



Committee of Sponsoring Organizations of the Treadway Commission

Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño

Resumen Ejecutivo



Junio 2017

Traducción al español



Este proyecto ha sido encargado por COSO (Committee of Sponsoring Organizations of the Treadway Commission), una organización que actúa como líder de pensamiento organizacional mediante el desarrollo de marcos y orientaciones generales sobre control interno, gestión del riesgo empresarial y disuasión del fraude dirigidos a mejorar el desempeño organizacional y la supervisión, así como a reducir el nivel de fraude en las organizaciones. COSO es una iniciativa del sector privado, patrocinada y financiada conjuntamente por:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

Committee of Sponsoring Organizations of the Treadway Commission

Miembros del Consejo

Robert B. Hirth Jr.
Presidente de COSO

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Autor

Principales Colaboradores

Miles E.A. Everson
Engagement Leader and Global and Asia, Pacific, and Americas (APA) Advisory Leader
Nueva York, EE.UU.

Dennis L. Chesley
Project Lead Partner and Global and APA Risk and Regulatory Leader
Washington DC, EE.UU.

Frank J. Martens
Project Lead Director and Global Risk Framework and Methodology Leader
British Columbia, Canadá

Matthew Bagin
Director
Washington DC, EE.UU.

Hélène Katz
Director
Nueva York, EE.UU.

Katie T. Sylvis
Director
Washington DC, EE.UU.

Sallie Jo Perraglia
Manager
Nueva York, EE.UU.

Kathleen Crader Zelnik
Manager
Washington DC, EE.UU.

Maria Grimshaw
Senior Associate
Nueva York, EE.UU.

Prólogo

En coherencia con la misión general que le ha sido encomendada, el Consejo de COSO encargó y publicó en 2004 el *Marco Integrado de Gestión del Riesgo Empresarial*. En los últimos diez años, esta publicación ha conseguido una amplia aceptación por parte de las organizaciones en sus esfuerzos por gestionar el riesgo. Sin embargo, también a lo largo de ese período, la complejidad del riesgo ha cambiado, han surgido nuevos riesgos y tanto los consejos de administración como los directivos han mejorado su conocimiento y su supervisión de la gestión del riesgo empresarial, al tiempo que demandan una mejor información sobre riesgos. La presente actualización de la publicación de 2004 aborda la evolución de la gestión del riesgo empresarial y la necesidad de que las organizaciones mejoren su enfoque de gestión del riesgo para satisfacer las exigencias de un entorno de negocio en continua evolución.

El documento actualizado lleva por título *Gestión del Riesgo Empresarial—Integrando Estrategia y Desempeño*, y pone de manifiesto la importancia de tener en cuenta el riesgo tanto en el proceso de definición de la estrategia como en la ejecución del desempeño. La primera parte de la publicación actualizada ofrece una perspectiva sobre los conceptos y aplicaciones actuales de la gestión del riesgo empresarial, que se encuentran en continua evolución. La segunda parte —*el Marco*— está organizada en cinco componentes fáciles de comprender que se adaptan a diferentes puntos de vista y estructuras operativas, y mejoran las estrategias y la toma de decisiones. En pocas palabras, esta actualización:

- Proporciona una mayor comprensión del valor de la gestión del riesgo empresarial al definir y llevar a cabo la estrategia.
- Mejora la alineación entre el desempeño y la gestión del riesgo empresarial para mejorar la definición de objetivos de desempeño y la comprensión del impacto del riesgo en el desempeño.
- Se adapta a las expectativas de gobierno y supervisión.
- Reconoce la globalización de los mercados y las operaciones y la necesidad de aplicar un enfoque común, aunque adaptado, en las distintas geografías.
- Presenta nuevas formas de concebir el riesgo para definir y alcanzar objetivos en un contexto de mayor complejidad empresarial.
- Amplía el concepto relacionado con el reporte de información para responder a las expectativas de mayor transparencia de las distintas partes interesadas.
- Se adapta a la evolución de las tecnologías y a la proliferación de datos y análisis para facilitar la toma de decisiones.
- Establece definiciones, componentes y principios básicos para todos los niveles de gestión que participan en el diseño, implantación y ejecución de técnicas de gestión del riesgo empresarial.

Asimismo, se pone a disposición de los lectores la publicación complementaria *Control Interno—Marco Integrado* de COSO. Estas dos publicaciones son distintas y siguen enfoques diferentes, por lo que una no reemplaza a la otra. Sin embargo, ambas publicaciones están relacionadas. *Control Interno—Marco Integrado* aborda el control interno, al que se hace referencia en parte en esta publicación actualizada, por lo que el documento anterior sigue siendo viable y adecuado para diseñar, implantar, llevar a cabo y evaluar el control interno, así como para la presentación de informes posteriores.

