REVISIÓN DE ESTÁNDARES RELEVANTES Y LITERATURA DE GESTIÓN DE RIESGOS Y CONTROLES EN SISTEMAS DE INFORMACIÓN[1]

MARLENE LUCILA GUERRERO JULIO, Mg.*
Profesora Asociada, Universidad Pontificia Bolivariana, Colombia.
marlene.guerrero@upb.edu.co

LUIS CARLOS GÓMEZ FLÓREZ, Mg.
Profesor titular, Universidad Industrial de Santander, Colombia.
lcgomezf@uis.edu.co

Fecha de recepción: 05-07-2010 Fecha de corrección: 07-12-2010 Fecha de aceptación: 03-10-2011

RESUMEN

La gestión de riesgos y controles en sistemas de información (GRCSI) es una actividad importante en los sistemas de gestión. No obstante, aunque en las organizaciones parece haber interés en su aplicación, la GRCSI aún no logra el impacto deseado, debido en gran parte a la falta de entendimiento de su sentido o propósito y a la ausencia de los procesos de cambio organizacional necesarios para su implantación. Este artículo presenta una revisión sobre los estándares de GRCSI más relevantes, con el fin de plantear una propuesta de integración de los roles y las actividades que las organizaciones deben desarrollar, y de analizar los niveles de riesgo y sus implicaciones frente a los sistemas de información.

PALABRAS CLAVE

Estándar, gestión de riesgos y controles, nivel de riesgo, sistemas de información.

Clasificación JEL: M15, M42

1 Este artículo se basó en el trabajo "Gestión de Riesgos y Controles en Sistemas de Información" desarrollado por Marlene Lucila Guerrero Julio (Autor 1) en la Maestría en Ingeniería Área Informática y Ciencias de la Computación de la Universidad Industrial de Santander, cuyo proyecto de grado de maestría fue dirigido por Luís Carlos Gómez Flórez (Autor 2).

* Autor para correspondencia. Dirigir correspondencia a: Universidad Pontificia Bolivariana, Kilómetro 7 vía Piedecuesta Edificio D Oficina 305C Floridablanca, Santander, Colombia.

ABSTRACT

Review of relevant standards and literature regarding information systems risk management and controls

Risk management and controls in information systems (RMCIS) are important activities involved with management systems. Nevertheless, although organizations seem to have an interest in its application, RMCIS has not yet achieved its real impact because there is an inadequate understanding of its meaning or purpose and there is also a lack of organizational change processes needed for its implementation. This article presents a review of the current most relevant RMCIS standards for the purpose of proposing an integration of the roles and activities that organizations should carry out, together with an analysis of the risk levels and their implications for information systems.

KEYWORDS

Information systems, risk level, risk management and controls, standard.

RESUMO

Revisão de padrões relevantes e literatura de gestão de riscos e controles em sistemas de informação

A gestão de riscos e controles em sistemas de informação (GRCSI) é uma atividade importante nos sistemas de gestão. No entanto, apesar de que nas organizações parece haver interesse em sua aplicação, a GRCSI ainda não atingiu o impacto desejado, devido em grande parte a falta de compreensão de seu sentido ou propósito e a ausência dos processos de mudança organizacional necessários a sua implantação. Este artigo apresenta uma revisão dos padrões mais relevantes da GRCSI, com o objetivo de apresentar uma proposta de integração das funções e as atividades que as organizações devem desenvolver, e de analisar os níveis de risco e suas implicações perante os sistemas de informação.

PALAVRAS CHAVE

Padrão, gestão de riscos e controles, nível de risco, sistemas de informação.

INTRODUCCIÓN

Según un estudio realizado por Singh y Brewer (2008) y soportado por diversas fuentes (Norton, 2004; PriceWaterhouseCouper, 2004; Wah, 1998), la gestión y el control de riesgos en sistemas de información no logra aún ganar la importancia necesaria para la gerencia organizacional, lo que se atribuye a dos premisas: en primera instancia, a la falta de comprensión de las cuestiones de riesgos y, en segundo lugar, al hecho de no contar con una cultura corporativa debidamente sensibilizada con los riesgos de su propio negocio.

La primera premisa está asociada con la falta de entendimiento sobre el sentido o propósito de las actividades de la gestión de riesgos y controles en sistemas de información (GRCSI en adelante), dado que si los directivos y los demás actores de las organizaciones no comprenden las razones de las políticas de seguridad de la información y de la gestión de riesgos, no apoyarán plenamente la lógica de la estrategia, haciendo poco probable que participen en su desarrollo o se adhieran a ellas más tarde (Farahmand, Navathe y Enslow, 2003; Hirsch y Ezingeard, 2008; Straub y Welke, 1998).

La segunda premisa, por su parte, está asociada con la ausencia de los procesos de cambio organizacional necesarios para la transformación de la cultura organizacional propicia para el desarrollo de la gestión de riesgos y controles (Cano, 2009). Esta premisa implica incorporar en la cultura organizacional la preocupación por las nociones de riesgo lo que a su vez se debe traducir en la planeación, organización y conducción de procesos orientados a lograr que los actores organizacionales se sientan insatisfechos con el estado actual de sus actuaciones ante la GRCSI. Igualmente, es importante que los actores involucrados se convenzan de la necesidad de cambio y se sientan dispuestos y motivados a enfrentarlo. Estos procesos de cambio organizacional son descritos por Schein (1991) como procesos de invalidación, inducción y motivación.

Ahora bien, estas premisas se acentúan debido a la diversidad de posturas sobre la forma más adecuada de desarrollar las actividades de GRCSI y la confusión que sus descripciones generan en los actores organizacionales. Lo anterior posibilita el desarrollo de investigaciones orientadas a responder ¿cómo podría la organización mejorar su comprensión acerca del sentido o propósito de la GRCSI?

Una aproximación a la respuesta se desarrolla en el presente artículo, abordando el conjunto de estándares de GRCSI reconocidos con el fin de realizar una revisión de los niveles de riesgo y plantear una propuesta para la integración de los roles y las actividades necesarias para llevarlo a cabo.

En la primera sección del documento se presentará una revisión de las actividades asociadas a la GRCSI relacionadas por los estándares relevantes de carácter nacional e internacional. En la segunda sección se elaborará una imagen enriquecida que permitirá plantear una postura propia sobre las actividades para la GRCSI. En la tercera sección se presentará la definición de los niveles de riesgo en los sistemas de información y su identificación en la organización.

En la cuarta sección se plantearán las conclusiones obtenidas a partir de la reflexión, así como recomendaciones sobre futuras investigaciones. Finalmente, en la quinta sección se expresarán algunos agradecimientos.

