ISSN 2389-8186
E-ISSN 2389-8194

Vol. 4, No. 2
Septiembre de 2017
doi: http://dx.doi.org/10.16967/rpe.v4n2a7

ARTÍCULOS ORIGINALES

¿Auditoría más efectiva después de COSO ERM 2017 o de ISO 31000:2009?

ALCINA AUGUSTA DE SENA PORTUGAL DIAS[a]

pp. 71-80

RESUMEN En este artículo se busca examinar la mayor efectividad de una auditoría después del uso de ERM 2017 o de la norma ISO 31000. A tal efecto, se considerará la existencia y evolución del COSO y se relacionará con los mayores escándalos financieros y sus resultados en términos de cronogramas de control. Se señalarán algunas críticas a COSO Cube y se describirá el nuevo marco ERM 2017. Por otra parte, la norma ISO 31000 se considerará como una directriz alternativa que se utilizará para fines de gestión de riesgos en cualquier organización. Se realiza una comparación entre las dos formas de gestión de riesgos. El proceso de auditoría se desarrollará después de comprender que la empresa cuenta con un proceso de gestión de riesgos implementado de cierta manera, puesto que los objetivos son diferentes pero los esquemas de control de gestión de riesgos son válidos. En términos de perspectiva para futuras investigaciones, se podría sugerir la identificación de organizaciones que utilizan un esquema (ERM) u otro (ISO), en el que se analicen y se comparen para evaluar su efectividad particular y valor acumulado.

PALABRAS CLAVE fraudes financieros, COSO, ISO 31000, ERM 2017, auditoría.

HISTORIA DEL ARTÍCULO
La versión original de este artículo fue escrita en inglés. Esta versión en español se publica con el fin de llegar a un público mas amplio. Para citar este artículo, por favor use la referencia original, así:

¿CÓMO CITAR?:
Dias, A. P. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000:2009?. *Perspectiva Empresarial*, *4*(2), 73-82. http://dx.doi.org/10.16967/rpe.v4n2a7

RECIBIDO: 18 de junio de 2017
APROBADO: 17 de agosto de 2017

CORRESPONDENCIA:
Alcina Portugal Dias, Jaime Lopes Amorim 465-004 Matosinhos tel 229050000, Portugal.

[a] *CEOS.PP – Centro de Estudios Sociales y Organizacionales; APQ- SCOPE; UNIAG; EUROPAGUNE (Universidade do Pais Basco). INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO. E-mail: alcina @iscap.ipp.pt*

ISSN 2389-8186
E-ISSN 2389-8194

Vol. 4, No. 2
Septiembre de 2017
doi: http://dx.doi.org/10.16967/rpe.v4n2a7

¿Una auditoría más eficaz después del COSO ERM 2017 o de la ISO 31000:2009?

ABSTRACT This paper seeks to consider the better effectiveness of an audit after the use of ERM 2017 or ISO 31000. To this effect, is COSO existence and evolution will be considered and related to the biggest financial scandals and its output in terms of control schedules. Some criticisms to COSO Cube will be pointed out, and the new ERM 2017 will be described. ISO 31000 will be considered as an alternative guideline to be used for Risk Management purposes in any organization. A comparison is made between the two sets of Risk management. The audit process will be developed after grasping that the company has a risk management implemented in a more certain fashion, as objectives are different but schemes of risk management control are valid. In terms of future research perspective, one could suggest the identification of organizations using one scheme (ERM) or another (ISO), analysing them and comparing them in order to evaluate their particular effectiveness and accrued value.

KEYWORDS Financial frauds, COSO, ISO 31000, ERM 2017, audit.

¿CÓMO CITO EL ARTÍCULO?
HOW TO CITE THIS PAPER?

CHICAGO:
Dias, Alcina Portugal. 2017. A more effective audit after COSO ERM 2017 or after ISO 31000:2009?". *Perspectiva Empresarial* 4(2): 73-82. http://dx.doi.org/10.16967/rpe.v4n2a7

MLA:
Dias, Alcina Portugal. "A more effective audit after COSO ERM 2017 or after ISO 31000:2009?". *Perspectiva Empresarial* 4.2 (2017): 73-82. Digital. http://dx.doi.org/10.16967/rpe.v4n2a7

Uma auditoria mais efetiva depois do COSO ERM 2017 ou do ISO 31000:2009?