El Consejo de COSO desea agradecer a PwC su destacada aportación al desarrollo de *Gestión del Riesgo Empresarial—Integrando Estrategia y Desempeño*. Su consideración plena de las aportaciones realizadas por las múltiples partes interesadas y sus análisis de valor han sido decisivos para garantizar que se hayan conservado los puntos fuertes de la publicación original, al tiempo que estos se han aclarado o ampliado en caso oportuno. El Consejo de COSO y PwC también desean agradecer al Consejo Asesor y a los Observadores sus aportaciones durante la revisión de la información, así como las sugerencias y comentarios ofrecidos.



Robert B. Hirth Jr.
Presidente de COSO



Dennis L. Chesley
Socio Responsable del Proyecto en PwC y
APA Risk and Regulatory Leader

Prólogo a la traducción

En un mundo cada vez más incierto y volátil, la gestión de riesgos ha ganado cada vez más importancia en las organizaciones y es una pieza clave a la hora de definir, adaptar e implantar la estrategia empresarial. La última crisis económica y financiera, cuyas consecuencias son hoy todavía visibles en muchos países, es un ejemplo manifiesto de la trascendencia del control de los riesgos empresariales y del buen gobierno corporativo en la gestión de las empresas.

Los riesgos (externos e internos) son cada vez más complejos y se entrelazan entre sí. Los cambios en el mercado y en el entorno geopolítico, las exigencias regulatorias, la seguridad de la cadena de suministros, la intensa competencia y los riesgos derivados de la tecnología son algunas de las incertidumbres que rodean la gestión de las empresas y su creciente dificultad exige una respuesta estratégica adecuada. Los consejos de administración, en particular, son responsables de garantizar que esa respuesta se traslade de forma eficiente a todas las fases de la gestión empresarial, desde la planificación estratégica y de negocio hasta la ejecución operacional y el control de los procesos.

Por todo ello, el Instituto de Auditores Internos de España, con la colaboración de PwC, ha editado la versión española del informe *Gestión del riesgo empresarial. Integrando estrategia y desempeño*, elaborado por COSO (Sponsoring Organizations of the Treadway Commission). El estudio constituye una valiosa aportación a la praxis de la gestión de los riesgos empresariales y ayudará a dirigir mejor las empresas, a aumentar su valor real en el largo plazo y a transmitir confianza a la sociedad.

Gonzalo Sánchez
Presidente
PwC España

Ernesto Martínez
Presidente
Instituto de Auditores Internos de España

El cambiante entorno de riesgos

Nuestra comprensión de los riesgos, esto es, el componente de “arte” y de “ciencia” de cada una de las opciones que elegimos, es una pieza clave de nuestra economía moderna. Cada elección que hacemos para la consecución de nuestros objetivos tiene sus riesgos. Desde las decisiones operativas de nuestro día a día hasta las decisiones clave adoptadas en los consejos de administración, la gestión del riesgo en todas estas elecciones forma parte de la toma de decisiones.

Dado que normalmente tratamos de conseguir una serie de resultados posibles, las decisiones rara vez son binarias, esto es, casi nunca tienen una única respuesta correcta o incorrecta. Por eso la gestión del riesgo empresarial puede considerarse tanto un arte como una ciencia. Y cuando se tiene en cuenta el riesgo a la hora de formular los objetivos estratégicos y de negocio de una organización, la gestión del riesgo empresarial contribuye a optimizar los resultados.

Nuestra comprensión del riesgo y nuestras prácticas de gestión del riesgo empresarial han mejorado enormemente en las últimas décadas. Pero el margen de error se está reduciendo. En el último Foro Económico Mundial se ha resaltado la “creciente volatilidad, complejidad y ambigüedad existente en el mundo”¹ Se trata de un fenómeno que todos reconocemos. Las organizaciones se enfrentan a desafíos que afectan a la fiabilidad, a la relevancia y a la confianza. Hoy en día, las distintas partes interesadas están más comprometidas y buscan una mayor transparencia y rendición de cuentas a la hora de gestionar el impacto del riesgo, al tiempo que evalúan de manera crítica la capacidad de los equipos de dirección para aprovechar las oportunidades. Incluso el éxito puede conllevar un riesgo, por ejemplo, el riesgo de no poder satisfacer una demanda inesperadamente alta o mantener el impulso comercial esperado.

Las organizaciones deben adaptarse en mayor medida al cambio. Han de pensar de forma estratégica cómo manejar la creciente volatilidad, complejidad y ambigüedad del entorno actual, especialmente en las altas esferas de la organización y en los consejos de administración, en donde hay mucho más en juego.

