BOLETIN DE ESTUDIOS ECONOMICOS

EL PROCESO DE GESTIÓN DE RIESGOS COMO COMPONENTE INTEGRAL DE LA GESTIÓN EMPRESARIAL

Mª. Isabel Martínez Torre-Enciso
Mª. Isabel Casares San José-Martí

VOL. LXV – SEPARATA DEL BOLETIN ABRIL 2011 – N.º 202

ASOCIACION DE
LICENCIADOS EN CIENCIAS ECONOMICAS
POR LA UNIVERSIDAD COMERCIAL DE DEUSTO

BILBAO

BOLETIN DE ESTUDIOS ECONOMICOS
Vol. LXVI - N.º 202 - Abril 2011
(Páginas 73-93)

EL PROCESO DE GESTIÓN DE RIESGOS COMO COMPONENTE INTEGRAL DE LA GESTIÓN EMPRESARIAL

Mª Isabel Martínez Torre-Enciso
Universidad Autónoma de Madrid
María Isabel Casares San José-Martí
Casares, Asesoría Actuarial y de Riesgos, S.L.

1. Introducción

Las organizaciones, no importa cual sea su actividad y tamaño, afrontan una serie de riesgos que pueden afectar a la consecución de sus objetivos. Todas las actividades de una organización están sometidas de forma permanente a una serie de amenazas, lo cual las hace vulnerables, comprometiendo su estabilidad. Accidentes operacionales, enfermedades, incendios, pérdidas de beneficios, catástrofes naturales, etc., son una muestra de este panorama, sin olvidar las amenazas propias del negocio. Hablar sobre gestión de riesgos ya no se limita al enfoque financiero tradicional o de cobertura. La gerencia de riesgos en realidad posee una visión holística de la compañía que contempla aspectos muy variados como la pérdida de control, la seguridad, así como diversas estrategias para prevenir, reducir o transferir el riesgo[1].

La gerencia de riesgos en un entorno global se está perfilando como una estrategia financiera y empresarial que proporciona una importante ventaja competitiva a las empresas que disponen de ella, así como un importante incremento de valor en el mercado. En este sentido, la norma básica y de obligado cumplimiento aplicada en el ámbito de las empresas cotizadas es COSO II (2004), si bien hasta ahora no existía una

[1] La norma UNE-ISO GUÍA 73:2009: *Definición de riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos*, define el "riesgo" como "la incidencia en la consecución de los objetivos de la organización".

norma global y amplia que pudiese aplicarse a todo tipo de empresas, todo tipo de sectores, a lo largo de toda la vida de una organización, y a la práctica totalidad de sus actividades.

Por ello, el objetivo del presente trabajo es analizar la gerencia de riesgos como componente integral de la gestión empresarial. Para ello, nos centraremos en cómo la nueva norma internacional ISO 31000:2009 publicada en noviembre de 2009 por la Organización Internacional para la Estandarización[2], está incidiendo en las prácticas y procesos de gestión de riesgos en el entorno de las empresas. Esta nueva norma internacional, voluntaria en su aplicación, permite dar un paso importante en el contexto global ya que favorece que cualquier empresa pueda realizar una gestión eficaz del riesgo al que se encuentra expuesta, mediante la identificación, análisis y evaluación de los riesgos, favoreciendo con estas prácticas la consecución de sus objetivos.

Aunque la gerencia de riesgos es un concepto intuitivo en el contexto de las empresas, la estandarización de estos procesos es algo relativamente reciente. La gestión integral de riesgos ha ganado impulso desde la década de los noventa, con la aparición de "Modelos de Gestión de Riesgos", algunos de ellos de carácter específico. Los antecedentes de la Norma Internacional ISO 31000:2009 los encontramos, de forma separada, referidos tanto a la terminología utilizada como a la metodología. Respecto a la *terminología*[3] utilizada, el antecedente más directo se encuentra en los "Estándares de Gerencia de Riesgos" elaborados por FERMA[4] (2003), que ya reflejaban la terminología recogida en la Guía ISO/CEI 73:2002 y que ahora se actualiza con la guía UNE-ISO GUÍA 73:2009 que ha sido traducido por AENOR[5] en 2010. La norma ISO 31000 ayuda a responder a uno de los interrogantes fundamentales en la gestión del riesgo: cómo llegar a todo el mundo para hablar sobre el riesgo de la misma manera.

[2] International Organization for Standardization – ISO. Véase: http://www.iso.org.

[3] Respecto a la terminología utilizada, existe una gran problemática procedente de las traducciones del documento oficial entre lo que es gerencia de riesgos y gestión de riesgos. Desde el punto de vista de las autoras de este artículo, la "gerencia de riesgos" es el conjunto de métodos que permiten identificar, analizar y evaluar los riesgos, minimizarlos, controlarlos y hacer un tratamiento financiero de los mismos. Por el contrario, la "gestión del riesgo" consiste en la aplicación de este conjunto de técnicas a los riesgos particulares.

[4] Federation of European Risk Management Associations. Véase, http: //www.ferma.eu

[5] Asociación Española de Normalización y Certificación. Véase, http://www.aenor.es

En cuanto a la *metodología*, hemos de buscar diferentes antecedentes dependiendo de las actividades de las empresas, si bien la norma australiana/neo zelandesa AS/NZS 4360[6] es especialmente relevante. Siguiendo la tendencia moderna de utilizar un enfoque integral de manejo de los riesgos citaremos, entre otros documentos relevantes, el Informe COSO II, conocido como "*Enterprise Risk Management*" (*ERM*), el cual se centra en los riesgos relativos a la información financiera, siendo obligatoria su aplicación para todas las empresas que cotizan en bolsa; BASILEA II (2004) es la norma de Gerencia de Riesgos para Entidades Financieras; y finalmente SOLVENCIA II (2009) es la norma de Gerencia de Riesgos de Entidades Aseguradoras que vienen a mejorar los procedimientos de control de riesgos del sector seguros, permitiendo a las entidades realizar una gestión de mayor calidad sobre sus fondos propios y aumentar la protección de los consumidores (Hernández Barros y Martínez Torre-Enciso, 2010). Todo este proceso de adaptación de la normativa referente a la gerencia de riesgos en diferentes instituciones tiene como objetivo final prevenir futuras crisis financieras como la actual, en la que algunas de las causas pueden atribuirse entre otras, a factores de tipo institucional (Martín Marín y Telléz Valle, 2009).

