Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo

eTOM risk management. A comparative analysis with the standards of corporative risk

Gestão de riscos em eTOM. Un análisis comparativo com os padrões de risco corporativo

Leonardo Ortiz Restrepo *
Francisco Javier Valencia Duque **
Universidad Nacional de Colombia Sede Manizales

Resumen

La gestión del riesgo es un proceso esencial en cualquier modelo de gestión empresarial. El presente artículo analiza este proceso dentro del modelo eTOM, principal referente del sector de telecomunicaciones, confrontándolo con tres de los principales estándares internacionales de gestión de riesgos, acudiendo para ello a la revisión bibliográfica y al uso de esquemas de armonización usados en propósitos similares. Como conclusión, se observa una baja alineación entre los procesos de gestión de riesgos de eTOM y los estándares internacionales de gestión de riesgos, debiendo acudir a normas más ajustadas con los planteamientos desarrollados por el modelo, por su orientación hacia controles y no hacia una metodología específica de gestión de riesgo.

Palabras clave: eTOM, gestión de riesgos, ISO/IEC 27005:2011, ISO/IEC 27002:2013, COSO-ERM, ISO 31000:2009.

Abstract

Risk management is an essential process in any business management model. This article analyzes this process within the model eTOM, main reference in the telecommunications sector, comparing it with three of the main international standards of risk management, going to do to the literature and the use of schemes harmonization used in similar purposes

Fecha de recepción del artículo: 24 de enero de 2017
Fecha de aceptación del artículo: 6 de Junio de 2017
DOI: http://dx.doi.org/10.22335/rlct.v9i1.334

* Ingeniero electrónico Espc. Gestión de Proyectos, Estudiante de Maestría en administración de empresas, Universidad Nacional de Colombia Sede Manizales. lortizr@unal.edu.co. Orcid http://orcid.org/0000-0002-8441-7035

** Phd. en Ingeniería, Industria y Organizaciones. Docente Universidad Nacional de Colombia Sede Manizales. fjvalenciad@unal.edu.co Orcid: http://orcid.org/0000-0002-0617-2386

review. In conclusion, a low alignment is observed between the processes of risk management eTOM and international standards of risk management and must attend norms tighter with the approach developed by the model, its orientation towards control and not towards a methodology specific risk management. In this sense it goes to the ISO / IEC 27002: 2013, primary benchmark for information technology controls and communications, finding a level of alignment only 29%**.**

Keywords: eTOM, risk management, ISO/IEC 27005:2011, ISO/IEC 27002:2013, COSO-ERM, ISO 31000:2009.

Resumo O gerenciamento de riscos é um processo essencial em qualquer modelo de gerenciamento de negócios. Este artigo analisa esse processo dentro do eTOM modelo, referência principal no setor de telecomunicações, comparando-o com três dos principais padrões internacionais de gerenciamento de risco, indo para a literatura e o uso de esquemas de harmonização utilizados em análises semelhantes. Em conclusão, observa-se um baixo alinhamento entre os processos de gerenciamento de risco eTOM e os padrões internacionais de gerenciamento de riscos e deve atender às normas mais rigorosas com a abordagem desenvolvida pelo modelo, sua orientação para o controle e não para uma gestão de risco específica da metodologia. Nesse sentido, el vai para o ISO / IEC 27002: 2013, benchmark primário para controles de tecnologia da informação e comunicações, encontrando um nível de alinhamento apenas de 29%

Palavras-chave: eTOM, gerenciamento de riscos, ISO / IEC 27005: 2011, ISO / IEC 27002: 2013, COSO-ERM, ISO 31000: 2009.

Introducción

En el campo organizacional, la gestión de riesgos es considerado un aspecto crítico para el logro de los objetivos de cualquier entidad, y las empresas de telecomunicaciones no están al margen de este tipo de procesos y más aún si se considera el rol que juegan en su conjunto actualmente en la competitividad de cualquier país.

Las diferentes industrias han desarrollado modelos de gestión específicos para estandarizar sus procesos y lograr niveles de eficacia y eficiencia en el cumplimiento de sus objetivos, tal es el caso de la industria de telecomunicaciones, donde se ha promulgado el modelo eTOM como un referente para cualquier empresa del sector que desee estandarizar sus procesos.

La industria de telecomunicaciones está compuesta por operadores, proveedores de servicios, integradores de sistemas y comercializadores que pueden favorecerse de la adopción de eTOM debido a que sus procesos han sido definidos de la manera más genérica posible y dada su independencia de la organización, la tecnología y el servicio. Es así como muchas de las organizaciones de telecomunicaciones a nivel internacional han adoptado el marco eTOM dentro de sus procesos.

Como parte de la adopción del modelo, los procesos de gestión de riesgos son un aspecto esencial dentro de este, por lo que es necesario establecer su nivel de alineación con los principales estándares de gestión de riesgos corporativo tales como ISO 31000 y COSO ERM y de manera particular por la orientación de este tipo de empresas hacia las tecnologías de información y comunicaciones con modelos de gestión de riesgos tecnológicos como la ISO/IEC 27005.

Autores como Bosetti (2015); Ernawati, Suhardi, & Nugroho (2012); Gjerdrum & Peter (2011); Kganakga (2014); Racz, Weippl, & Seufert (2010); Vanegas & Pardo (2014) han realizado análisis de alineación de los diferentes estándares internacionales de gestión de riesgos y han concluido que aunque se encuentren relacionados total o parcialmente, estos referentes sirven para que otros autores avancen en este tópico y cada organización encuentre la herramienta que más se ajuste a sus necesidades.

El proceso de alineación que se desarrollará en este trabajo parte de un análisis general de la similitud de procesos de la gestión de riesgos entre el modelo eTOM y los diferentes referentes, y de manera particular en su análisis final al establecer el referente más pertinente entre el modelo eTOM y la norma ISO/IEC 27002:2013 se utilizó el modelo hframework propuesto en Pardo, Pino, Garcia, Baldassarre, & Piattini(2013) con algunos ajustes planteados por los autores de este trabajo.

1. El marco de referencia eTOM

Las empresas de telecomunicaciones hacen parte de uno de los sectores más dinámicos de la economía, a través de las cuales se proporcionan un conjunto de servicios que permiten aportar a la competitividad de otros sectores. Su evolución y complejidad tecnológica han llevado a la necesidad de contar con modelos de gestión maduros que permitan el logro de los objetivos de manera más eficaz y eficiente, de allí que la asociación industrial Telemanagement Forum (en adelante TM Forum) haya propuesto a principios de la década del 90, un marco de referencia específico para el sector, denominado en su momento TOM (por sus siglas en inglés de Telecommunications Operations Map) y a partir del año 2000 con su versión mejorada establecida como eTOM (enhanced Telecommunications Operations Map).

El modelo eTOM es un modelo funcional, estándar y generalizado, utilizado como referencia para analizar las actividades de las redes y servicios al interior de una organización en el sector de telecomunicaciones (Bellafkih, Raouyane, Ranc, Errais, & Ramdani, 2012).

Según la recomendación M.3050.4 de 2007 de la ITU-T (telecommunication standardization sector), eTOM se inició como programa de trabajo regido por TM Forum, que en el año de 2004 aprobó la versión GB921 V4.0, conforme a las recomendaciones internacionales de la industria de las telecomunicaciones.