RESUMO Este artigo busca considerar a maior efetividade de uma auditoria depois do uso de ERM 2017 ou ISO 31000. Para isso, a existência e evolução do COSO será considerada e relacionada aos maiores escândalos financeiros e a sua saída em termos de programas de controle. Algumas críticas ao COSO Cube serão levantadas e o novo ERM 2017 será descrito. A ISO 31000 será considerada uma diretriz alternativa a ser usada pelos propósitos do Gerenciamento de Risco em qualquer organização. Uma comparação PE feita entre dois tipos de Gerenciamento de Risco. O processo auditado será desenvolvido depois de entender que a companhia tem gerenciamento de risco implementado de uma forma específica, assim como os objetivos são diferentes, mas os esquemas de controle de gerenciamento de risco são válidos. Em termos de perspectiva de futuras pesquisas, poderíamos sugerir a identificação de organizações usando um esquema (ERM) ou outro (ISO), analisando-os e comparando-os de forma a avaliar sua efetividade particular e valor acumulado.

PALAVRAS CHAVE auditoria, COSO, ERM 2017, fraudes financeiras, ISO 31000.

Introducción

Este documento considera los principios COSO como algo crucial para el logro de cualquier auditoría, en particular en lo que se refiere a la gestión del riesgo empresarial o Enterprise Risk Management (ERM). Al mismo tiempo, nuestro objetivo es reflexionar sobre el uso de ISO 31000 como una guía alternativa para la gestión de riesgos. Los escándalos financieros mencionados permitirán argumentar la importancia del desarrollo y la implementación de procedimientos y medidas de control atribuidas al control interno. Por lo tanto, se describirá ERM 2017 y se sugerirá ISO 31000 como una alternativa. Finalmente, se hará una reflexión con respecto a los diferentes problemas de control de riesgos y su efecto en los procedimientos de auditoría.

Escándalos financieros

Enron, Parmalat y Worldcom, entre muchos otros, sufrieron fraudes que conmocionaron al mundo financiero y engañaron a las partes interesadas al prometerles altos dividendos por algo que realmente no valía nada (Merton, Peron, 1993; Anomaly et al 2014; Donaldson, Preston 1995). Estas empresas intentaron aumentar sus ganancias y encubrir sus deudas mediante técnicas fraudulentas, un falso aumento del valor de los activos y esquemas de ingresos acumulados, lo que aparentemente traía buenos beneficios y alta distribución de dividendos. Los dividendos altos hacen que los accionistas estén contentos y que ambicionen recibir más y más. Las empresas también se sienten felices, porque la gente quiere unirse a ellas y comprar sus acciones. El dinero fluye y los accionistas se alegran porque reciben más y más dinero. Sin embargo, no se fijan en la exactitud de la información divulgada en los estados financieros. Simplemente confían en ella y en todas las personas involucradas en su procesamiento, hasta que alguien revela que la información no es cierta. De esta manera las partes interesadas son defraudadas (Donaldson, Preston 1995), pues su expectativa es muy diferente a la realidad. Estos eventos violaron las principales ideas de las siguientes teorías:

En cuanto a la teoría contable, se violaron e ignoraron todos los principios asociados a la preparación de estados financieros (Business Press Ed, 2004; Wolk et al, 2008). Igualmente, si la divulgación de los estados financieros no es confiable, la teoría de la RSE (Dion, 2001; Frynas, Stephan, 2015) también se incumple. Todas las partes interesadas (Donaldson & Preston, 1995) fueron engañadas y esto afecta a los diferentes actores involucrados con las empresas: la sociedad, los accionistas, los empleados, el gobierno y otros. Cuando las compañías fracasan y se declaran en bancarrota, se dejan de lado todos los principios e ideas que la literatura menciona sobre fundamentos económicos y políticos (Anomaly et al, 2014). Se violan todos los conceptos y las ideas que se deben considerar para manejar una organización de manera eficaz y esto tiene graves consecuencias para la empresa en su conjunto (Merton y Peron, 1995). Al final, también podrían cuestionarse los principios de legitimidad (Suchman, 1995) al considerar que las cosas correctas en el lugar correcto no funcionaban en absoluto. Esto significa que los valores, la tradición y la cultura de la organización se dejaron de lado y se violó la jerarquía inherente. En consecuencia, esto nos lleva a la perspectiva institucional (Bruton, Ahlstrom, Li, 2010) en cuanto a los problemas éticos (Bruton, Ahlstrom, Li, 2010) y estos siguen siendo los efectos más relevantes de los escándalos financieros.