Ante la gran variedad, complejidad y naturaleza de los riesgos que amenazan a una organización, el nuevo Estándar Internacional desarrollado por la ISO propone unas pautas genéricas sobre cómo gestionar los riesgos de forma sistemática y transparente. El diseño y la implantación de la gestión de riesgos dependerá de las diversas necesidades de cada organización, de sus objetivos concretos, del contexto en el que opera, de la estructura, las operaciones, los procesos, los servicios, etc.

Este artículo avanza sobre las normas ya establecidas y analiza en profundidad la nueva Norma Internacional ISO 31000 comparándola con las anteriores, principalmente con COSO II, norma que ha permitido desde 2004 utilizar un enfoque integral de manejo de los riesgos conocido como "*Enterprise Risk Management*" (*ERM*), con el fin de evaluar, administrar y comunicar estos riesgos de una manera integral, basados en los objetivos estratégicos de la organización (Escorial, 2010). En este artículo analizaremos "el proceso de gerencia de riesgos" de la ISO 31000, tercera de las tres partes principales de la norma junto con

[6] Risk Management AS/NZS 4360:2004.

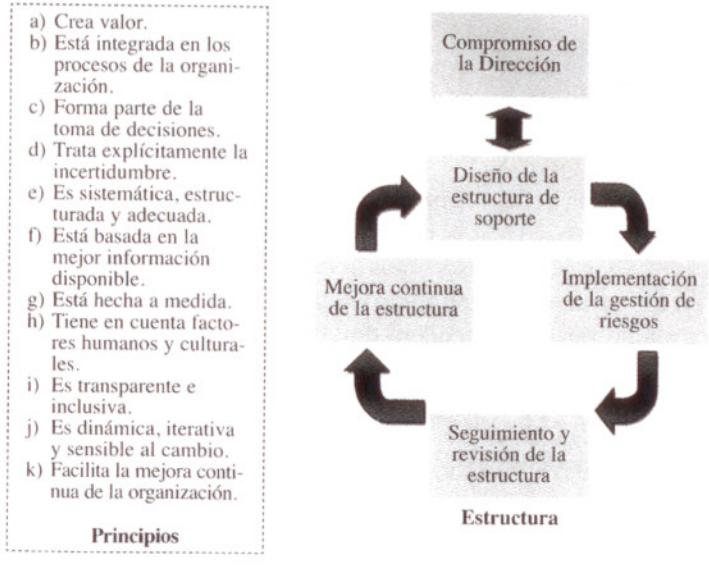
"los principios para la gestión de riesgos" y "la estructura de soporte del sistema".

2. Los principios para la gestión de riesgos y la estructura de soporte

Aunque el trabajo que se presenta tiene por objetivo el análisis del "proceso de gerencia de riesgos", éste se sustenta sobre las otras dos partes de la norma que la preceden, por lo que es necesario, al menos, un breve cometario de las mismas. El siguiente cuadro 1 muestra los principios y la estructura organizativa propuestos en la norma ISO 31000.

Cuadro 1

Principios y la estructura organizativa propuestos en la norma ISO 31000



Fuente: UNE-ISO 31000 (2009): *Gestión del riesgo. Principios y directrices*, p. 7.

Los "principios para la gestión del riesgo"[7] buscan establecer el enfoque cultural e ideológico con que se deben gestionar los riesgos en toda

[7] UNE-ISO 31000 (2009), pp. 13-14.

organización. Estos elementos suelen no ser considerados relevantes al no ser tangibles y medibles, si bien son tan importantes como cualquier otro aspecto de la organización. Este enfoque cultural e ideológico respalda la respuesta de las personas que forman las organizaciones según sus propias percepciones y actitudes. Es por ello que la percepción y actitud de todos los miembros de la organización va a determinar la poca o mucha probabilidad de éxito que tendrá la adopción de un nuevo modelo o técnica en su seno.

La nueva norma incide en la necesidad de formar las actitudes de todos los relacionados con la organización y de crear un clima y una cultura organizativa proclive al establecimiento de políticas de riesgo, con la idea de que las medidas y procesos de gerencia de riesgo sean aceptadas y asumidas como algo bueno por los miembros de las diferentes organizaciones.

La "estructura del sistema de gestión" denominada también "marco de trabajo"[8], establece y define los componentes necesarios para realizar una buena gestión de los riesgos e indica que el proceso debe iniciarse en la alta dirección de la empresa, mostrando su compromiso y emitiendo directrices para la gerencia de riesgos (política de riesgos) (Hubbard, 2009). Esta estructura debe seguir con el diseño del marco de referencia en el cual se va a desempeñar la gerencia de riesgos, empezando por entender el contexto interno y externo de la organización, las variables que pueden afectar su desempeño en los aspectos relevantes del negocio y en todos los niveles: estratégico, táctico y operativo.

En este marco se debe definir la responsabilidad de la estructura organizacional con respecto a la gestión de riesgos, buscando una perspectiva funcional e integral del negocio mediante la formación de equipos de trabajo multidisciplinares que abarquen todos los niveles de la organización. De la misma manera, debe establecerse un comité directivo que se encargue de la revisión periódica, integral y estratégica de la gerencia de riesgos. Es importante establecer mecanismos de comunicación internos y extèrnos con las partes interesadas, así como identificar las necesidades de todo tipo de recursos y su posible provisión para que la gerencia de riesgos se haga de manera adecuada, posible, efectiva, realista, incrementando valor para las empresas que la implantan.