Gestión del Riesgo Empresarial-Integrando Estrategia y Desempeño constituye un marco de trabajo para consejos de administración y equipos de dirección de entidades de cualquier tamaño. Este Marco profundiza en el nivel actual de gestión de riesgos que existe en el curso ordinario de las actividades de negocio. Asimismo, demuestra cómo la integración de las prácticas de gestión del riesgo empresarial en toda la entidad contribuye a acelerar el crecimiento y a mejorar el desempeño. Además, contiene principios que pueden aplicarse en la práctica, desde la toma de decisiones estratégicas hasta la consecución de resultados.

A continuación, explicamos por qué tiene sentido que los equipos de dirección y los consejos de administración utilicen el marco de gestión del riesgo empresarial², qué han logrado las organizaciones aplicando la gestión del riesgo empresarial y qué otros beneficios se pueden obtener mediante su uso continuado. Por último, concluimos nuestro informe con una mirada hacia el futuro.

Guía de gestión del riesgo empresarial para la dirección

El equipo de dirección tiene la responsabilidad general de gestionar el riesgo para la entidad, pero es importante que vaya más allá: mejorando el diálogo entre el consejo de administración y las distintas partes interesadas sobre el uso de la gestión del riesgo empresarial para obtener una ventaja competitiva. Para ello, ha de empezar por la implantación de capacidades de gestión del riesgo empresarial como parte de la selección y el perfeccionamiento de la estrategia.

¹ Informe de riesgos mundiales 2017, 11ª edición, Foro Económico Mundial (2016).

² El Marco usa el término “consejo de administración” o “consejo” para referirse al máximo órgano de gobierno, incluidos el consejo, el consejo de supervisión o vigilancia, los socios generales o los propietarios.

En particular, a través de este proceso, la dirección comprenderá mejor cómo, al considerar de manera expresa el riesgo, se puede influir en la elección de la estrategia. La gestión del riesgo empresarial enriquece el diálogo del equipo de dirección al añadir una mayor perspectiva sobre las fortalezas y debilidades de la estrategia a medida que cambian las condiciones y sobre lo bien que encaja la estrategia con la misión y visión de la organización. Permite a la dirección sentirse más segura de que se han analizado estrategias alternativas y se han tenido en cuenta las aportaciones de aquellos integrantes de la organización que implantarán la estrategia seleccionada.

Una vez que se establece la estrategia, la gestión del riesgo empresarial constituye una fórmula efectiva para que la dirección desempeñe su función, sabiendo que la organización está en sintonía con los riesgos que pueden impactar en la estrategia y que los está gestionando bien. La aplicación de la gestión del riesgo empresarial ayuda a generar confianza y seguridad en las distintas partes interesadas con respecto al entorno actual, lo que exige un mayor análisis que antes sobre la forma en la que se abordan los riesgos y si se están gestionando activamente o no.

Guía de gestión del riesgo empresarial para el consejo de administración

Los consejos de administración desempeñan una función de supervisión que ayuda a apoyar la creación de valor en una entidad y a evitar su declive. Tradicionalmente, la gestión del riesgo empresarial ha ocupado un sólido papel de apoyo a nivel del consejo. Ahora se espera, cada vez más, que los consejos de administración supervisen la gestión del riesgo empresarial.

El Marco ofrece consideraciones importantes para que los consejos de administración puedan definir y abordar sus responsabilidades de supervisión del riesgo. Estas consideraciones incluyen el gobierno y la cultura; la estrategia y el establecimiento de objetivos; el desempeño; la información, las comunicaciones y el reporte; y la revisión y monitorización de las prácticas y técnicas para mejorar el desempeño de las entidades.

Preguntas para la dirección

¿Son capaces todos los integrantes del equipo de dirección —y no solo el director de riesgos— de expresar cómo se tiene en cuenta el riesgo a la hora de seleccionar la estrategia o en la toma de decisiones del negocio? ¿Pueden articular claramente el apetito al riesgo de la entidad y cómo podría influir en una decisión específica? Las respuestas a estas preguntas pueden arrojar luz sobre cuál es realmente la mentalidad de asunción de riesgos en la organización.

Los consejos de administración también pueden pedir a los miembros de la alta dirección que analicen no sólo los procesos de riesgo sino también la cultura. ¿En qué medida permite o impide la cultura una asunción responsable de riesgos? ¿Qué perspectiva adopta la dirección para efectuar un seguimiento de la cultura de riesgos y cómo ha cambiado dicha perspectiva? A medida que el entorno evolucione —y sin duda alguna evolucionará, independientemente de que lo detecte o no la entidad— ¿cómo puede el consejo de administración confiar en que el equipo de dirección será capaz de dar una respuesta adecuada y oportuna?

