LA GESTIÓN DE RIESGOS Y CONTROLES EN SISTEMAS DE INFORMACIÓN

M. L. Guerrero Julio[1], Universidad Pontificia Bolivariana, Bucaramanga
L.C Gómez Flórez[2], Universidad Industrial de Santander UIS, Bucaramanga
Recibido Noviembre 16, 2011 – Aceptado Febrero 14, 2012
http://dx.doi.org/10.18566/puente.v6n1.a02

***Resumen*—Los Sistemas de Información adquieren cada vez más importancia en las organizaciones por el apoyo que brindan a la sistematización y la organización de la información. No obstante, debido a diversas vulnerabilidades y a amenazas, los Sistemas de Información pueden poner en riesgo la integridad, la confidencialidad y la disponibilidad de la información. En este marco de ideas se propuso el proyecto de investigación "Gestión de Riesgos y Controles en Sistemas de Información", el cual pretendía diseñar los procesos que posibiliten el "hacer" de esta labor en las organizaciones. El siguiente artículo presenta los resultados de dicho proyecto, mostrando de manera general los niveles de riesgo propuestos y los métodos propuestos por cada actividad.**

***Palabras Clave*— Controles, Gestión, Riesgos, Seguridad de la Información, Sistemas de Información.**

***Abstract*— Information systems are becoming increasingly important in organizations for their support to the systematization and organization of information. However, due to various threats and vulnerabilities, the information systems can compromise the integrity, confidentiality and availability of information. In this framework of ideas was proposed the research project "Risk Management and Control Information Systems", aimed to design the processes that enable the "do" of this work in organizations. The following article presents the results of this project, showing generally the risk levels proposed and the methods proposed for each activity.**

***Keywords*— Controls, Information Security, Information Systems, Management, Risk.**

[1] M. L. Guerrero Julio, M.Sc. Docente tiempo completo de la Universidad Pontificia Bolivariana.e-mail: marlene.guerrero@upb.edu.co
[2] L.C. Gómez Flórez, Profesor titular adscrito a la Escuela de Ingeniería de Sistemas e informática de la Universidad Industrial de Santander. E-mail: lcgomezf@uis.edu.co

I. INTRODUCCIÓN

En la actualidad, la incorporación de sistemas de información para apoyar los procesos de negocio en las organizaciones busca propiciar un aumento en su competitividad y en la rapidez con la que se toman decisiones acertadas [1], [2], [3], [4].

No obstante, la calidad de los Sistemas de Información es un tema de constante preocupación en las organizaciones. En 2007 el Standish Group llevo a cabo un estudio en donde se logró determinar que el 23% de los desarrollos de software fallan, en contraste con un 49% cuyo desarrollo es cuestionado y sólo un 28% satisfactorio [5]. Esta preocupación ha ocasionado que las organizaciones sean cada vez más conscientes de las pérdidas económicas acarreadas por los riesgos asociados a la falta de calidad en los sistemas de información.

Es en este escenario que el grupo de Investigación en Sistemas y Tecnologías de la Información STI llevo a cabo el proyecto de investigación "*Gestión de Riesgos y Controles en Sistemas de Información - GRCSI",* con el propósito de apoyar a las organizaciones en el reconocimiento de las implicaciones de la ocurrencia de un determinado espacio de riesgo dentro de su entorno complejo, a partir del diseño de un modelo centrado en niveles de riesgo y basado en la revisión y la integración de las actividades para la GRCSI propuestas por los estándares y la literatura.

En este artículo se presentan los resultados y las conclusiones más relevantes obtenidas del proceso de investigación sobre la gestión de riesgos y controles en sistemas de información y sobre los métodos sugeridos para apoyar a la dirección de tecnologías de información en el "*hacer*" de la GRCSI.

II. LA SEGURIDAD DE LA INFORMACIÓN EN EL MARCO DE LA GRCSI

Cuando se habla sobre GRCSI es importante abordar el tema de la seguridad de la información, el cual permitirá abrir la discusión sobre los riesgos y las amenazas a las cuales se ven expuestos los Sistemas de Información en la actualidad.

La seguridad de la información es un tema de especial interés tanto para las organizaciones como para diversas empresas consultoras a nivel internacional y nacional. En concordancia con esto, empresas de reconocido prestigio en el ámbito de la consultoría como lo son Price Waterhouse Coopers, Deloitte y Ernst & Young desarrollan continuamente investigaciones orientadas a establecer el estado de la seguridad de la información en las organizaciones.

