información que manejan. Esta actividad debe ser desarrollada por los jefes del departamento de tecnologías de información en concordancia con los administradores funcionales y de negocio. Las tareas que la organización podría utilizar para llevar a cabo esta actividad se describen a continuación:

- Entrevista a los actores de los sistemas de información sobre la conducta ante riesgos. Determinar la cultura de riesgo de los actores relacionados con los sistemas de información permite detectar y generar estrategias de mitigación de los riesgos ocasionados por dolo o negligencia (desconocimiento, falta de apropiación) de los actores. El método propuesto para esta actividad son las listas de verificación con preguntas orientadas a descubrir la conducta organizacional de los actores de sistemas de información ante los riesgos.

3.3.2. Actividad A2. Identificar los activos críticos

Los activos críticos relacionados con los sistemas de información son: la información, los servicios, las aplicaciones informáticas, los equipos informáticos, los soportes de información, el equipamiento auxiliar, las redes de comunicaciones, las instalaciones y las personas. Identificar los activos críticos es una actividad incluida en los modelos planteados por OCTAVE (marco de evaluación de amenazas operacionalmente críticas, activos y vulnerabilidades) en Alberts (1999) y MAGERIT (metodología de análisis y gestión de riesgos de los sistemas de información), que permitieron plantear comparaciones que tienden a detectar las integraciones en las subactividades y a diseñar los métodos relacionados con esta actividad (fig.4).

De igual manera, esta actividad busca determinar la información sensible y crítica, con el fin de identificar la información que puede estar expuesta a determinado nivel de riesgo. Información sensible es aquella que debe ser especialmente protegida, pues su revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o algo (Ribagorda, 1997; TCSEC, 1985). Por su parte, la información crítica es aquella de vital importancia para la organización, cuya pérdida o destrucción podría tener efectos adversos para la seguridad y la disponibilidad de los procesos de negocio (Norma RFC4949, 2007).

Las actividades pertinentes para la identificación de los activos críticos que se describen a continuación deberán ser responsabilidad inicialmente de la dirección de tecnologías de información.

3.3.2.1. Subactividad A.2.1. Catalogar los activos relacionados con los sistemas de información

Ofrecer información a la organización sobre los recursos asociados a los sistemas de información es de suma importancia para la toma de decisiones acertadas sobre las políticas y las estrategias de control relacionadas con sus vulnerabilidades. Esta actividad debe ser desarrollada por los jefes de seguridad de sistemas de información.

Para esta actividad se puede desarrollar un *software* de catalogación de activos que permita gestionar y controlar los recursos asociados a los sistemas de información o se puede llevar manualmente un consolidado de catalogación de activos.

3.3.2.2. Subactividad A.2.2. Determinar la información sensible y crítica

Clarificar qué la información que es sensible y crítica permite a las organizaciones generar estrategias para protegerla contra su divulgación, modificación o pérdida. Esta actividad es responsabilidad de los jefes del departamento de tecnologías de información. Una de las tareas que la organización podría utilizar para llevar a cabo esta actividad se describe a continuación:

- Revisar las bases de datos y los informes de los sistemas de información para detectar la información sensible y crítica. El contraste