La función de supervisión de riesgos del consejo de administración puede incluir, pero sin limitarse a ello:

- Revisar, cuestionar y acordar con la dirección:
 - La estrategia propuesta y el apetito al riesgo.
 - La alineación de la estrategia y los objetivos de negocio con la misión, visión y valores clave de la entidad.
 - Las principales decisiones de negocio, incluidos aspectos como fusiones, adquisiciones, asignaciones de capital, financiación y decisiones relacionadas con dividendos.
 - La respuesta a dar ante fluctuaciones significativas en el desempeño de la entidad o en la visión del riesgo a nivel de cartera.
 - Las respuestas ante casos de desviación con respecto a los valores clave.
- Aprobar los incentivos y remuneración del equipo de dirección.
- Participar en la relación con inversores y demás partes interesadas.

A más largo plazo, la gestión del riesgo empresarial también puede mejorar la resiliencia de las empresas —la capacidad de anticipar y responder ante el cambio. Ayuda a las organizaciones a identificar los factores que representan no sólo el riesgo, sino también el cambio, y cómo ese cambio podría afectar al desempeño y exigir un cambio en la estrategia. Al ver estos cambios con mayor claridad, una organización puede elaborar su propio plan; por ejemplo, ¿debe retirarse o invertir en un nuevo negocio? La gestión del riesgo empresarial proporciona el marco adecuado para que los consejos de administración evalúen el riesgo y adopten una mentalidad de resiliencia.

Logros de la gestión del riesgo empresarial

COSO publicó en 2004 el *Marco Integrado de Gestión del Riesgo Empresarial*. El propósito de esa publicación era ayudar a las entidades a proteger y a aumentar el valor para las distintas partes interesadas. Su filosofía subyacente era que “el valor se maximiza cuando el equipo de dirección establece la estrategia y los objetivos para lograr un equilibrio óptimo entre las metas de crecimiento y rentabilidad y los riesgos relacionados, y despliega los recursos de manera eficiente y efectiva para alcanzar los objetivos de la entidad.”³

Desde su publicación, el *Marco* se ha utilizado con éxito en todo el mundo, en todos los sectores y en organizaciones de todo tipo y tamaño para identificar riesgos, gestionar dichos riesgos dentro de un apetito al riesgo definido y facilitar la consecución de objetivos. Sin embargo, si bien es cierto que multitud de organizaciones ya han aplicado el *Marco* en la práctica, la realidad es que puede utilizarse en mayor medida. Asimismo, el *Marco* se beneficiaría de un análisis en mayor profundidad y con mayor claridad de determinados aspectos, y de una mejor comprensión de los vínculos existentes entre la estrategia, el riesgo y el desempeño. Por tanto, como respuesta a ello, el *Marco* actualizado en esta publicación:

- Conecta más claramente la gestión del riesgo empresarial con una amplia serie de expectativas de las distintas partes interesadas.
- Posiciona el riesgo en el contexto del desempeño de una organización, en lugar de ser el objeto de un ejercicio aislado.
- Permite a las organizaciones anticiparse mejor al riesgo para que puedan adelantarse a él, entendiendo que el cambio crea oportunidades y no solo crisis potenciales.

Esta actualización también responde a la petición de que se haga un mayor hincapié en cómo la gestión del riesgo empresarial dota de información a la estrategia y a su desempeño.

Beneficios de una gestión eficaz del riesgo empresarial

Todas las organizaciones deben establecer una estrategia y ajustarla periódicamente, siendo conscientes siempre de las oportunidades en constante cambio para crear valor y de los desafíos que se presentarán en la búsqueda de ese valor. Para ello, necesitan el mejor marco posible para optimizar la estrategia y el desempeño.

Y es ahí donde entra en juego la gestión del riesgo empresarial. Las organizaciones que integran la gestión del riesgo empresarial a todos los niveles de la entidad pueden conseguir muchos beneficios, entre otros (aunque sin limitarse a ellos):

- *Aumentar la gama de oportunidades disponibles:* Al tener en cuenta todas las posibilidades –tanto los aspectos positivos como negativos del riesgo– la dirección puede identificar nuevas oportunidades y desafíos únicos asociados con las oportunidades actuales.

Despejando falsas creencias

Hemos escuchado algunos conceptos erróneos sobre el *Marco* original desde que se introdujo en 2004. Para que no haya dudas:

La gestión del riesgo empresarial no es una función ni un departamento. Es la cultura, las capacidades y las prácticas que las organizaciones integran con el proceso de definición de la estrategia y aplican cuando la llevan a la práctica, con el propósito de gestionar el riesgo a la hora de crear, preservar y materializar el valor.

La gestión del riesgo empresarial va más allá de un mero listado de riesgos. Requiere algo más que hacer un inventario de todos los riesgos de la organización. Es un ejercicio más amplio e incluye prácticas que la dirección debe poner en marcha para gestionar activamente el riesgo.

La gestión del riesgo empresarial abarca más que el control interno. También aborda otros temas como el establecimiento de la estrategia, la gobernanza, la comunicación con las distintas partes interesadas y la medición del desempeño. Sus principios son aplicables en todos los niveles de la organización y en todas las funciones.