Estos fraudes sacudieron el mercado financiero estadounidense. Se podrían analizar desde una perspectiva de análisis PESTAS: política, económica, social, tecnológica, ambiental y sostenible. La gran consecuencia de estos eventos llevó a que la SEC (Securities Exchange Commission) y todas las asociaciones representativas de contabilidad, auditoría y gestión vieran la necesidad de organizar un comité para la supervisión de las empresas.

TABLA 1. Escándalos financieros y violación de principios

TEORÍAS	BIBLIOGRAFÍA
Contabilidad	Business Press Ed, 2004; Wolk et al, 2008
Responsabilidad social empresarial (RSE)	Dion, 2001; Frynas, Stephan, 2015
Economía política	Anomaly, Jonny & Brennan, Geoffrey,2014
Legitimidad	Suchman, 1995
Partes interesadas	Donaldson & Preston, 1995
Institucional	Bruton, Ahlstrom, Li, 2010
Ética	Dion, 2001; Frynas & Stephan, 2015
Negocios	Merton & Peron 1995

COSO - Committee of Sponsoring Organizations of the Treadway Commission

Dichos escándalos financieros, que básicamente ocurrieron a partir de 2001 en los Estados Unidos, provocaron serias reacciones en las entidades financieras supervisoras. COSO, impulsado por la SEC, emitió pautas para reforzar el control interno y la gestión de riesgos de la organización. Veamos la evolución de COSO desde su creación (tabla 2).

En primer lugar, es importante aclarar la conformación de este comité dedicado a responsabilizar a las empresas por la preparación, presentación de informes y divulgación de sus estados financieros. COSO se formó en 1985 para patrocinar a la Comisión Nacional de Informes Financieros Fraudulentos (la Comisión Treadway). El primer presidente de la Comisión Nacional fue James C. Treadway, Jr., vicepresidente ejecutivo y asesor general de Paine Webber Incorporated, además de ex comisionado de la SEC. La Comisión Treadway fue originalmente patrocinada y fundada por cinco asociaciones e institutos contables con sede en los Estados Unidos:

American Institute of Certified Public Accountants	**AICPA**
American Accounting Association	**AAA**
Financial Executives International	**FEI**
Institute of Internal Auditors	**IIA**
Institute of Management Accountants	**IMA**

La Comisión Treadway recomendó que las organizaciones que la patrocinan trabajen juntas para desarrollar una guía integrada sobre control interno. Estas cinco organizaciones conformaron lo que actualmente se conoce como COSO (Comité de organizaciones patrocinadoras de la comisión Treadway). COSO desarrolló recomendaciones para las empresas públicas y sus auditores independientes, para la SEC y otros reguladores y para las instituciones educativas. Las empresas incluían representantes de la industria, contabilidad pública, empresas de inversión y la Bolsa de Nueva York. En 2002, el marco de control fue emitido por COSO, al mismo tiempo que la ley SOx entró en vigor. En 2006 COSO se pronunció una vez más sobre la información financiera. Paralelamente a todas estas medidas de control interno, la difusión e implementación a nivel mundial de las NIIF (Normas Internacionales de Información Financiera) y las NIA (Normas Internacionales de Auditoría) se convirtieron en algo crucial para la armonización global de la información contable y la presentación de informes.

En 2016, COSO revisó el documento final sobre ERM titulado "Alineación del riesgo con la estrategia y el rendimiento", el cual fue divulgado en 2017. En este se redefinieron los siguientes objetivos en cuanto a la estrategia y el papel de la ERM:

