Vanegas Devia, Gonzalo Andrés; Pardo, César Jesús
Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT
Sistemas & Telemática, vol. 12, núm. 30, 2014, pp. 35-48
Universidad ICESI
Cali, Colombia

Sistemas & Telemática,
ISSN (Versión impresa): 1692-5238
EditorSyT@icesi.edu.co
Universidad ICESI
Colombia

Artículo original

Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT

Mogrit: Towards a IT risks management model for MSME

Gonzalo Andrés Vanegas Devia
andevank@gmail.com
Universidad de San Buenaventura
Cali-Colombia

César Jesús Pardo, Ph.D.
cpardoc@eafit.edu.co
Grupo de Investigación I+D+I en TIC
Universidad EAFIT, Medellín, Colombia

Fecha de recepción: Agosto 1 de 2014
Fecha de aceptación: Septiembre 16 de 2014

Palabras clave
Mejora de procesos; riesgos de TI; modelos; estándares; MiPyMEs.

Keywords
Software Process Improvement, IT Risk, Models, Standards, Harmonization, SMEs

Colciencias tipo 1

Resumen

Actualmente, los proyectos de desarrollo de software pueden fracasar por múltiples factores. En ese sentido, tanto la gestión de proyectos –que permite establecer el camino a seguir–, como el análisis de los riesgos es cada vez más necesario. Este artículo presenta la armonización de modelos de riesgos de TI (e.g., CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE, RISK IT) y algunas normas enfocadas en brindar soporte a los riesgos (e.g., ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006, y UNE 71504:2008) y realiza un análisis comparativo, de alto y bajo nivel, que permite conocer las características más comunes y representativas de cada uno de ellos. Con los resultados obtenidos, se establecen los beneficios y la manera en la que los modelos comparados y su implementación pueden ser armonizados, y de esta manera dar soporte a los procesos de gestión dentro de las actividades de desarrollo de una organización. En este sentido, el artículo provee una perspectiva más clara de las diferencias, similitudes y posibles integraciones entre modelos y estándares de riesgos de TI para MiPyMEs que desarrollan software.

Abstract

Nowadays, software development projects can fail for multiple factors. In this sense, both project management that establishes the way forward as analysis of the risks, which may face a software development project, is becoming increasingly necessary. This paper presents the harmonization of IT Risk models such as: CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE, RISK IT and some models to support the IT Risk such as: ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006, and UNE 71504:2008. It also presents a comparative analysis of high and low level, which allows knowing the most common, and representative of each model. Likewise, with the results obtained, are established the benefits and the manner in which the models compared can be harmonized to carry out their implementation of a harmonized wayand thus to support management processes within development activities of an organization. This work provides a clearer view of the differences, similarities and possible integrations between IT Risk models and standards for Small and medium enterprises of software development.

I. Introducción

Actualmente las grandes organizaciones dependen del uso de la tecnología –donde la información es un activo vital– para ser exitosas y lograr su continuidad en el mercado. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización; por ello, la evaluación y la gestión de riesgos surge como una prioridad para la mayoría de las organizaciones.

El análisis de riesgos es un proceso iterativo debido a los cambios de las condiciones enmarcadas en la mejora continua de las organizaciones La administración de riesgos es un método sistemático que permite planear, identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con una actividad, función o proceso, para que la organización pueda reducir pérdidas y aumentar sus oportunidades.

La gestión de riesgos en proyectos de desarrollo de software tiene varios usos, permite evitar fallas muy comunes en ellos, como son: su terminación por fuera del cronograma establecido, las modificaciones en los presupuestos y el incumplimiento de las especificaciones del cliente. La gestión de riesgos en la ingeniería de software presenta un acercamiento preventivo a favor de la terminación de los proyectos en un tiempo y con un presupuesto estipulados; los proyectos basados en la gestión de riegos tienen la habilidad de reducir costos del proyecto y su tiempo de finalización, e incrementar su calidad. Sin estos factores, los proyectos tendrían grandes riesgos respecto de los ingresos y la confiabilidad del cliente, los cuales, en el peor escenario, pueden significar la quiebra de las compañías participantes en él. En los inicios de 2000, las empresas desarrolladoras de software en sus proyectos no utilizaban un sistema metodológico en la gestión de riesgo, simplemente se enfocaban en lograr un desarrollo que diera respuesta al problema en el que se está trabajando. Frente a esto, la complejidad en el desarrollo del software se incrementó, haciendo que el marco de trabajo fuera modificado, lo que obligó a estas empresas a darle a la gestión de riesgos mayor importancia, ya que ella contribuye a la reducción de la incertidumbre involucrada en el desarrollo de software y a la reducción de posibles fallas del proyecto.