1. REVISANDO LAS ACTIVIDADES DE GRCSI EN EL MARCO DE LOS ESTÁNDARES

Un programa de gestión de riesgos tiene como principal objetivo llevar los riesgos a un nivel aceptable, en el desarrollo de algunas actividades o funciones (Boehm, 1991; ISACA, 2002; Peltier, 2001) y haciendo uso eficaz de los recursos para mitigarlos y controlarlos (Smith, McKeen y Staples, 2001). En la actualidad se pueden identificar varios estándares que, aunque en su mayoría no tienen como principal objetivo el establecimiento de un modelo de GRCSI, aportan elementos fundamentales al momento de considerar las actividades a desarrollar por una organización.

Un primer grupo integrado por cuatro estándares está dirigido a la seguridad de los sistemas de información. Este grupo se conforma del Operationally Critical Threat, Asset, and Vulnerability Evaluation – OCTAVE (Alberts, Behrens, Pethia y Wilson, 1999), el Risk Management Guide for Information Technology Systems SP800-30 (Stonebumer, Coguen y Feringa, 2002), la Metodología de Análisis y Gestión de Riesgos de los sistemas de información MAGUERIT Versión 2.0 (1997) y el Managing Risk from Information Systems SP800-39 (Ross, Katzke, Johnson, Swanson y Stoneburner, 2008). En ellos, la GRCSI es tenida en cuenta para garantizar la continuidad de los procesos de negocio que tienen un nivel determinado de dependencia de los sistemas de información y para evaluar y generar salvaguardas de las distintas amenazas a las que se exponen los sistemas de información por su naturaleza o por fuentes externas.

En estos estándares se entiende la *seguridad de los sistemas de información* como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de la información almacenada o transmitida y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles (Baskerville, 1993; Harold y Tipton, 2006; Ministerio de Administraciones Públicas, 1997). Otros estándares revisados no proveen una definición exacta sobre este tema.

Un segundo grupo de cuatro estándares está orientado a los aspectos de seguridad de la información, en donde la GRCSI encaja como elemento destinado a garantizar la disponibilidad, la integridad, la confidencialidad y la confiabilidad de la información. Este grupo lo conforman la norma ISO 27005 (ISO, 2008), el Information Security Maturity Model – ISM3 (2009), el Open Information Security Risk Management - SOMAP (2006) y el Método Armonizado para la Gestión de Riesgos (Clusif, 2007).

La *seguridad de la información* es definida como la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización (ISO, 2005;

Whitman y Mattord, 2005). Esta definición es tenida en cuenta por todos los estándares de seguridad de la información revisados.

Complementando los dos grupos de estándares anteriores, en lo relacionado con la GRCSI, se encuentra el Estándar Australiano de Administración de Riesgos AS/NZS 4360 (2004), el cual está orientado a la administración de riesgos organizacionales, ofreciendo una identificación de las oportunidades y amenazas para la adecuada toma de decisiones de acuerdo con cada contexto organizacional.

Ahora bien, si se reconoce a la GRCSI como parte de la seguridad de los sistemas de información y de la seguridad de la información (Blakley, McDermott y Geer, 2001) y estas a su vez como parte del entorno organizacional, es prioritario distinguir cuáles serían los roles asociados a la GRCSI con el fin de determinar las actividades y la respectiva asignación de responsabilidades que las organizaciones deberían implementar (Ashenden, 2008; Ashenden y Ezingeard, 2005). Algunos de los estándares revisados ofrecen una perspectiva sobre los roles supeditados a la GRCSI en las organizaciones (ver Tabla 1), lo cual permitió identificar cuál sería el personal que estaría involucrado o comprometido en la GRCSI.

La especificación de los roles de la GRCSI posibilita abordar las actividades involucradas en este proceso. En este punto, los estándares revisados proveen diferentes posturas sobre cómo llevarlas a cabo. Por ello, se realizó una comparación ubicando para cada estándar el listado de actividades en orden lógico y asociándolas mediante las similitudes y diferencias entre ellas, para finalmente obtener una propuesta de actividades resultado de su agrupación. La Tabla 2 presenta el resultado del ejercicio anteriormente descrito.

Como se puede observar, en algunas casillas en las que se agrupan las actividades aparecen diferentes nombres, esto evidencia que aunque los estándares relacionan actividades con diferente nombre, tienen definiciones o propósitos similares. De igual manera, en el Gráfico 1 aparece una imagen enriquecida que ilustra el resultado de la agrupación de las actividades para la GRCSI, permitiendo apreciar la secuencia e interacción entre ellas.

Tabla 1. Roles identificados por los estándares respecto de la GRCSI

Roles	Perspectiva
• Administradores funcionales y de negocio • Departamento de seguridad de la información ◆ Jefes de información (CIO) ◆ Jefes de seguridad de sistemas de información (ISSO) ◆ Profesionales de seguridad de tecnologías de información ◆ Entrenadores de seguridad/profesionales en materia de seguridad • Operarios • Stakeholders • Propietarios de los sistemas de información	Toda la organización deberá estar comprometida e involucrada con los procesos de la GRCSI. La GRCSI es responsabilidad de la administración y del personal capacitado en el área de la seguridad de la información y de la seguridad de los sistemas de información.

Fuente. Elaboración propia.

Tabla 2. Cuadro comparativo de las actividades relacionadas por los estándares para la GRCSI

Actividad estándar	ISO 27005	OCTAVE	ISM3	AS/NZS	SP800-30	SOMAP	MAGUERIT	MEHARI	SP800-39
A1. Establecer el contexto. Medir y caracterizar el estado actual de la seguridad de los sistemas y la organización. Evaluar la exposición inherente.	X		X	X	X			X	X
A2. Identificar y valorar los activos críticos.		X					X		
A3. Identificar las amenazas y las vulnerabilidades de la organización.		X	X		X		X		
A4. Identificar los componentes claves y las vulnerabilidades técnicas que ocasionan los riesgos.		X		X	X				
A5. Evaluar el riesgo. Identificar el riesgo. Estimar el riesgo. Valorar el riesgo.	X	X		X	X	X	X		X
A6. Determinar y evaluar el impacto.							X	X	
A7. Evaluar la gravedad del escenario.								X	
A8. Tratar el riesgo. Identificar las exigencias de seguridad y las normas existentes. Desarrollar estrategias de protección basadas en buenas prácticas. Implementar protecciones.	X	X	X	X	X	X	X		X
A9. Aceptar el riesgo. Dar prioridad a la inversión de los procesos de seguridad.	X		X					X	X
A10. Comunicar el riesgo.	X							X	
A11. Realizar seguimiento al riesgo. Establecer un plan de reducción de los riesgos. Monitorear y revisar.	X	X	X	X	X	X	X	X	X
A12. Documentar resultados.					X				X