TABLA 3. Nuevos objetivos de COSO ERM 2017

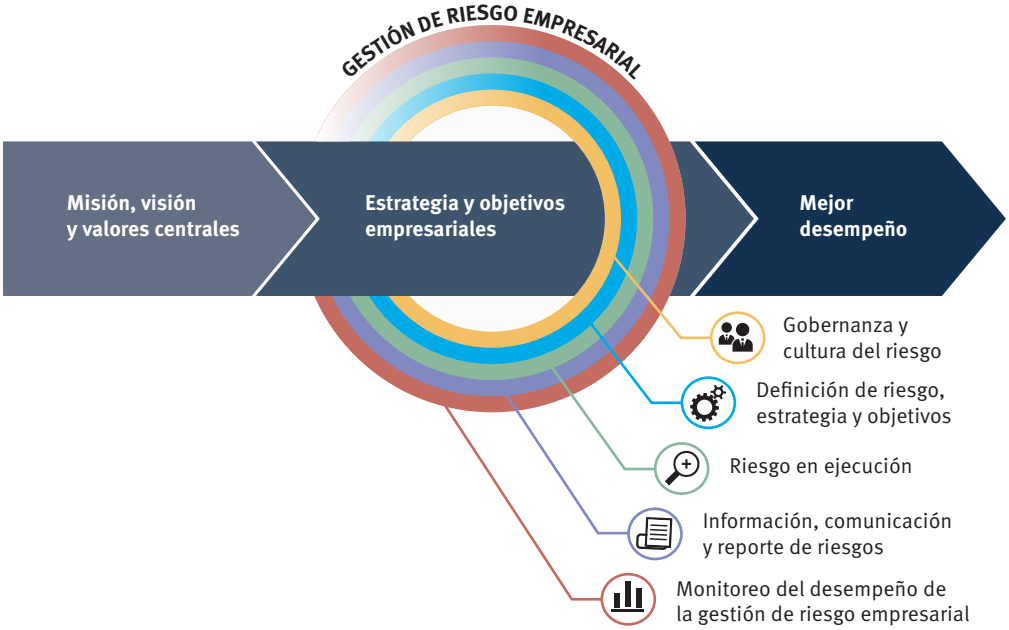
OBJETIVOS
Mejorar la alineación entre rendimiento y ERM
Ajustar las expectativas de gobierno y supervisión
Reconocer la globalización y la necesidad de aplicar un enfoque común pero ajustado a la medida
Presentar nuevas formas de ver el riesgo al establecer y alcanzar objetivos en un contexto de una mayor complejidad
Expandir los informes para lograr una mayor transparencia
Ajustarse a la evolución de la tecnología

En resumen, se puede decir que esta actualización renombra el marco como "ERM, alineación del riesgo con la estrategia y el rendimiento". Esta actualización también reconoce la importancia de la estrategia y el desempeño de la entidad e

TABLA 2. Evolución de COSO hasta 2006

	1934	1985	1992	2001/02	SOx 02	2003	2006
EE.UU.	**SEC**	**Inicio de COSO**	**Marco de control de COSO**	**Mayores escándalos financieros**	**Sarbannes Paul, Oxley Michael** (Senadores de EE.UU.) **= Ley SOx** **NIIF y NIA**	**Reporte de credibilidad de IFAC** **NIIF y NIA**	**Informes financieros de COSO** **NIIF y NIA**
UE y resto del mundo		↓		Mayores escándalos financieros	Ley canadiense 198, Loi sur la Secutité Française, código Turnbull del Reino Unido, J-SOx (2007) en Japón NIIF y NIA	Directrices europeas sobre control interno NIIF y NIA	Directrices europeas NIIF y NIA

FIGURA 1. ERM 2017



Source: https://commsrisk.com/new-coso-erm-framework-out-for-comment

integra la gestión del riesgo con la toma de decisiones. Es posible pensar que el marco COSO ERM podría responder algunas preguntas, sugerencias y críticas hechas por la literatura. La nueva figura de COSO ya no será el famoso cubo, sino esta nueva (Figura 1):

La estructura de cubo fue transformada hacia un proceso COSO ERM como un nuevo enfoque de gestión de riesgos y es una forma de transformar los insumos en productos. Significa que la perspectiva de ERM para cualquier tipo de organización se basa en un conocimiento profundo de la misión, visión y valores centrales de la misma, lo que es crucial para comprender los riesgos asociados. Esta creencia generalmente proviene de la alta gerencia, combinada con una buena administración de los recursos humanos y materiales de la organización para mejorar su desempeño. Para lograrlo, se debe considerar la organización bajo una perspectiva de marco de riesgos: la gobernanza del riesgo y la cultura asociada a lo más alto de la jerarquía; la estrategia de riesgo vinculada al establecimiento de objetivos conectados a las unidades estratégicas de negocios; el riesgo en ejecución, que se refiere a abordar el riesgo encontrado en las diferentes áreas o sectores y la comunicación de riesgos, que debe informar a todas las partes involucradas en la organización sobre el estado del arte del entorno de riesgo específico. Por último, este proceso de análisis de riesgos hace una evaluación final de su existencia, pues debe monitorear el desempeño de la empresa en cuanto a la gestión de riesgos. Esta parte probablemente es difícil de lograr. Para llevar a cabo una ERM eficaz, se debe realizar un análisis de riesgos profundo, ya que los puntos y las razones de los eventos que presentan un riesgo son tantos y tan diferentes que cuando la evaluación se realiza sobre un riesgo, puede surgir otro que no se había estimado previamente. Sin embargo, este nuevo marco de COSO ERM parece ser distinto al anterior. Se puede decir que esta actualización de COSO finalmente es una reacción a todas las críticas y sugerencias hechas a lo largo de los años. La literatura, como se explica a continuación, reveló algunas opiniones que distaban bastante de la inspiración tradicional de COSO descrita en el cubo de gestión de riesgos.