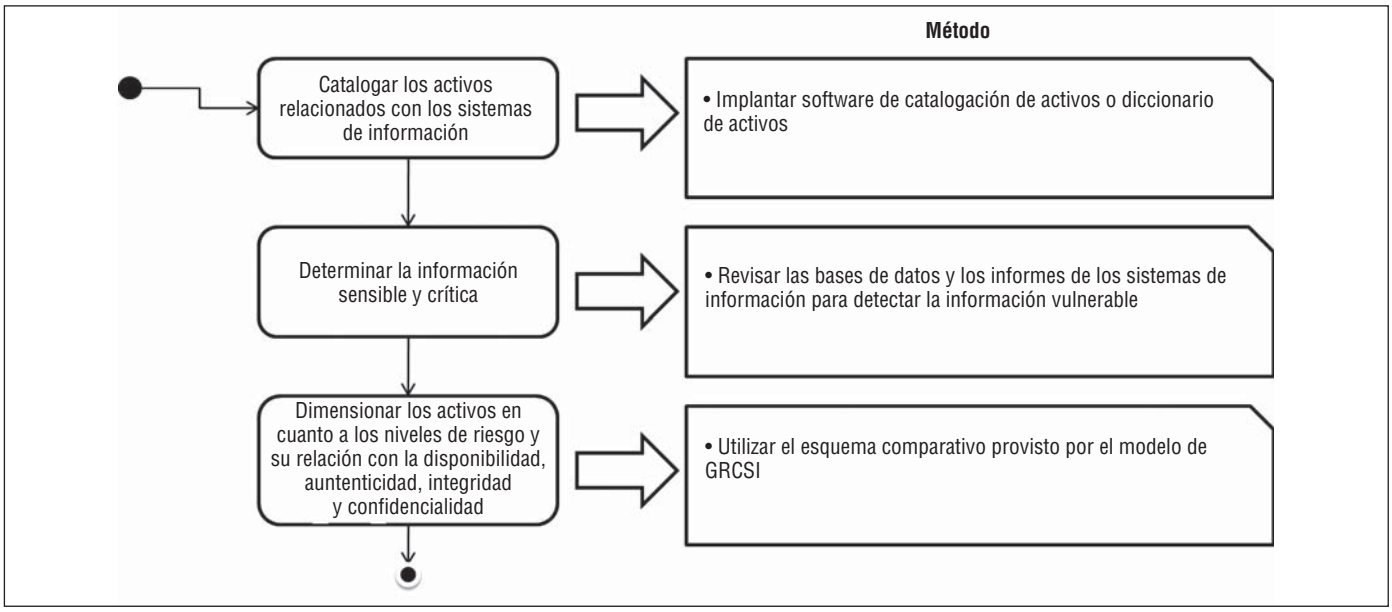

Figura 4. Métodos definidos para la actividad A2. GRCSI: gestión de riesgos y controles en sistemas de información.
Fuente: tomado de Guerrero (2010), p.99.

entre la base de datos del sistema de información y sus niveles de servicio permitirá identificar la información que es susceptible de resguardo o que hay que proteger. Cabe destacar que cada organización debe decidir esto a partir de lo crítica que sea la información y de los activos afectados por esta. Un esquema que se podría utilizar para realizar dicho contraste requiere una definición del nivel de servicio detectado, las tablas de la base de datos que las soporta y la información sensible y crítica que manejan.

3.3.2.3. Subactividad A2.3. Dimensionar los activos en cuanto a los niveles de riesgo y su relación con la disponibilidad, la autenticidad, la integridad y la confidencialidad

Esta actividad corresponde al grupo de trabajo de seguridad de tecnologías de información y sistemas de información e implica reconocer los activos que pueden estar expuestos a determinados niveles de riesgo. De igual manera, en esta actividad se debe tener en cuenta los criterios de seguridad que podrían verse afectados. En el trabajo propuesto por Guerrero (2010), se presenta un modelo para relacionar estos tres factores (activos, niveles de riesgo, criterios de seguridad).

3.3.3. Actividad A3. Identificar y evaluar las amenazas y vulnerabilidades de los activos críticos

Identificar y evaluar los hechos o actividades que permitirían concretar una violación de seguridad y las condiciones del entorno del sistema de información que ante determinada circunstancia podrían dar lugar a que se produjesen dichas violaciones, que afectaran a alguno de los activos de la compañía, es uno de los aspectos más importantes en materia de GRCSI. Esta actividad está incluida en los modelos inmersos en OCTAVE, ISM3 (2006), SP800-30 y MAGERIT, los cuales permitieron plantear comparaciones tendentes a detectar la integración de las subactividades y a diseñar los métodos a seguir para identificar los activos críticos.

