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.)