La primera investigación a la que se hará alusión es a la desarrollada por Price Waterhouse Coopers – PWC en su informe "Qué esperan los Ejecutivos de la Seguridad de la Información" [6], en el que se entrevistaron a 7300 ejecutivos de tecnologías de la información de diversos negocios en Asia, Norte América, Sur América y China. En esta investigación se encontró que la mayoría de las empresas actualmente han dado mayor prioridad y han incrementado sus investigaciones en programas de seguridad y gestión de riesgos y controles en sistemas de información.

En la Fig. 1, PWC presenta las siete estrategias principales a las que actualmente las empresas le están apuntando en materia de seguridad de la información.

- *Estrategia 1. Incrementar el enfoque de protección de datos.*
- *Estrategia 2. Priorizar las investigaciones de seguridad basadas en riesgo.*
- *Estrategia 3. Fortalecer los programas de gestión de riesgos y controles de la compañía.*
- *Estrategia 4. Reducir, mitigar o transferir los principales riesgos.*
- *Estrategia 5. Reenfocar el núcleo de las estrategias existentes.*
- *Estrategia 6. Acelerar la adopción de tecnologías de automatización relacionadas con la seguridad para incrementar la eficiencia u reducir costos.*
- *Estrategia 7. Adoptar un reconocido marco de trabajo de seguridad como un medio para la preparación de próximos requerimientos regulatorios.*

Los resultados de la entrevista están agrupados de acuerdo con las respuestas "algo importante", "importante", "muy importante" o "máxima prioridad".

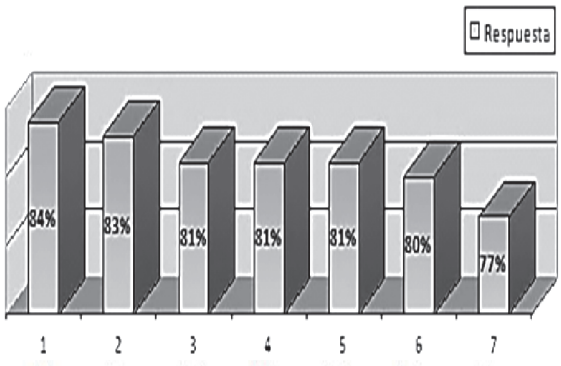

Fig. 1. Resultados de las estrategias aplicadas por las empresas en materia de seguridad. Fuente: Adaptada de Brenner (2009).

Otro aspecto muy importante del estado de la seguridad de la información es provisto por Deloitte en su "Informe Anual de Seguridad de la Información en las Instituciones Financieras" [7] en el que se entrevistaron a más de 200 instituciones financieras, bancos y compañías aseguradoras de la región EMEA (Europa, Oriente Medio y África), Norte América, Latinoamérica, Japón y la región de Asia y Pacífico con el ánimo de profundizar sobre las estrategias utilizadas por estas organizaciones en materia de seguridad de la información, el presupuesto que se destina y las principales amenazas, ataques y soluciones tecnológicas para combatirlas.

En este informe, se destacan las tendencias claves en el mundo en materia de seguridad de la información, entre las cuales se encuentran:

1. Cumplimiento regulatorio.
2. Gestión de accesos e identidades.
3. Protección de información y prevención de fugas.
4. Mejoras en las infraestructuras de seguridad.
5. Gobierno de la seguridad.

En la Fig. 2, Deloitte presenta las principales barreras para garantizar la seguridad de la información que fueron detectadas en el estudio.