Algunas críticas hechas a COSO

Demidenko y MacNutt (2010) afirman que debe considerarse una escala de madurez ética basada en el deber y la responsabilidad de la implementación práctica para garantizar una mejor

gobernanza, además de contribuir con principios teóricos al debate sobre la buena gobernanza y la ética de la gestión de riesgo empresarial (ERM).

Williamson (2007) dice que el marco de COSO (2004) sobre gestión de riesgo empresarial es una valiosa contribución a la práctica emergente de ERM, pero tiene serias limitaciones al no proporcionar un estándar viable para identificar la efectividad de ERM. Su definición de riesgo desvía la atención de las oportunidades y de las incertidumbres que quedan fuera de su perspectiva de sistemas racionales cerrados. Al adoptar un enfoque de orden y control, ignora la gestión de incertidumbres compartida con partes externas y las implicaciones sociales de ERM. Como resultado, se crearán amenazas si se sigue ampliamente este marco, lo que parece probable ya que la ERM se institucionaliza dentro de las regulaciones, la práctica profesional y las normas de buena gestión esperadas. Además, una encuesta canadiense en 2007 que analizó el enfoque de COSO reveló que las principales debilidades técnicas del marco COSO ERM eran las siguientes:

Estas críticas parecen haber sido consideradas por el nuevo COSO ERM 2017. En lugar de un cubo, tenemos un proceso con una entrada y una salida teniendo en cuenta el evento cultural, un aspecto muy importante que no se mencionaba en el esquema anterior. Además de este nuevo enfoque de COSO, debemos mencionar que muchas empresas han utilizado una solución alternativa: ISO 31000.

ISO 31000

Muchas empresas prefieren usar este estándar para la gestión de riesgos porque es más fácil trabajar con él. Su contenido se resume brevemente en la figura 2 y la información específica se describe en el anexo 1:

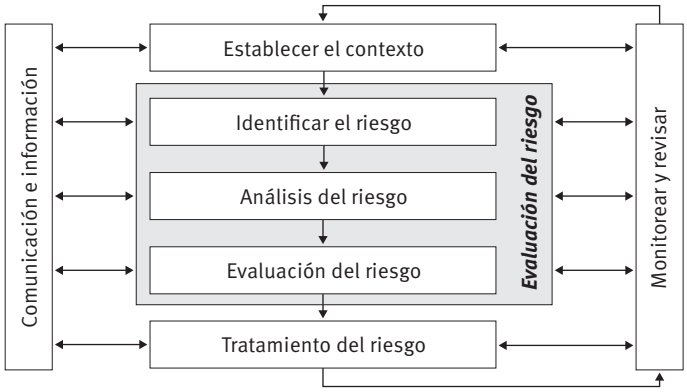
- **Establecer el contexto:** en primer lugar, la empresa tiene que definir el contexto para el análisis de riesgos y esto significa los límites del desarrollo de la actividad de la organización que pueden ser afectados por el riesgo. De esta manera, estamos definiendo el alcance de la aplicación del análisis de riesgos. Algunas características de la empresa que serán consideradas para este propósito son el entorno, los valores, la jerarquía, el liderazgo y el objetivo de la organización. Esto prácticamente encaja en el concepto de entrada del nuevo marco COSO ERM.
- **Evaluación del riesgo:** debe considerarse el contexto mencionado y el riesgo debe ser identificado, analizado y evaluado. El riesgo del contexto se evalúa siguiendo la estructura de la organización. Posteriormente, se analiza su origen y los efectos que se produzcan. Solo cuando se culminen estas fases se puede tener una idea de cuánto importa ese riesgo, es decir, de su importancia o relevancia.
- **Tratamiento del riesgo**: esta es la última fase del proceso y se refiere a todos los procedimientos necesarios para evitar que el riesgo se materialice.