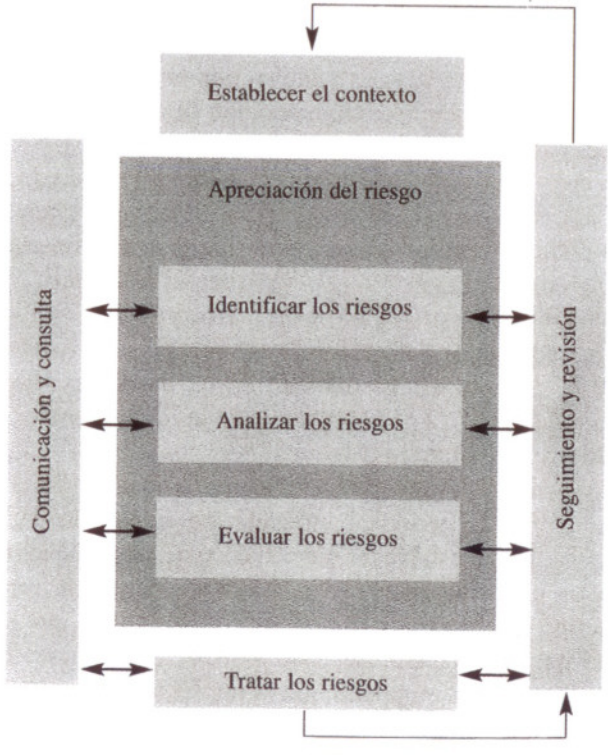
[8] UNE-ISO 31000 (2009), pp. 15-19.

3. El proceso de gestión de riesgos

Junto con los "principios" y "la estructura" que debe seguir la empresa para el desarrollo de este enfoque, el "Proceso de Gerencia de Riesgos" es uno de los tres pilares básicos de la Norma 31000. Es precisamente este pilar el que consideramos más importante al ser el que realmente permite gestionar los riesgos cuando estos se materializan en el contexto de la empresa. Sin embargo, y aunque no sea objeto de este trabajo, no debemos olvidar que este último pilar debe estar precedido y apoyado en los dos primeros si se quiere que el conjunto de la gerencia de riesgos sea eficaz para el logro de los objetivos de la empresa.

Cuadro 2

El proceso de gerencia de riesgos propuestos en la norma ISO 31000



Fuente: UNE-ISO 31000 (2009): *Gestión del riesgo. Principios y directrices*, p. 7.

El artículo se centrará, en el establecimiento del proceso de gestión del riesgo y cómo éste debe ser una parte integrante de la gestión global de la organización, debe integrarse en la cultura, filosofía y en las prácticas de la empresa, así como adaptarse a los procesos de negocio de la organización. En el cuadro 2 se representan los diferentes componentes del proceso de gerencia de riesgos recogidos en la ISO 31000 y la relación existente entre los mismos, que se explican en las siguientes líneas: comunicación y consultas; establecimiento del contexto; apreciación del riesgo (identificación, análisis y evaluación); tratamiento del riesgo; seguimiento y revisión; registro del proceso de gestión del riesgo.

3.1. *Comunicaciones y consultas*

A diferencia de la norma previa COSO II que sitúa la "información y comunicación"[9] como uno de los últimos pilares del proceso de la Gerencia de Riesgos, la Norma ISO 31000 considera "la comunicación y las consultas"[10] como el primer punto del proceso, mostrando la gran relevancia del mismo e indicando que las comunicaciones y las consultas con las partes interesadas, tanto externas como internas a la organización, deben realizarse en todas las etapas del proceso de gestión del riesgo.

La norma propone el desarrollo de planes de comunicación y consulta para tratar temas relativos al riesgo en sí mismo, a sus causas, a sus posibles consecuencias, y a las medidas a tomar para tratarlo. La norma aporta un nuevo "enfoque consultivo", más profundo que el enfoque informativo tradicional, cuyos objetivos son muy amplios y unificadores abarcando desde la idea de ayudar a establecer adecuadamente el contexto, hasta favorecer una gestión de cambio adecuada durante el proceso de gestión del riesgo, pasando por otros objetivos tales como: asegurar que los intereses de las partes interesadas se comprendan y se tengan en consideración; ayudar a asegurar que los riesgos se identifican adecuadamente; reunir diferentes áreas de experiencia para analizar los riesgos; asegurar que las diferentes opiniones se tienen en cuenta de forma adecuada al definir los criterios de riesgo y en la evaluación de los riesgos; conseguir la aprobación y el apoyo para un plan de tratamiento de riesgos; etc.

[9] COSO II (2004), pp. 85-101.
[10] UNE-ISO 31000 (2009), pp. 20-21.

Este pilar no se limita a una descripción detallada, amplia y genérica de la información, o de cómo fluye ésta de abajo hacia arriba en la organización y viceversa, sino que avanza en las aplicaciones y utilidades de esa información en todos los niveles. De aquí la importancia de que las comunicaciones y consultas externas e internas sean, como dice la norma, "veraces, pertinentes, exactas y entendibles, teniendo en cuenta los aspectos confidenciales y de integridad personal, para asegurarse de que las personas implicadas en la implementación del proceso de gestión del riesgo y las partes interesadas comprendan las bases que sirven y servirán para tomar decisiones, así como las razones por las que determinadas acciones son necesarias".

3.2. *Establecimiento del contexto*

El contexto en el que se define y desarrolla cualquier tipo de planificación determina y delimita su utilidad y aplicación. En este sentido, COSO II establece como prioridad el análisis del "ambiente interno"[11] de la organización que se adentra en cuestiones de filosofía y cultura del riesgo, compromiso, autoridad y responsabilidad en materia de riesgos, integridad y valores éticos, etc. Sin embargo, y a pesar de ser el documento que utilizan las empresas cotizadas, hay ciertos aspectos de relaciones internas-externas que no quedan contempladas.

Como segundo punto, la norma ISO 31000 determina el "establecimiento del contexto"[12], no sólo físico, sino principalmente relacional, de forma que sienta las bases para que la organización pueda articular sus objetivos, definir los parámetros externos e internos a tener en cuenta en la gestión del riesgo[13], relacionar éstos con el alcance del proceso particular de gestión del riesgo, así como establecer el alcance y los criterios de riesgo para el proceso restante. En este sentido la norma habla de un contexto externo e interno para referirse después al contexto del proceso de gestión de riesgos y finalmente a la definición de los criterios de riesgo.