Teniendo en cuenta lo anterior, este artículo provee de una serie de recomendaciones que guían en la gestión y el análisis de riesgos en TI, lo que permite mantener una estrategia de protección y de reducción de riesgos, justifica una mejora continua en la seguridad de la información, minimiza el impacto en la reducción de costos y evita las pérdidas de dinero, tiempo y mano de obra.

Aparte de esta introducción, el artículo está organizado como sigue: en la sección 2 se presenta el estado del arte, donde se exponen los modelos y normas internacionales de estudio y los trabajos relacionados; la sección 3 presenta el estudio comparativo de cada uno de los modelos y las normas; la sección 4 presenta la armonización de

múltiples modelos para la gestión de riesgos de TI; y por último, la sección 5 presenta las conclusiones e identifica trabajo a futuro.

II. Estado del arte

En la elaboración de este artículo, se tuvo en cuenta los siguientes modelos de gestión del riesgo: CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE, RISK IT, y algunas normas ISO enfocadas en dar soporte a los riesgos, tales como: ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006 y UNE 71504:2008. Desde su aparición, las normas y los modelos de riesgo han venido evolucionando de acuerdo con la forma como se administra la información en las empresas, brindando el conocimiento que permite tomar decisiones para disminuir costos y aumentar la rentabilidad.

A. Modelos y normas relacionadas con la gestión de riesgos en TI

BS 7799 – 3

Es una norma publicada por el *British Standard Institute*. Proporciona una guía para soportar los requisitos establecidos por ISO/IEC 27001:2005 con respecto a todos los aspectos que debe cubrir el ciclo de análisis y gestión del riesgo en la construcción de un sistema de gestión de la seguridad de la información [SGSI]. El objetivo de esta norma es dar efectiva seguridad de la información a través de un programa permanente de actividades de gestión de riesgos. Además, incluye la identificación y evaluación del riesgo, mediante la implementación de controles para su reducción, monitoreo y revisión, y el mantenimiento y la mejora continua del sistema basado en el control del riesgo (BSI, 2006).

CRAMM

Es una metodología de análisis de riesgos desarrollada en el Reino Unido por la agencia central de cómputo y telecomunicaciones [CCTA]. La primera versión apareció en 1987 y aún está vigente la versión 5.1. Es el método de análisis de riesgos preferido en los organismos de la administración pública. Se compone de tres etapas, cada una apoyada por cuestionarios, objetivos y directrices. Las dos primeras se encargan de identificar y analizar los riesgos para el sistema, y la tercera recomienda la manera en que estos riesgos deben ser gestionados (Seguridad Informática, 2005).

COBIT .4.1

Es un marco de referencia internacional aceptado por la mayoría de empresas como buenas prácticas para el control interno de la información. COBIT ha sido diseñado para facilitar el uso de las TI desde un enfoque de inversión que debe estar bien administrado y está basado en los estándares y las mejores prácticas de la industria, y ayuda a salvar la brecha entre los riesgos del negocio, las necesidades de control y los aspectos propiamente técnicos. COBIT provee de buenas prácticas, gracias a un marco de dominios: planificar y organizar; adquirir e implementar; entrega y soporte; y monitorear y evaluar (EAFIT, 2007)

ISO 27005

Esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información (ISO/IEC, 2011a).

ISO 31010 [6]

Es una norma publicada por la Organización Internacional de Normalización [ISO] y la Comisión Electrotécnica Internacional [IEC] enfocada en la gestión de riesgos. Su propósito es brindar información basada en pruebas y análisis para tomar decisiones sobre cómo seleccionar y determinar el tratamiento de los riesgos. El marco de gestión del riesgo de esta norma proporciona las políticas, los procedimientos y las disposiciones organizativas que integran la gestión de riesgos en toda la organización a todos los niveles. Como parte de este marco, la organización debe tener una política o estrategia para decidir cuándo y cómo los riesgos deben ser evaluados (ISO/IEC, 2011b).