La gestión del riesgo empresarial no es una “lista de verificación”. Es un conjunto de principios sobre los cuales se pueden construir o integrar procesos para una organización en particular, y es un sistema de seguimiento, aprendizaje y mejora del desempeño.

La gestión del riesgo empresarial puede ser utilizada por organizaciones de cualquier tamaño. Si una organización tiene una misión, una estrategia y unos objetivos —y la necesidad de tomar decisiones que tengan plenamente en cuenta el riesgo— podrá aplicar la gestión del riesgo empresarial. Puede y debe ser utilizada por todo tipo de organizaciones, desde pequeñas empresas hasta organizaciones no gubernamentales, pasando por organismos públicos y grandes compañías del Fortune 500.

³ *Marco Integrado de Gestión del Riesgo Empresarial, Resumen Ejecutivo, COSO (2004).*

- *Identificar y gestionar el riesgo en toda la entidad:* Cada entidad se enfrenta a innumerables riesgos que pueden afectar a muchas partes de la organización. A veces, un riesgo puede originarse en una parte de la entidad, pero puede afectar a otra parte diferente. En consecuencia, la dirección identifica y gestiona estos riesgos a nivel de toda la entidad para sostener y mejorar el desempeño.
- *Aumentar los resultados positivos y las ventajas a la vez que se reducen las sorpresas negativas:* La gestión del riesgo empresarial permite a las entidades mejorar su capacidad para identificar riesgos y establecer respuestas adecuadas, reduciendo las sorpresas y costes o pérdidas relacionados, al tiempo que se benefician de los nuevos desarrollos.
- *Reducir la variabilidad del desempeño:* Para algunas organizaciones, el verdadero desafío no tiene tanto que ver con las sorpresas y las pérdidas, sino más bien con la variabilidad del desempeño. Unos resultados que superen las expectativas o se adelanten a los calendarios previstos pueden causar tanta preocupación como unos resultados inferiores a las expectativas o retrasos en los calendarios. La gestión del riesgo empresarial permite que las organizaciones se anticipen a los riesgos que afectarían al desempeño e implanten las medidas necesarias para minimizar los trastornos y maximizar las oportunidades.
- *Mejorar el despliegue de recursos:* Todo riesgo puede considerarse una petición de recursos. Dado que los recursos son finitos, si se dispone de una información sólida sobre riesgos, la dirección puede evaluar las necesidades generales de recursos, establecer prioridades en su despliegue y mejorar su asignación.
- *Mejorar la resiliencia de las empresas:* La viabilidad a medio y largo plazo de una entidad depende de su capacidad para anticiparse y responder al cambio, no sólo para sobrevivir sino también para evolucionar y prosperar. Esto es posible, en parte, gracias a una gestión eficaz del riesgo empresarial. Es cada vez más importante a medida que se acelera el ritmo de cambio y aumenta la complejidad en el entorno empresarial.

Estos beneficios ponen de relieve el hecho de que el riesgo no debe considerarse únicamente como una limitación o un reto potencial a la hora de establecer y llevar a cabo una estrategia. Por el contrario, el cambio que subyace al riesgo y las respuestas de la organización ante el riesgo dan lugar a oportunidades estratégicas y a capacidades diferenciadoras clave.

El papel del riesgo en la selección de estrategias

La selección de la estrategia consiste en tomar decisiones y aceptar los pros y los contras. Por tanto, tiene sentido aplicar la gestión del riesgo empresarial a la estrategia, ya que se trata del mejor enfoque para diferenciar entre el componente de “arte” y de “ciencia” que intervienen en la toma de decisiones bien informadas.

El riesgo es un aspecto clave de muchos procesos de definición de estrategias. Sin embargo, a menudo evaluamos el riesgo principalmente en relación con su efecto potencial sobre una estrategia determinada. En otras palabras, las conversaciones se centran en los riesgos con respecto a una estrategia existente: Tenemos una estrategia en marcha, ¿qué podría afectar a la relevancia y viabilidad de nuestra estrategia?

Pero hay otras preguntas que hacer en torno a la estrategia, y a las organizaciones cada vez se les da mejor plantearlas: ¿Hemos modelado la demanda del cliente con precisión? ¿Cumplirá nuestra cadena de suministro las expectativas tanto en cuestiones de plazo como de presupuesto? ¿Emergerán nuevos competidores? ¿Está nuestra infraestructura tecnológica a la altura de las circunstancias? Estas son el tipo de preguntas que los directivos afrontan a diario, y responder a ellas es clave para implantar una estrategia.

Sin embargo, el riesgo con respecto a la estrategia elegida es sólo uno de los aspectos que se deben considerar. Como se subraya en este Marco, hay dos aspectos adicionales de la gestión del riesgo empresarial que pueden tener un efecto mucho mayor en el valor de una entidad: la

posibilidad de que la estrategia no esté alineada y las consecuencias resultantes de la estrategia elegida.