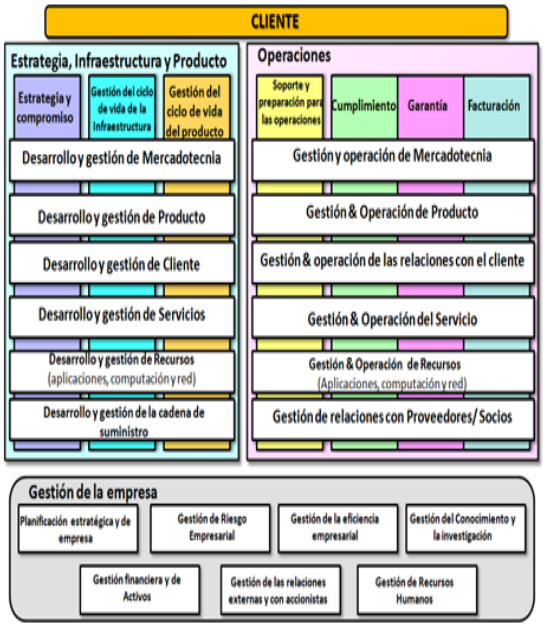
Autores como Carrillo Alvarez & Medina Ramirez (2006); Latifi & Nasiri (2013); Ospina & Gallego (2008) señalan que la contribución más importante de eTOM, es la estandarización de los procesos de negocios, actuando así como un marco de referencia, para las empresas de telecomunicaciones y de otros sectores.

Por lo tanto, las entidades de las industrias de las telecomunicaciones, que incluyen operadores, proveedores de servicios, integradores de sistemas, vendedores o socios, pueden favorecerse mediante la adopción de eTOM; además, el marco puede ser utilizado por todas estas entidades, ya que se define de la manera más genérica posible, dada su independencia de la organización, la tecnología y el servicio.

1.1 Estructura por procesos de eTOM

Este artículo se desarrolla sobre la versión 16.0 de eTOM, de acuerdo a la guía de Addendum D "Descomposición de procesos y descripciones" (TeleManagement Forum, 2012; TMforum, 2016). En la figura 1, se observa el mapa de procesos de negocios estándar orientado a las telecomunicaciones, en el cual se incluyen la integración de todos los servicios y proveedores.

Figura 1. Modelo eTOM - Nivel 1



Fuente**:** Elaboración propia a partir de (TMforum, 2016).

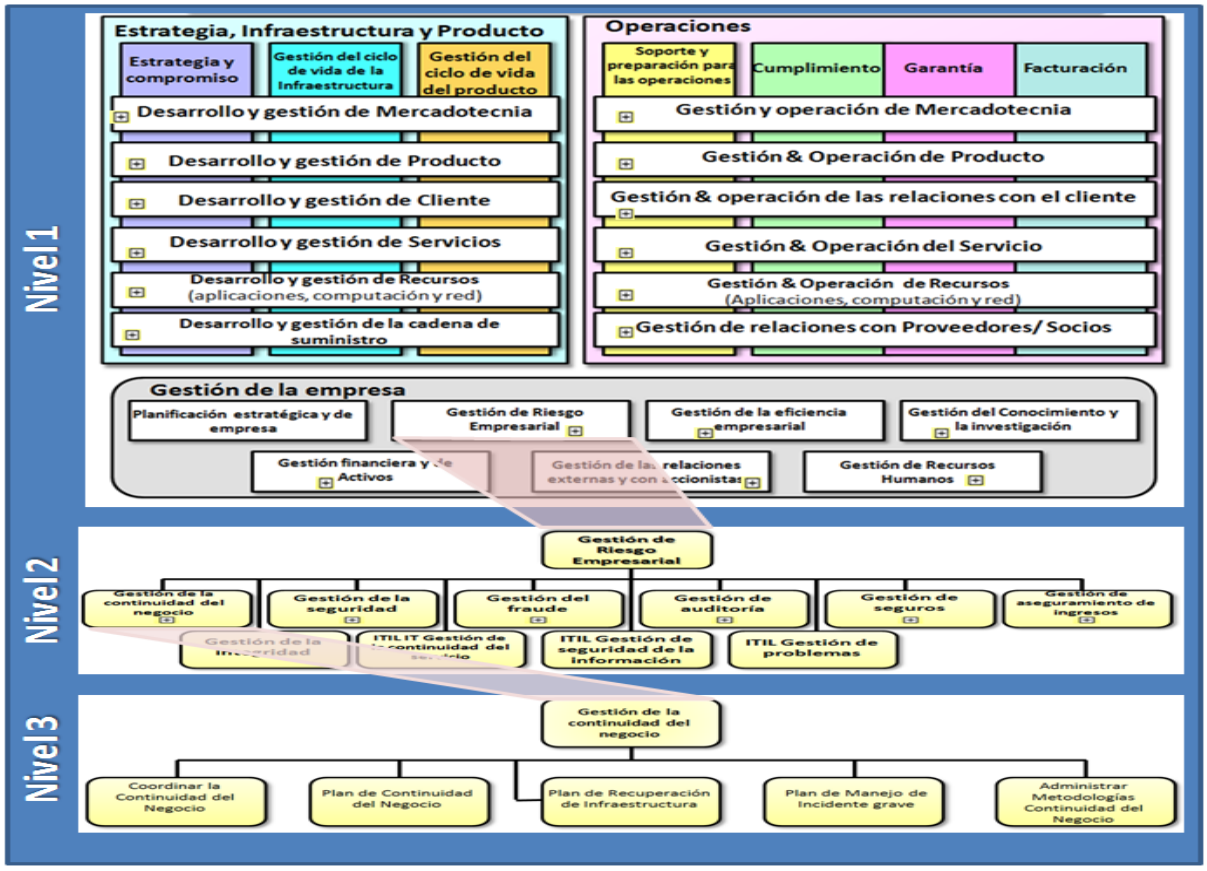


Figura 2. Niveles de interacción del marco eTOM

Fuente: Autor

El modelo eTOM es un marco de referencia orientado a procesos el cual se despliega en niveles. Su primer nivel está compuesto por tres macroprocesos: el de estrategia, infraestructura y producto (que equivale a los procesos estratégicos en una organización tradicional); el de operaciones (que corresponde a los procesos misionales en una organización tradicional) y el de gestión de la empresa (equivalente a los procesos de apoyo en una organización tradicional).

Cada uno de estos macroprocesos a su vez, cuentan con sus respectivos procesos tanto verticales como horizontales, de acuerdo al nivel de impacto y funcionalidad sobre ciertas operaciones de la organización.

El modelo eTOM, según el nivel conceptual de los procesos, contiene cuatro niveles para cada macroproceso. En la figura 2, se observa lo anterior, aclarando que la jerarquía de este marco permite que, este enfoque por módulos sea de fácil actualización y se pueda reutilizar de forma independiente.

1.2. Modelo de riesgos en eTOM

La gestión de riesgo empresarial del modelo eTOM hace parte del macroproceso de gestión, el cual a su vez en el nivel 2 del modelo se desglosa en 10 subprocesos, (figura 3). Los subprocesos que incorpora la gestión del riesgo de eTOM van desde aspectos tan genéricos como la gestión de la seguridad hasta aspectos tan específicos como la gestión del fraude y la gestión de los seguros.

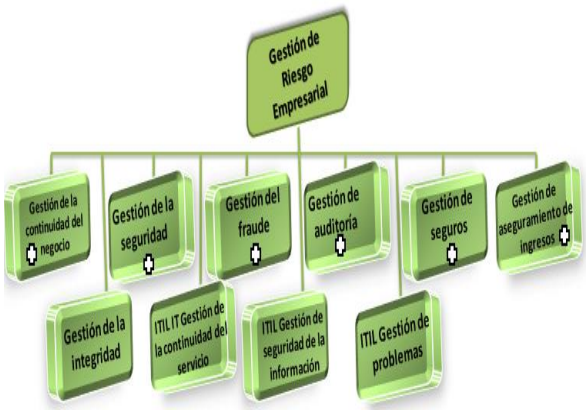


Figura 3. Procesos de gestión de riesgo empresarial del modelo eTOM - Nivel 2. Fuente: Adaptado de TMforum, 2016

Al realizar un análisis general de los subprocesos que incorpora el modelo eTOM, en lo relacionado con la gestión del riesgo, se observa más que un marco metodológico para incorporar la gestión del riesgo en los demás procesos del modelo, una serie de aspectos generales y específicos asociados a controles que se combinan con procesos puntuales de ITIL, e incluso con parámetros con los cuales se mide el impacto en otros esquemas de gestión de seguridad de la información (ISO/IEC 27001:2013), como es la gestión de la integridad.