ITIL v3

Fue desarrollada al reconocer que las organizaciones dependen cada vez más de la informática para alcanzar sus objetivos corporativos, lo que ha dado como resultado la creciente necesidad de servicios informáticos de calidad que correspondan a los objetivos del negocio y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar en el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones (Axwloa, 2011).

MAGERIT

Es un método formal para investigar los riesgos que soportan los sistemas de información. Es una norma establecida por el Gobierno español con el fin de brindar una metodología de sistemas de información de riesgos en su análisis y gestión. El propósito de MAGERIT está relacionado con el uso de medios electrónicos, informáticos y tecnológicos, sujetos a ciertos riesgos que se deben minimizar con medidas de seguridad, para mitigar la desconfianza en el uso de estos medios. Su utilización está enfocada en las personas que utilizan los sistemas de información y sobre los riesgos y vulnerabilidades a que está expuesta la información (MHAP, 2012).

OCTAVE

Es una técnica efectiva de evaluación de riesgos desarrollada en el Centro de Coordinación CERT en *Carnegie Mellon University*. Octave es un conjunto de herramientas, técnicas y métodos para la evaluación del riesgo. Tiene en cuenta también la definición de los activos incluyendo: personas, hardware, software, información y sistemas. Hay tres componentes que conforman la base de su cuerpo de conocimiento:

Octave, en su metodología original, definida para las grandes empresas, que describe conjuntos de criterios (i.e., principios, atributos y resultados); Octave-S, similar a la original, pero dirigido a empresas con garantía limitada; y Octave Allegro, un enfoque simplificado para la evaluación de la información de seguridad y garantía (CERT, 2008).

Octave proporciona una línea base que se puede utilizar para enfocar la mitigación y mejorar de actividades; asimismo, equilibra los riesgos operativos, las prácticas de seguridad y la tecnología, lo cual permite tomar decisiones de protección de información con base en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados con la información crítica (CERT, 2008).

Existen varios criterios de Octave que definen un conjunto de enfoques para la evaluación de los riesgos en una organización, en la seguridad de la información, utilizando un conjunto de principios, atributos y salidas (CERT, 2008).

RISK IT

Es un marco de trabajo a nivel mundial enfocado a las TI y publicado por ISACA. RISK IT proporciona una visión global sobre los riesgos empresariales asociados con todas las actividades relacionadas con TI. RISK IT pretende ser una herramienta práctica para la gestión de riesgos basada en los conceptos de valor y beneficios que la organización obtiene a través de sus iniciativas de TI. Al igual que COBIT, RISK IT se concentra en el cumplimiento de los objetivos de la organización. Este modelo puede personalizarse para cualquier tipo de empresa en cualquier ubicación geográfica. RISK IT se define como una serie de guías para la gestión eficaz de los riesgos de TI. Dichas guías se basan en los principios comúnmente aceptados en ERM, que se han aplicado en el ámbito de las TI. El modelo del proceso de los riesgos de TI está diseñado y estructurado para que las organizaciones puedan poner los principios en práctica y comparar sus resultados (ISACA, 2013).

UNE 71504

Es una norma realizada por la Asociación Española de Normalización y Certificación [AENOR], orientada al análisis y la gestión de riesgos para los sistemas de información. Esta norma define la gestión de riesgos con base en las siguientes fases principales: caracterización de activos, caracterización de las amenazas, cálculo del riesgo intrínseco, caracterización de las salvaguardas, cálculo del riesgo efectivo, evaluación de riesgos, tratamiento de riesgos, y administración de la gestión de los riesgos (Agendum, 2007).

La Tabla 1 resume cada uno de los modelos y las normas relacionadas con la gestión de riesgos en TI

B. Trabajos Relacionados

En la elaboración de este artículo se encontraron varios trabajos relacionados que hablan sobre la gestión de riesgos en TI, lo cuales tienen en común algunos puntos que se expondrán en la propuesta metodológica que se presenta en la sección Propuesta de este documento; a continuación, se describen brevemente dos de ellos.