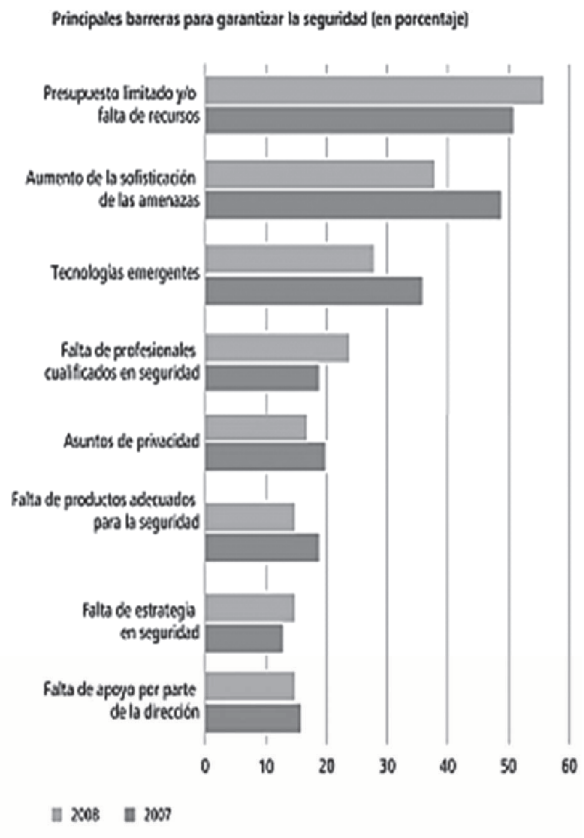

Fig. 2. Principales barreras detectadas por Deloitte para Garantizar las Seguridad. Fuente. Deloitte (2009)

Como se puede observar, el presupuesto es uno de los principales factores que impiden un adecuado aseguramiento de la información, seguido por la sofisticación de las amenazas actuales y las tecnologías emergentes.

Por último, se hará referencia al informe publicado por Ernst & Young denominado "Managing Risk in the Current Climate" [8], en donde se especifican las áreas que las organizaciones deben atender en materia de seguridad y gestión de riesgos.

Entra las áreas mencionadas por Ernst & Young se encuentran:

- Incrementar la Comunicación y Visibilidad de los Riesgos
- Definir Políticas y Procedimientos de Riesgos.
- Subcontratar la Gestión de Riesgos.
- Implementar la Tecnología Relevante parta el Gobierno de las Metas de los Procesos.

Por su parte, normatividades como Maguerit [9] apoyan la idea de la seguridad de los sistemas de información, la cual tiene como objetivo principal el resguardo de los recursos asociados a los SI. En este sentido, la Seguridad de los Sistemas de Información busca garantizar que los SI cumplan con los criterios de confidencialidad, autenticidad, integridad y disponibilidad, entendiéndose estos últimos cuatro términos como se presenta en la tabla I.

TABLA I
CRITERIOS DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

CRITERIO	DESCRIPCIÓN
Confidencialidad	Protección de la información sensible contra revelación no autorizada.
Integridad	Precisión y completitud de la información. Validez de la información de acuerdo con las expectativas de la empresa.
Disponibilidad	Accesibilidad a la información cuando sea requerida por los procesos del negocio. Protección de los recursos y capacidades asociadas a los mismos.
Autenticidad	"*Propiedad que permite que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores*" [9].

Fuente. Elaboración Propia

Asegurar los recursos asociados a los SI es hoy en día un factor clave para las organizaciones, circunstancia por la cual se han establecido estándares a nivel mundial que buscan ofrecer guías o pautas sobre este tema.

La implementación de un modelo de gestión de riesgos y controles permite una reducción en los costos administrativos y operacionales, ya que se previenen los daños o alteraciones que se pueden realizar a la información teniendo en cuenta que la confidencialidad, integridad y disponibilidad de la misma de mantengan y además se controlen aspectos que tiene que ver con pérdidas que ocasionen mayores gastos de recuperación y restablecimiento.

Teniendo esto presente, la investigación planteada por el grupo STI tenía las siguientes pretensiones [10]:

- Diagnosticar las tendencias de la gestión de riesgos y controles y la calidad de sistemas de información, incluyendo los estándares, la literatura y las prácticas, con el fin de fundamentar el desarrollo de la propuesta.
- Diseñar los procesos, pautas y modelos de Sistema de actividad Humana – SAH que posibiliten la gestión de los riesgos y controles en SI teniendo en cuenta el pensamiento blando.
- Aplicar el modelo de gestión de riesgos y controles al sistema EscuelaCol 1.0 con el propósito de ilustrar su utilización y contribuir a la posible mejora de la herramienta.