Conforme a la guía GB921 Addendum D y a lo descrito por el grupo TMforum (2016), se presentan en la tabla 1, los procesos de gestión de riesgo empresarial hasta el nivel 3, los últimos cuatro procesos llegan hasta un nivel 2 de detalle.

Tabla 1

Procesos de gestión de riesgo empresarial del marco eTOM - Nivel 3

Marco eTOM	
Gestión de la Continuidad del negocio	Coordinar la Continuidad del Negocio; Plan de Continuidad del Negocio; Plan de Recuperación de Infraestructura;Plan de Manejo de Incidente grave;Administrar Metodologías Continuidad del Negocio
Gestión de la seguridad	Administrar Gestión proactiva de la Seguridad; Monitorear tendencias de la industria para la gestión de la seguridad; Definir Políticas y Procedimientos de gestión de la seguridad; Ayudar con implementación de Gestión de la Seguridad; Manejo de Gestión de la Seguridad reactiva, entre otros.
Gestión del fraude	Gestión de Políticas de Fraude; Apoyo a las Operaciones de
Gestión de auditoria	Definir Directiva de auditoría; Definir Mecanismo de Auditoría;Valorar las actividades operacionales; Evaluar las actividades operacionales; Informe de Auditoría; Aplicar Mecanismos de Auditoría de forma proactiva
Gestión de seguros	Identificar riesgos asegurables; Analizar costo de seguro / Beneficios; Proporcionar Consejos de Seguros; Manejo Seguro de Cartera
Gestión de aseguramiento de ingresos	Administrar Ingresos Política de Garantía; Manejo de Operaciones de Aseguramiento de Ingresos; Apoyo de Ingresos Operaciones de Aseguramiento
Gestión de la integridad	Promover y exigir la integridad de personas, productos y procesos de la empresa.
ITIL Gestión continuidad del servicio	Modelo o plantilla para saber como otras áreas de proceso se alinean con el enfoque ITIL
ITIL Gestión de seguridad de la información	Modelo o plantilla para saber como otras áreas de proceso se alinean con el enfoque ITIL, además de satisfacer un acuerdo de servicio establecido con los usuarios/propietarios

Fuente: Autores

2. Marcos de gestión de riesgos a nivel internacional

Para efectos de llevar a cabo un análisis comparativo de los procesos de gestión de riesgos que incorpora el modelo eTOM y teniendo en cuenta que en el ámbito académico y profesional los dos principales referentes en materia de gestión de riesgos corporativos son: COSO-ERM y la norma ISO 31000:2009, se ha tomado como referentes de comparación ambos modelos, adicionando a dicha evaluación, y por ser las empresas del sector, intensivas en tecnologías de información y comunicaciones, la norma ISO/IEC 27005:2011.

2.1 Modelo COSO-ERM

En el año de 2004, COSO-ERM o Comité de las organizaciones patrocinadoras de la comisión de Gestión de Riesgos de negocio Treadway, cuya sigla en inglés es committee of sponsoring organizations of the treadway commission enterprise risk management, fue reconocido ampliamente en este campo (Beasley, Branson, & Hancock, 2010; Buhr, Nel, & Santos, 2006).

De acuerdo a lo anterior, la administración de riesgos empresariales, en adelante ERM (Enterprise Risk Management), y teniendo presente lo planteado por Frigo & Anderson (2014) identifica y define ocho componentes interrelacionados: 1. medio ambiente interno, 2. establecimiento de objetivos,3. identificación de eventos,4. evaluación de riesgos, 5. respuesta a los riesgos, 6. actividades de control, 7. información y comunicación y 8. seguimiento.

A su vez, el modelo COSO ERM es ampliamente aceptado por las organizaciones, porque describe claramente los elementos como clave de un proceso de ERM, aunque varios autores como Beasley et al., (2010); Di Serio, de Oliveira, & Schuch (2011); Krstić & Đorđević (2012), afirman que éste modelo es demasiado teórico y que contiene una orientación muy superficial.

El modelo COSO surgió en 1992, y pese a que tuvo diferentes modificaciones en sus objetivos y emisiones de informes, aún conserva aquellos factores que lo hacen importante en las organizaciones. Así, en la figura 4, se aprecian los aspectos que se han adicionado a este marco de referencia en el transcurso de los años.

Figura 4. Evolución del modelo COSO
Fuente: Autores

2.2 Norma ISO 31000:2009

Es necesario partir de un esquema generalmente aceptado del riesgo y es allí, donde el estándar ISO31000 toma relevancia. La gestión de riesgos es definida como el desarrollo de las actividades coordinadas, para gestionar y controlar riesgos dentro de una organización (Purdy, 2010;Luko, 2013; Vandijck, 2014).

Vandijck (2014), afirma que la norma citada actúa como una "sombrilla", bajo la cual se alinean más de 60 estándares en el área de gestión de riesgos, de ahí que pueda ser empleada en organizaciones del sector público o privado.

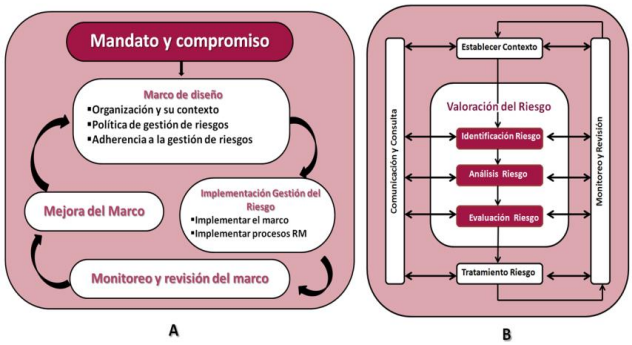


Figura 5. Marco de gestión de riesgos Proceso para el manejo del riesgo basados en ISO 31000:2009

Fuente: Adaptado de (Airmic, Alarm, & Irm, 2010)

La norma ISO 31000:2009 describe los componentes de un marco de aplicación de gestión de riesgos. En la figura 5A, se ofrece una versión simplificada de éste marco de adaptación, e incluye los pasos esenciales en la

apropiación y en el apoyo continuo del proceso de gestión de riesgos.

2.3 Norma ISO/IEC 27005:2011

Teniendo presente que eTOM es un marco de procesos orientado a empresas de tecnologías de información y comunicaciones, se ha seleccionado éste estándar internacional como una norma pertinente, para establecer la relación existente entre eTOM y los estándares internacionales de gestión de riesgos.

Ya desde hace algunos años, las organizaciones venían experimentando la necesidad de acordar normas que permitieran asegurar los procesos de información y de intercambio. Es precisamente este objetivo, lo que llevó a la creación de la norma ISO/IEC 27005, estándar cuyo propósito es establecer un "sello de confianza", para los componentes de la seguridad de la información dentro de las empresas (Lalanne, Munier, & Gabillon, 2013).

La norma ISO 27005 fue publicada en el año 2008 y su principal finalidad es la de proporcionar directrices para la gestión de riesgos de seguridad de la información, mas, teniendo en cuenta la afirmación de los autores Lalanne et al., (2013), dado que la norma ISO/IEC 27005:2011 proporciona recomendaciones, por ende utiliza muy a menudo el condicional, el cual se observa claramente en la figura 6; por tal motivo no es necesario seguir todos los pasos del método, es decir, el implementador aplica lo que es más adecuado para su caso de estudio.

La norma ISO/IEC 27005:2011 es aplicable en toda organización y sustituye las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000 de gestión de la información y comunicaciones de tecnología de seguridad (Márquez, 2016).

3. Alineación del marco eTOM con el modelo COSO-ERM, la norma ISO 31000:2009 y la norma ISO/IEC 27005:2011

Muchos marcos, modelos y normas, explican cómo implementar la gestión del riesgo de una manera eficaz. Éstos documentos cumplen con un amplio consenso en todo el mundo, lo cual pone de manifiesto una búsqueda creciente, en la armonización de las prácticas de gestión de riesgos a nivel internacional, a fin de tener en cuenta las particularidades de cada organización.