El contexto externo es el entorno en que la organización busca conseguir sus objetivos. Abarca los ámbitos físicos cercanos así como el

[11] COSO II (2004), pp. 9-18.
[12] UNE-ISO 31000 (2009), pp. 21-23.
[13] Véase, MARTINEZ GARCÍA, C. (2009).

entorno social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local. Pero no se ciñe a ellos, sino que incluye los factores y las tendencias clave que tengan impacto sobre los objetivos de la organización. Constituye un avance importante sobre la concepción de la norma anterior. No así el contexto interno, que no es otro que el ambiente interno ya comentado (estructura, funciones, responsabilidades, objetivos, políticas, cultura, sistemas de información, filosofía, etc.).

El contexto del proceso de la gestión del riesgo variará de acuerdo con las necesidades de la organización. Se deberían tener en cuenta todos aquellos factores que permitan asegurar que el enfoque adoptado para la gestión del riesgo es apropiado a las circunstancias, a la organización y los riesgos que afectan al logro de sus objetivos. En este sentido, se deberían establecer los objetivos, las estrategias, el alcance y los parámetros de las actividades de la organización, o de aquellas partes de la organización donde se aplica el proceso de gestión del riesgo. La gestión del riesgo se debería emprender teniendo en cuenta todo lo necesario para justificar los recursos que se han de utilizar para llevarla a cabo, así como las responsabilidades y las autoridades de quienes la llevan a cabo.

La definición de los criterios de riesgo se refiere al establecimiento de los criterios que la empresa va a utilizar para evaluar la importancia del riesgo global y de los riesgos particulares. Dichos criterios dependerán de múltiples factores como las causas y las consecuencias de un riesgo, cómo se pueden medir estas causas, los métodos de definición de probabilidad[14], cuándo un riesgo es aceptable o no (Aymerich Lobo, J. I., Fernández Isla, G., García Aranda, M. e Iturmendi Morales, G., 1998). Los criterios que la empresa elija deben reflejar los valores de la empresa, sus objetivos y sus recursos, siempre teniendo en cuenta que puede haber exigencias externas de tipo legal o reglamentario que obliguen a ajustar e incluso modificar dichos criterios.

3.3. *Apreciación del riesgo*

Tanto en COSO II[15] como en la Norma ISO 31000, la "apreciación del riesgo"[16] se refiere al proceso de evaluación cualitativa y cuantitativa de

[14] Véase, HAMPTON, J. J. (2009).
[15] COSO II (2004), pp. 29-68.
[16] UNE-ISO 31000 (2009), pp. 23-25.

la exposición al riesgo en las diferentes actividades o procedimientos de la empresa. Abarca entonces el proceso global de identificación, de análisis y de evaluación del riesgo. La apreciación de los riesgos del negocio comienza con el planeamiento estratégico y el riesgo de cambios en el entorno e intenta analizar los riesgos en las unidades operativas a través de la cadena de valor en una visión a largo plazo de las operaciones. La consideración de los riesgos se efectúa esencialmente bajo el punto de vista económico y financiero en cuanto a la repercusión que pueden tener sobre el conjunto de la empresa en su prevención, control y reposición de las pérdidas por accidentes y siniestros. Esta apreciación y análisis de los riesgos y su posterior gestión contempla la participación de dos elementos fundamentales como son las fuentes de riesgos y los sujetos de la acción de los riesgos, que pueden interaccionar entre sí generándose un tercer elemento, los efectos negativos (Martínez Torre-Enciso, 2002).

a) Identificación del riesgo

La identificación de los riesgos a los que está sometida una empresa es la base de la gerencia de riesgos. El primer paso del análisis debe consistir siempre en la identificación y conocimiento detallado de las posibles fuentes, orígenes o causas de los riesgos, así como los sujetos que pueden verse afectados por los mismos, sus consecuencias potenciales, las áreas de impactos, etc. No todos los acontecimientos que suceden en una empresa son susceptibles de interpretarse como un riesgo, ni todos llegan a materializarse. El objetivo de esta etapa consiste en generar una lista exhaustiva de riesgos denominada "decálogo de riesgos"[17], basada en aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos.

A diferencia de COSO II que en su capítulo 4 exponen algunas técnicas empleadas para la identificación de eventos (inventarios de eventos, talleres y grupos de trabajo dirigidos, entrevistas, cuestionarios, encuestas, etc.), la norma ISO 31000 no especifica las "herramientas y técnicas de identificación del riesgo" que pueden ser utilizadas, si bien deja la puerta abierta al uso de aquellas que se adapten mejor a los objetivos, aptitudes y riesgos a los que la empresa esté expuesta.

[17] Véase, Martínez Torre-Enciso, M. I. (2002).

b) Análisis del riesgo

COSO II incluye en su capítulo 4 tanto la identificación como el análisis, si bien la norma ISO 31000 separa ambos conceptos de forma clara y precisa. Para la ISO 31000 el análisis del riesgo implica "desarrollar una comprensión del riesgo" permitiendo avanzar sobre el concepto inicial de identificación. El análisis del riesgo implica aquí no sólo la consideración de las causas y las fuentes del riesgo, sino también el estudio de sus posibles consecuencias positivas y negativas así como la probabilidad de que estas consecuencias puedan ocurrir, para lo que se sugiere identificar los factores que afectan a las consecuencias y a la probabilidad, la interdependencia de los diferentes riesgos y sus fuentes, etc.

El análisis del riesgo se puede realizar con diferentes grados de detalle, dependiendo del riesgo, de la finalidad del análisis y de la información, de los datos y recursos disponibles. El análisis puede ser cualitativo (alto, medio, bajo), semi-cuantitativo o cuantitativo (valor en riesgo, flujos de caja en riesgo, distribuciones de pérdidas, back-testing, análisis de sensibilidad, etc.)[18] o una combinación de los tres casos, dependiendo de las circunstancias, con el objetivo de determinar la probabilidad e impacto (tangible e intangible) de los posibles eventos[19]. Dependiendo de los casos se puede necesitar más de un valor numérico o descriptor para especificar las consecuencias y su probabilidad, para diferentes momentos, lugares, grupos o situaciones.

El análisis del riesgo proporciona elementos de entrada para la evaluación del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como sobre las estrategias y los métodos de tratamiento del riesgo más apropiados.

c) Evaluación del riesgo

En base a los resultados de la identificación y del análisis del riesgo la finalidad de la evaluación del riesgo es ayudar a la toma de decisiones, determinando los riesgos a tratar, la forma de tratamiento más adecuada para adaptar los riesgos adversos a un nivel tolerable y la prioridad para implementar el tratamiento determinado.