Tabla 1. Resumen de los modelos y normas relacionadas con la gestión de riesgos en TI

Modelo	Organización	Publicación	Actualización	País	Estructura
AS/NZS ISO31000	ISO	2004	2009	Australia Nueva Zelanda	11 principios / 5 procesos
BS 77993	BSI	2006	-	Reino unido	6 procesos
COBIT	CCTA	2003	-	Reino unido	5 principios / 37 procesos
CRAMM	ISACA	2008	2012	Estados Unidos	3 fases
EBIOS	ANSSI	2002	2010	Francia	5 fases
ISO/IEC 27005	ISO	2008	-	Suiza	6 procesos
ISO/IEC 31010	ISO	2009	-	Suiza	4 principios / 5 procesos
ITIL	ITIL	2001	2011	Suiza	5 principios
MAGERIT	Gobierno de España	2006	2012	España	Vol. 1, Método / Vol.2, Catálogo / Vol. 3 Guía
OCTAVE	SEI	2001	2007	Estados Unidos	Octave: 3 fases / Octave s: 3 fases / Octave allegro: 4 fases
RISK IT	ISACA	2009	2011	Estados Unidos	3 principios
UNE 71504	AENOR	2008	-	España	4 fases

Guía de gestión de riesgos para sistemas de tecnología de la información

Esta guía proporciona una base para el desarrollo de un programa de gestión de riesgos efectiva; contiene tanto las definiciones como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI. El objetivo de la gestión de riesgos es permitir a la organización llevar a cabo su Misión, mejorando la seguridad de la información, con énfasis en la forma como ésta es almacenada y trasmitida a nivel organizacional. La guía permite tomar decisiones de gestión de riesgos con conocimiento de causa, justificando los gastos que forman parte de un presupuesto de TI; de igual manera, ayuda a la administración en la elaboración de documentos como apoyo derivado de la gestión de riesgos (Stoneburner, Gouguen, & Feringa, 2002).

Metodologías y herramientas de evaluación de riesgo establecido actual

Este informe está estructurado en ocho capítulos. El primero contiene una introducción al tema; el segundo, una introducción al campo de la seguridad de la información de

gestión de riesgos; el tercero presenta una visión general de los métodos de evaluación de riesgos más comunes; el cuarto describe las diversas maneras de conceptualizar el riesgo que cada marco implica; el quinto expone los índices de las herramientas de software disponibles y los asigna a sus marcos pertinentes; el sexto expone los intentos de extraer las principales características de cada una de las metodologías y herramientas identificadas; el séptimo sugiere una pauta para seleccionar el método más adecuado; y, finalmente, el octavo presenta algunas conclusiones basadas en el análisis anterior. Su objetivo general es obtener una mejor comprensión de las diferencias clave y los puntos comunes entre las distintas metodologías y herramientas del estado de la técnica de evaluación de riesgo de la información (Ionita, Hartel, Pieters, & Wieringa, 2013).

III. Propuesta (Método)

En el proceso de desarrollo de este trabajo se utilizó una metodología que serviría de estrategia para llevar a cabo la comparación y posterior armonización de los modelos y estándares que dan soporte a la gestión de riesgos (Pardo, 2012).

Esta metodología se compone de cuatro etapas, como ilustra la Figura 1, las cuales se describen a continuación:

» Etapa 1. Identificar los modelos y las normas relacionadas con la gestión de riesgos en las tecnologías de la información: CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE, RISK IT y algunas normas enfocadas a dar soporte a los riesgos como: ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006, y UNE 71504:2008.

» Etapa 2. Comparar cada uno de los modelos relacionados con la gestión de riesgos en las tecnologías de la información, realizando un análisis detallado de cada una de sus características, ventajas y desventajas, tomando los elementos comunes entre sí y agrupándolos de acuerdo con su enfoque.