TABLA 4. Algunas debilidades de COSO

DEBILIDADES TÉCNICAS DE COSO ERM	
Está enfocado internamente y el contexto no está establecido en términos de factores externos e internos ni influencias	Las “respuestas al riesgo”, las “actividades de control” y el “monitoreo” se confunden. “Control” se usa como un verbo y como sustantivo
Se ignoran las partes interesadas y su objetivo en términos de establecer los criterios de riesgo	Se dice que los riesgos “ocurren” y la probabilidad es cuándo ocurren
Los riesgos se ven como eventos, no se asocian al efecto de la incertidumbre en los objetivos	Se usa el riesgo inherente, concepto bastante confuso y defectuoso que es innecesario.
El riesgo se estima incorrectamente en términos de la probabilidad de un evento y sus consecuencias. Esto produce ‘riesgos fantasmas’ y no lleva a un tratamiento efectivo y apropiado del riesgo	El “apetito de riesgo” y la “tolerancia al riesgo” se mezclan y confunden. Se consideran de manera ingenua y simplista
Los riesgos solo se ven con una luz negativa y el tratamiento del riesgo (respuesta) solo se relaciona con su mitigación	La descripción del proceso de gestión de riesgos se mezcla con el marco requerido para la implementación efectiva de la gestión de riesgos mediante la integración

Fuente: Canadian Survey, 2007

FIGURA 2. ISO 31000: 2009



Adaptado de: http://broadleaf.com.au/resource-material/iso-31000-2009-setting-a-new-standard-for-risk-management

Después de la implementación de ISO 31000 en una organización, todos estos pasos (contexto, evaluación del riesgo y tratamiento del riesgo) deben ser monitoreados y continuamente auditados. Las conclusiones finales se abordan y se comunican a todas las personas involucradas en este proceso en la organización. Parece ser una manera simple de enfrentar y posicionar los riesgos de la organización. Es posible establecer la siguiente comparación entre el nuevo proceso de COSO ERM e ISO 31000.

Los números usados en la tabla anterior de ISO 31000 se usarán para identificar las áreas equivalentes en ERM 2017, como puede observarse en la tabla 6.

A continuación se presenta una explicación de la tabla 5 (números del 1 al 5), también conocida como ISO 31000:

1. Establecer el contexto / gobernanza y cultura del riesgo: riesgo de contexto significa el alcance de la aplicación del análisis de riesgo. Para ello, se considerarán algunas características de la empresa como entorno, valores, jerarquía, liderazgo y objetivo de la organización. Bajo ISO, la estrategia de riesgo y los objetivos se incluyen en este contexto, mientras que para ERM 2017 son autónomos. Esto casi se ajusta a la gobernanza y cultura del riesgo del nuevo COSO. La gobernanza del riesgo es una especie de concepto sombrilla

TABLA 5. Breve resumen de ISO 31000

ISO 31000:2009		
Comunicación y consultoría	Establecer el contexto	Monitorear y revisar
	Evaluación del riesgo	
	Identificación	
	Análisis	
	Evaluación	
	Tratamiento del riesgo	

TABLA 6. COSO ERM 2017

ERM 2017 – NUEVO PROCESO	CONEXIÓN CON LA ESTRUCTURA ORGANIZACIONAL
Gobernanza y cultura del riesgo (1)	Alta dirección
Estrategia de riesgos / establecimiento de objetivos (1) y (2.1)	Unidades estratégicas de negocio (UEN)
Riesgo en ejecución (2.2) y (2.3)	Nivel funcional
Información, comunicación y reporte de riesgos (4)	Sistemas de información de gestión y análisis de riesgos
Monitoreo del desempeño de ERM (5)	Todos los procesos de la organización

que cubre el riesgo de la empresa y la cultura significa la percepción de los valores que son importantes para el desarrollo de la actividad de la empresa. Esto generalmente se obtiene del contacto con la alta dirección de la compañía.

2. La evaluación de riesgos es un elemento que solo pertenece a ISO y significa evaluación de riesgos como resultado de:

— Identificación de riesgo, que para ERM 2017 está asociada a establecer el objetivo.

— Análisis del riesgo mediante la búsqueda de sus causas, lo que para ERM 2017 se denomina riesgo en ejecución.

— Evaluación de riesgos, algo que en esta etapa de análisis solo es considerado por ISO 31000, lo que significa que después de identificar y analizar el riesgo, podemos evaluarlo. Para ERM 2017, esto se hace al final mediante la medición del desempeño de la empresa luego de implementar la gestión de riesgos (5).