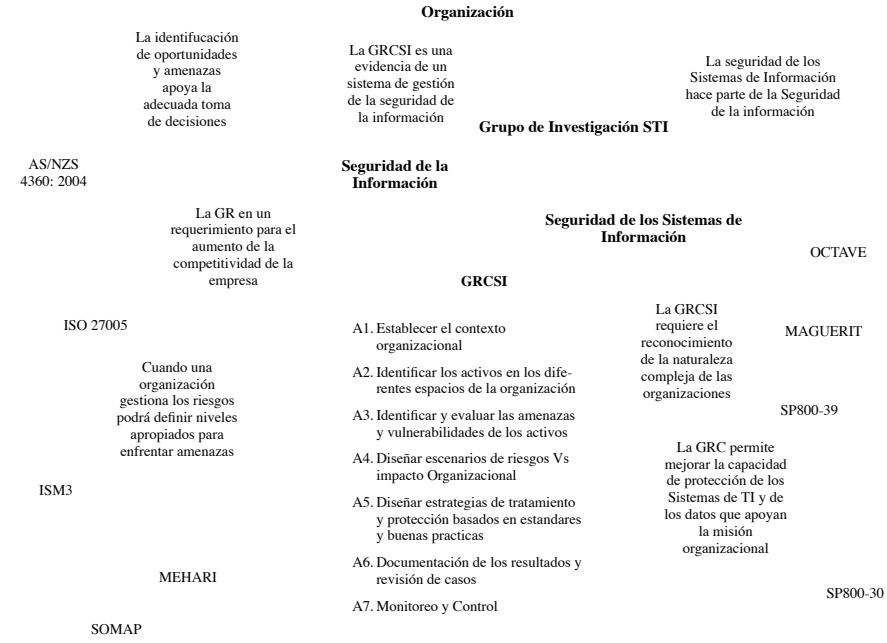
Nota. X: actividad incluida en el estándar.
Fuente: Elaboración propia.

2. ELABORACIÓN DE UNA IMAGEN ENRIQUECIDA DE LAS ACTIVIDADES PARA LA GRCSI

La GRCSI se encuentra rodeada por un alto componente social, político y humano (Checkland y Holwell, 1998; Checkland y Scholes, 1999a, 2000). Esto conlleva que puedan existir perspectivas diferentes aunque a veces complementarias sobre cómo se deberían llevar a cabo estas actividades en una organización. Es en este punto en el que el pensamiento de sistemas blandos (Checkland y Poulter, 2006; Checkland y Scholes, 1999b) se convierte en una de las metodologías más propicias para este tipo de estudios, en los cuales se debe trabajar con diferentes perspectivas de una misma situación, las que son examinadas y discutidas en torno a un proceso sistémico de aprendizaje (Checkland, 2000) con el fin de definir acciones orientadas a su mejoramiento.

Los riesgos tienen un impacto potencial en el sistema de gestión de la seguridad (Chittister y Haimes, 1993; Fairley, 1994); por lo tanto, la GRCSI es una labor que requiere el esfuerzo y coordinación de los entes de la organización en favor de la protección de los activos del negocio y del cumplimiento de la misión organizacional

Gráfico 1. Imagen enriquecida – integración de las actividades



CONVENCIONES

Acuerdos en la investigación	Posturas comunes	Puntos de vista o perspectivas de los actores involucrados

Fuente: Elaboración propia con base en Guerrero (2010).

(McFadzean, Ezineard y Birchall, 2007). No obstante, los modelos proveídos por los diferentes estándares sólo son guías o pautas y cada organización debe velar por reconocer en su naturaleza intrínseca y en su contexto, las necesidades y requerimientos de gestión (Landoll, 2005).

De la comparación de los estándares revisados, se logró evidenciar algunas actividades claves vinculadas a cada uno de ellos y en las cuales se pudo detectar que existían coincidencias. Lo anterior permitió crear la imagen enriquecida del Gráfico 1, en la que se puede observar la perspectiva planteada por el grupo de investigación en "Sistemas y Tecnologías de la Información (STI)[2]" y que es compartida por la mayoría de los estándares presentados, en especial por el estándar SOMAP. Bajo esta

2 Grupo de investigación en Sistemas y Tecnologías de la Información (STI) de la Universidad Industrial de Santander, clasificación B de Colciencias.

perspectiva, se presenta la GRCSI como parte del sistema de seguridad de los sistemas de información y como reflejo del sistema de gestión de riesgos a nivel organizacional. Esta idea es apoyada por los estándares AS/NZS, MAGUERIT y OCTAVE, en los cuales la identificación de los niveles de riesgo en los sistemas de información es un factor clave para el aumento de la competitividad de las organizaciones, al apoyar la acertada toma de decisiones sobre la inversión en la protección de los activos.

Por su parte, estándares como ISO 27005 (ISO, 2008) ayudan a considerar la GRCSI dentro del esquema de calidad organizacional como un requerimiento para aumentar su competitividad.

Por otro lado, de acuerdo con la perspectiva planteada por los estándares SP800-39, SP800-30, MEHARI e ISM3, el impacto generado por los riesgos es diferente pues depende de los escenarios organizacionales en que se presenten. Esto implica que las organizaciones deberán definir los niveles apropiados de riesgo teniendo en cuenta su naturaleza compleja, para posteriormente asociarlos con los escenarios en los cuales se podrían presentar.

Considerando las actividades comunes encontradas anteriormente en la revisión de los estándares y la imagen enriquecida elaborada, en la Tabla 3 se plantea una posible consolidación de las actividades necesarias para la GRCSI.

El proceso de cambio organizacional necesario para la implantación de la GRCSI implica no sólo el reconocimiento de las actividades a desarrollar de acuerdo con los estándares, sino el asimilar y asociar los niveles de riesgo con los eventos inseguros que se podrían presentar, de manera que se logre un alineamiento organizacional con las políticas de seguridad y un entendimiento de las implicaciones de los riesgos frente a los sistemas de información. A continuación se presenta una revisión sobre los niveles de riesgo en sistemas de información, el cual permitirá abordar el tema de la importancia de la GRCSI en el entorno organizacional.

3. NIVELES DE RIESGO EN LOS SISTEMAS DE INFORMACIÓN Y SU IDENTIFICACIÓN EN LA ORGANIZACIÓN

Un nivel de riesgo es una clasificación, en el plano organizacional y de sistemas de información, de los espacios en los que se pueden presentar determinados riesgos. En la literatura, PriceWaterhouseCooper –PWC (Elissondo, 2008) define siete niveles de riesgo asociados a los sistemas de información y algunos controles utilizados para mitigarlos, los cuales, tal y como se muestra en diversos estudios (Castilla, Herrera, Llanes y Sánchez, 2004; Contraloría General de la República de Nicaragua -CGRN, 1995), dan cuenta de aplicaciones y resultados plausibles en contextos reales. Los niveles definidos por PWC se presentan en la Tabla 4.