[18] Véase, McNEIL, A. J., FREY, R., EMBRECHTS, P. (2005).
[19] Véase, CROUHY, M., GALAI, D. and MARK, R. (2005).

En este sentido, aparece la Norma Internacional ISO 31010[20] como soporte estándar para la ISO 31000, la cual proporciona orientación para la selección y aplicación de técnicas sistemáticas de evaluación del riesgo. Estas técnicas de evaluación de riesgos pueden ser clasificadas de diferentes maneras con el fin de facilitar la comprensión de sus aplicaciones, elementos de entrada, procesos, resultados y relativas fortalezas y limitaciones[21]. La tabla 1 que se expone a continuación, resume el Anexo A[22] de la norma ISO 31010 la cual pone en relación las técnicas potenciales y sus categorías. En este cuadro resumen se observa la existencia de más de treinta métodos de evaluación, ordenados por su nombre y clasificados por su aplicabilidad (FA: Fuertemente aplicables. NA: No se aplica. A: Aplicable) en cada una de las diferentes fases de identificación, análisis y evaluación de los riegos.

Así mismo, la norma dispone de un Anexo B[23] donde cada una de las 31 técnicas presentadas está desarrollada en cuanto a la naturaleza de la evaluación que con ella se suministra y las líneas directrices para su aplicabilidad en ciertas situaciones. Se trata de una explicación resumida pero muy útil por la posibilidad de comparación entre las diversas alternativas o métodos de valoración. La ISO 31010 sin embargo, no recoge la totalidad de las técnicas que a día de hoy se utilizan en el mercado, incluyendo en sus páginas algunas técnicas que difícilmente se pueden aplicar en el mundo actual.

Cuando la evaluación de riesgos se lleva a cabo de conformidad con esta norma ISO 31010 se contribuye al buen desarrollo de otras actividades de gestión de riesgo como: comprender el riesgo y aportar información para la toma las decisiones; contribuir a la comprensión de los riesgos con el fin de ayudar en la selección de las opciones de tratamiento; identificar los factores relevantes que puedan contribuir a potenciar o reducir los riesgos; determinar los puntos débiles en los sistemas y las organizaciones; comparar los riesgos mediante sistemas alternativos, tecnologías o enfoques; comunicar riesgos e incertidumbres; ayudar a establecer prioridades; evaluar los riesgos por su valor residual; considerar la tolerancia al riesgo en otras partes diferentes de la organización; etc.

[20] IEC/ISO 31010: 2009, *Risk Management-Risk Assessment Techniques*.

[21] La norma IEC/ISO 31010: 2009, *Risk Management-Risk Assessment Techniques*, editada en Francés y en Ingles, está siendo actualmente traducida por el "grupo de trabajo sobre las ISO" de la Asociación Española de Gerencia de Riesgos y Seguros (AGERS) (Enero 2011).

[22] IEC/ISO 31010, pp. 21-26.

[23] IEC/ISO 31010, pp. 28-89.

Tabla 1

Herramientas utilizadas para la evaluación del riesgo: aplicación (ISO 31010)

Herramientas y técnicas	Proceso de evaluación del riesgo					
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Tormenta de ideas (Brainstorming)	FA	NA	NA	NA	NA	B01
Entrevistas estructuradas o semi-estructuradas	FA	NA	NA	NA	NA	B02
Delphi	FA	NA	NA	NA	NA	B03
Lista verificación (Check-lists)	FA	NA	NA	NA	NA	B04
Análisis preliminar de riesgos	FA	NA	NA	NA	NA	B05
Estudios de riesgos operacionales (HAZOP)	FA	FA	A	A	A	B06
Análisis de riesgos y puntos de control críticos (HACCP)	FA	FA	NA	NA	FA	B07
Valoración de riesgo medioambiental	FA	FA	FA	FA	FA	B08
Que pasaría si (What if)	FA	FA	FA	FA	FA	B09
Análisis de escenario	FA	FA	A	A	A	B10
Análisis del impacto en el negocio	A	FA	A	A	A	B11
Análisis de causa	NA	FA	FA	FA	FA	B12
Análisis modal de fallos potenciales y sus efectos (ANFE-FMEA)	FA	FA	FA	FA	FA	B13
Análisis de árbol de fallos	A	NA	FA	A	A	B14
Análisis de árbol de sucesos	A	FA	A	A	NA	B15
Análisis de causa consecuencia	A	FA	FA	A	A	B16
Análisis de causa efecto	FA	FA	NA	NA	NA	B17
Análisis de niveles de protección	A	FA	A	A	NA	B18
Árbol de decisión	NA	FA	FA	A	A	B19
Análisis de fiabilidad humana	FA	FA	FA	FA	A	B20
Análisis de la pajarita	NA	A	FA	FA	A	B21

Herramientas y técnicas	Proceso de evaluación del riesgo					
	Identificación del riesgo	Análisis del riesgo			Evaluación del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Mantenimiento centrado en la confiabilidad	FA	FA	FA	FA	FA	B22
Análisis de errores de diseño (SNEAK)	A	NA	NA	NA	NA	B23
Análisis de Markov	A	FA	NA	NA	NA	B24
Simulación de Monte Carlo	NA	NA	NA	NA	FA	B25
Estadísticas y redes Bayesianas	NA	FA	NA	NA	FA	B26
Curvas FN	A	FA	FA	A	FA	B27
Índices de riesgos	A	FA	FA	A	FA	B28
Matriz de consecuencia/probabilidad	FA	FA	FA	FA	A	B29
Análisis coste/beneficio	A	FA	A	A	A	B30
Análisis de decisión multicriterio	A	FA	A	FA	A	B31

Fuente: Elaborado por el Grupo de Trabajo sobre la ISO 31000-ISO 31010 de AGERS (Asociación Española de Gerencia de Riesgos y Seguros) en enero de 2011. (FA: Fuertemente aplicables. NA: No se aplica. A: Aplicable)

La evaluación de los riesgos va a permitir establecer las estrategias oportunas que favorezcan la reducción de la frecuencia y la intensidad del impacto del riesgo. Entre dichas estrategias también se puede decidir "no hacer nada", y si bien es una estrategia improbable, en algunas circunstancias tiene sentido no tratar el riesgo de ninguna otra manera que manteniendo los controles existentes (Martínez Torre-Enciso, 2000). En otras ocasiones, la evaluación del riesgo puede llevar a la decisión de realizar un análisis en mayor profundidad.