III. RESULTADOS DE LA CONCEPCIÓN DEL MODELO

El modelo concebido se fundamentó en la revisión de los los frameworks y la literatura asociada a la gestión de riesgos y controles en sistemas de información [11]. Entre los frameworks revisados se tuvieron en cuenta:

- Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). Su principal objetivo es el de garantizar la seguridad de los SI y una de sus particularidades, es que puede ser realizado por personal perteneciente tanto a las unidades funcionales como al área de TI de la organización [12].
- ISM3 o Cubo ISM (Information Security Maturity Model) - ISM3 RA (Risk Assessment). Este modelo extiende los principios de calidad de la norma ISO9001 para el sistema de gestión de la seguridad de la información. ISM3 es un estándar orientado por procesos que utiliza niveles de madurez [13]. ISM3 reconoce que cada organización tiene un contexto y recursos únicos y que por lo tanto los diferentes procesos deben ser aplicados cuidadosamente, ya que pueden requerir más tiempo del esperado o requerir un orden lógico diferente. Las implementaciones de ISM3 son compatibles con la ISO27001, CMMI, COBIT e ITIL.
- AS/NZS 4360:2004 Estándar Australiano de Administración de Riesgos. El estándar australiano para la administración de riesgos AS/NZS: 2004 proporciona un marco genérico para establecer el contexto, la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de riesgos [14]. Este estándar considera que la gestión de riesgos debe ser una filosofía organizacional y que debe ser parte de su cultura de manera que no sea vista como una actividad separada de los procesos de la organización.
- Risk Management Guide for Information Technology Systems SP800 - 30. Esta guía promueve el seguimiento y aprendizaje de los riesgos a través de su transferencia y documentación y se enfoca en la premisa que un proceso eficaz de gestión del riesgo es un componente importante de un exitoso programa de seguridad informática y tiene como fin principal proteger a la organización y su capacidad para llevar a cabo su misión, no sólo sus activos de TI. Por lo tanto, el proceso de gestión de riesgos no debe ser tratado primordialmente como una función técnica realizada por los expertos que operan y administran los sistemas de información, sino como una función esencial de gestión de la organización [15].
- Open Information Security Risk Management. La guía para la gestión de riesgos de seguridad de la información fue creada por The Security Officers Management and Analysis Project – SOMAP [16]. SOMAP considera que los riesgos pueden surgir de un proceso actual o de algún acontecimiento futuro.
- MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Versión 2.0. Fue creada por el Ministerio de Administraciones Públicas de España y tiene como principales objetivos concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y preparar a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso [9].
- Método Armonizado para la Gestión de Riesgos – MEHARI. Fue desarrollado por el

CLUSIF (Club se la Seguridad de la Información de Francia) para ayudar a tomar decisiones (a los responsables de la seguridad, administradores de riesgos y gerentes) en la gestión de la seguridad de la información y en la minimización de los riesgos. MEHARI específica que una situación de riesgo se caracteriza por la potencialidad y los efectos inherentes a la ausencia de cualquier medida de seguridad y ofrece un marco metodológico, instrumentos y bases de conocimiento para analizar los principales problemas. explorar las vulnerabilidades, reducir la gravedad de los riesgos y supervisar la seguridad de la información [17].

- ISO 27005. Esta Norma es la primera de la serie ISO 27000 que proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una Organización. Esta guía es aplicable a todos los tipos de organización. Aunque no proporciona o recomienda una metodología específica, establece una serie de factores, para determinar el alcance real del sistema de gestión de la seguridad de la información (SGSI) [18].
- Managing Risk from Information Systems SP800-39. Una Perspectiva Organizacional. La guía para la gestión de riesgos de sistemas de información fue desarrollada por el Instituto Nacional de estándares y Tecnología (National Institute of Standards and Technology - NIST). La SP800-39 proporciona a las organizaciones un proceso estructurado y flexible para la gestión de riesgos relacionados con el funcionamiento y el uso de sistemas de información. Este documento es utilizado por las organizaciones para determinar una adecuada reducción del riesgo necesaria para proteger los sistemas de información y la infraestructura de apoyo a la misión de organización y los procesos de negocio [19].

En la revisión de los frameworks descritos anteriormente y de otros documentos de especial importancia como el Estándar de Auditoria de Sistemas de Información de ISACA y el Modelo Estándar de Control Interno – MECI se pudieron evidenciar descripciones asociadas a la concepción sobre riesgo y control, los cuáles se presentan de manera resumida en la tabla II.

Entonces, tomando en cuenta las investigaciones anteriores se puede decir que un riesgo es "la posibilidad de ocurrencia de un acto o evento que podría tener un efecto adverso en la organización y en sus sistemas de información". Esta definición debe ser contrastada con algunos conceptos que suelen utilizarse asociados al riesgo, tales como amenaza, vulnerabilidad, impacto y salvaguardas.