Las actividades a desarrollar para la identificación y evaluación de vulnerabilidades y amenazas deberán ser responsabilidad inicialmente de la dirección de tecnologías de la información. Aunque las vulnerabilidades y amenazas de los activos relacionados con los sistemas de información tienen que ver en primera instancia con la propia naturaleza del sistema de información, en la investigación se provee un esquema de relación entre amenazas, vulnerabilidades y activos de los sistemas de información. Las amenazas se catalogaron utilizando el catálogo propuesto por el Ministerio de Administraciones Públicas (2006).

3.3.4. Actividad A4. Diseñar escenarios de riesgos con respecto a su impacto organizacional

Un escenario de riesgo es la descripción hipotética de un mal funcionamiento del sistema de información. La evaluación del impacto potencial de un escenario de riesgo provee a la organización las herramientas necesarias para la medición y la actuación.

Aunque cada sistema de información por su naturaleza intrínseca estará expuesto a escenarios de riesgo específicos, estándares como MEHARI (marco armonizado para el análisis de riesgos) proveen una lista de 170 escenarios, clasificados en 12 familias (CLUSIF, 2007), que se puede utilizar como guía. Por otro lado, MAGERIT, presenta algunas consideraciones que se deben tener en cuenta al momento de definir los escenarios de riesgo: identificar las causas que originan el escenario, especificar las consecuencias directas e indirectas del hecho que el escenario se produzca y medir la probabilidad de que ocurra. Las actividades propuestas para llevar a cabo la actividad A4 se muestran a continuación y los métodos planteados se presentan en la figura 5.

3.3.4.1. Subactividad A4.1. Creación de una base específica de escenarios de riesgo

Muchos factores pueden originar un escenario de riesgo, y es precisamente esto lo que deriva en la probabilidad de que este se concrete. A partir de la referencia de la base de escenarios MEHARI, se identifican los escenarios específicos, teniendo en cuenta los siguientes criterios planteados por MAGERIT:

- El tipo de consecuencia.
- Las causas que pueden dar lugar a la situación de riesgo.
- La probabilidad de que se produzca el escenario.

La probabilidad de ocurrencia se dará de acuerdo con niveles: nivel 4, muy probable; nivel 3, es probable; nivel 2, es poco probable; nivel 1, es muy poco probable, y nivel 0, no se considera.

Como estrategia de organización de la información sobre los escenarios específicos detectados, se propone un esquema que contenga la descripción del escenario de riesgo, las consecuencias directas o indirectas del escenario y la probabilidad de ocurrencia.

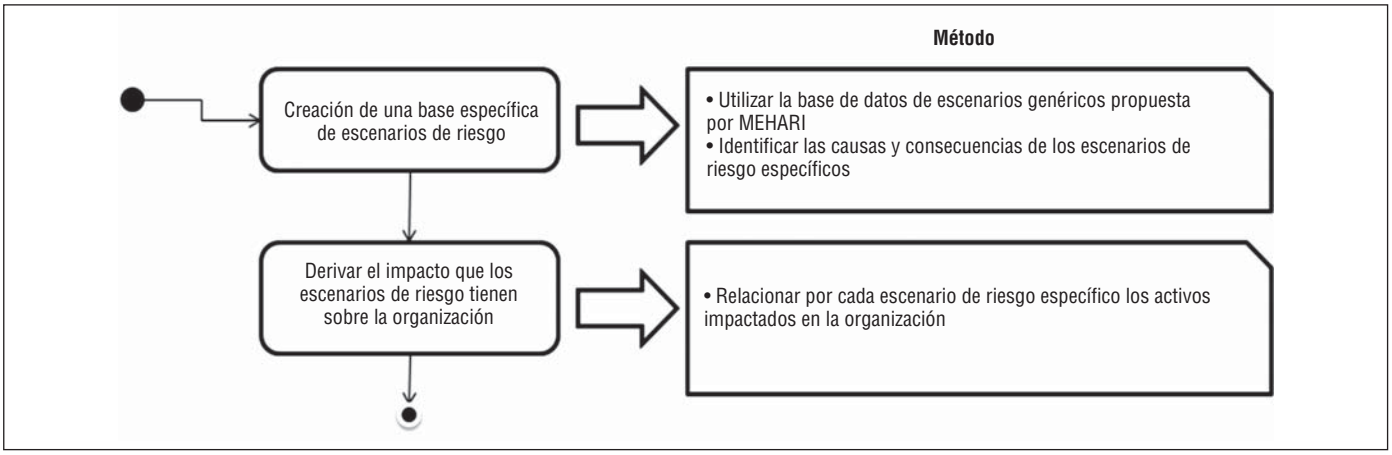

Figura 5. Métodos definidos para la actividad A4.
Fuente: tomado de Guerrero (2010), p. 104.