Estos siete niveles de riesgo son el punto de partida de la propuesta de esta investigación, los cuales se enriquecieron a partir de la indagación realizada en los estándares de seguridad de la información y en los de seguridad de los sistemas de información. Esto permitió la identificación, en el plano organizacional y

Tabla 3. Actividades planteadas para la GRCSI

Actividad	Descripción
A1. Establecer el contexto organizacional	Clarificar la estrategia de la organización en términos de los sistemas de información con el fin de especificar aquellos que apoyan los procesos de negocio. De igual manera se debe determinar la información sensible y especificar los roles de los actores y sus responsabilidades en el uso de sistemas de información. La información sensible es aquella, así definida por su propietario, que debe ser especialmente protegida, pues su revelación, alteración, pérdida o destrucción, puede producir daños importantes a alguien o algo (Ribagorda, 1997; TCSEC, 1985). Algunos autores y normas como la RFC4949 de 2007, suelen denominarla información crítica, haciendo alusión a que es necesaria para el desarrollo y la evaluación del cumplimiento de los procesos de negocio.
A2. Identificar los activos críticos en los diferentes espacios de la organización	Catalogar los activos y la información sensible con el fin de relacionarlos con los niveles de riesgo y con los criterios de la seguridad de los sistemas de información (la disponibilidad, autenticidad, integridad y confidencialidad).
A3. Identificar y evaluar las amenazas y vulnerabilidades de los activos	Detectar y evaluar las condiciones del entorno del sistema de información que, ante una determinada circunstancia, podrían dar lugar a una violación de seguridad, afectando a alguno de los activos de la compañía y a aquellos hechos o actividades que permitirían concretarlas. Entiéndanse los conceptos de amenaza y vulnerabilidad y riesgo, en el sentido planteado por Silberfich (2009), en donde se explica que la amenaza es una condición del entorno del sistema de información, que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando alguno de los activos de la compañía. Por su parte, la vulnerabilidad es una condición propia del sistema de información o de su naturaleza intrínseca que permite concretar una amenaza y el riesgo es la posibilidad de que se produzca un impacto en la organización cuando una amenaza se concreta.
A4. Diseñar escenarios de riesgo en términos de su impacto organizacional	Diseñar escenarios en los cuales se posibilitaría la existencia de los riesgos. Esta actividad permite ponderar el impacto organizacional que cada uno de los escenarios tendría en los activos del negocio.
A5. Diseñar estrategias de tratamiento y protección basados en estándares y buenas prácticas	Seleccionar alternativas de mitigación que mejoren la seguridad de la organización mediante la reducción del riesgo.
A6. Documentar los resultados y revisar casos	Realizar seguimiento y desarrollar un aprendizaje de los casos de estudio generados a partir de la documentación de los resultados de la gestión.
A7. Monitorear y controlar	Contrastar los resultados obtenidos con las especificaciones de mejoramiento con el fin de generar nuevas estrategias o nuevas definiciones de espacios de riesgo.

Fuente: Elaboración propia.

de sistemas de información, de los espacios en los que se pueden presentar los niveles de riesgo.

En primera instancia se unificaron los riesgos de acceso general y de acceso a funciones de procesamiento y se categorizaron como "acceso". Se hizo esta categorización porque ambos niveles de riesgo apuntan a que personas, autorizadas o no, tienen acceso a la información o a las funciones de procesamiento de los sistemas de información con el fin de leer, modificar o eliminar la información o los segmentos de programación o con el fin de ingresar transacciones no

Tabla 4. Niveles de riesgo y sus medios controles según PWC

Nivel	Riesgo	Definición	Medios de control
1	Acceso general	Riesgo que surge cuando personas no autorizadas tienen acceso a los archivos de datos o a los programas de aplicación; permitiéndoles leer, modificar, agregar o eliminar algún ítem o segmento de programas.	Software de control de acceso, análisis de logs e informes gerenciales, control de acceso físico y protección de datos.
2	Acceso a funciones de procesamiento	Riesgo que surge cuando personas autorizadas tienen acceso a las funciones de procesamiento de las transacciones de los programas de aplicación; permitiéndoles leer, modificar, agregar o eliminar datos o ingresar transacciones no autorizadas para su procesamiento.	Segregación de funciones en el departamento de sistemas (organización de la estructura jerárquica de acceso al sistema de información) y control de acceso, de manera que se creen políticas de seguridad informática en las que se determinen las actuaciones de las personas asociadas al sistema de información y se especifiquen las funciones de procesamiento que se deberán proteger de ellas.
3	Ingreso de datos	Riesgo que se ocasiona cuando los datos permanentes y de transacciones ingresados para el procesamiento, pueden ser imprecisos, incompletos o ingresados más de una vez.	Controles de edición y validación (formato, campos faltantes, límites, validación, procesamiento de duplicados, correlación de campos, balanceo, digito verificador), controles de lote y doble digitación de campos críticos.
4	Ítems rechazados o en suspenso	Riesgo que surge cuando las transacciones rechazadas y/o pendientes no son detectadas, analizadas y corregidas.	Controles programados, los cuales incluyen servidores espejo, bloqueo del cliente y bases de datos en la máquina cliente que permitan guardar la última transacción realizada para que posteriormente pueda ser actualizada, controles de usuario que permitan verificar anomalías en las transacciones realizadas por la máquina cliente.
5	Procesamiento	Riesgo que se ocasiona cuando las transacciones a ser procesadas por el sistema de información, se pierden o se procesan de forma incompleta, inexacta o en el periodo contable incorrecto.	Formularios prenumerados, rutinas de control de secuencia, controles de balanceo, de lote, rótulos de archivos, transmisión de datos y procedimientos de enganche y recuperación.
6	Estructura organizativa del departamento de sistemas	Riesgo que surge cuando la estructura organizacional y/o los procedimientos operativos del departamento de sistemas no garantizan un ambiente de procesamiento que conduzca al manejo adecuado de la información.	Segregación de funciones en el departamento de sistemas, controles y procedimientos operativos.
7	Cambios a los programas	Riesgo que surge cuando los programadores efectúan cambios incorrectos y/o no autorizados en el software de aplicación.	Procedimientos de iniciación, aprobación y documentación, procedimientos de catalogación y mantenimiento, intervención de los usuarios, procedimientos de prueba y supervisión efectiva.

Fuente: Adaptada de Elissondo (2008).

autorizadas para que sean procesadas por los sistemas de información. Como contribución a la definición planteada por PWC, se incorporó a esta concepción los ataques que se dan por Man in the Middle (Haig, 2009), los cuales son conocidos en criptografía como ataques en los que el enemigo adquiere la capacidad de leer (*sniffing*), insertar (*spoofing*), denegar (negación de servicio) y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. Un método de control comúnmente utilizado para proteger los sistemas de información de estos ataques es reemplazar todos los protocolos inseguros por protocolos

seguros, es decir, reemplazar http por https, telnet por ssh (versión 2), pop3 por secure pop, etc. De igual manera, tomando como referencia a ISM3, se incorpora a este nivel el acceso indebido ocasionado por software malicioso y el registro incorrecto del acceso de usuarios por parte del sistema de información (es decir, errores en la bitácora del sistema de información).