TABLA II
CONCEPCIONES SOBRE RIESGO Y CONTROL EN SISTEMAS DE INFORMACIÓN.

ESTÁNDAR	RIESGO	CONTROL
Estándar de Auditoria de SI – Documento S11 - ISACA.	La posibilidad de ocurrencia de un acto o evento que podría tener un efecto adverso en la organización y en sus sistemas de información [20].	Políticas y procedimientos implementados para alcanzar un objetivo de control relacionado [20].
AS/NZS 4360:2004 Estándar Australiano de Administración de Riesgos.	La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se le mide en términos de consecuencias y probabilidades [12].	Parte de la administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos [12].
Modelo Estándar de Control Interno – MECI.	¿Qué puede suceder?, ¿Dónde y Cuándo?, ¿Cómo y por qué? Determinar consecuencias y posibilidades [21]	***Control de Gestión***. Métodos Procedimientos Actuaciones Acciones Admón. Información, Admón. Recursos ***Control Estratégico.*** Esquema de organización Planes Principios Normas ***Control de Evaluación.*** Mecanismos de Evaluación y Verificación [21]
MAGERIT – Versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.	Administración de riesgos, incluye políticas, procedimientos, guías, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, gerencial o legal [9].	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización [9].

Fuente. Guerrero y Gómez (2010)

- Amenaza. Una persona o cosa vista como posible fuente de peligro o catástrofe.
- Riesgo. Probabilidad de que una amenaza se materialice y que produzca un impacto en los activos de la organización.
- Vulnerabilidad. Situación creada por la falta de controles con la que la amenaza podría afectar los activos de la organización.
- Impacto. Es el daño producido por la ocurrencia de una amenaza.
- Salvaguardas. Protecciones u acciones que disminuyen el riesgo.

Teniendo en cuenta la definición de riesgo planteada, se puede decir que las organizaciones están expuestas a diferentes niveles de riesgo, los cuales se pueden clasificar dependiendo de su espacio de ocurrencia.

El modelo planteado para la identificación de estos niveles de riesgo se fundamentó en la propuesta inicial de siete niveles de Price Waterhouse Cooper mostrada en [22], los cuales fueron redefinidos y actualizados, llegando a la clasificación presentada en la Fig. 3. y en la Tabla III.

Fig. 3. Propuesta de Niveles de Riesgo

De igual manera, en la revisión se lograron contrastar las actividades propuestas para el desarrollo de la GRCSI, las cuales se unificaron y dieron lugar al modelo de actividades y métodos que se presenta en la tabla IV.

TABLA III
DEFINICIONES SOBRE LOS NIVELES DE RIESGO

NIVEL DE RIESGO	DEFINICIÓN
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 SI.
Ingreso de Información	Este nivel de riesgo surge cuando la información es ingresada a los SI 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.
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.
Procesamiento	Este nivel de riesgo surge cuando los procesos de los SI 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.
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 SI, no se actualicen los SI y no se reaccione adecuadamente ante contingencias.
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 perdida de información, repetición de esfuerzo, inconsistencias en los procesos e inconformidad en los clientes y usuarios.

Fuente. Guerrero y Gómez (2011)