3. El tratamiento de riesgos para ISO significa que algo realmente se hizo y todos los procedimientos necesarios se llevaron a cabo para evitar que el riesgo sucediera. En COSO, este aspecto se puede encontrar en la última fase: monitoreo del desempeño de ERM (5).
4. Mientras que "comunicación y consultoría" está presente en cada parte del proceso bajo ISO, para ERM 2017 aparece al final (4).
5. El monitoreo y la revisión se incluyen tanto en ISO como en ERM 2017. Bajo ISO, es un proceso interactivo aplicable en cada momento de cada etapa del proceso y ERM se enfoca en la gestión de riesgos con la intención de evaluar su desempeño en la empresa.

Conclusión

Es bien sabido que un buen control de los procedimientos internos de cualquier tipo de organización ayudará al proceso de auditoría, pues permite cierta seguridad sobre la opinión acerca de los estados financieros respectivos.

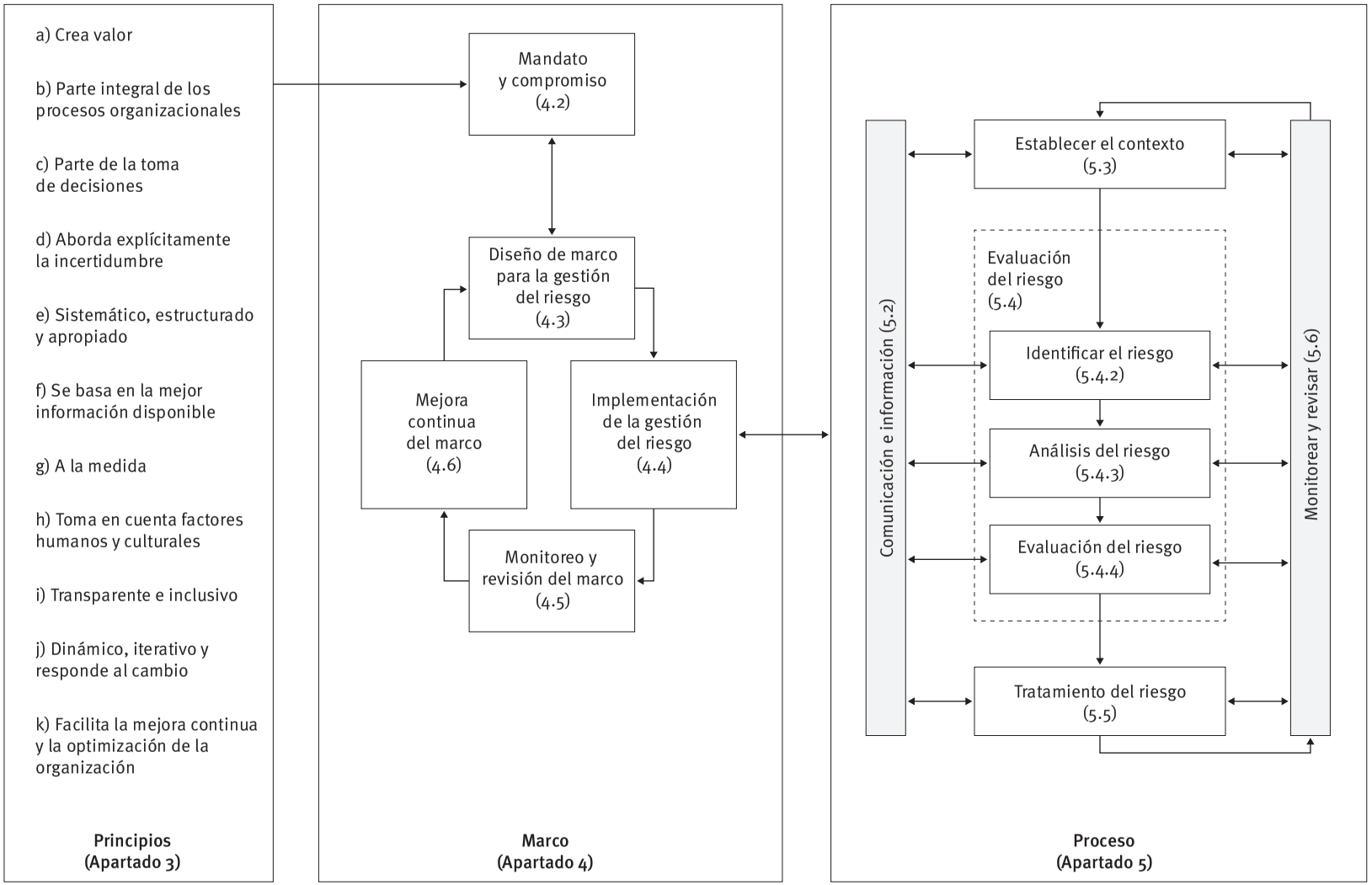
Según la literatura (Williamson, 2007; Demidenko y MacNutt, 2010), COSO se consideraba como una perspectiva desafiante. Luego se describió ERM 2017 e ISO 31000: 2009 (gestión del riesgo) se consideró como una alternativa. Ambos grupos de lineamientos fueron considerados y comparados en función de la gestión del riesgo. Se analizaron los contenidos de ambos y es posible sostener que los dos se enfocan en las mismas áreas. Sin embargo, parece que ISO fue bastante innovadora mucho antes de la actualización de ERM en 2017.