La primera de ellas, la **posibilidad de que la estrategia no esté alineada con la misión, visión y valores clave de una organización** es fundamental para las decisiones que subyacen en la selección de estrategias. Cada entidad tiene una misión, una visión y unos valores clave que definen lo que está tratando de conseguir y cómo quiere llevar a cabo sus actividades de negocio. Algunas organizaciones se muestran escépticas a la hora de adoptar verdaderamente su filosofía corporativa. Sin embargo, se ha demostrado que la misión, la visión y los valores clave son importantes, y más aún cuando se trata de gestionar el riesgo y demostrar resiliencia durante períodos de cambio.

La estrategia elegida debe apoyar la misión y la visión de la organización. Una estrategia que no esté alineada aumenta la posibilidad de que la organización no cumpla su misión y visión, o pueda comprometer sus valores, aun cuando la estrategia se lleve a cabo con éxito. Por tanto, la gestión del riesgo empresarial considera la posibilidad de que la estrategia no esté alineada con la misión y la visión de la organización.

El otro aspecto adicional son las **consecuencias resultantes de la estrategia elegida**. Cuando la dirección desarrolla una estrategia y baraja distintas alternativas con el consejo de administración, toman decisiones con respecto a los pros y los contras inherentes a dicha estrategia. Cada estrategia alternativa tiene su propio perfil de riesgos —esto es, las consecuencias que se derivan de la estrategia. El consejo de administración y la dirección deben determinar si la estrategia encaja con el apetito al riesgo de la organización y cómo ayudará a la organización a establecer objetivos y, en última instancia, a asignar los recursos de manera eficiente.

Por tanto, la clave es que: La gestión del riesgo empresarial tiene que ver tanto con comprender las consecuencias resultantes de la estrategia y la posibilidad de que la estrategia esté desalineada como con gestionar los riesgos para establecer los objetivos. La figura siguiente muestra estas consideraciones en el contexto de la misión, la visión, los valores clave, y como motor de la dirección y el desempeño general de una entidad.



La gestión del riesgo empresarial, tal y como se ha venido practicando, ha ayudado a muchas organizaciones a identificar, evaluar y gestionar los riesgos de la estrategia. Pero las causas más significativas de destrucción de valor están arraigadas en la posibilidad de que la estrategia no respalde la misión y visión de la entidad, y las consecuencias resultantes de la estrategia.

La gestión del riesgo empresarial mejora la selección de estrategias. Elegir una estrategia requiere una toma de decisiones estructurada que analice el riesgo y alinee los recursos con la misión y visión de la organización.

Un Marco claramente definido

Gestión del Riesgo Empresarial—Integrando Estrategia y Desempeño destaca la importancia de la gestión del riesgo empresarial en la planificación estratégica y su integración en todos los niveles de la organización, ya que el riesgo influye y alinea la estrategia y el desempeño en todos los departamentos y funciones.



El propio Marco es un conjunto de principios organizados en cinco componentes interrelacionados:

1. **Gobierno y cultura:** El Gobierno marca el tono en la entidad, reforzando la importancia de la gestión del riesgo empresarial y estableciendo responsabilidades de supervisión al respecto. La cultura hace referencia a los valores éticos, a los comportamientos deseados y a la comprensión del riesgo en la entidad.
2. **Estrategia y establecimiento de objetivos:** La gestión del riesgo empresarial, la estrategia y el establecimiento de objetivos funcionan juntos en el proceso de planificación estratégica. Se establece un apetito al riesgo y se alinea con la estrategia; los objetivos del negocio ponen en práctica la estrategia al tiempo que sirven de base para identificar, evaluar y responder ante el riesgo.
3. **Desempeño:** Es necesario identificar y evaluar aquellos riesgos que puedan afectar a la consecución de los objetivos estratégicos y de negocio. Los riesgos se priorizan en función de su gravedad en el contexto del apetito al riesgo. Posteriormente, la organización selecciona las respuestas ante el riesgo y adopta una visión a nivel de cartera con respecto al nivel de riesgo que ha asumido. Los resultados de este proceso se comunican a las principales partes interesadas en el riesgo.
4. **Revisión y monitorización:** Al examinar el desempeño de la entidad, una organización puede determinar cómo funcionan los componentes de gestión del riesgo empresarial con el paso del tiempo en un entorno de cambios sustanciales, y qué aspectos son susceptibles de revisar y modificar.
5. **Información, comunicación y reporte:** La gestión del riesgo empresarial requiere un proceso continuo de obtención e intercambio de la información necesaria, tanto de fuentes internas como externas, que fluya hacia arriba, hacia abajo y a lo largo de todos los niveles de la organización.