3.3.4.2. Subactividad A4.2. Derivar el impacto de los escenarios de riesgo en la organización

Las consecuencias directas e indirectas de los escenarios de riesgo permiten determinar el impacto en los activos de la organización. En este sentido, se denomina «impacto» a la magnitud del daño derivado del hecho que un riesgo se materialice. Un esquema que se podría utilizar para organizar la información de esta actividad debe incluir la descripción del escenario, su impacto en los activos de la organización y el criterio de seguridad afectado (disponibilidad, integridad, autenticidad y/o confidencialidad).

En cuanto a la disponibilidad, se debe responder a la pregunta: ¿qué importancia tendría que el activo no estuviese disponible cuando se requiera? Con respecto a la autenticidad: ¿qué importancia tendría que quien accede al activo no fuese quien se cree? En el caso de la integridad: ¿qué importancia tendría que el activo fuese modificado indebidamente? Y por último, para la confidencialidad: ¿qué importancia tendría que el activo fuese conocido por personas no autorizadas?

3.3.5. Actividad A5. Diseñar estrategias de tratamiento y protección

Una de las actividades más representativas en la GRCSI es diseñar las estrategias de tratamiento y mitigación de los riesgos encontrados. Esta actividad implica seleccionar estrategias de mitigación que mejoren la seguridad de la empresa mediante la reducción del riesgo. Actualmente, estándares como ISO 27005 (guía para la evaluación y los requerimientos de calidad de productos *software*), OCTAVE, ISM3, AS/NZS 4360:2004, SP800-30, SOMAP (2009) (*handbook open source* para la gestión de riesgos de seguridad de la información), MAGERIT y la SP800-39 publicada por Ross (2008) proveen información sobre el propósito de esta actividad, lo cual permitió la integración de las actividades que se muestran a continuación y el diseño de los métodos para llevarlas a cabo (fig. 6). Las actividades propuestas para realizar la actividad A5 se describen a continuación.

3.3.5.1. Subactividad A5.1. Identificar las estrategias de mitigación candidatas

Con base en el levantamiento de los escenarios de riesgo realizado en la actividad A4.1, se procede a asociar cada escenario de riesgo con los niveles definidos por Guerrero y Gómez (2010). Posteriormente se identifica el tipo de estrategia de mitigación (control) más adecuada para su tratamiento.

3.3.5.2. Subactividad A5.2. Seleccionar la alternativa más adecuada en costo y recursos disponibles

Una vez que se ha determinado en qué nivel de riesgo se encuentra el sistema de información, los líderes de seguridad deben seleccionar la alternativa más conveniente para la organización en términos no sólo de la relación costo-beneficio, sino también de los recursos que se encuentran disponibles para su implantación.

3.3.5.3. Subactividad A5.3. Elaborar e implementar un plan para el tratamiento del riesgo

Desarrollar y establecer un plan permite llevar a cabo de manera ordenada las decisiones tomadas y planeadas para el tratamiento del riesgo. Para la correcta elaboración de un plan de tratamiento de riesgos, el estándar AS/NZS propone los siguientes elementos:

- Identificar el orden de prioridad del riesgo.
- Especificar las posibles opciones de tratamiento.
- Seleccionar las opciones factibles.
- Describir los resultados del análisis de costo-beneficio y determinar si se acepta o se rechaza la propuesta de tratamiento.
- Especificar la persona responsable de implementar la opción.
- Elaborar un calendario de implementación.
- Especificar cómo será monitoreado el riesgo y las opciones de tratamiento.