Por otro lado, enfoques sobre sistemas de información como los presentados por Laudon y Laudon (2008) y McLeod (2000), permiten argumentar que actualmente estos sistemas han pasado de un enfoque centrado en los datos a uno centrado en la información y el conocimiento. De acuerdo con esto, los sistemas de información utilizan la información que es capturada por diversos medios para la ejecución de las transacciones y el apoyo a la toma de decisiones. Siguiendo este orden de ideas, es apropiado pretender que en la actualidad no se hable de un riesgo de ingreso de datos sino de un riesgo de ingreso de información.

En cuanto al nivel de riesgo de procesamiento, se reestructuró la definición con el fin de centrarse en el riesgo que surge cuando los procesos de los sistemas de información no garantizan el adecuado procesamiento de la información, ocasionando que las salidas esperadas no sean correctas, la información se pierda y los procesos subsecuentes fallen o se retarden.

En cuanto al sexto nivel de riesgo, el de la estructura organizativa del departamento de sistemas, se incorporaron los riesgos establecidos por ISM3 que surgen en el caso de la destrucción de instalaciones y/o sistemas de información, o del cambio o pérdida del personal clave. Esto puede ocurrir porque no se han actualizado los sistemas de información o porque no se cuenta con adecuados procedimientos para garantizar la continuidad del negocio.

Por otro lado, dado el despliegue y la incorporación de las tecnologías de la información y de las redes en los procesos de negocio en toda la organización, no tiene sentido pensar que este nivel de riesgo se dé únicamente en el departamento de sistemas, ya que el riesgo de un inadecuado manejo de la información ocasionado por un inapropiado ambiente de procesamiento, podría presentarse en cualquier dependencia e involucrar a todo el personal de la organización encargado de desarrollar los procesos y de operar los sistemas de información. Por tal motivo, este nivel se denominará "estructura organizativa".

De esta manera, cada una de las definiciones de los niveles de riesgo proporcionadas por PWC se reestructuraron teniendo en cuenta las descripciones sobre riesgo y nivel de riesgo, procurando que para cada nivel de riesgo, la definición contara con los siguientes elementos:

- Dónde ocurre. Es la denominación de cada nivel de riesgo.
- Qué lo ocasiona. Cuáles son las causas que posibilitan la ocurrencia del riesgo.
- Impacto posible. Conjunto de posibles efectos sobre los activos de la organización.

Así y a través de la identificación de los criterios de la seguridad de los sistemas de información afectados (1. Disponibilidad, 2. Autenticidad, 3.

Integridad, 4. Confidencialidad) por cada nivel de riesgo y de los actores involucrados, se logró enriquecer la propuesta de PWC, llegando a las definiciones presentadas en la Tabla 5 y al esquema mostrado en el Gráfico 2.

Tabla 5. Niveles de riesgo – propuesta de enriquecimiento de las definiciones

Nivel de riesgo	Definición	Criterios de la seguridad de los sistemas de información afectados				Actores involucrados
		1	2	3	4	
Acceso	Este nivel de riesgo surge cuando personas autorizadas o no, tienen acceso a la información o a las funciones de procesamiento de los sistemas de información con el fin de leer, modificar o eliminar la información o los segmentos de programación o con el fin de ingresar transacciones no autorizadas para que sean procesadas por los sistemas de información.	X	X	X	X	Personal interno o externo de la organización y/o departamento de sistemas.
Ingreso de información	Este nivel de riesgo surge cuando la información es ingresada a los sistemas de información de manera imprecisa, incompleta o más de una vez, ocasionando que las transacciones no puedan ser ejecutadas y/o que la información no sea correcta.		X	X		Personal de la organización, proveedores y clientes de ella, encargados de realizar las transacciones en los sistemas de información.
Ítems rechazados o en suspenso	Este nivel de riesgo surge cuando no se detectan, analizan y corrigen las transacciones rechazadas y/o pendientes, ocasionando que la información no se actualice correctamente o se pierda o que las transacciones no se ejecuten.	X		X		Clientes, personal del departamento de sistemas.
Procesamiento	Este nivel de riesgo surge cuando los procesos de los sistemas de información no garantizan el adecuado procesamiento de la información, ocasionando que las salidas esperadas no sean correctas, la información se pierda y los procesos subsecuentes fallen o se retarden.	X		X		Clientes, personal del departamento de sistemas.
Estructura organizativa	Este nivel de riesgo surge cuando la estructura organizativa no garantiza un adecuado ambiente para el procesamiento de la información y/o no define apropiados planes de continuidad del negocio, ocasionando que no existan procedimientos definidos y optimizados para el manejo de la información y de los sistemas de información, no se actualicen los sistemas de información y no se reaccione adecuadamente ante contingencias.	X	X	X	X	Personal de la organización encargado de desarrollar los procesos. Personal interno o externo encargado de la operación de los sistemas de información. Proveedores de servicios de tecnologías de información.
Cambio a los programas	Este nivel de riesgo surge cuando los programadores efectúan cambios incorrectos, no autorizados y/o no documentados en el software de aplicación, ocasionando pérdida de información, repetición de esfuerzo, inconsistencias en los procesos e inconformidad en los clientes y usuarios.	X	X	X	X	Personal adscrito al departamento de sistemas o de los proveedores de servicios de tecnologías de información encargados del mantenimiento del software.

Nota. 1. Disponibilidad 2. Autenticidad 3. Integridad 4. Confidencialidad.

Fuente: Elaboración propia.

Gráfico 2. Niveles de riesgo en sistemas de información

▲1. Nivel de riesgo acceso. 2. Nivel de riesgo de ingreso de información 3. Nivel de riesgo ítems rechazados o en suspenso. 4. Nivel de riesgo procesamiento. 5. Nivel de riesgo estructura organizativa. 6. Nivel de riesgo cambio a los programas.

Fuente: Elaboración propia.

Por otro lado, los controles proporcionados en el esquema de PWC se ampliaron teniendo en cuenta los aportes suministrados por MAGUERIT y por la norma RFC4949 (2007), obteniendo el resultado presentado en la Tabla 6.

Como se puede observar, algunos de los estándares revisados soportan y ayudan a complementar los niveles de riesgo propuestos por PWC. No obstante, son relativamente pocos los que ofrecen una descripción guiada por niveles de riesgo que contribuya a que las organizaciones reconozcan el impacto de los riesgos en sus procesos de negocio.

Ahora bien, la comprensión sobre el sentido o el propósito organizacional de los diferentes estándares en lo concerniente a los diversos modelos de GRCSI, no se logra únicamente teniendo claridad sobre los niveles de riesgo, los roles y las actividades a desarrollar, también es necesario reconocer cuándo se puede utilizar un determinado estándar según el propósito de gestión de riesgos requerido (ver Gráfico 3).