Figura 6. Proceso de gestión de riesgos de seguridad de la información ISO/IEC 27005:2011

Fuente: Adaptado de (Lalanne et al., 2013)

Lo anterior se debe probablemente a la creciente competencia global, que incita a la mejora de los sistemas de gobierno corporativo, como una clave para apoyar el éxito de la compañía y la confianza en las partes interesadas (Bosetti, 2015).

3.1 Trabajos relacionados

Partiendo de las investigaciones de autores como Bosetti (2015); Ernawati, Suhardi, & Nugroho (2012); Gjerdrum & Peter (2011); Kganakga (2014) quienes coinciden en que los dos marcos de referencia corporativos COSO ERM y la norma ISO 31000:2009, poseen más aspectos en común que en oposición. En ese orden de ideas, el marco COSO ERM es una directiva compleja, de múltiples y complicadas capas, que muchas organizaciones han encontrado de difícil implementación, además de tener como base el control y el cumplimiento. Por su parte, la norma ISO

proporciona un enfoque más racional y más fácil de comprender, basado en un proceso de gestión adaptable a la gestión existente y a las iniciativas estratégicas.

De forma complementaria, los autores Ernawati et al., (2012) exponen una metodología basada en ISO 31000:2009, denominada diseño metodológico de investigación de ciencias (por sus siglas en inglés DSRM, Design Science Research Methodology), a través del cual se realiza comparación con el COSO ERM, llegando de igual forma a la conclusión de que ambos se encuentran alineados en sus procesos.

Otros autores como Vanegas & Pardo (2014), exponen una metodología basada en la combinación de varias actividades, que están presentes en los procesos de gestión de riesgos de las normas y de modelos, como: ISO/IEC 27005, ISO 31000, BS 7799-3:2006, UNE 71504:2008, CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE y RISK IT. Dicha metodología logra evidenciar a través de una identificación, comparación, caracterización y armonización, que la mayoría de estas normas y marcos de referencia tienen relación entre sí, a pesar de que algunas normas expongan un nivel de detalle más profundo en sus procesos y por consiguiente, un modelo podría soportar a otro.

La organización internacional de normalización, de acuerdo a Racz, Weippl, & Seufert (2010), afirma que la norma ISO 31000:2009 e ISO/IEC 27005:2008 tratan la ERM y la gestión de riesgos de seguridad de la información en dos normas distintas. Por lo tanto, para que exista una alineación de TI con el negocio, se debe realizar principalmente a través del gobierno de TI y de la gestión de marcos como COBIT e ITIL.

Autores como Racz, et al,(2010) proponen como metodología de cuatro pasos, para comparar un marco de gestión de riesgos con un marco de TI, los cuales son: seleccionar los marcos que se van a comparar, identificar los elementos comunes de los marcos, analizar las referencias del marco de gestión de riesgos a los riesgos de TI y viceversa, y por último, se discuten y se suman los resultados.

Los marcos utilizados fueron ISO 31000:2009, COSO ERM, ISACA Risk IT y COBIT versión 5, ISO 27005:2008, pero el mayor énfasis está entre COSO ERM e ISACA Risk IT, siendo este último el más detallado, a comparación de los seleccionados inicialmente; con lo cual se concluye que tener un sólo marco de TI es cuestionable, y que la mayoría de estos procesos coinciden con los componentes de ERM, además, de que los procesos restantes se pueden integrar.

En relación con análisis comparativos de marcos de gestión de riesgos corporativos o tecnológicos con eTOM, son escasas las publicaciones existentes al respecto.

3.2 Alineación de los procesos de gestión de riesgos de eTOM

El proceso de alineación previsto, se llevará a cabo en dos niveles: el primero a nivel general, donde se considerarán los procesos comunes existentes entre el modelo de referencia eTOM y los tres (3) estándares internacionales. En el segundo nivel y teniendo presente, tal y como se concluye del análisis de primer nivel, se contemplará la poca alineación de los procesos de gestión de riesgos a nivel internacional con eTOM y también, el que éstos se encuentren más orientados al establecimiento de controles, por lo que los investigadores han optado por realizar el análisis comparativo con el estándar ISO/IEC 27002:2013, norma orientada a establecer las mejores prácticas de control de tecnologías de información y comunicaciones.

3.2.1 Alineación general de estándares: análisis de primer nivel

Una vez analizada la relación existente entre los estándares internacionales de gestión de riesgos y el marco eTOM, tal como se puede apreciar en la tabla 2, se puede concluir que los estándares y modelos son de hecho complementarios, e idealmente deben ser utilizados en conjunto, pero al intentar alinearlo con el marco eTOM, falta un poco más de precisión para lograr los aspectos de seguridad que se requieren; teniendo en cuenta que los estándares ISO 27005:2011, ISO 31000:2009 y el modelo COSO

ERM están alineados en sus procesos, en lo que se refiere al marco eTOM, no existe un acoplamiento integral de éstos procesos.

La existencia de estándares de administración de riesgos y las buenas prácticas de gobierno corporativo, son una condición necesaria pero no suficiente para el éxito de una entidad. Es por esto, que surge la necesidad de identificar los aspectos relacionados entre los cuatro marcos de referencia, para el área de gestión de riesgos en el sector de telecomunicaciones, con el propósito de facilitar su implementación y mantenimiento para la medición de la gestión, ya que hoy en día las empresas lo administran por separado.

Como se puede observar en la tabla 2, al realizar el análisis comparativo de los tres estándares internacionales de gestión de riesgos, con los procesos de gestión de riesgo empresarial que establece eTOM, estos se encuentran relacionados tan solo con las fases de evaluación y de tratamiento de riesgo.

Tabla 2.

Alineación de los estándares ISO 27005:2011, ISO31000:2009, COSO ERM y eTOM en sus procesos

ISO 27005:2008	ISO 31000:2009	COSO ERM	eTOM
Establecimiento del contexto	Establecer contexto	Medio ambiente interno Establecimiento de objetivos	
Identificación del riesgo	Identificación del riesgo	Identificación de eventos	
Estimación del riesgo	Análisis del riesgo	Evaluación de Riesgos	Gestión de la continuidad del negocio Gestión de la seguridad Gestión del Fraude Gestión de Auditoría Gestión de Seguros Gestión de Aseguramiento de ingresos Gestión de la integridad ITIL Gestión continuidad del servicio ITIL Gestión de seguridad de la información ITIL Gestión de problemas
Evaluación del riesgo Aceptación del riesgo	Evaluación del riesgo		
Implementar el plan de tratamiento de riesgo	Tratamiento del riesgo	Respuesta a los Riesgos Actividades de control	
Monitoreo y revisión del riesgo	Monitoreo y revisión	Supervisión	
Comunicación y consulta del riesgo	Comunicación y consulta	Información y Comunicación	

Fuente: Elaboración propia

En lo que tiene que ver con la fase de evaluación, es importante tener en cuenta que ésta por lo general, contempla dos subfases: la determinación del riesgo inherente y la determinación del riesgo residual; la primera está orientada a determinar el riesgo actual, sin tener en cuenta los controles, mientras que la segunda tiene en cuenta los controles existentes.

Con respecto a la fase de tratamiento del riesgo, su orientación corresponde a la definición de nuevos controles que permitan complementar la mitigación del riesgo, para aquellos riesgos residuales que lo requieran.

De acuerdo a lo anterior, la relación de los estándares internacionales de gestión de riesgos, con los procesos de gestión de riesgo empresarial del modelo eTOM, solamente se relacionan con los controles que permiten mitigar el riesgo; lo cual quiere decir que, la norma internacional con la que se debe correlacionar los procesos de gestión de riesgo empresarial de eTOM, es aquella que establezca un marco de controles relacionados con el ámbito tecnológico, por ser eTOM un marco de referencia para empresas, cuyo eje de negocio son las TIC's.