3.3.6. Actividad A6. Documentación de resultados y revisión de casos

Documentar los resultados es una actividad que permitirá a las organizaciones realimentar sus resultados y aprender sobre las situaciones de riesgo presentadas a partir de la revisión de los casos históricos más representativos y sus respectivas estrategias de tratamiento. Un esquema que se podría utilizar para la documentación de casos debería incluir la descripción del caso presentado, la frecuencia de ocurrencia, el (los) mecanismo(s) de mitigación y los resultados obtenidos.

3.3.7. Actividad A7. Monitoreo y control

El monitoreo y el control ayudan a evaluar si las estrategias de mitigación de los riesgos implantadas lograron el alcance propuesto. Un programa continuo de monitoreo bien diseñado y bien administrado puede transformar efectivamente una evaluación estática de los controles de seguridad y de los procesos de determinación del riesgo, en un proceso dinámico que proporciona información esencial del estado de la seguridad, en el momento necesario para que los administradores puedan tomar decisiones acertadas. El monitoreo y el control proporcionan a las organizaciones herramientas eficaces para producir cambios en torno a los planes de seguridad, los informes de evaluación de la seguridad y los planes de acción.

4. Conclusiones

La propuesta desarrollada presenta una integración de las actividades relacionadas por los estándares de GRCSI y los métodos que se

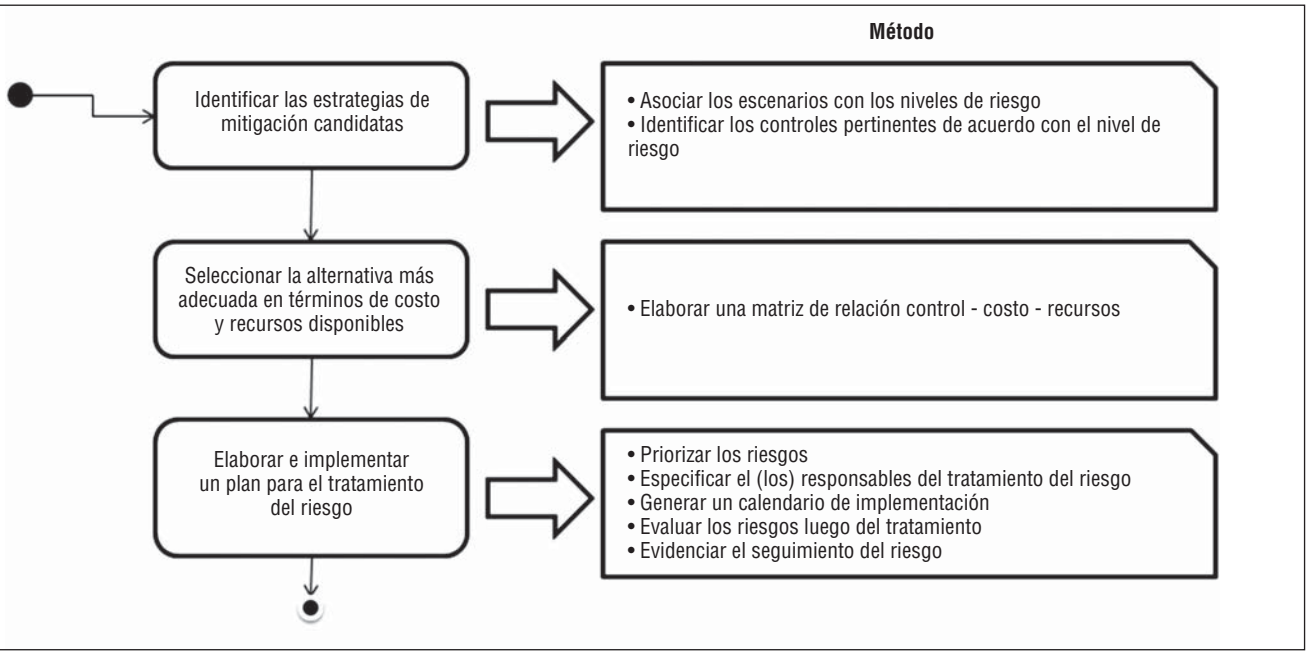

Figura 6. Métodos definidos para la actividad A5.
Fuente: tomado de Guerrero (2010), p. 108.

puede utilizar para que los involucrados en la organización las lleven a cabo. La propuesta centra su atención en el sentido de la GRCSI utilizando un esquema basado en niveles de riesgo y se guía por la definición original diseñada para la transformación organizacional.