La escogencia de la aplicación de los estándares implica un reconocimiento de las necesidades propias de cada organización (García y Martínez, 2008). En la Tabla 7 se presenta una conclusión de la aplicación de los estándares revisados respecto de las necesidades de gestión de riesgos de la organización.

Tabla 6. Niveles de riesgo y controles

Nivel	Riesgo	Controles	Descripción
1	Acceso	Segregación de funciones en la organización	Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores ocasionados por accesos autorizados o no autorizados.
		Anti-keylogger	Aplicación diseñada para evitar, detectar y/o eliminar programas tipo keylogger, es decir, aquellos que registran las pulsaciones que realiza un usuario sobre su teclado. Puede tratarse de una aplicación independiente o una herramienta dentro de otra, como puede ser un antivirus o un anti espía (tipo de aplicación que se encarga de buscar, detectar y eliminar spywares en el sistema. Los spywares son aplicaciones informáticas que recolectan información valiosa de la computadora desde donde está operando).
		Control de acceso (contraseñas encriptadas, certificados digitales, dispositivos a nivel de tokens o tarjetas, lectores biométricos, alarmas, firma electrónica, dispositivos RFID -sigla en inglés que hace referencia a dispositivos de identificación por radiofrecuencia-, control de número de intentos fallidos)	Control de acceso a los servicios, a las aplicaciones, al sistema operativo, a los soportes de información, a las instalaciones, etc.
		Registro de actuaciones e incidentes	Registros a nivel de logs que permitan determinar lo que los usuarios hacen en el sistema e informes gerenciales sobre la ocurrencia de fallas que afecten el buen funcionamiento del acceso de los usuarios a los sistemas de información.
		Administración de cuentas	Desactivación de cuentas de usuarios inactivos y cambio periódico de claves de acceso.
		Desconexiones automáticas	Desconexiones de sesión por tiempo sin actividad dentro del sistema.
		Asegurar los protocolos de transferencia	Reemplazar todos los protocolos inseguros por protocolos seguros (http por https, telnet por ssh (versión 2), pop3 por secure pop, etc.).
		Cifrado y marcado de información	El cifrado consiste en el envío codificado de la información que transita por la red (texto cifrado o criptograma), para prevenir su alteración o pérdida. Por su parte, el marcado consiste en la incorporación de etiquetas o marcas a la información de acuerdo con atributos definidos por el usuario (v. gr., reservada, confidencial, información personales, etc.) o con información adicional acerca de la estructura del texto enviado.
2	Ingreso de información	Edición y validación	Comprobación de tipo de formato, campos faltantes, límites, validación, procesamiento de duplicados, correlación de campos, balanceo, dígito verificador.
		Lote	Procesar la información por lotes de manera que se pueda comprobar que la información ingresada es correcta.

Tabla 6. Niveles de riesgo y controles (Cont.)

Nivel	Riesgo	Controles	Descripción
		Doble digitación de campos críticos	Incluir en el sistema dos veces la misma información. Se destina a más de un digitador a introducir la información en el sistema en archivos diferentes y posteriormente se hace una comparación de los contenidos de los archivos (mediante un programa especial o el sistema operativo).
		Lectores de código de barras y lectores RFID	Los lectores de código de barras y los lectores RFID mejoran la exactitud en el ingreso de información a los sistemas de información, ya que envían la información capturada directamente a la computadora o terminal como si la información hubiera sido tecleada.
		Intervención efectiva de los operarios en el procesamiento automatizado de información con código de barras o RFID	Aunque los usuarios no conozcan la totalidad de los códigos, pueden estar en capacidad de discernir sobre fallas en la captura de la información de los tipos de producto, por ejemplo, si el código detectado es el de un tipo de leche pero el producto que se escaneó es mantequilla. De igual manera, si el código o tag (etiqueta electrónica) no es reconocido por los lectores, el usuario puede estar en capacidad de reportar estos errores.
		Mantenimiento preventivo de los escáneres de los lectores de código de barras y de los lectores de tags	Procedimientos de diagnóstico sobre el estado de los lectores con el fin de impedir desgastes o daños en los aparatos que ocasionen lecturas inadecuadas.
3	Ítems rechazados o en suspenso	Controles programados	Son aquellos que se programan en las rutinas del sistema de información (v. gr., llamado a servidores espejo o llamado a bases de datos en la máquina cliente que permitan guardar la última transacción realizada para que posteriormente pueda ser actualizada).
		Interrupción de las operaciones del cliente	Bloqueo de la maquina cliente hasta que se restablezca la conexión.
		Controles de usuario	Verificación de anomalías en las transacciones realizadas por la maquina cliente.
4	Procesamiento	Formularios prenumerados y rutinas de control de secuencia	Asignar a los formularios del sistema de información una numeración correlativa en original y copias, en forma simultánea a su procesamiento e impresión.
		Consistencia en la recuperación de las transacciones	Recuperación adecuada de las transacciones luego de interrupciones en el procesamiento.
		Protección contra software malintencionado	Protección frente a código dañino: virus, troyanos, malware, puertas traseras, etc.
		Control de lote	Procesar la información por paquetes de manera que se pueda comprobar la adecuada salida de los procesos.
		Totalización de valores críticos	Comparar los totales de valores críticos antes y después del procesamiento.
		Rótulos de archivos	Identificación del contenido de los archivos utilizando patrones de rotulación.
		Controles de balanceo	Equilibrar y contrastar las variables correlacionadas y las actualizaciones del sistema de información.
		Procedimientos de enganche y recuperación	Mecanismos que al reiniciar la ejecución de un proceso interrumpido permitan continuar con el mismo sin repetir operaciones o sin dejar de procesar algunas. Lo mismo que mecanismos que permitan recuperar información que por la interrupción pueda quedar sin registro de su nuevo estado.

Tabla 6. Niveles de riesgo y controles (Cont.)