3.4. *Tratamiento del riesgo*

El tratamiento del riesgo implica la selección y la implementación de una o varias opciones para modificar los riesgos (Fernández Isla, 2007), opciones que aparecen desarrollando el siguiente proceso cíclico: evaluar un tratamiento del riesgo; decidir si los niveles de riesgo residual son tolerables; si no son tolerables, generar un nuevo tratamiento del riesgo; evaluar la eficacia de este tratamiento.

"Una vez evaluados los riesgos relevantes, la dirección determina cómo responder a ellos". Así comienza el capítulo 6 de COSO II[24], en el que se hace una referencia a la "respuesta" ante los riesgos como estrategia de "tratamiento". Frente a las opciones clásicas de respuesta enumeradas en COSO II (evitar, reducir, compartir), la ISO 31000[25] amplía el abanico de posibilidades en un intento de abarcar tanto medidas de control como medidas o estrategias de financiación:

a) Evitar el riesgo decidiendo no iniciar o continuar con la actividad que causa el riesgo.
b) Aceptar o aumentar el riesgo a fin de perseguir una oportunidad.
c) Eliminar la fuente del riesgo.
d) Modificar la probabilidad.
e) Cambiando las consecuencias.
f) Compartir el riesgo con otras partes (incluyendo los contratos y la financiación del riesgo)[26].
g) Retener el riesgo en base a una decisión informada.

Un buen tratamiento del riesgo implica la implementación de una o varias estrategias combinadas, de forma que la selección de las mismas debe implicar que la empresa va a obtener una reducción de los costes, un incremento de valor global, así como otro tipo de ventajas teniendo en cuenta los requisitos legales, reglamentarios, de responsabilidad social, etc. Cuando la empresa quiere implementar más de una estrategia debe establecer un "plan de tratamiento" en el que se identifique el orden de prioridad en que se deberían implementar los tratamientos de riesgo individuales, así como los porcentajes sobre el coste total a aplicar a cada tratamiento individual. La finalidad de los planes de tratamiento del riesgo consiste en documentar la manera en que se implantarán las opciones de tratamiento elegidas y su integración en los procesos de gestión de la organización (Casares, 2005).

3.5. *Seguimiento y revisión y Registro del proceso de gestión del riesgo*

"El seguimiento y la revisión" son una innovación de la norma ISO 31000[27], al referirse a cómo el proceso de tratamiento del riesgo debería

[24] COSO II (2004), pp. 69-78.
[25] UNE-ISO 31000 (2009), pp. 25-26.
[26] Véase, CASARES SAN JOSE-MARTI, I. (2010).
[27] UNE-ISO 31000 (2009), pp. 26-27.

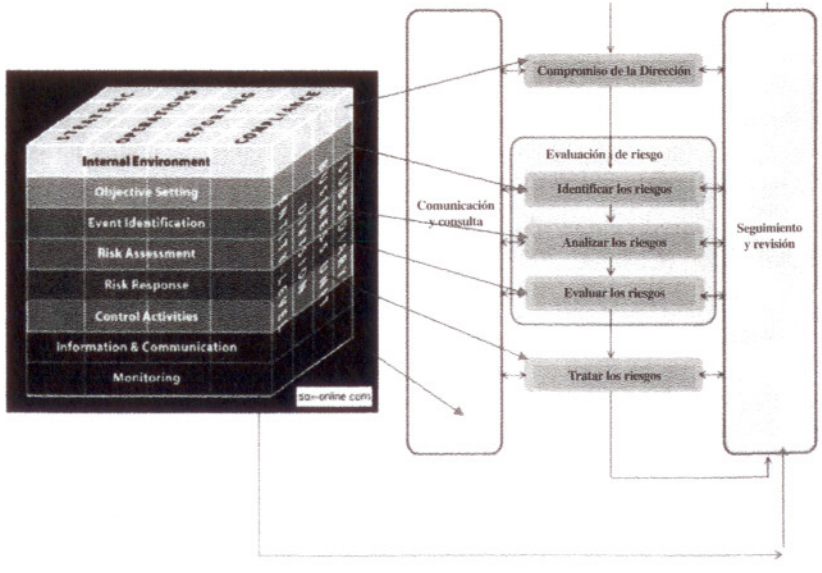
someterse a una verificación o una vigilancia regular y abarcar todos los aspectos del proceso de gestión del riesgo. Este proceso de seguimiento y revisión sobre los planes de tratamiento del riesgo proporciona una medida del funcionamiento de los mismos, cuyos resultados, registrados en informes internos y externos, se pueden incorporar en la gestión del funcionamiento global de la organización, en su medición y en las actividades externas e internas. Todos estos procesos de gestión del riesgo deben registrarse para proporcionar la base para la mejora de los métodos y de las herramientas, así como del proceso en su conjunto.

4. **Conclusiones**

A lo largo de estas líneas se ha hecho un análisis comparativo de las normas ISO 31000:2009 y COSO II:2004 siguiendo las pautas y relaciones señaladas en el cuadro 3, en el que se observa el paralelismo entre el tradicional cubo establecido por COSO II para su "Enterprise Risk Management" y las nuevas fases del "proceso de gerencia de riesgos" establecidas por la ISO 31000.

Cuadro 3

Análisis comparativo de las normas internacionales COSO II e ISO 31000



Fuente: Elaboración propia.