Los cinco componentes, en el marco actualizado, están respaldados por un conjunto de principios⁴. Estos principios cubren todo los aspectos, desde el gobierno hasta la monitorización. Son manejables en tamaño, y describen las prácticas aplicables de diferentes formas y para distintos tipos de organizaciones, independientemente de su tamaño, tipo o sector.

La adhesión a estos principios puede proporcionar, a la dirección y el consejo, una expectativa razonable de que la organización entiende y se esfuerza por gestionar los riesgos asociados con su estrategia y los objetivos de la empresa.

 Gobierno y Cultura	 Estrategia y Establecimiento de Objetivos	 Desempeño	 Revisión y Monitorización	 Información, Comunicación y Reporte
<ol style="list-style-type: none"> 1. Ejerce la Supervisión de Riesgos a través del Consejo de Administración 2. Establece Estructuras Operativas 3. Define la Cultura Deseada 4. Demuestra Compromiso con los Valores Clave 5. Atrae, Desarrolla y Retiene a Profesionales Capacitados 	<ol style="list-style-type: none"> 6. Analiza el Contexto Empresarial 7. Define el Apetito al Riesgo 8. Evalúa Estrategias Alternativas 9. Formula Objetivos de Negocio 	<ol style="list-style-type: none"> 10. Identifica el Riesgo 11. Evalúa la Gravedad del Riesgo 12. Prioriza Riesgos 13. Implementa Respuestas ante los Riesgos 14. Desarrolla una Visión a nivel de Cartera 	<ol style="list-style-type: none"> 15. Evalúa los Cambios Significativos 16. Revisa el Riesgo y el Desempeño 17. Persigue la Mejora de la Gestión del Riesgo Empresarial 	<ol style="list-style-type: none"> 18. Aprovecha la Información y la Tecnología 19. Comunica Información sobre Riesgos 20. Informa sobre el Riesgo, la Cultura y el Desempeño

Mirando hacia el futuro

No hay duda de que las organizaciones continuarán enfrentándose a un futuro lleno de volatilidades, complejidades y ambigüedades. La gestión del riesgo empresarial será una pieza clave del enfoque que las organizaciones adopten para gestionar estas circunstancias y prosperar en el tiempo. Con independencia del tipo y tamaño de una entidad, las estrategias deben mantenerse fieles a su misión. Y todas las entidades deben mostrar rasgos que impulsen una respuesta eficaz con respecto al cambio, como pueda ser una ágil toma de decisiones, la capacidad de responder de manera coherente y la capacidad de adaptación para dar un giro y reposicionarse, al tiempo que mantienen unos altos niveles de confianza entre las distintas partes interesadas.

De cara al futuro, vemos varias tendencias que influirán en la gestión del riesgo empresarial. Cuatro de las tendencias más destacadas son las siguientes:

- **Abordar la proliferación de datos:** A medida que se disponga de más y más datos y aumente la velocidad a la que estos se puedan analizar, será necesario adaptar la gestión del riesgo empresarial. Los datos provendrán tanto de dentro como de fuera de la entidad y se estructurarán de nuevas formas. Las herramientas avanzadas de análisis y de visualización de datos evolucionarán y serán muy útiles para comprender el riesgo y su impacto –tanto positivo como negativo.
- **Aprovechar la inteligencia artificial y la automatización:** Mucha gente considera que ya hemos entrado en la era de los procesos automatizados y de la inteligencia artificial. Con independencia de lo que cada uno crea, es importante que las prácticas de gestión del riesgo empresarial tengan en cuenta el impacto de estas y otras futuras tecnologías, y aprovechen sus capacidades. Se pueden identificar relaciones, tendencias y patrones previamente irreconocibles, los cuales pueden proporcionar una rica fuente de información crítica para la gestión del riesgo.
- **Gestionar el coste de la gestión de riesgos:** Una preocupación frecuente expresada por muchos directivos es el coste de la gestión de riesgos, de los procesos de cumplimiento y de las actividades de control en comparación con el valor que generan. A medida que evolucionen las prácticas de gestión del riesgo empresarial, será importante que las

⁴ Al final del presente documento se ofrece una descripción más completa de estos veinte principios.

actividades que abarquen el riesgo, el cumplimiento, el control e incluso la gobernanza se coordinen de manera eficiente para proporcionar el máximo beneficio a la organización. Esta puede ser una de las mejores oportunidades para que la gestión del riesgo empresarial redefina su importancia para la organización.

- *Construir organizaciones más fuertes:* A medida que las organizaciones vayan integrando mejor la gestión del riesgo empresarial con la estrategia y el desempeño, se presentará una oportunidad para fortalecer la resiliencia. Al conocer los riesgos que tendrán un mayor impacto en la entidad, las organizaciones pueden utilizar la gestión del riesgo empresarial para ayudar a poner en marcha capacidades que les permitan actuar con prontitud. De este modo, surgirán nuevas oportunidades.