Nivel	Riesgo	Controles	Descripción
		Transmisión de información	Cifrar la información que transita por la red de manera que no se ocasionen fallas por modificaciones realizadas sin consentimiento.
5	Estructura organizativa	Segregación de funciones	Separar o independizar las funciones de los usuarios de los sistemas de información con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores.
		Controles y procedimientos operativos	Coordinar adecuadamente la responsabilidad en el manejo de la información. Establecer manuales de operación y controles operativos diarios. Supervisar a los usuarios privilegiados. Controlar el software sensible. Controlar el desarrollo de sistemas. Generar políticas y planes de contingencia. Desarrollar procedimientos y lineamientos de seguridad. Definir la función de administración de seguridad y entrenar a los profesionales en seguridad.
		Planes de continuidad	Diseñar planes de recuperación de los servicios prestados por los sistemas de información.
		Copias de seguridad	Elaborar procedimientos para la realización periódica de backups y para su respectivo almacenamiento (gestión de servicios de custodia de información).
		Capacitar usuarios	Capacitar al personal encargado de utilizar y realizar mantenimiento a los sistemas de información.
		Revisión de la configuración	Procedimientos para las actualizaciones periódicas de la configuración de los sistemas de información.
		Procedimientos de mantenimiento para los sistemas de información	Generar procedimientos para el mantenimiento preventivo y correctivo de los sistemas de información. Utilización de órdenes de trabajo para controlar los mantenimientos realizados.
6	Cambio a los programas	Procedimientos de iniciación, aprobación y documentación	Generar órdenes de trabajo al momento de realizar cambios a los sistemas de información, informando a los usuarios correspondientes los cambios a realizar. En caso de que los cambios sean considerables se debe proceder nuevamente a capacitar a los usuarios.
		Procedimientos de catalogación y mantenimiento	Establecer políticas para llevar a cabo los mantenimientos preventivos y correctivos de los sistemas de información y documentar los resultados obtenidos en los mismos.
		Intervención de los usuarios	Catalogación de la información provista por los usuarios del sistema de información respecto de fallas ocasionadas por las transacciones.
		Procedimientos de prueba	Realizar las pruebas de subsistemas y las pruebas de integridad del sistema de información cuando se consolidan los módulos.
		Supervisión efectiva	Revisión periódica de las actividades desarrolladas por los programadores de software.

Fuente: Elaboración propia.

Gráfico 3. Alineamiento de los estándares sobre GRCSI con las actividades del negocio

Fuente: Elaboración propia.

Tabla 7. Selección de estándares de acuerdo con la necesidad organizacional

Propósito de gestión de riesgos	Estándar
Manejo del riesgo de los activos relacionados con la información	ISM3, SOMAP, MEHARI o ISO 27005
Aseguramiento de los activos relacionados con los sistemas de información (personas, máquinas, líneas de comunicación, etc.)	SP800-39, MAGUERIT u OCTAVE
Gestión de los riesgos asociados con el gobierno de las tecnologías de la información, en lo referente al aprovisionamiento, soporte y administración de la infraestructura, de las aplicaciones y de los activos software	SP800-30 u OCTAVE
Gestión de riesgos a nivel organizacional relacionados más con las estrategias de la organización que con las de la dirección de la tecnología de información	AS/NZS o SP800-39

Fuente: Elaboración propia.

4. CONCLUSIONES

Una adecuada comprensión de los niveles de riesgo asociados con los sistemas de información ayudará a las organizaciones a reconocer las implicaciones de la ocurrencia de un determinado espacio de riesgo dentro de su entorno, logrando con esto apropiarse del sentido o propósito de las políticas de seguridad y su respectivo alineamiento con los procesos de negocio.

Los niveles de riesgo de PWC ofrecen una descripción que contribuye a que las organizaciones reconozcan el impacto de los riesgos en sus procesos. No obstante, al aplicar una metodología para la revisión de la estructura de sus definiciones, se logró evidenciar que no todas contenían los elementos asociados a los conceptos de nivel de riesgo y riesgo. Esto posibilitó la discusión y definición de una estructura en la que se diferenciara dónde ocurre y qué ocasiona el nivel de riesgo, además de cuál es el impacto posible para la organización.

Por su parte, abordar la complejidad de la ausencia de los procesos de cambio organizacional necesarios para llevar a cabo una adecuada GRCSI, es una labor que implica en los actores involucrados, el reconocimiento de las actividades organizacionales necesarias para su implantación en el negocio y de las responsabilidades que, como partícipes en el proceso de cambio, deben estar dispuestos a enfrentar.

La integración de las actividades relacionadas por los estándares permitirá concretar futuras investigaciones orientadas a la definición de los procesos culturales y de cambio organizacional requeridos para llevar a cabo la GRCSI. De igual manera, posibilitará el diseño de modelos de GRCSI basados en definiciones-raíz orientadas a establecer análisis de riesgos, amenazas, vulnerabilidades, subactividades y métodos concretos con el fin de llevar el riesgo a niveles aceptables, mitigando su impacto en los activos de la organización (Baskerville, 1993). Estos métodos podrán incluir listas de verificación, niveles de madurez, criterios de dependencia de los procesos de negocio respecto de los sistemas de información, planes de continuidad y seguimiento de riesgos, entre otros.

5. AGRADECIMIENTOS

Los autores expresan sus agradecimientos al grupo de investigación en "Sistemas y Tecnologías de la Información (STI)" adscrito a la Escuela de Ingeniería de Sistemas de la Universidad Industrial de Santander y a la Vicerrectoría de Investigación y Extensión de esta universidad, por el apoyo recibido para la realización de esta investigación mediante la financiación del proyecto de investigación desarrollado por León y Gomez (2010) denominado "Propuesta de un modelo para la evaluación de calidad de productos software utilizados como apoyo a la biomedicina"; código 5545.

REFERENCIAS BIBLIOGRÁFICAS

1. Alberts, C., Behrens, S., Pethia, R. y Wilson, W. (1999). Operationally critical threat, asset, and vulnerability evaluations (OCTAVESM) framework, Version 1.0. TECHNICAL REPORT. CMU/SEI-99-TR-017. ESC-TR-99-017. Carnegie Mellon, SEE.
2. Ashenden, D. (2008). Information security management: A human challenge? *Proceeding of Information Security Technical Report, 13*(4), 195-201.
3. Ashenden, D. y Ezingeard, J.N. (2005). *The need for a sociological approach to information security risk management*. Documento no publicado, presentado en la 4th Annual Security Conference, Las Vegas, Nevada, Estados Unidos.
4. AS/NZS 4360:2004. (2004). *Estándar Australiano. Administración*

de Riesgos (3ª ed.). Sydney: Standards Australia International.

5. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(4), 375414.

6. Blakley, B., McDermott, E. y Geer, D. (2001). Information security is information risk management. In *NSPW '01 Proceedings of the 2001 workshop on new security paradigms* (pp. 97-104). New York, NY: ACM.

7. Boehm, B.W. (1991). Software risk management: principles and practice. *IEEE Software, 8*(1), 32-41.

8. Cano, J. (2009). Monitoreo y evolución de la seguridad de la información. *Revista ACIS,* 110, 4-13.

9. Castilla, M., Herrera, L., Llanes, E. y Sánchez, D. (2004). *Estudio de riesgos y controles del sistema de información de la Biblioteca Germán Bula Meyer.* Recuperado el 25 de mayo de 2009, de http://www.scribd.com/doc/16445970/Riesgos-y-ControlProteccion-de-Datos-Biblioteca-GBM

10. Checkland, P. (2000). *Systems thinking, systems practice. Includes a 30-year retrospective.* New York, NY: John Wiley & Sons.

11. Checkland P. y Holwell, S. (1998). *Information, systems and information systems: making sense of the field.* New York, NY: John Wiley & Sons.