De la comparativa anterior se concluye que la nueva norma internacional ISO 31000 aporta importantes avances sobre la noma previa, desde el mismo momento que tiene por objetivo ayudar a las organizaciones de todo tipo y tamaño a gestionar el riesgo con efectividad. Entre los avances más significativos, destacamos los siguientes:

- Establece principios que deben seguirse para una gestión eficaz del riesgo.
- Hasta ahora no existía una norma global y amplia que pudiese aplicarse a todo tipo de empresas, todo tipo de sectores, a lo largo de toda la vida de una organización, y a la práctica totalidad de las actividades de la empresa.
- Esta nueva norma internacional es voluntaria en su aplicación, y permite dar un paso importante en el contexto global de los riegos ya que favorece que cualquier empresa pueda realizar una gestión eficaz del riesgo al que se encuentra expuesta, mediante la identificación, análisis y evaluación de los riesgos, favoreciendo con estas prácticas la consecución de sus objetivos.
- La norma ISO 31000 ayuda a responder a uno de los interrogantes fundamentales en la gestión del riesgo: cómo llegar a todo el mundo para hablar sobre el riesgo de la misma manera, ya que unifica criterios, procesos, vocabulario, etc.
- Es una norma aplicable a cualquier tipo de riesgo, de cualquier naturaleza, causa y origen, ya sean sus consecuencias positivas o negativas para la organización.
- La norma provee de los principios, el marco de trabajo y un proceso destinado a gestionar cualquier tipo de riesgo de una manera transparente, sistemática y creíble dentro de cualquier alcance o contexto.
- El contexto externo queda definido más allá del tradicional incluyendo factores y tendencias importantes que tengan impacto sobre los objetivos de la organización, lo que constituye un avance importante sobre la concepción de la norma anterior.
- Norma de reconocimiento internacional.
- Modelo simple de entender y aplicar en comparación con otros modelos existentes.

Todos estos avances favorecen la gestión eficaz de los riesgos en las empresas de cualquier tamaño o actividad, con el objetivo de hacer frente a aquellos factores internos y externos que generan incertidumbre, lo que va a permitir a las empresas: aumentar la probabilidad de alcanzar los objetivos fijados; identificar las oportunidades, fortalezas, debilida-

des y amenazas de la organización; cumplir con las normativas legales y reglamentarias aplicables y las normas internacionales; mejorar el gobierno corporativo; mejorar la presentación de los informes financieros; establecer un punto de partida para la toma de decisiones; asignar los recursos necesarios para el tratamiento del riesgo; mejorar la eficacia y eficiencia operacional; mejorar la prevención y gestión de siniestros, así como ser capaces de minimizar las pérdidas; etc.

Son muchos, como se ha indicado, los avances que aporta la nueva norma y que facilitan la gerencia de riesgos en este nuevo contexto. Sin embargo, consideramos que la norma se queda corta en algunos aspectos, entre los que destacamos los siguientes:

- La definición de riesgo de la ISO 31000 es completamente diferente a la definición de otras normas previas, lo que ha abierto el debate respecto a la definición de riesgo. La ISO 31000 define el riesgo como "el efecto de la incertidumbre en los objetivos", mientras que otro estándar sobre riesgo ha definido previamente el riesgo como "la incertidumbre que, si ocurre, tendrá un efecto en los objetivos". Pensamos que en un intento por simplificar la definición ésta se ha simplificado excesivamente.
- Aunque se persigue hacer un análisis amplio de los riesgos de la empresa, no garantiza que se identifiquen todas las zonas de riesgo, con los perjuicios que ello conlleva.
- La norma no especifica las "herramientas y técnicas de identificación del riesgo" que pueden ser utilizadas, si bien deja la puerta abierta al uso de aquellas que se adapten mejor a los objetivos, aptitudes y riesgos a los que la empresa esté expuesta.
- No ofrece taxonomías de riesgo, mapas de calor o de otras plantillas para el desarrollo de la documentación y los informes de riesgo.
- Se trata de una norma muy corta (34 páginas respecto a las 125 de COSO II), que abarca todos o casi todos los aspectos a considerar en la gerencia de riesgos, pero no profundiza en ellos.

Los pros y los contras, los avances y las limitaciones son en sí mismos muy positivos al permitir a la casi desconocida "gerencia de riesgos" saltar a la primera página de periódicos y revistas, favoreciendo con ello que el gran público conozca la existencia de estas prácticas y concienciando a los empresarios de todo tipo de la importancia de gestionar eficazmente sus riesgos en este nuevo contexto para "la mejor consecución de sus objetivos empresariales".

Bibliografía

AYMERICH LOBO, J. I.; FERNÁNDEZ ISLA, G.; GARCÍA ARANDA, M. e ITURMENDI MORALES, G. (1998): *Gerencia de riesgos y seguros en la empresa*, Editorial MAPFRE, Madrid.

BASILEA II, (2004): *Convergencia internacional de medidas y normas de capital - Marco revisado*, junio.

CASARES SAN JOSÉ-MARTÍ, I. (2005): "Gerencia de riesgos asegurables", *Actuarios*, nº 23, Julio-Agosto, pp. 38-40.

—(2007): "La necesidad del control interno en las empresas: gerencia de riesgos", *La Gaceta de los Negocios*, 22/05/07, Madrid.

—(2010): "Aplicación de la gerencia de riesgos a las empresas de mediación", *Revista Aseguradores del Consejo General de los Colegios de Mediadores de Seguros*. Mayo 2010. Madrid.

CHAPMAN, R. J. (2006): *Tools and Techniques for Enterprise Risk Management*, John Wiley & Sons.

COMITÉ DE SUPERVISIÓN BANCARIA DE BASILEA II (2004): *Aplicación de Basilea II. Principios Prácticos*, Comité de Supervisión Bancaria de Basilea II, Basilea.

—(2005): *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*, Basel Committee on Banking Supervision, Basilea.

COSO II (2004): *Enterprise Risk Management. Integrated Framework*, COSO.

—(2004): *Gestión de Riesgos Corporativos-Marco Integrado: Técnicas de Aplicación*, Committee of Sponsoring Organizations of Treadway Commission, Septiembre.

CROUHY, M.; GALAI, D. and MARK, R. (2005): *The essentials of risk management*. McGraw-Hill Professional.

DIRECTIVA 2009/138/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II).

ESCORIAL BONET, A. (2010): *ISO 31000:2009 - La gestión de riesgos como componente integral de la gestión empresarial*, véase en http://www.riskia.com/Files/Billeder/ Articulo_-_ISO_31000_Angel_Escorial%5B1%5D.pdf

FERMA (2003): *Estándares de Gerencia de Riesgos*, Bruselas, Bélgica. Véase http://www.agers.es/pdf/noticiasinteres/Estandares_de_Gerencia_de_Riesgos.pdf.