La norma internacional que cumple dichos requisitos es la ISO/IEC 27002:2013. Como lo enuncian Chakir, Chergui, Medromi, & Sayouti (2015), establece directrices y principios generales para preparar, implementar, mantener y mejorar la gestión de seguridad de la información, es decir, los objetivos de este estándar proporcionan una orientación general, sobre los efectos aceptados colectivamente en la gestión de seguridad de la información. Autores como Al-ahmad & Mohammad (2013) afirman también, que la selección de los controles de la norma ISO/IEC 27002:2013, se debe realizar sobre la base de una evaluación detallada y estructurada, para así poder determinar qué controles específicos son apropiados y cuáles no lo son, para el caso de estudio del modelo eTOM.

3.2.2 Alineación del modelo de gestión de riesgos de eTOM con la norma ISO/IEC 27002:2013

Cabe destacar que para este análisis, se consideraron los procesos del macroproceso de gestión de riesgo empresarial framework 16.0 (TMforum, 2016) hasta el nivel 3, con el fin de orientar adecuadamente su inserción en los 114 controles de la norma ISO/IEC 27002:2013.

El macroproceso de gestión de riesgo empresarial en el marco eTOM presenta 6 procesos, en donde como se ha vislumbrado anteriormente, se forma la necesidad de estudiar la coexistencia entre eTOM y el estándar ISO 27002:2013. La siguiente tabla muestra el mapeo, entre uno de los procesos de la gestión de riesgo empresarial de eTOM y la norma ISO/IEC 27002:2013.

Tabla 3. Relación entre el proceso de gestión de continuidad del negocio del marco eTOM y el estándar ISO/IEC 27002:2013

eTOM Framework 16.0		ISO 27002:2013	
Gestión de continuidad del negocio 1.7.2.1	1.7.2.1.1 Coordinar la continuidad del negocio	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
		7.2.1	Responsabilidades de gestión
	1.7.2.1.2 Plan de continuidad del negocio	17.1.1	Planificación de la continuidad de la seguridad de la información.
	1.7.2.1.3 Plan de recuperación de infraestructura	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.
	1.7.2.1.4 Plan de manejo de incidente grave	17.1.2	Implantación de la continuidad de la seguridad de la información.
	1.7.2.1.5 Administrar metodologías continuidad del negocio	-	-

Fuente: Elaboración propia

En el apéndice se aprecian en detalle, cada uno de los procesos de gestión de riesgo empresarial de eTOM y el respectivo mapeo con los controles de la norma ISO/IEC 27002:2013.

3.2.2.1 Armonización de la ISO/IEC 27002:2013 con los procesos de gestión de riesgo empresarial del modelo eTOM

De acuerdo a Valencia Duque (2015) "la armonización de modelos tiene como objetivo establecer los elementos comunes de los diferentes modelos propuestos, con el fin de realizar una aproximación a un modelo" (p.145), es decir, solucionar las diferencias entre los múltiples modelos y de este modo, poder lograr y soportar los objetivos estratégicos de la organización. Además de reutilizar aquellas características positivas de un modelo y así, aprovechar las soluciones que brindan.

En la literatura académica varios autores plantean modelos de armonización, es el caso de Ferchichi, Bigand, & Lefebvre (2008), cuyo modelo se basa en las siguientes fases: selección de modelos, análisis de la sinergia de los modelos, construcción del modelo integrado y la adaptación del modelo integrado al contexto

de la empresa; Kelemen (2009) establece once pasos, para unificar diferentes modelos de procesos de calidad de software; por último, Pardo, Pino, Garcia, Baldassarre, & Piattini (2013), plantean un esquema llamado hframework, en donde su metodología se basa en 3 métodos homogenización, comparación e integración. Para efectos de la armonización que aquí desarrolla, se utilizó el modelo hframework, dada la necesidad de integrar el proceso de gestión de riesgo empresarial del modelo eTOM con la norma ISO/IEC 27002:2013.

3.2.2.2 Metodología mediante el esquema hframework

Para llevar a cabo la armonización, se ejecutó la estrategia empleada por Pardo et al., (2013), con algunos ajustes establecidos por los autores.

- Homogenización: En esta fase, se identifican los elementos en común entre los macroprocesos de gestión de riesgo empresarial del modelo eTOM y la norma ISO/IEC 27002:2013 a alto nivel.

Tabla 4. Estructura común de elementos de proceso de gestión de riesgo empresarial de eTOM y la norma ISO/IEC 27002:2013

Procesos de Gestión de riesgo empresarial eTOM		ISO/IEC 27002:2013
1.7.2.1	Gestión de continuidad de negocio	17.1.3-17.1.1-17.2.1-17.1.2-7.2.1
1.7.2.2	Gestión de la seguridad	Todos los numerales
1.7.2.3	Gestión del fraude	-
1.7.2.4	Gestión de auditoría	12.7.1
1.7.2.5	Gestión de seguros	-
1.7.2.6	Gestión de aseguramiento de ingresos	-
1.7.2.7	Gestión de la integridad	-
1.7.2.8	ITIL Gestión continuidad del servicio	-
1.7.2.9	ITIL Gestión de seguridad de la información	Todos los numerales
1.7.2.10	ITIL Gestión de problemas	9.2.1-9.2.2-9.2.3-9.2.4-9.4.2-9.4.3-10.1.2-12.1.2-12.1.3-12.6.1-14.2.2-14.2.4

Fuente: Elaboración propia

Como se puede apreciar en la tabla 4, el 50% de los procesos de gestión de riesgos de eTOM, se encuentran relacionados con la ISO/IEC 27002:2013, destacando que los procesos 1.7.2.2 (gestión de la seguridad) y 1.7.2.9 ITIL (gestión de seguridad de la información de eTOM) a este nivel, equivalen a todos los controles de la ISO/IEC 27002:2013, por ser esta una norma orientada a controles de seguridad de la información.

Comparación entre modelos: Como señala Pardo et al., (2013), en esta etapa se identifican las posibles relaciones entre los modelos, con mucho más nivel de detalle para el caso del macroproceso de gestión de riesgo empresarial hasta el nivel 3. Tabla 6.

Para efectos de análisis, se establecerá la siguiente escala: (Tabla 5)

Tabla 5. Escala de calificación del nivel de relación de control

Calificación del nivel de relación del control	
0	No existen controles relacionados
1	Existen controles relacionados de forma indirecta
2	Existen controles relacionados de forma directa

Fuente: Elaboración propia.

Tabla 6. Conjunto de relaciones identificadas entre los procesos de gestión de riesgo empresarial eTOM y los controles de ISO/IEC 27002:2013