12. Checkland P. y Poulter, J. (2006). *Learning for action. A short definitive account of soft systems methodology and its use for practitioners, teachers and students.* New York, NY: John Wiley & Sons.

13. Checkland, P. y Scholes, J. (1999a). Information, Systems, and Information Systems. *Cybernetics and humans knowing, 6*(3), 91-95.

14. Checkland, P. y Scholes, J. (1999b). *Soft system methodology in action.* New York, NY: John Wiley & Sons.

15. Checkland, P. y Scholes, J. (2000). Soft systems methodology in action: a thirty year retrospective. *System research and behavioral science, 17*, S11-S58.

16. Chittister, C. y Haimes, Y.Y. (1993). Risks associated with software development: a holistic framework for assessment and management. *IEEE Transactions on Systems, Man and Cybernetics*, *23*(3), 710-723.

17. Clusif, M. (2007). *Guide de l'analyse des risques.* Recuperado el 11 de diciembre de 2009, de http://www.clusif.asso.fr

18. Contraloría General de la República de Nicaragua -CGRN. (1995). *Normas técnicas de control interno para el sector público*. Recuperado el 18 de abril de 2009, de http://legislacion.asamblea.gob.ni/normaweb.nsf/%28$All%29/804DEAE046418EEB062571790058C3B5?OpenDocument

19. Elissondo, L. (2008). *Auditoria y Seguridad de Sistemas de Información.* Recuperado el 8 de noviembre de 2011, de http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=175&Itemid=19

20. Fairley, R. (1994). Risk management for software projects. *IEEE Software, 11*(3), 57-67.

21. Farahmand, F., Navathe, S. y Enslow, P. (2003). *Managing vul-*

nerabilities of information systems to security incidents. Documento no publicado, presentado en The 5th International Conference on Electronic Commerce, Pittsburgh, PA, Estados Unidos. Recuperado de http://portal.acm.org/citation.cfm?id=948050

22. García, J. y Martínez, C. (2008). Análisis y control de riesgos de seguridad informática: control adaptativo un cambio de paradigma hacia la gestión de riesgos orientada al control adaptativo. *Revista Sistemas ACIS*, 105. Recuperado de http://www.acis.org.co/fileadmin/Revista_105/JMGarcia.pdf

23. Guerrero, M. (2010). *Gestión de riesgos y controles en sistemas de información.* Tesis de Maestría no publicada, Universidad Industrial de Santander, Bucaramanga, Colombia.

24. Haig, B. (2009). *Man in the Middle.* New York, NY: Grand Central Publishing.

25. Harold, F. y Tipton, M.K. (Eds.). (2006). *Information Security Management Handbook* (5a ed.). Danver, MA: CRC Press.

26. Hirsch, C. y Ezingeard, J.N. (2008). Perceptual and cultural aspects of risk management alignment: a case study. *Journal of Information System Security, 4*(1), 1551-0123.

27. ISACA. (2002). *Documento S11.* Recuperado el 19 de junio de 2009, de http://www.isaca.org

28. ISM3 Consortium. (2009). *Information security management maturity model. Versión 2.0.* Madrid, España.

29. ISO. (2005). *ISO/IEC 27001:2005(E) Information technology - Security techniques - Information security management systems - Requirements.* Londres: International Organization for Standardization and International Electrotechnical Commission.

30. ISO. (2008) *Introduction to ISO 27005 (ISO27005).* ICONTEC.

31. Landoll, D. (2005). *The security risk assessment handbook: A complete guide for performing security risk assessments*. Boca Raton, FL: Auerbach.

32. Laudon, K. y Laudon, J. (2008). *Sistemas de información gerencial* (10ª ed.). México: Prentice Hall.

33. Leon, N. y Gomez, L.C. (2010). *Propuesta de un modelo para la evaluación de calidad de productos software utilizados como apoyo a la biomedicina.* Bucaramanga: Vicerrectoria de Investigación y Extensión, Universidad Industrial de Santander.

34. McFadzean, E., Ezineard, J.N. y Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on Information Security strategy at board level. *Online Information Review, 31*(5), 622–660.

35. McLeod, R. (2000). *Sistemas de información gerencial* (7ª ed.). México: Prentice Hall.

36. Ministerio de Administraciones Públicas. (1997). *MAGUERIT. Metodología de Análisis y Gestión de Riesgos de los sistemas de información*. España: Autores.

37. Norma RFC4949. (2007). *Internet Security Glossary, Version 2.* Recuperado el 24 de febrero de 2010, de http://www.ietf.org/rfc/rfc4949.

38. Norton, R. (2004). Crooked managers. Changing technology. Financial surprises. Who knows what company-killers lie ahead?

Here's how directors can protect themselves. Institute of Public Administration of Canada. Toronto: Longwoods Publishing Corporation.

39. Peltier, T. (2001). *Information security risk analysis*. Boca Raton, FL: Auerbach Publications.

40. PriceWaterhouseCoopers. (2004). *Managing risk: An assessment of CEO preparedness*. Recuperado de http://www.pwc.com.

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

42. Ross, R., Katzke, S., Johnson, A., Swanson, M. y Stoneburner, G. (2008). *Managing risk from information systems an organizational perspective, Special Publication 800-839.* Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

43. Schein, E.H. (1991) *Psicología de la Organización*. México: Prentice-Hall.

44. Silberfich, P.A. (2009). *Análisis y Gestión de riesgos en TI ISO 27005 – Aplicación Práctica.* Documento no publicado presentado en el Quinto Congreso Argentino de Seguridad de la Información, Argentina.

45. Singh, S. y Brewer, R. (2008). *The evolution of risk and controls from score-keeping to strategic partnering. KPGM International*. Recuperado el 18 de diciembre de 2009, de http://sociedaddelainformacion.wordpress.com/category/seguridad/gestion-de-riesgos/

46. Smith, H., McKeen, J. y Staples D. (2001). Risk management in information systems: Problems and potential. *Communications of the Association for Information Systems, 7*(13).

47. SOMAP. (2006). *Open Information Security Risk Management Handbook. Versión 1.0.* Recuperado el 15 de diciembre de 2009, de http://ufpr.dl.sourceforge.net/project/somap/Infosec%20Risk%20Mgmt%20Handbook/Version%201.0/somap_handbook_v1.0.0.pdf

48. Stonebumer, G., Coguen, A. y Feringa, A. (2002). Risk Management Guide for *Managing risk from information systems an organizational perspective, Special Publication 800-830.* Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

49. Straub, D. y Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

50. TCSEC - Trusted Computer Systems Evaluation Criteria, DoD 5200.28-STD, Department of Defense, United States of America, 1985.

51. Wah, L. (1998). The risky business of managing IT risks. *Management Review, 87*(5), 6.

52. Whitman, M. y Mattord, H. (2005). *Principles of information security* (2a ed.). Boston, MA: Thomson Course Technology.