FERNÁNDEZ ISLA, G. (2007): "La transferencia de riesgos", *Actuarios*, nº 26, Julio, pp. 35-37.

HAMPTON, J. J. (2009): *Fundamentals of Enterprise Risk Management*, AMACOM, Litchfield, Connecticut, USA.

HERNÁNDEZ BARROS, R. y MARTÍNEZ TORRE-ENCISO, M. I. (2010): "La nueva regulación europea de seguros privados: SOLVENCIA II", *Boletín de Estudios Económicos*, Vol. LXV, Nº 199, Abril, pp. 75-92.

HUBBARD, D. W. (2009): *The failure of risk management: why it´s broken and how to fix it*, John Wiley & Sons, England, May.

IEC/ISO 31010: 2009, *Risk Management-Risk Assessment Techniques*.

INFORME UNE-ISO GUÍA 73 IN (2009): *Gestión del riesgo. Vocabulario*. Traducido por AENOR (Asociación Española de Normalización y Certificación).

INTERNATIONAL STANDARD ISO/FDIS 31000:2009 (E): *Risk Management. Principles and guidelines*.

ISO GUIDE 73: 2009 (E): *Risk Management. Vocabulary*.

ISO 31000: (2009): *de Gestión de Riesgos - Principios y Directrices*.

ISO/CEI 73: (2002): *Risk management — Vocabulary — Guidelines for use in standards*.

MARTÍN MARÍN, J. L. y TELLÉZ VALLE, C. (2009): "La regulación y supervisión del Sistema Financiero ante la crisis económica", *Boletín de Estudios Económicos*, Vol. LXIV, Nº 198, Diciembre, pp. 441-468.

MARTINEZ GARCÍA, C. (2009): "Gestión integral de riesgos corporativos como fuente de ventaja competitiva: cultura positiva del riesgo y reorganización estructural", *Cuadernos de la Fundación Mapfre*, Nº 134, Instituto de Ciencias del Seguro, Madrid.

MARTÍNEZ TORRE-ENCISO, M. I. (2000): "La elección de la estrategia correcta para evitar el desastre", *Anuario Jurídico y Económico Escurialense*, Ed. Real Colegio Universitario "Escorial-Mª Cristina", San Lorenzo del Escorial, Vol. XXXIII, pp. 485-499.

—(2002): "La gerencia de riesgos", *Anuario Jurídico y Económico Escurialense*, Ed. Real Colegio Universitario "Escorial-Mª Cristina", San Lorenzo del Escorial, Vol. XXXV, pp. 425-458.

MARTÍNEZ TORRE-ENCISO, M. I. y HERNÁNDEZ BARROS, R. (2010): "Solvency II, the European insurance regulation based on risk", *Revista Universitaria Europea*, Nº 12, pp. 119-134.

MCNEIL, A. J.; FREY, R.; EMBRECHTS, P. (2005): *Quantitative Risk Management: Concepts, Techniques, and Tools*, Princeton University Press.

NORMA ESPAÑOLA UNE-ISO 31000 (2009): *Gestión del riesgo. Principios y Directrices*. Traducido por AENOR (Asociación Española de Normalización y Certificación.

ONG, M. K. (2005): *Risk management. A modern perspective*, Elsevier, Chicago, Illinois.

UNE-ISO GUÍA 73: 2009: *Gestión del riesgo. Vocabulario*.

ZÁRRAGA ARANCETA, E. (2007): "Propuesta de un modelo: el análisis objetivo del corredor de seguros", *Gerencia de riesgos y seguros*, Fundación MAPFRE, Instituto de Ciencias del Seguro, nº 98, 2º cuatrimestre 2007, Madrid, pp. 54-66. También en: http://www.mapfre.com/fundacion/html/revistas/gerencia/n098/estud_03.html.

Páginas Web

AENOR	http://www.aenor.es
AGERS	http://www.agers.es

CEIOPS	http://www.ceiops.org
FERMA	http: //www.ferma.eu
FUNDACIÓN MAPFRE	http://www.fundacionmapfre.com/cienciasdelseguro
CEA	http://www.icea.es
ISO	http://www.iso.org
KPMG	http://www.kpmg.com
PRICEWATERHOUSECOOPERS	http://www.pwc.com
TIEMS	http://www.tiems.org

RESUMEN

La gerencia de riesgos en un entorno global se está perfilando como una estrategia financiera y empresarial que proporciona una importante ventaja competitiva a las empresas que disponen de ella, así como un importante incremento en el mercado. En este sentido, la norma básica aplicada en el ámbito de las empresas cotizadas es COSO II, si bien, hasta ahora no existía una norma global y amplia que pudiese aplicarse a todo tipo de empresas, todo tipo de sectores, a lo largo de toda la vida de una organización, y a la práctica totalidad de sus actividades.

Este artículo profundiza en los avances que la Norma ISO 31000:2009 hace sobre el documento COSO II (2004) analizando cómo esta Norma Internacional aporta principios y directrices genéricas sobre la gestión del riesgo que pueden ser utilizados por cualquier empresa, asociación (pública, privada o comunitaria) o personas a nivel de grupo o individualmente, siempre dentro de las Normas de Buen Gobierno Corporativo que exigen el establecimiento de una gerencia de riesgos que permita la toma de decisiones en éste ámbito.

Palabras clave: Gestión eficaz del riesgo, Identificación y Evaluación de los riesgos, eficacia y Eficiencia Operacional, Estructura Organizativa.

SUMMARY

Risk management in a global environment is emerging as a financial and business strategy that provides a significant competitive advantage to companies that have this processes, as well as a significant increase in market value. In this sense, the basic rule applied in the field of listed companies is COSO II, although so far there was no broad, global standard that would apply to all types of businesses, all industries, throughout the entire the life of an organization and almost all of its activities.

This article deals with the progress that the ISO 31000:2009, made on the COSO II (2004) document analyzing how this International Standard provides generic principles and guidelines on risk management that can be used by any company, association (public, private or community) or people at the group or individually, always within the Corporate Governance Guidelines which call for a risk management to enable decision making in this field.

Key words: Effective risk management, identification and assessment of risk, operational efficiency and effectiveness, Organizational Structure.