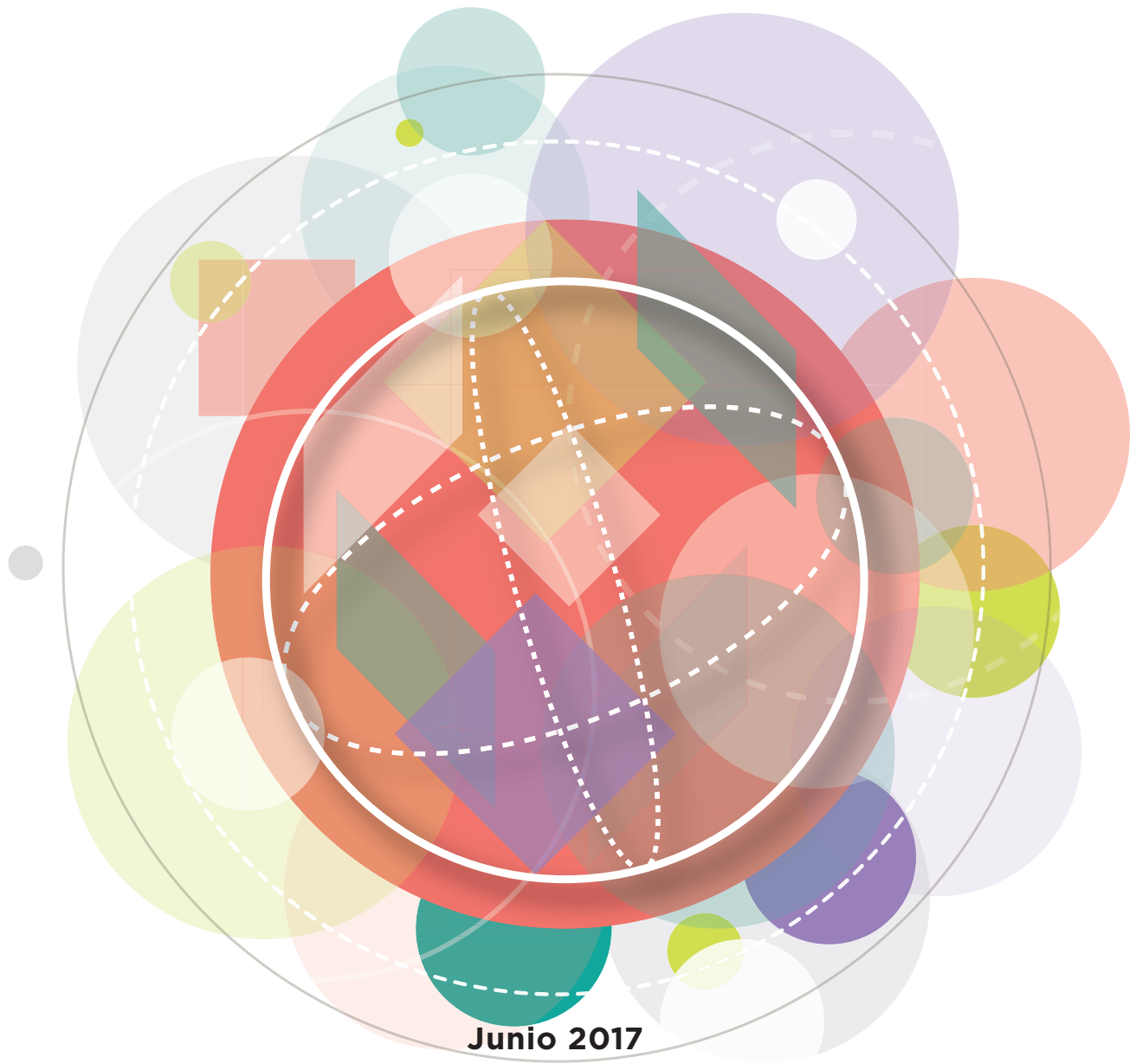




Committee of Sponsoring Organizations of the Treadway Commission

Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño



Junio 2017

Volumen I

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
New York, USA

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

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

Matthew Bagin
Director
Washington DC, USA

Hélène Katz
Director
New York, USA

Katie T. Sylvis
Director
Washington DC, USA

Sallie Jo Perraglia
Gerente
New York, USA

Kathleen Crader Zelnik
Gerente
Washington DC, USA

Maria Grimshaw
Senior Associate
New York, USA

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 de reporte 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, y 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, las exigencias regulatorias, la seguridad de la cadena de suministros o la intensa competencia 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 Sanchez
Presidente
PwC España