» Etapa 3. Agrupar las características comunes en el proceso de gestión del riesgo,

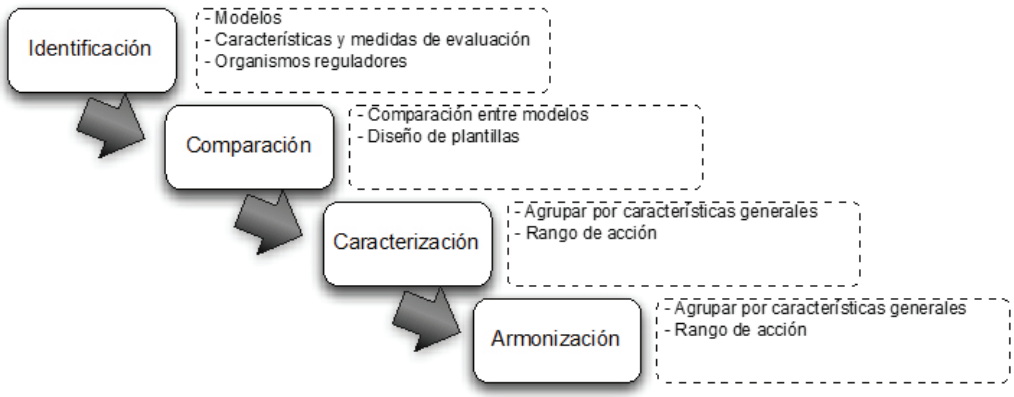

Figura 1. Etapas de la metodología propuesta

de manera que se agrupan por fases y en cada fase se describen los elementos comunes de gestión de riesgos.

» Etapa 4. Realizar un informe ejecutivo donde se muestren los resultados obtenidos del análisis de las dos etapas anteriores, de modo que se entreguen las recomendaciones y conclusiones en la gestión de riesgos.

IV. Resultados y discusión

Después de analizar cada modelo y poner en práctica la metodología propuesta, se evidenció que los modelos se encuentran altamente relacionados en el proceso de gestión de riesgos; se construyeron varias plantillas que permitieran ver claramente cómo un modelo puede soportar a otro. La Tabla 2 presenta, a modo de ejemplo la plantilla utilizada para relacionar las normas ISO/IEC 27005 y ISO/IEC 31010. Teniendo cada una de las relaciones entre cada modelo y cada norma, se construye una plantilla que agrupa, por etapas, cada uno de los pasos en la gestión de riesgos, con el fin de caracterizar los modelos y lograr identificar las áreas de acción, donde se gestione y administre el riesgo.

En la Tabla 2 se propone una serie de etapas donde se agrupan cada uno de los procesos de gestión de riesgos en cada una de las normas y modelos. Los nombres de las etapas fueron establecidos tomando en cuenta las relaciones encontradas en la comparación hecha con cada uno de los modelos y normas; a su vez, se define un modelo lógico para ubicar cada proceso en las etapas definidas en el análisis (caracterización de los modelos).

Tabla 2. Plantilla que describe la relación entre los modelos y las normas de gestión de riesgos en TI

		Proceso de gestión						
		ISO/IEC 31010						
		Comunicar y consultar	Establecer el contexto	Identificar los riesgos	Análisis de riesgos	Evaluar los riesgos	Tratar los riesgos	Seguimiento y revisión
Proceso de gestión ISO/IEC 27005	Comunicar los riesgos	◉						
	Establecer el contexto		●					
	Identificar los riesgos			●				
	Analizar los riesgos				○			
	Evaluación					●		
	Tratamiento					○	◉	
	Aceptación					○	◉	
	Monitoreo y revisión							●

Convenciones: Total● Parcial◘ Medio○ Bajo: ◉ Ninguno: ○

Tabla 3. Relación porcentual utilizada para la comparación

Acrónimo	Descripción	Porcentaje
S	Fuertemente relacionado	(86% a 100%)
L	Relacionado en gran medida	(51% a 85%)
P	Parcialmente relacionado	(16% a 50%)
W	Débilmente relacionado	(1% a 15%)
N	No relacionado	0%

Después de encontrar las relaciones entre los modelos, es posible determinar porcentualmente el cubrimiento o soporte de un modelo a otro modelo por medio de la escala de comparación definida por Pardo, Pino, García, Baldassarre, y Plattini (2010) (Tabla 3) y la plantilla diseñada durante la realización de este proyecto.

A continuación se presenta un ejemplo tomando como referente el análisis porcentual para las normas ISO/IEC 27005 y ISO/IEC 31010 (ver Tabla 4).