La GRCSI no es una tarea simple, ya que son muchos los activos que se debe proteger y son muchas y diversas las amenazas a que pueden estar expuestos. A esto se suma la naturaleza compleja del sistema organizacional en la que se circunscribe, lo cual conlleva necesidades de protección específicas. Por tal motivo, la GRCSI es una labor que lleva tiempo, requiere esfuerzo, cuesta dinero y no es suficiente con realizarla una sola vez.

La complejidad de la GRCSI se debe abordar metodológicamente, de manera que se cubra la mayor parte posible de lo que se desea cubrir y se logre explicar a los diferentes entes implicados lo que se necesita y se espera de ellos como partícipes del proceso de GRCSI.

De esta forma, la GRCSI debe contar con el compromiso y el empeño de la dirección de tecnologías de la información, los responsables de la gerencia y los sectores estratégicos de la organización y las diversas áreas de tecnologías de la información, ya que a menudo las decisiones de protección de la información se realizan *ad-hoc,* por la experiencia previa del departamento de tecnologías de la información con las vulnerabilidades y las amenazas que actualmente se conocen, ocasionando que se tienda a no gestionar los riesgos de manera sistemática o que no los administren las personas adecuadas.

La propuesta para el desarrollo de la GRCSI permite proponer diversos métodos para la gestión de riesgos y controles en sistemas de información, que posteriormente podrán generar proyectos orientados a construir herramientas *software* que permitan sistematizarlos, de manera que su utilización sea más amplia.

La investigación presentada en este artículo abre camino al desarrollo de estudios relacionados con la cultura organizacional hacia los riesgos y controles en sistemas de información, que permitan indagar sobre los procesos de cambio organizacional necesarios para una adecuada incorporación de la GRCSI en las organizaciones.

Agradecimientos

Los autores expresan sus agradecimientos al grupo de investigación en sistemas y tecnologías de la información, a la Maestría en Ingeniería Área Informática y Ciencias de la Computación de la Universidad Industrial de Santander (UIS) y a la Vicerrectoría de investigación y extensión, también de la UIS, por el apoyo recibido para la realización de esta investigación mediante la financiación del proyecto de investigación «Propuesta de un modelo para la evaluación de calidad de productos *software* utilizados como apoyo a la biomedicina», código 5545 (León, 2009). De igual manera, al acompañamiento realizado por el proyecto EscuelaCol 2.0 en la ilustración de la aplicación del modelo de GRCSI diseñado (Díaz y Naranjo, 2010).

Bibliografía

Adams, J. (2005). Risk management, it's not rocket science: it's more complicated. *Journal The Social Affair Unit. Risk Management Magazine-Social Affairs Unit.* Disponible en: http://www.socialaffairsunit.org.uk/blog/archives/000318.php

Aguilera, A., & Riascos, S. (2009). Direccionamiento estratégico apoyado en las Tics. *Estudios Gerenciales, 25(111), 127-146*

Alberts, C. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM) Framework, Version 1.0.* Technical Report. SEE, Carnegie Mellon.

Standards Association of Australia. (2004). *AS/NZS 4360, Estándar Australiano de Administración de Riesgos* (3.ª ed.). Australia: Standards. Disponible en: www.imfperu.com/facipub/download/contenido/dnl/fp_cont/902/dlfnc/file/standard__adm_risk_as_nzs_4360_1999.pdf

Cater-Steel, A., & Al-Hakim, L. (2009). *Information systems research methods, epistemology, and applications.* Queensland: IGI Publishing.

Checkland, P. (2000a). *Soft systems methodology: a thirty year retrospective.* Lancashire: Wiley.