Ernesto Martínez
Presidente
Instituto de Auditores Internos de España

Índice

Aplicación del Marco: poniéndolo en contexto	1
1. Introducción	3
2. Comprensión de los términos: riesgo y gestión del riesgo empresarial	9
3. Estrategia, objetivos de negocio y desempeño	13
4. Integración de la gestión del riesgo empresarial	17
5. Componentes y principios	21
 Marco	 25
6. Gobierno y cultura	27
7. Estrategia y establecimiento de objetivos	45
8. Desempeño	65
9. Revisión y Monitorización	89
10. Información, comunicación y reporte	97
 Glosario de términos principales	 109



Aplicación del Marco: **Poniéndolo en contexto**

1. Introducción

Integrar las técnicas de gestión del riesgo empresarial en todos los niveles de la organización mejora la toma de decisiones en materia de gobierno, estrategia, definición de objetivos y operaciones del día a día. Contribuye a mejorar el desempeño al vincular más estrechamente la estrategia y los objetivos de negocio al riesgo. La diligencia requerida para integrar la gestión del riesgo empresarial proporciona a la entidad una hoja de ruta claramente definida para la creación, preservación y consecución de valor.

Todo análisis sobre la gestión del riesgo empresarial¹ ha de comenzar con esta premisa subyacente: cada entidad —ya sea con ánimo de lucro, sin ánimo de lucro o pública— existe para aportar valor a sus distintas partes interesadas. La presente publicación se basa en una premisa relacionada con la anterior: todas las entidades afrontan riesgos en su búsqueda del valor. Los conceptos y principios de la gestión del riesgo empresarial establecidos en esta publicación se aplican a todas las entidades con independencia de su estructura jurídica, tamaño, sector o geografía.

El riesgo afecta a la capacidad de una organización para lograr la estrategia y los objetivos de negocio. Por lo tanto, un reto para la dirección es determinar el nivel de riesgo² que la organización está dispuesta y es capaz de aceptar. La gestión eficaz del riesgo empresarial ayuda a los consejos de administración y a los equipos de dirección a optimizar los resultados con el objetivo de mejorar las capacidades para crear, preservar y, en último término, lograr la consecución de valor.

La dirección tiene muchas opciones en cuanto a la forma en que puede aplicar las técnicas de gestión del riesgo empresarial, y ningún enfoque es universalmente mejor que otro. Sin embargo, para cualquier entidad, un enfoque puede proporcionar mayores ventajas que otro o estar más alineado con la filosofía general de gestión de la organización. El presente Marco establece una estructura conceptual básica de ideas que la organización puede integrar en otras prácticas que se lleven a cabo dentro de la entidad. A los lectores que busquen información más allá de un marco, o que busquen diferentes prácticas para integrar los conceptos de la gestión del riesgo empresarial en su entidad, les resultarán de utilidad los apéndices del Volumen II de esta publicación.

La gestión del riesgo empresarial afecta al valor

El valor de una entidad viene determinado en gran medida por las decisiones que toma la dirección —desde las decisiones estratégicas más generales hasta las decisiones que afectan al día a día. Esas decisiones pueden determinar si se consigue crear, preservar, erosionar o consecución del valor.

- El valor se *crea* cuando los beneficios derivados de los recursos empleados superan el coste de esos recursos. Por ejemplo, se crea valor cuando se diseña y se lanza con éxito al mercado un nuevo producto y su margen de beneficio es positivo. Estos recursos pueden ser personas, capital financiero, tecnología, procesos y presencia en el mercado (marca).

1 Los términos definidos están vinculados al Glosario de términos principales la primera vez que se utilizan en el documento.

2 En la presente publicación, “riesgos” (plural) se refiere a uno o más actos potenciales que pueden afectar a la consecución de los objetivos. “Riesgo” (singular) se refiere a todos los actos potenciales (en términos colectivos) que pueden afectar a la consecución de los objetivos.



- El valor se *preserva* cuando el valor de los recursos empleados en las operaciones del día a día sostiene los beneficios creados. Por ejemplo, se preserva el valor a través de la entrega o prestación de bienes y servicios excelentes, y mediante el mantenimiento de una adecuada capacidad de producción, lo cual se traduce en clientes y partes interesadas satisfechos y leales.
- El valor se *erosiona* cuando la dirección implanta una estrategia que no genera los resultados esperados o no ejecutan las tareas diarias. Por ejemplo, se erosiona el valor cuando se consumen recursos significativos para desarrollar un nuevo producto que posteriormente se abandona.
- El valor se *materializa* cuando las partes interesadas perciben los beneficios generados por la entidad. Los beneficios pueden ser monetarios o no monetarios.