La implementación dependerá del perfil de la organización y de la probabilidad de un uso diferente de las pautas de riesgo. Para las empresas que solían trabajar con ISO, sobre todo las que tienen la certificación de calidad ISO 9001, probablemente trabajar con ISO 31000 sería la mejor opción. Sin embargo, es importante decir que esta nueva versión de ERM parece estar muy bien adaptada al mercado global, así como a sus organizaciones.

Posibles investigaciones futuras

En términos de investigación futura, podría sugerirse la identificación de organizaciones que usan un esquema u otro (ERM o ISO) y compararlas para evaluar su efectividad particular y valor acumulado.

ANEXO 1. Relaciones entre principios, marco y procesos de gestión del riesgo



REFERENCES

Accounting Theory, (2004) 4th Edition, U.K, Business Press Thomson Learning

Anomaly, Jonny & Brennan, Geoffrey (2014). Social Norms, The Invisible Hand, and the Law. *University of Queensland Law Journal* 33 (2).

Bruton, Ahlstrom, Li (2010) Institutional Theory and Entrepreneurship: Where Are We Now and Where Do We Need to Move in the Future? *Entrepreneurship Theory and Practice,*3 (3) pp 421–440

Dermot Williamson (2007). The COSO ERM framework: a critique from systems theory of management control, *International Journal of Risk Assessment and Management*, 7(8), pp 1089-1119 **doi:** http://dx.doi.org/10.1504/IJRAM.2007.015296

Dion, M.(2001), 'Corporate Citizenship and Ethics of Care: Corporate Values, Codes of Ethics and Global Governance', in J. Andriof and M. McIntosh (ed.), *Perspectives on Corporate Citizenship* (Greenleaf, Sheffield, UK), pp. 118–138

Donaldson, Preston (1995) The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications *Academy of Management Review, vol. 20 , 1, pp 65-91*

Elena Demidenko, Patrick McNutt (2010). "The ethics of enterprise risk management as a key component of corporate governance", *International Journal of Social Economics*, 37 (10), pp.802-815, doi: 10.1108/03068291011070462

Frynas G., Stephan S., (2015) Political Corporate Social Responsibility: Reviewing Theories and Setting New Agendas, *International Journal of Review Management*, 17(4), pp. 483–509

IIA Institute of Internal Auditors - Global Technology Audit Guide (GTAG®) 1 Information Technology Risk and Controls (2012)

Mark C. Suchman (1995) Managing Legitimacy: Strategic and Institutional Approaches ,*Academy Management Review , 20(3) 571-610;*

Merton, R., Peron, A.,(1993) Theory of risk capital in financial firms, *Applied Corporate Finance,* 6 (3), pp 16–32

OECD (2014), *Risk Management and Corporate Governance*, Corporate Governance, OECD Publishing. *http://dx.doi.org/10.1787/9789264208636-en*

Omolehinwa, O. (2003), Foundation of Accounting, Lagos Pumark Nigeria Ltd.

Ponemon Institute LLC (2013), *The State of Risk-Based Security*.

Schroeder, H. (2014), "An art and science approach to strategic risk management", *Strategic Direction*, Vol. 30 No 4 2014, pp. 28-30.

Wolk Harry I, Dodd James L and Rozycki John J (2008). Accounting Theory: Conceptual Issues in a Political and Economic Environment, 7th edition, Sage Publications Inc. California

World Business Council for Sustainable Development (**WBCSD**) http://www.wbcsd.org/.

World Economic Forum (2016), *The Global Risks Report 2016*, 11th edition.

On line references

Canada Survey (2007): n*a.theiia.org/standardsguidance/Public%20Documents/IIA_Risk_Summit_Practitioner_Answers.pdf*

ISO 31000:2009 *http://broadleaf.com.au/resource-material/iso-31000-2009-setting-a-new-standard-for-risk-management*

COSO ERM 2017 https://commsrisk.com/new-coso-erm-framework-out-for-comment