TABLA IV
ACTIVIDADES PROPUESTAS PARA LA GRCSI

ACTIVIDAD	SUB ACTIVIDAD	MÉTODOS
A1. Establecer el contexto organizacional.	A.1.1. Identificar la Estrategia de la Organización en términos de los SI	1. Entrevistar a los Jefes del Departamento de Sistemas o Administradores de TI. 2. Revisar la Documentación sobre las Políticas Organizacionales de Adquisición, Implementación y Uso de los SI.
	A.1.2. Especificar los SI que apoyan los procesos de negocio	1. Determinar la Dependencia de los Procesos de Negocio Respecto de los SI. 2. Determinar los niveles de servicio de los SI. 3. Revisar la documentación de los SI.
	A.1.3. Especificar los roles de los actores y sus responsabilidades en la GRCSI	Entrevistar a los Actores de los SI sobre la Conducta Ante Riesgos.
A2. Identificar los activos críticos en los diferentes espacios de la organización.	A.2.1. Catalogar los Activos Relacionados con los SI	Implantar software de catalogación de activos
	A.2.2. Determinar la Información Sensible y Crítica	Revisar las Bases de Datos y los Informes de los SI para Detectar la Información Vulnerable
	A.2.3. Dimensionar los activos en cuanto a los niveles de riesgos y su relación con la disponibilidad, autenticidad, integridad y confidencialidad.	Comparar los niveles de riesgo versus los activos en riesgo y su relación con los criterios de seguridad.
A3.Identificar y evaluar las amenazas y vulnerabilidades[1] de los activos.		Relacionar las amenazas y vulnerabilidades con los activos de los SI.
A4. Diseñar escenarios de riesgo en términos de su impacto organizacional.	A.4.1. Creación de una base especifica de escenarios de riesgo.	1. Utilizar una BD para la descripción de los escenarios de riesgo. 2. Identificar las causas y consecuencias de los escenarios de riesgo.
	A.4.2. Derivar el impacto que los escenarios de riesgo tienen sobre la organización.	Relacionar los escenarios de riesgo con los activos impactados en la organización.
A5. Diseñar estrategias de tratamiento y protección basados en estándares y buenas prácticas.	A.5.1. Identificar las estrategias de mitigación candidatas.	1. Asociar los escenarios de riesgo con los niveles de riesgo. 2. Identificar los controles pertinentes de acuerdo con los niveles encontrados.
	A.5.2. Seleccionar la alternativa más adecuada en términos de costo y recursos disponibles.	Elaborar una matriz de relación Control – Costo - Recurso
	A.5.3. Elaborar e Implementar un plan para el tratamiento del riesgo	1. Priorizar los riesgos 2. Especificar los responsables del tratamiento de los riesgos. 3. Generar un calendario de implementación. 4. Evaluar los riesgos luego del tratamiento. 5. Evidenciar el seguimiento del riesgo.
A6. Documentar los Resultados y revisar casos.		Documentar los casos versus frecuencia de ocurrencia, mecanismos de mitigación y resultados.
A7. Monitorear y Controlar.		

[1] Amenaza: 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. Vulnerabilidad: hecho o actividad que permite concretar una amenaza y el Riesgo es la posibilidad de que se produzca un impacto en la organización (Silberfich, 2009).

IV. CONCLUSIONES

La Gestión de riesgos y Controles en Sistemas de Información no debe verse divorciada de la calidad del software, ya que la calidad es uno de los factores fundamentales a tener en cuenta para evitar la ocurrencia de los riesgos asociados a los SI. Durante el desarrollo de aplicaciones se garantiza a través de distintas metodologías y técnicas de aseguramiento de la calidad del software que las aplicaciones se ajusten a los estándares y que tengan la menor cantidad de errores posibles. No obstante, amenazas relacionadas con la naturaleza misma del sistema de información o con factores externos pueden llegar a verse reflejados en la ocurrencia de riesgos. Es en este punto en que modelos de gestión de riesgos y controles en sistemas de información como el planteado en esta investigación ayudan a las

organizaciones y a los desarrolladores de software a reconocer no sólo los niveles de riesgo de los SI sino también las implicaciones sobre los activos organizacionales que su ocurrencia pudiera ocasionar.

El modelo brinda a las organizaciones una serie de actividades definidas y organizadas metodológicamente para llevar a cabo la gestión de riesgos y controles en Sistemas de Información – GRCSI, las cuales son producto de la revisión e integración de las actividades relacionadas por los estándares y la literatura sobre GRCSI.

La integración de las actividades relacionadas por los estándares, permitirán concretar futuras investigaciones, orientadas a la definición de los procesos culturales y de cambio organizacional requeridos para llevar a cabo la GRCSI.

Para cada una de las actividades se propuso un conjunto de métodos, los cuales apoyan a los distintos involucrados en el "hacer" que conlleva la GRCSI.

Por otro lado, el modelo centra la GRCSI en la concepción de niveles de riesgo, lo cual permite apoyar a las organizaciones en el reconocimiento de los espacios organizacionales y de sistemas de información en los que se podría dar la ocurrencia de riesgos.

De igual manera, el modelo propuesto contribuye a la definición de medidas de mitigación asociadas a cada uno de los niveles de riesgo, las cuales deben ser posteriormente profundizadas por parte de las organizaciones de acuerdo con la complejidad de su entorno.