La forma en la que se crea el valor depende del tipo de entidad. Las entidades con ánimo de lucro crean valor mediante la implantación con éxito de una estrategia que sopesa las oportunidades del mercado frente a los riesgos de perseguir esas oportunidades. Las entidades públicas y sin ánimo de lucro pueden crear valor mediante la entrega o prestación de bienes y servicios que sopesan sus oportunidades de servir a la comunidad en general frente a cualquier riesgo asociado. Con independencia del tipo de entidad de que se trate, la integración de las técnicas de gestión del riesgo empresarial con otros aspectos del negocio mejora la confianza e infunde una mayor seguridad en las partes interesadas.

Misión, Visión y Valores clave

La Misión, la Visión y los Valores Clave³ definen lo que una entidad se esfuerza por conseguir y cómo quiere llevar a cabo sus actividades. Comunican a las distintas partes interesadas el propósito de la entidad. Para la mayoría de las entidades, la misión, la visión y los valores clave permanecen estables a lo largo del tiempo y se suelen reafirmar mediante la definición de una estrategia. Sin embargo, también pueden evolucionar a medida que cambian las expectativas de las partes interesadas. Por ejemplo, un nuevo equipo de dirección puede presentar ideas diferentes con respecto a la misión de crear valor para la entidad.

En el Marco (Capítulos 6 a 10), se analizan la misión y la visión en el contexto de una organización que establece y define su estrategia y objetivos de negocio. Los valores clave se analizan en el contexto de la cultura que la entidad desea adoptar.

- **Misión:** El propósito principal de la entidad, que establece lo que quiere lograr y su razón de ser.
- **Visión:** Aspiraciones de la entidad de cara a su estatus futuro o lo que la organización pretende lograr con el paso del tiempo.
- **Valores clave:** Las creencias e ideales de la entidad sobre lo que es bueno o malo, aceptable o inaceptable, que influyen en el comportamiento de la organización.

La gestión del riesgo empresarial afecta a la estrategia

La “estrategia” se refiere al plan de una organización para lograr su misión y visión, considerando sus valores clave. Una estrategia adecuadamente definida conduce a una asignación eficiente de recursos y a una toma de decisiones eficaz. También proporciona una hoja de ruta para establecer objetivos de negocio en toda la entidad.

La gestión del riesgo empresarial⁴ no crea la estrategia de la entidad, pero influye en su desarrollo. Una organización que integra las técnicas de gestión del riesgo empresarial en la definición de su

3 Téngase en cuenta que algunas entidades utilizan diferentes términos, como “credo”, “propósito”, “filosofía”, “creencias fundamentales” y “políticas”. Independientemente de la terminología utilizada, los conceptos que subyacen a la misión, a la visión y los valores clave, proporcionan una estructura para comunicarse a través de toda la entidad.

4 A lo largo de este documento, “gestión del riesgo empresarial” hará referencia a la cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo de cara a la creación, preservación y materialización del valor. No hace referencia a una función, grupo o departamento de una entidad. Las consideraciones específicas sobre el modelo operativo se analizan en el Apéndice B del Volumen II.

estrategia aporta a la dirección la información sobre riesgos que necesita tener en cuenta para considerar estrategias alternativas y, en última instancia, para adoptar la estrategia elegida.

La gestión del riesgo empresarial está vinculada al negocio

Las prácticas de gestión del riesgo empresarial se integran con todos los demás aspectos de la empresa, incluyendo el gobierno corporativo, la gestión del desempeño y las prácticas de control interno.

Gobierno corporativo

El gobierno corporativo constituye el concepto más amplio. Normalmente se refiere a la distribución de funciones, facultades y responsabilidades entre las partes interesadas, el consejo de administración y la dirección. Algunos aspectos del gobierno corporativo quedan fuera de la gestión del riesgo empresarial (por ejemplo, la contratación y evaluación de los miembros del consejo de administración, el desarrollo de la misión, la visión y los valores clave de la entidad).

Gestión del desempeño

El desempeño hace referencia a las acciones, tareas y funciones necesarias para materializar o exceder la estrategia y los objetivos de negocio de una entidad. La gestión del desempeño se centra en desplegar los recursos de manera eficiente. Se trata de medir esas acciones, tareas y funciones con respecto a objetivos predeterminados (tanto a corto como a largo plazo) y determinar si se están logrando esos objetivos. Dado que existe una amplia variedad de riesgos –tanto conocidos como desconocidos– que pueden afectar al desempeño de una entidad, se puede utilizar una extensa gama de medidas:

- Medidas financieras, como el retorno de las inversiones, los ingresos o la rentabilidad.
- Medidas operativas, como horas de funcionamiento, volúmenes de producción o porcentajes de capacidad.
- Medidas de obligación, como el cumplimiento de acuerdos de nivel de servicio o requisitos de cumplimiento normativo.
- Medidas de proyectos, como el lanzamiento de un nuevo producto en un plazo determinado.
- Medidas de crecimiento, como la ampliación de la cuota de mercado en un mercado emergente.
- Medidas de las partes interesadas, como la formación y habilidades laborales básicas para la población activa que se encuentra en desempleo y necesita mejorar sus competencias.