En resumen, la gestión del riesgo empresarial tendrá que cambiar y adaptarse al futuro para proporcionar sistemáticamente los beneficios señalados en el *Marco*. Con el enfoque adecuado, los beneficios derivados de la gestión del riesgo empresarial superarán con creces las inversiones y proporcionarán a las organizaciones confianza en su capacidad para gestionar el futuro.

Agradecimientos

Un agradecimiento especial a las siguientes empresas y organizaciones por permitir la participación de los Miembros del Consejo Asesor y Observadores.

Miembros del Consejo Asesor

Empresas y organizaciones

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Lee Marks)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

Organismos de educación superior y asociaciones

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Douglas J. Anderson)

Firmas de servicios profesionales

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

Antiguo consejero de COSO

- Presidente de COSO, 2009–2013 (David Landsittel)

Observadores

- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)

Componentes y principios

1. **Ejerce la supervisión de riesgos a través del consejo de administración**—El consejo de administración supervisa la estrategia y lleva a cabo las responsabilidades de gobierno para apoyar a la dirección en la consecución de los objetivos estratégicos y de negocio.
2. **Establece estructuras operativas**—La organización establece estructuras operativas con el fin de alcanzar los objetivos estratégicos y de negocio.
3. **Define la cultura deseada**—La organización define los comportamientos deseados que caracterizan la cultura a la que aspira la entidad.
4. **Demuestra compromiso con los valores clave**—La organización demuestra su compromiso con los valores clave de la entidad.
5. **Atrae, desarrolla y retiene a profesionales capacitados**—La organización está comprometida con contar un capital humano alineado con los objetivos estratégicos y de negocio.
6. **Analiza el contexto empresarial**—La organización considera los efectos potenciales del contexto empresarial sobre el perfil de riesgo.
7. **Define el apetito al riesgo**—La organización define el apetito al riesgo en el contexto de la creación, preservación y materialización del valor.
8. **Evalúa estrategias alternativas**—La organización evalúa las estrategias alternativas y el impacto potencial en el perfil de riesgos.
9. **Formula objetivos de negocio**—La organización considera el riesgo al tiempo que establece los objetivos de negocio en los distintos niveles, alineados y apoyados en la estrategia.
10. **Identifica el riesgo**—La organización identifica el riesgo que impacta en la consecución de los objetivos estratégicos y de negocio.
11. **Evalúa la gravedad del riesgo**—Evalúa la Gravedad del Riesgo.
12. **Prioriza riesgos**—La organización prioriza los riesgos como base para la selección de respuestas a adoptar ante los riesgos.
13. **Implementa respuestas ante los riesgos**—La organización identifica y selecciona las respuestas ante los riesgos.
14. **Desarrolla una visión a nivel de cartera**—La organización desarrolla y evalúa una visión del riesgo a nivel de cartera.
15. **Evalúa los cambios significativos**—La organización identifica y evalúa los cambios que pueden afectar sustancialmente a los objetivos estratégicos y de negocio.
16. **Revisa el riesgo y el desempeño**—La organización revisa el desempeño de la entidad y tiene en consideración el riesgo.
17. **Persigue la mejora de la gestión del riesgo empresarial**—La organización persigue mejorar la gestión del riesgo empresarial.
18. **Aprovecha los sistemas de información y la tecnología**—La organización utiliza los sistemas de información y tecnología de la entidad para lograr la gestión del riesgo empresarial.
19. **Comunica información sobre riesgos**—La organización utiliza canales de comunicación como soporte a la gestión del riesgo empresarial.
20. **Informa sobre el riesgo, la cultura y el desempeño**—La organización informa sobre el riesgo, la cultura y el desempeño a múltiples niveles y a través de toda la entidad.

Copyright © 2017 by Committee of Sponsoring Organizations of the Treadway Commission, (“COSO”) strictly reserved. No parts of this material may be reproduced in any form without the written permission of COSO.

Permission has been obtained from the copyright holder, COSO, to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of COSO.

ISBN 978-84-948405-1-7

Depósito Legal: M-19732-2018

Copyright © 2017 del Committee of Sponsoring Organizations of the Treadway Commission, (“COSO”). Este material no será reproducido total o parcialmente de ninguna forma sin autorización por escrito de COSO.

El Instituto de Auditores Internos de España ha obtenido del propietario del Copyright, Committee of Sponsoring Organizations of the Treadway Commission, (“COSO”), permiso para publicar esta traducción, cuyo contenido es el mismo que el original, salvo los cambios aprobados. Este documento, en su totalidad o parte, no puede ser reproducido, almacenado o remitido de forma electrónica, mecánica, fotocopia, grabación o cualquier otra sin permiso por escrito de COSO.