Subprocesos de Gestión de riesgo de eTOM a nivel 3				ISO/IEC 27002:2013 Controles	Nivel de relación promedio
Gestión de riesgo empresarial del modelo eTOM	Gestión de continuidad del negocio	1.7.2.1.1	Coordinar la continuidad del negocio	**17.1.3(1)-7.2.1(1)**	**1**
		1.7.2.1.2	Plan de continuidad del negocio	**17.1.1(2)**	**2**
		1.7.2.1.3	Plan de recuperación de infraestructura	**17.2.1(1)**	**1**
		1.7.2.1.4	Plan de manejo de incidente grave	**17.1.2(1)**	**1**
		1.7.2.1.5	Administrar metodologías continuidad del negocio	**0**	**0**
	Gestión de la seguridad	1.7.2.2.1	Administrar gestión proactiva de la seguridad	**0**	**0**
		1.7.2.2.2	Monitorear tendencias de la industria para la gestión de la seguridad	**0**	**0**
		1.7.2.2.3	Definir políticas y procedimientos de gestión de la seguridad	**5.1.1(2)-5.1.2(1)-6.1.3(1)-7.2.1(1)-7.2.3(1)-9.2.1(1)-9.2.2(1)-9.2.3(1)-9.2.4(1)-9.4.2(1)-9.4.3(1)-12.1.1(1)-13.2.1(2)-14.2.1(1)-15.1.1(1)-18.2.2(2)**	**1,19**
		1.7.2.2.4	Ayudar con la implementación de Gestión de la Seguridad	**6.1.2(1)-12.1.2(1)-12.1.3(1)-12.1.4(1)-12.4.1(1)-12.4.3(1)-15.2.1(2)**	**1,14**
		1.7.2.2.5	Manejo de gestión de la seguridad reactiva	**0**	**0,00**
		1.7.2.2.6	Detectar Amenazas y violaciones potenciales de seguridad	**14.1.1(1)**	**1,00**
		1.7.2.2.7	Investigar amenazas y violaciones potenciales de seguridad	**7.1.1(2)-16.1.7(1)**	**1,50**
		1.7.2.2.8	Definir prevención Gestión de la seguridad	**8.1.1(2)-8.1.2(2)-8.1.3(2)-8.1.4(2)-16.1.4(1)**	**1,80**
		1.7.2.2.9	Definir monitoreo para facilitar la gestión de la seguridad	**5.1.1 (1)-8.2.1(1)-8.2.2(1)-5.1.2(1)**	**1,33**
		1.7.2.2.10	Definir análisis de gestión de la seguridad	**5.1.1(2)-8.2.1(1)-14.1.1(2)**	**1,67**
		1.7.2.2.11	Definir políticas y procedimientos para facilitar detección de incidentes	**16.1.1(1)-16.1.2(2)-16.1.3(1)-16.1.4(1)-16.1.6(2)-16.1.7(2)**	**1,50**
		1.7.2.2.12	Definir políticas y procedimientos de gestión de incidentes	**16.1.5(2)-16.1.1(1)**	**1,50**
	Gestión del fraude	1.7.2.3.1	Gestión de políticas del fraude	**0**	**0**
		1.7.2.3.2	Apoyo a las operaciones de fraude	**0**	**0**
		1.7.2.3.3	Dirección de operaciones de fraude	**0**	**0**
	Gestión de auditoría	1.7.2.4.1	Definir directiva de auditoría	**0**	**0**
		1.7.2.4.2	Definir mecanismo de auditoría	**0**	**0**
		1.7.2.4.3	Valorar las actividades operacionales	**0**	**0**
		1.7.2.4.4	Evaluar las actividades operacionales	**0**	**0**
		1.7.2.4.5	Informe de auditoría	**12.7.1(2)**	**2**
		1.7.2.4.6	Aplicar mecanismos de auditoría de forma proactiva	**0**	**0**
	Gestión de seguros	1.7.2.5.1	Identificar riesgos asegurables	**0**	**0**
		1.7.2.5.2	Analizar costo de seguro/Beneficio	**0**	**0**
		1.7.2.5.3	Proporcionar consejos de seguros	**0**	**0**
		1.7.2.5.4	Manejo seguro de cartera	**0**	**0**
	Gestión de aseguramiento de ingresos	1.7.2.6.1	Administrar ingresos política de garantía	**0**	**0**
		1.7.2.6.2	Manejo de operaciones de aseguramiento de ingresos	**0**	**0**
		1.7.2.6.3	Apoyo de ingresos operaciones de aseguramiento	**0**	**0**
	Gestión de la integridad	1.7.2.7	-	**0**	**0**
	ITIL G. continuidad del servicio	1.7.2.8	-	**0**	**0**
	ITIL Gestión de seguridad de la información	1.7.2.9	-	**16.1.1(1)-16.1.2(2)-16.1.3(1)-16.1.4(2)-16.1.6(2)-6.1.1(2)-6.1.3(1)-6.1.5(2)-18.2.1(2)-18.2.2(1)-5.1.1(2)-5.1.2(2)-12-3-1(1)-15.1.1(2)-17.1.1(2)-17.1.2(2)-17.1.3(2)-13.2.4(2)**	**1,72**
	ITIL Gestión de problemas	1.7.2.10	-	**9.2.1(2)-9.2.2(1)-9.2.3(2)-9.2.4(1)-9.4.2(1)-9.4.3(2)-10.1.2(2)-12.1.2(2)-12.1.3(1)-12.6.1(2)-14.2.2(2)-14.2.4(2)**	**1,67**

Fuente: Elaboración propia

Análisis porcentual entre modelos: Al encontrar las correlaciones, entre procesos de la gestión de riesgo empresarial del modelo eTOM y la norma ISO/IEC 27002:2013, se determina porcentualmente el cubrimiento de un modelo a otro, Acorde a Pardo et al., (2013): fuertemente relacionado (86-100%), relacionado en gran medida (51-85%), parcialmente relacionado (16-50%), débilmente relacionado (1-15%), no relacionado (0%). Se opta además por la siguiente ecuación:

$$\vartheta_{Gestión\ riesgos\ eTOM} = \frac{\sum Nivel\ relación\ promedio}{Max.\ valor\ calificación\ x\ Cant.\ subprocesos\ del\ proceso\ eTOM}$$

Donde ϑ es el índice de cohesión del proceso de gestión de riesgos de eTOM, determinando así, la similitud metodológica con la norma ISO para éste caso.

A partir de las relaciones y los resultados identificados en la tabla 7, se puede asegurar lo siguiente:

•Las categorías de los procesos de la gestión de riesgo empresarial de eTOM están parcialmente relacionadas con la norma ISO/IEC 27002:2013, debido a que el rango porcentual está en un 29,21%;

•El proceso ITIL Gestión de seguridad de la información obtuvo un 86,11%, siendo el que

presenta una mayor correlación con la norma ISO/IEC 27002:2013 y a pesar de no tener subprocesos en nivel 3, tiene mayor énfasis en los aspectos de seguridad; lo cual confirma que el macroproceso de gestión de riesgo empresarial;

Tabla 7. Relación porcentual entre los procesos de gestión de riesgos de eTOM y la norma ISO/IEC 27002:2013

		ISO/IEC 27002:2013
		Controles
Gestión de riesgo empresarial del modelo eTOM	Gestión de continuidad del negocio	50,0%
	Gestión de la seguridad	52,6%
	Gestión del fraude	0,0%
	Gestión de auditoría	20,0%
	Gestión de seguros	0,0%
	Gestión de aseguramiento de ingresos	0,0%
	Gestión de la integridad	0,0%
	ITIL Gestión continuidad del servicio	0,00%
	ITIL Gestión de seguridad de la información	86,11%
	ITIL Gestión de problemas	83,33%
Total		29,21%

Fuente: Elaboración propia.

Procesos como gestión del fraude, gestión de seguros, gestión de aseguramiento de ingresos, gestión de la integridad e ITIL gestión de continuidad del servicio, no presentan controles relacionados con la norma ISO/IEC 27002:2013..

Conclusiones

El modelo eTOM es el modelo de referencia para los procesos desarrollados por las empresas de telecomunicaciones a nivel internacional y por lo tanto, los procesos relacionados con la gestión de riesgos que incorpora, se convierten de igual forma, en la base sobre la cual este tipo de empresas desarrollan la gestión de la incertidumbre.

Al realizar un análisis del nivel de interrelación existente entre las prácticas de gestión de riesgos establecidas en eTOM y los dos principales marcos de referencia de gestión de riesgos corporativa como son ISO 31000:2009 y COSO ERM y uno de los principales marcos de gestión de riesgos a nivel tecnológico como es la ISO/IEC 27005:2011 no se encuentra una alta interrelación, debido básicamente a que la mayoría de los procesos de riesgos planteados por eTOM corresponden a controles específicos y no a procesos de identificación, análisis, evaluación y tratamiento de riesgos, como lo establecen los referentes internacionales.

Es importante destacar que el modelo eTOM establece dentro de su catálogo de procesos de gestión de riesgos, una referencia directa a ITIL en lo relacionado con seguridad, continuidad del servicio y gestión de problemas, de igual forma contempla como parte de sus procesos, la gestión de uno de los criterios de impacto con los cuales se mide la seguridad de la información, como es la integridad.