El modelo diseñado no tiene la pretensión de convertirse en un patrón para todas las organizaciones, por lo cual la definición inicial de los controles sugeridos para los seis niveles de riesgo planteados es un punto de partida que posteriormente puede ser ampliado por los responsables de la GRCSI en cada organización.

REFERENCIAS

[1] M. Bennett y F. Bennett. "Object Oriented Systems Analysis and Design Using UML", McGraw Hill, 2005.

[2] K.C. Laudon y J.P. Laudon. "Sistemas de Información Gerencial", Prentice Hall, 2010.

[3] R. Pressman. "Ingeniería del Software – Un enfoque práctico". McGrawHill, 2008.

[4] I. Sommerville. "Ingeniería del Software". Prentice Hall, 2007.

[5] M. Piattini. "Calidad de Sistemas de Información", Alfa y Omega, 2007.

[6] B. Brenner. "The Global State of Information Security", www.pwc.com/gx/en/information-security-survey, 2009.

[7] Deloitte. "Confianza y Garantía. Informe Anual de Seguridad de la Información en Instituciones Financieras", Febrero 2009.

[8] Ernst & Young. "Managing Risk in the Current Climate". 2009.

[9] Ministerio de Administraciones Públicas. "MAGUERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", 1997.

[10] M. Guerrero y L. Gómez. "Gestión de riesgos y controles en Sistemas de Información". Tesis de Maestría, 2010.

[11] M. Guerrero y L. Gómez. "Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información". Revista Estudios Gerenciales, Vol. 27, No. 120, 2011.

[12] C. Alberts. "Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVESM) Framework, Version 1.0". TECHNICAL REPORT. CMU/SEI-99-TR-017. ESC-TR-99-017, 1999.

[13] ISM3 Consortium. "Information Security Managemente Maturity Model. Versión 2.0", 2009.

[14] AS/NZS. "Estándar Australiano. Administración de Riesgos". Tercera edición, 2004.

[15] G. Stonebumer. "Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology". NIST, Special Publication 800-30, 2002.

[16] SOMAP. Open Information Security Risk Management Handbook. Versión 1.0, 2006.

[17] CLUSIF. "MEHARI 2007. Guide de l'analyse des risques", http://www.clusif.asso.fr, 2007.

[18] ISO Directory. "Introduction To ISO 27005 (ISO27005)". ICONTEC, 2008.

[19] R. Ross. "Managing Risk from Information Systems. Recommendations of the National Institute of Standards and Technology. Gaithersburg", NIST Special Publication 800-39, 2008.

[20] ISACA. "Documento S11". http://www.isaca.org, 2002.

[21] Ministerio de Administraciones Públicas. "Modelo Estándar de Control Interno – MECI", Decreto 1599, 2005.

[22] L. Elissondo. "Informática Aplicada a los Negocios - Seguridad en los Sistemas de Información", 2008.

BIOGRAFÍA

Marlene Lucila Guerrero Julio. Ingeniera de Sistemas (2.003), Especialista en Docencia Universitaria de la Universidad Cooperativa de Colombia, Magister en Ingeniería Área Informática y Ciencias de la Computación de la Universidad Industrial de Santander. Profesor de tiempo completo de la Universidad Pontificia Bolivariana. Miembro del grupo de investigación STI de la Universidad Industrial de Santander y del grupo GIINFO de la Universidad Pontificia Bolivariana. Ha desarrollado su trabajo investigativo en las temáticas de: Gestión de Riesgos y Controles en Sistemas de Información, Auditoria, Modelado y Simulación con Dinámica de Sistemas e informática educativa. Correo: marlene.guerrero@upb.edu.co

Luis Carlos Gómez Flórez. Ingeniero de Sistemas (1.988), Magister en Informática (1.990) egresado de la Universidad Industrial de Santander. Miembro fundador de los grupos de investigación SIMON (1991) y STI (2001), siendo director de este último. Profesor titular adscrito a la Escuela de Ingeniería de Sistemas e informática de la Universidad Industrial de Santander a la que se encuentra vinculado desde 1992 y en la que además ha desempeñado los cargos de jefe de la División de Servicios de Información (1994 – 1999) y en la actualidad el de Director de Investigación y Extensión de la Facultad de Ingenierías Físico Mecánicas y Editor de la Revista UIS Ingenierías. Correo: lcgomezf@uis.edu.co