Checkland, P. (2000b). *Systems, thinking, systems pactice. includes a 30-year retrospective.* Chichester: Wiley.

Checkland, P., & Griffin, R. (1970). Management information systems: a systems view. *Journal of Systems Engineering, 1,* 29-42.

Checkland, P., & Scholes, J. (1999a). Information, systems, and information systems. *Cybernetics and Humans Knowing, 6.*

Checkland, P., & Scholes, J. (1999b). *Soft system methodology in action.* London: Wiley.

Checkland P., & Poulter, J. (2006). *Learning for action. a short definitive account of soft systems methodology and its use for practitioners, teachers and students.* Chichester: Wiley.

Checkland P., & Holwell, S. (1998). *Information, systems and information systems: making sense of the field.* Chichester: Wiley.

CLUSIF. (2007). *MEHARI 2007. Guide de l'analyse des risques.* Disponible en: http://www.clusif.asso.fr

Consortium ISM3. (2006). *Information security management maturity model. Version 2.0.* Madrid. Disponible en: http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf

Díaz, M., & Naranjo, M. (2010). *Herramienta software open source orientada a apoyar los procesos de evaluación y promoción en la educación básica primaria Escuelacol 2.0.* Proyecto de Pregrado. Universidad Industrial de Santander. Disponible en: http://tangara.uis.edu.co/biblioweb/pags/cat/popup/pa_detalle_matbib.jsp?parametros=154165|%20|24|80

Gómez, L., & Olave, Y. (2007). Una reflexión sistémica sobre los fundamentos conceptuales para sistemas de información. *Revista Colombiana de Computación, 8,* 71-92.

Guerrero, M. (2010). *Gestión de riesgos y controles en SI. Proyecto investigación de Maestría.* Universidad Industrial de Santander. Disponible en: http://tangara.uis.edu.co/biblioweb/pags/cat/popup/pa_detalle_matbib.jsp?parametros=155422|%20|14|58

Guerrero, M., & Gómez, L. (2011). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información. *Estudios Gerenciales, 27(121), 195-218.* Disponible en: http://www.icesi.edu.co/revistas/index.php/estudios_gerenciales/article/view/1124

ISACA, 2007. *Student Book COBIT 4.1.* ISACA, Estados Unidos.

Laudon, K., & Laudon, J. (2008). *Sistemas de información gerencial.* México: Prentice Hall.

León, N. (2009). *Propuesta de un modelo para la evaluación de calidad de productos software utilizados como apoyo a la biomedicina* [documento no publicado]. Vicerrectoría de Investigación y Extensión, Universidad Industrial de Santander.

Ministerio de Administraciones Públicas, (2006). *MAGERIT 2.0. Catálogo de Elementos.* Madrid. Disponible en: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit

Norma RFC4949. (2007). *Internet security glossary version 2.* Disponible en: http://www.ietf.org/rfc/rfc4949

Paulk, M., Weber, C., Curtis, B., & Chrissis, M. (2001). *The capability maturity model: guidelines for improving the software process.* Pittsburgh: Addison-Wesley.

Piattini, M. (2007). *Análisis y diseño de aplicaciones informáticas de gestión.* Bogotá: Alfa y Omega.

Ribagorda, A. (1997). *Glosario de términos de seguridad de las T.I.* Madrid: CODA.

Ross, R. (2008). *Managing risk from information systems. recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-39, Gaithersburg.

Silberfich, P.A. (2009). *Análisis y gestión de riesgos en TI ISO 27005 – Aplicación Práctica.* Quinto Congreso Argentino de Seguridad de la Información.

SOMAP. (2006). *Open information security risk management handbook*. *Versión 1.0.* Disponible en: http://www.somap.org/methodology/handbook.html

Stonebumer, G. (2002). *Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology. NIST.* Special Publication 800-30, Estados Unidos. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

TCSEC. (1985). *Trusted computer systems evaluation criteria, DoD 5200.28-STD, Department of Defense, United States of America.* Disponible en: http://csrc.nist.gov/publications/history/dod85.pdf