Lo anterior pone de manifiesto cierto nivel de complejidad al momento de seleccionar el marco de referencia más adecuado para dilucidar la base sobre la cual se fundamenta o se relacionan los controles establecidos por el modelo eTOM. Sin embargo, y teniendo presente que el sector de telecomunicaciones es intensivo en tecnologías de información y comunicaciones, el marco de referencia más pertinente para realizar el análisis de relación entre lo establecido por eTOM con los estándares internacionales de riesgos y dado su foco hacia controles específicos y no hacia procesos de gestión del riesgo, es la norma ISO/IEC 27002:2013, la cual establece 114 controles de tecnologías de información, los cuales, una vez confrontados y utilizando referentes bibliográficos de armonización de modelos, se encuentra un nivel de relación de tan solo el 29,21% siendo el proceso "ITIL gestión de la seguridad de la información" por su generalidad, el proceso con mayor nivel de cohesión con la norma internacional.

Como conclusión final, se puede afirmar que los procesos de gestión de riesgos establecidos en el modelo eTOM, tienen un bajo nivel de relación con los principales marcos de gestión de riesgos y controles existentes actualmente a nivel internacional.

Referencias bibliográficas

Airmic, Alarm, & Irm. (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. *Risk Management*, 7(1), 20. doi:10.1016/j.solmat.2010.12.013

Al-ahmad, W., & Mohammad, B. (2013). Addressing Information Security Risks by Adopting Standards. *International Journal of Information Security Science*, 2(2), 28–43. Retrieved from http://eds.a.ebscohost.com.libezproxy.open.ac.uk/eds/pdfviewer/pdfviewer?sid=e1bf8be9-84ad-4d50-91fa-f9414e22825c@sessionmgr4003&vid=0&hid=4210

Beasley, Branson, B., & Hancock, B. (2010). COSO's 2010 report on ERM: Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework. COSO's 2010 Report on ERM | Thought Leadership in ERM.

Bellafkih, M., Raouyane, B., Ranc, D., Errais, M., & Ramdani, M. (2012). eTOM-Conformant IMS Assurance Management. (Dr. Jesús Ortiz, Ed.)Telecommunications Networks - Current Status and Future Trends.

Bosetti, L. (2015). Risk management standards in global markets. Quaesti Management and Marketing, 81–86. Retrieved from https://www.theirm.org/knowledge-and-resources/risk-management-standards.aspx

Buhr, R., Nel, a., & Santos, M. Dos. (2006). Enterprise Risk Management: A New Philosophy. 2006 *IEEE International Engineering Management Conference*. doi:10.1109/IEMC.2006.4279884

Carrillo Alvarez, A. del P., & Medina Ramirez, R. (2006). *Construcción del modelo gerencial de operación y mantenimiento para la zona larga distancia de la vicepresidencia infraestructura de la empresa Colombia telecomunicaciones S.A. ESP.* Tesis de maestría. Bucaramanga: Universidad Industrial de Santander.

Chakir, A., Chergui, M., Medromi, H., & Sayouti, A. (2015). An approach to select effectively the best framework IT according to the axes of the governance IT , to handle and to set up an objective IT*. IEEE,* 1–8.

Di Serio, L. C., de Oliveira, L. H., & Schuch, L. M. S. (2011). Organizational risk management - A case study in companies that have won the Brazilian quatity award prize. *Journal of Technology Management and Innovation,* 6(2), 230–243. doi:10.4067/S0718-27242011000200016

Ernawati, T., Suhardi, & Nugroho, D. R. (2012). IT risk management framework based on ISO 31000:2009. System Engineering and Technology (ICSET) 2012 *International Conference on Bandung*, 1–8. doi:10.1109/ICSEngT.2012.6339352

Ferchichi, A., Bigand, M., & Lefebvre, H. (2008). *An Ontology for Quality Standards Integration. In First International Workshop on Model Driven Interoperability for Sustainable Information Systems*. MDISIS 2008. Montpellier (France), 17–30.

Frigo, B. M. L., & Anderson, R. J. (2014). RISK MANAGEMENT FRAMEWORKS : Adapt, Don't Adopt. *Strategic Finance*, 96(1), 49–53.

Gjerdrum, D., & Peter, M. (2011). The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework. *Risk Management*, (21), 8–12. Retrieved from http://www.soa.org/library/newsletters/risk-management-newsletter/2011/march/jrm-2011-iss21-gjerdrum.aspx

Kelemen, Z. D. (2009). A process based unification of process-oriented software quality approaches. In 2009 4th IEEE International Conference on Global Software Engineering, *ICGSE* 2009, 285–288. doi:10.1109/ICGSE.2009.39

Kganakga, T. (2014). The impact of Enterprise Risk Management (ERM) on the internal control system of organisations in the mining industry. S.c.

Krstić, J., & Đorđević, M. (2012). Internal control and enterprise risk management – From traditional to revised COSO model. *Economic Themes*, 50(2), 151–166. Retrieved from http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=b2b66c9f-8c69-41b7-8f63-cd93831d670e@sessionmgr4004&vid=2&hid=4101

Lalanne, V., Munier, M., & Gabillon, A. (2013). *Information Security Risk Management in a World of Services*. 2013 International Conference on Social Computing, 586–593. doi:10.1109/SocialCom.2013.88

Latifi, F., & Nasiri, R. (2013*). Enhancement of eTOM Assurance Domain by Integration with COBIT5 Framework*. The Society of Digital Information and Wireless Communications (SDIWC), 44–49.

Luko, S. N. (2013). Risk Management Terminology. *Quality Engineering*, 25(3), 292–297. doi:10.1080/08982112.2013.786336

Lustosa, T. C., Iano, Y., Loschi, H. J., & Moretti, A. (2015). The importance of Integrated Network Management and Telecom Service Through *Time. IEEE*, 2(1). 1–5.

Márquez, M. P. A. (2016). Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI. Tesis. Universidad de Azuay.

Ospina, M. del P. S., & Gallego, I. V. (2008). Estructuración del proceso para la habilitación del aprovisionamiento de equipos EDA en la empresa de telecomunicaciones de Bogotá. Proyecto de grado. Tesis de maestría. Universidad de San Buenaventura Bogotá.

Pardo, C., Pino, F. J., Garcia, F., Baldassarre, M. T., & Piattini, M. (2013). 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), 125–143. doi:10.1016/j.jss.2012.07.072

Purdy, G. (2010). ISO 31000:2009 - Setting a new standard for risk management: Perspective. *Risk Analysis*, 30(6), 881–886. doi:10.1111/j.1539-6924.2010.01442.x

Racz, N., Weippl, E., & Seufert, A. (2010). Questioning the need for separate IT risk management frameworks frameworks. *Informatik 2010*, 10. 245–252.

TeleManagement Forum. (2012). Business Process Framework (eTOM) Addendum D: Process Decompositions and Descriptions. Retrieved from http://www.tmforum.org/BusinessProcessFramework/1647/home.html

TMforum. (2016). Business Process Framework eTOM. Retrieved May 2, 2016, from https://www.tmforum.org/tm-forum-frameworx/browse-clickable-model/

Valencia Duque, F. J. (2015). La Auditoría Continua, una herramienta para la modernización de la función de auditoría en las organizaciones y su aplicación en el Control Fiscal Colombiano. Tesis de doctorado. Universidad Nacional de Colombia. Retrieved from http://www.bdigital.unal.edu.co/50332/1/10280374.2015.pdf\nhttp://www.bdigital.unal.edu.co/50332/

Vandijck, I. (2014). The ISO_31000 Standard: a different perspective on Risk and Risk Management An analysis from a security perspective. *Optimit,* 1 (0). 6.