Tabla 4. Análisis porcentual encontrado para las normas ISO/IEC 27005 Y ISO/IEC 31010

		Proceso de gestión						
		ISO/IEC 31010						
		Comunicar y consultar	Establecer el contexto	Identificar los riesgos	Análisis de riesgos	Evaluar los riesgos	Tratar los riesgos	Seguimiento y revisión
Proceso de gestión ISO/IEC 27005	Comunicar los riesgos	17%						
	Establecer el contexto		14%					
	Identificar los riesgos			11%				
	Analizar los riesgos				18%			
	Evaluación					12%		
	Tratamiento						10%	
	Aceptación						8%	
	Monitoreo y revisión							10%

A. Evaluación metodológica en la gestión de riesgos en TI

La propuesta metodológica de este trabajo surge del estudio realizado a cada uno de los modelos y estándares relacionados con la gestión de riesgos en TI, donde se tomaron los procesos y las actividades existentes de cada uno de ellos, obteniendo la unión de todas las características y los principios comunes (como se mencionó en la sección 2). La metodología propuesta está basada en la combinación de las actividades

descritas en los procesos de gestión de riesgos de cada uno de los modelos; esta propuesta permitirá a las empresas desarrolladoras de software –u organizaciones que tengan procesos en TI–, lograr identificar, analizar y dar seguimiento a los riesgos en sus proyectos en desarrollo, de modo que estos puedan ser terminados en el cronograma establecido. Para realizarla, se toma como punto de partida el diagnóstico del equipo de trabajo en la organización, teniendo en cuenta los roles y las funciones asignadas a cada integrante del equipo; también se deben incluir los activos con que cuentan para iniciar el proyecto de desarrollo de software –o el proceso que se lleva en TI–: Es importante involucrar la infraestructura y los activos tecnológicos, ya que permiten establecer el contexto en el momento que aparezca un riesgo o que una amenaza atente contra los procesos que se desarrollan en TI. Para gestionar los riesgos se recomienda la siguiente metodología:

Identificar el contexto de la organización

Proporcionar los parámetros básicos para la gestión de riesgo teniendo en cuenta el alcance y los criterios que se van a utilizar durante el proceso. Incluye la consideración de parámetros internos y externos relevantes para la organización, en su conjunto, así como los antecedentes de los riesgos particulares que se están evaluando. Al establecer el contexto, se determinan: el programa de evaluación de los riesgos, los objetivos de la evaluación de riesgos y los criterios del riesgo.

Definir los roles y las responsabilidades del personal relacionado con TI

Determinar los actores que intervienen, llevando un manual de funciones que permita tener claro el papel de cada uno en la organización, de manera que cuando ocurra un riesgo se puedan determinar las posibles fallas por donde se originó el riesgo.

Identificar los activos tecnológicos de la organización

Un activo es algo que tiene valor o utilidad para la organización teniendo en cuenta la continuidad de sus operaciones comerciales; es por eso que un activo necesita protección, para garantizar las operaciones comerciales y la continuidad del negocio.

Identificar los riesgos, amenazas y vulnerabilidades

Los riesgos deben ser identificados de manera que se puedan entender antes de ser analizados y gestionados correctamente. Esta identificación debe tener un enfoque detallado que permita abarcar todos los eventos posibles, de modo que se clasifiquen los riesgos en las categorías definidas en la estrategia de gestión del riesgo, de tal manera que los riesgos formen una línea base para el inicio de actividades en la gestión de riesgo. Los riesgos deben ser revisados periódicamente para reexaminar las posibles fuentes de riesgo y revisar las condiciones cambiantes, revisando los riesgos que se pasaron por alto o aquellos que no existían en la última revisión.

Analizar los riesgos

El análisis de riesgos implica su identificación a partir de fuentes internas y externas;

cada riesgo es evaluado para determinar su probabilidad y sus consecuencias. Los riesgos se categorizan con base en la evaluación establecida en la estrategia de gestión de riesgos, proporcionando información suficiente para su manejo, estableciendo un nivel de análisis con base en lo que es apropiado y razonable.

Evaluar los riesgos, determinando el nivel de riesgo

Este es el proceso donde se consolida la identificación, el análisis y la evaluación de los riesgos, es en este punto donde se determina su prioridad para el tratamiento adecuado.