Vanegas, D. G. A., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs : MOGRIT. *Revista S&T*, 12(30), 35–48. Retrieved from http://www.redalyc.org/articulo.oa?id=411534000003

Apéndice

1. Mapeo de procesos de gestión de riesgos de eTOM en el nivel 3, con los controles de la norma ISO/IEC27002:2013

eTOM Framework 16.0			ISO 27002:2013	
Gestión de continuidad del negocio 1.7.2.1	1.7.2.1.1	Coordinar la continuidad del negocio	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
			7.2.1	Responsabilidades de gestión.
	1.7.2.1.2	Plan de continuidad del negocio	17.1.1	Planificación de la continuidad de la seguridad de la información.
	1.7.2.1.3	Plan de recuperación de infraestructura	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.
	1.7.2.1.4	Plan de manejo de incidente grave	17.1.2	Implantación de la continuidad de la seguridad de la información.
	1.7.2.1.5	Administrar metodologías continuidad del negocio	-	-
Gestión de la seguridad 1.7.2.2	1.7.2.2.1	Administrar gestión proactiva de la seguridad	-	-
	1.7.2.2.2	Monitorear tendencias de la industria para la gestión de la seguridad	-	-
	1.7.2.2.3	Definir políticas y procedimientos de gestión de la seguridad	5.1.1	Conjunto de políticas para la seguridad de la información.
			5.1.2	Revisión de las políticas para la seguridad de la información.
			6.1.3	Contacto con las autoridades.
			7.2.1	Responsabilidades de gestión.
			7.2.3	Proceso disciplinario.
			9.2.1	Gestión de altas/bajas en el registro de usuarios.
			9.2.2	Gestión de los derechos de acceso asignados a usuarios.
			9.2.3	Gestión de los derechos de acceso con privilegios especiales.
			9.2.4	Gestión de información confidencial de autenticación de usuarios.
			9.4.2	Procedimientos seguros de inicio de sesión
			9.4.3	Gestión de contraseñas de usuario.
			12.1.1	Documentación de procedimientos de operación.
			13.2.1	Políticas y procedimientos de intercambio de información.
			14.2.1	Política de desarrollo seguro de software
			15.1.1	Política de seguridad de la información para suministradores.
			18.2.2	Cumplimiento de las políticas y normas de seguridad.
	1.7.2.2.4	Ayudar con la implementación de Gestión de la Seguridad	6.1.2	Segregación de tareas.
			12.1.2	Gestión de cambios.
			12.1.3	Gestión de capacidades.
			12.1.4	Separación de entornos de desarrollo, prueba y producción.
			12.4.1	Registro y gestión de eventos de actividad.
			12.4.3	Registros de actividad del administrador y operador del sistema.
			15.2.1	Supervisión y revisión de los servicios prestados por terceros
	1.7.2.2.5	Manejo de gestión de la seguridad reactiva	-	-
	1.7.2.2.6	Detectar Amenazas y violaciones potenciales de seguridad	14.1.1	Análisis y especificación de los requisitos de seguridad.
	1.7.2.2.7	Investigar amenazas y violaciones potenciales de seguridad	7.1.1	Investigación de antecedentes.
			16.1.7	Recopilación de evidencias.
	1.7.2.2.8	Definir prevención Gestión de la seguridad	8.1.1	Inventario de activos.
			8.1.2	Propiedad de los activos.
			8.1.3	Uso aceptable de los activos.
			8.1.4	Devolución de activos.
			16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones
	1.7.2.2.9	Definir monitoreo para facilitar la gestión de la seguridad	5.1.1	Conjunto de políticas para la seguridad de la información.
			8.2.1	Directrices de clasificación.
			8.2.2	Etiquetado y manipulado de la información.
			5.1.2	Revisión de las políticas para la seguridad de la información.
	1.7.2.2.10	Definir análisis de gestión de la seguridad	5.1.1	Conjunto de políticas para la seguridad de la información.
			8.2.1	Directrices de clasificación.
			14.1.1	Análisis y especificación de los requisitos de seguridad.
	1.7.2.2.11	Definir políticas y procedimientos para facilitar detección de incidentes	16.1.1	Responsabilidades y procedimientos.
			16.1.2	Notificación de los eventos de seguridad de la información.
			16.1.3	Notificación de puntos débiles de la seguridad.
			16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.
			16.1.6	Aprendizaje de los incidentes de seguridad de la información.
			16.1.7	Recopilación de evidencias
	1.7.2.2.12	Definir políticas y procedimientos de gestión de incidentes	16.1.5	Respuesta a los incidentes de seguridad.
			16.1.1	Responsabilidades y procedimientos.
Gestión del fraude 1.7.2.3	1.7.2.3.1	Gestión de políticas del fraude	-	-
	1.7.2.3.2	Apoyo a las operaciones de fraude	-	-
	1.7.2.3.3	Dirección de operaciones de fraude	-	-
Gestión de auditoría 1.7.2.4	1.7.2.4.1	Definir directiva de auditoría	-	-
	1.7.2.4.2	Definir mecanismo de auditoría	-	-
	1.7.2.4.3	Valorar las actividades operacionales	-	-
	1.7.2.4.4	Evaluar las actividades operacionales	-	-
	1.7.2.4.5	Informe de auditoría	12.7.1	Controles de auditoría de los sistemas de información.
	1.7.2.4.6	Aplicar mecanismos de auditoría de forma proactiva	-	-
Gestión de seguros 1.7.2.5	1.7.2.5.1	Identificar riesgos asegurables	-	-
	1.7.2.5.2	Analizar costo de seguro/Beneficio	-	-
	1.7.2.5.3	Proporcionar consejos de seguros	-	-
	1.7.2.5.4	Manejo seguro de cartera	-	-
Gestión de aseguramiento de ingresos 1.7.2.6	1.7.2.6.1	Administrar ingresos política de garantía	-	-
	1.7.2.6.2	Manejo de operaciones de aseguramiento de ingresos	-	-
	1.7.2.6.3	Apoyo de ingresos operaciones de aseguramiento	-	-
Gestión de la integridad 1.7.2.7	-	-	-	-
ITIL Gestión continuidad del servicio 1.7.2.8	-	-	-	-
ITIL Gestión de seguridad de la información 1.7.2.9	-	-	16.1.1	Responsabilidades y procedimientos.
	-	-	16.1.2	Notificación de los eventos de seguridad de la información
	-	-	16.1.3	Notificación de puntos débiles de la seguridad.
	-	-	16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.
	-	-	16.1.6	Aprendizaje de los incidentes de seguridad de la información.
	-	-	6.1.1	Asignación de responsabilidades para la segur. de la información
	-	-	6.1.3	Contacto con las autoridades
	-	-	5.1.1	Conjunto de políticas para la seguridad de la información.
	-	-	18.2.1	Revisión independiente de la seguridad de la información
	-	-	12.3.1	Copias de seguridad de la información.
	-	-	5.1.2	Revisión de las políticas para la seguridad de la información
	-	-	18.2.2	Cumplimiento de las políticas y normas de seguridad.
	-	-	15.1.1	Política de seguridad de la información para suministradores.
	-	-	17.1.1	Planificación de la continuidad de la seguridad de la información.
	-	-	17.1.2	Implantación de la continuidad de la seguridad de la información.
	-	-	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad
	-	-	13.2.4	Acuerdos de confidencialidad y secreto.
	-	-	6.1.5	Seguridad de la información en la gestión de proyectos.
ITIL Gestión de problemas 1.7.2.10	-	-	9.2.1	Gestión de altas/bajas en el registro de usuarios
			9.2.2	Gestión de los derechos de acceso asignados a usuarios.
			9.2.3	Gestión de los derechos de acceso con privilegios especiales.
			9.2.4	Gestión de información confidencial de autenticación de usuarios.
			9.4.2	Procedimientos seguros de inicio de sesión.
			9.4.3	Gestión de contraseñas de usuario.
			10.1.2	Gestión de claves.
			12.1.2	Gestión de cambios.
			12.1.3	Gestión de capacidades
			12.6.1	Gestión de las vulnerabilidades técnicas
			14.2.2	Procedimientos de control de cambios en los sistemas.