Tratar los riesgos, definir e implementar los planes de mitigación

Terminada la evaluación del riesgo, se ejecutan las medidas correctivas, se escoge una serie de opciones para mitigar el riesgo; este es un proceso repetitivo que tiene como fin determinar su tolerabilidad en contra de los criterios establecidos, con el fin de decidir si se requiere un tratamiento posterior. Los riesgos son monitoreados cuando superan los umbrales establecidos, los planes de mitigación de riesgos se despliegan para devolver el esfuerzo afectado a un nivel de riesgo aceptable. Si el riesgo no puede ser mitigado, se puede invocar un plan de contingencia.

Aceptar el riesgo

En este punto del proceso, toma parte la alta dirección de la organización que es la encargada de determinar el nivel de impacto del riesgo y de decidir si se acepta o no, teniendo en cuenta sus consecuencias. Aceptar el riesgo incluye asumir las responsabilidades frente a las insuficiencias encontradas luego de haber tratado el riesgo (si ha quedado algún riesgo residual).

Llevar un control de seguimiento y monitoreo del riesgo tratado

Como parte del proceso de gestión, los riesgos y los controles deben ser monitoreados y revisados periódicamente para verificar que las hipótesis sobre los riesgos sigan siendo válidas.

Registrar el proceso de gestión de riesgos

Se debe llevar un histórico de todos los incidentes, que permita llevar una auditoría independiente en la gestión de riesgos con el fin de garantizar que se ha realizado una buena gerencia de riesgos.

Para un mayor entendimiento, esta de propuesta se resume en la Figura 2.

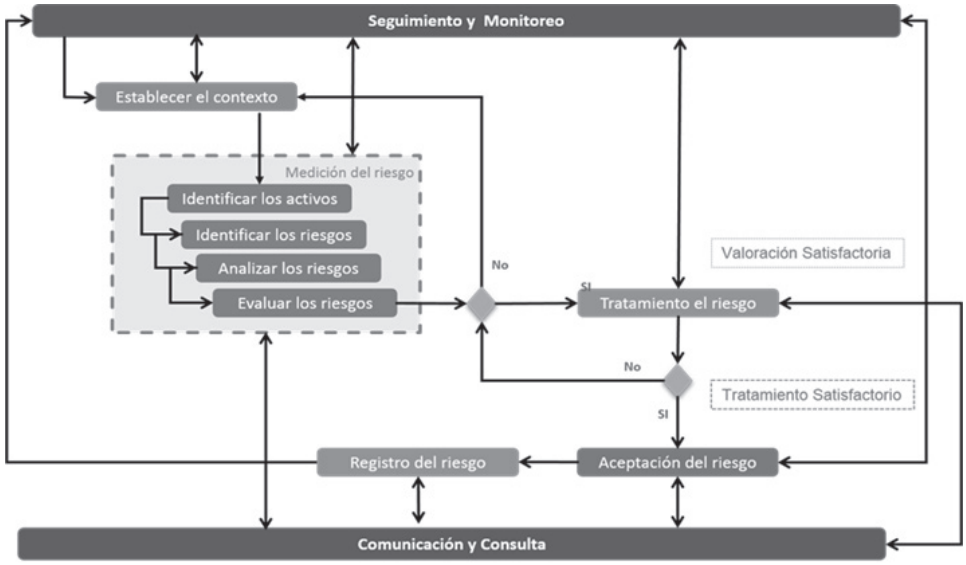

Figura 2. Propuesta Metodológica en la gestión de riesgos en TI

Conclusiones

El análisis realizado permitió evidenciar que la mayoría de las normas y modelos aquí descritas están relacionados entre sí, aunque algunas normas presentan procesos más detallados, con un nivel más profundo que otros modelos. Asimismo, se observó que hay normas y modelos con similitudes en la definición de sus procesos, tales como actividades similares entre sí. Por otra parte, también se encontraron algunas actividades que complementaban y mejoraban las descripciones de otras actividades, dando como resultado la característica en la que un modelo es capaz de soportar a otro modelo.

La gestión de riesgos permite evitar el fracaso de proyectos de desarrollo de software, estimulando la terminación del mismo de modo que se incrementa la calidad en los proyectos entregados, reduciendo costos y cumpliendo con las necesidades del cliente, lo que impacta positivamente en su satisfacción. Una buena gestión de riesgos tiene como habilidad entregar a tiempo los productos esperados a partir de las metas que se plantearon y con el cronograma de actividades establecido.

Esta metodología, aunque no es oficial, esta soportada por las actividades que están descritas en los procesos de gestión de riesgos definidos en normas y estándares certificados y avaladas por organismos internacionales como la ISO, IEC, ISACA e ICONTEC, entre otros, lo que permite fácilmente certificarse en algunos de los modelos existentes que la conforman. La implementación de estos procesos determina, de alguna manera, seguir las prácticas que permitan cumplir con los atributos de calidad, alcanzando con éxito los objetivos de las organizaciones o la terminación de un proyecto de desarrollo de software.

Referencias bibliográficas

Agendum. (2007). *Norma UNE 71504*. Retrieved from http://www.agedum.com/NormaUNE71504/tabid/118/Default.aspx

Axwloa. (2011). *ITIL, continual service improvement*. Norwich, UK: TSO

British Standards [BSI] (2006). *Information security management systems. Part 3: Guidelines for information security risk management* [BS 7799-3:2006] London, UK: BSI

CERT [Software Engineering Institute, Carnegie Mellon University]. (2008). *Octave*. Retrieved from http://www.cert.org/octave/

International Organization for Standardization [ISO]., & International Electrotechnical Commission [IEC]. (2011a). *ISO/IEC 27005: gestión de riesgos de seguridad de la Información*. Geneve, Swizerland: ISO

International Organization for Standardization [ISO]., & International Electrotechnical Commission [IEC]. (2011b). *Risk management — Risk assessment techniques* [IEC/FDIS 31010]. Retrieved from http://www.previ.be/pdf/31010_FDIS.pdf

Ionita, D. Hartel, P.H., Pieters, W. & Wieringa, R.J. (2013). *Current established risk assessment methodologies and tools* [Technical report, TR-CTIT-14-04]. Enschede, The Netherlands: Centre for Telematics and Information Technology, University of Twente

ISACA (2013). *The RISK IT Framework* [online]. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

Ministerio de Hacienda y Administraciones Públicas [MHAP]. (2012). *MAGERIT – versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información*. Madrid, España: MHAP

Pardo, C. (2012). *A framework to support the harmonization between multiple models and standards* [Tesis doctoral]. Universidad Castilla–La Mancha: Ciudad Real, España

Pardo, C., Pino, F., García, F., Baldassarre, M., & Plattini, M. (2010). From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies. *Journal of Systems and Software, 86(1), 25-43*

Seguridad Informática (2005). *Herramienta de Evaluación de Riesgo-CRAMM, Metodologías de análisis de riesgos* [en línea]. Retrieved from http://seguridadinformaticaufps.wikispaces.com/Herramienta+de+Evaluacion+de+Riesgo-CRAMM

Stoneburner, G., Gouguen, A., & Feringa, A. (2002). *SP 800-30. Risk management guide for information technology systems* [technical report]. Gaithersburg, MD: National Institute of Standards & Technology

Universidad EAFIT (2007). *COBIT: modelo para auditoria y control de sistemas de información*. Medellín, Colombia: EAFIT

Currículum vitae

Gonzalo Andrés Vargas Devia

Ingeniero de Sistemas de la Universidad de San Buenaventura de Cali (Colombia), con interés profesional en el análisis de riesgos de las tecnologías de la información y el desarrollo de software.

Cesar Jesús Pardo Calvache

Ingeniero de sistemas de la Universidad del Cauca (Colombia) e Ingeniero en Informática (homologación del Ministerio de Educación de España); Magister y Doctor en Tecnologías Informáticas Avanzadas de la Universidad de Castilla-La Mancha (España); miembro del Grupo de Investigación I+D+I en TIC y docente del departamento de Informática y Sistemas de la Universidad Eafit (Medellín). Sus áreas de interés son: mejora de procesos, calidad de proceso y producto, armonización de múltiples modelos, gestión del conocimiento, ideación e innovación, metodologías ágiles, entre otros.