Los objetivos de desempeño siempre llevan riesgos asociados. Por ejemplo, los grandes productores agrícolas asumen un cierto riesgo en relación con su capacidad para producir los volúmenes necesarios para satisfacer las necesidades de los clientes y cumplir sus objetivos de rentabilidad. Del mismo modo, las compañías aéreas asumen un cierto grado de riesgo en relación con su capacidad para operar todos los vuelos dentro de los plazos previstos. Sin embargo, las compañías aéreas pueden prever que exista un menor riesgo por el hecho de que puedan operar solo el 90% o incluso el 80% de sus vuelos regulares sin retrasos (en lugar del 100% de sus vuelos regulares). En ambos ejemplos, existe un nivel de riesgo asociado a la gestión de cara a lograr los objetivos de desempeño predeterminados —volumen de producción y operación de vuelos.

Una entidad puede mejorar su desempeño general integrando la gestión del riesgo empresarial con las operaciones del día a día y vinculando más estrechamente los objetivos de negocio con el riesgo.

Control interno

La gestión del riesgo empresarial incorpora algunos conceptos de control interno. Por “control interno” se entiende el proceso llevado a cabo por la dirección y el resto de personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos. El control interno ayuda a la organización a identificar y analizar los riesgos para alcanzar esos objetivos y cómo gestionar los riesgos. Permite que la dirección se mantenga centrada en las operaciones de la entidad y en la consecución de sus objetivos de desempeño, cumpliendo al mismo tiempo las leyes y regulaciones pertinentes. Sin embargo, debe tenerse en cuenta que algunos conceptos relacionados con la gestión del riesgo empresarial no se tienen en cuenta dentro del control interno (por ejemplo, los conceptos de apetito al riesgo, tolerancia, estrategia y objetivos se establecen dentro de la gestión del riesgo empresarial, pero se consideran condiciones previas al control interno).

Para evitar redundancias, algunos conceptos relacionados con el control interno que son comunes tanto a esta publicación como a *Control Interno—Marco Integrado* no se han repetido aquí (por ejemplo, el riesgo de fraude relacionado con los objetivos de confiabilidad de la información financiera, las actividades de control relacionadas con los objetivos de cumplimiento de las leyes, reglamentos y normas que sean aplicables y las evaluaciones continuas y separadas relacionadas con los objetivos de eficacia y eficiencia de las operaciones). Sin embargo, algunos de los conceptos comunes relativos al control interno se desarrollan más detalladamente en el apartado Marco⁵ (por ejemplo, el gobierno de la gestión del riesgo empresarial). Animamos al lector a que revise *Control Interno—Marco Integrado*⁶ como parte de la aplicación del Marco incluido en esta publicación.

Beneficios de la gestión del riesgo empresarial

Una organización debe identificar los desafíos que le depara el futuro y adaptarse a ellos. Debe comprometerse con la toma de decisiones con una conciencia tanto de las oportunidades para crear valor como de los riesgos que desafían a la organización en la creación de valor. En resumen, debe integrar las técnicas de gestión del riesgo empresarial con la definición de la estrategia y las técnicas de gestión del desempeño y, de este modo, logrará beneficios relacionados con el valor.

Los beneficios de integrar la gestión del riesgo empresarial incluyen la capacidad de:

- *Aumentar la gama de oportunidades disponibles:* Al tener en cuenta todas las posibilidades razonables —tanto los aspectos positivos como negativos del riesgo— se pueden identificar oportunidades para la entidad y desafíos únicos asociados a las oportunidades actuales y futuras. Por ejemplo, cuando la dirección de una empresa alimentaria local valoró los riesgos potenciales que podían afectar a su objetivo de negocio de conseguir un crecimiento sostenible de los ingresos, determinaron que los principales clientes de la empresa estaban cada vez más concienciados con la salud y estaban cambiando su dieta. Este cambio indicaba una posible disminución de la demanda futura de los productos de la empresa. Como respuesta a ello, la dirección identificó fórmulas para desarrollar nuevos productos y mejorar los ya existentes, lo que le permitió mantener los ingresos de los clientes actuales (preservando el valor) y generar ingresos adicionales atrayendo a una base de consumidores más amplia (creando valor).
- *Aumentar los resultados positivos y las ventajas a la vez que se reducen las sorpresas negativas:* La gestión del riesgo empresarial permite a una organización mejorar su capacidad de identificar riesgos y establecer respuestas apropiadas, aumentando los resultados positivos y reduciendo las sorpresas negativas y los costes o pérdidas relacionados. Por ejemplo, una empresa manufacturera que suministra a sus clientes piezas de recambio de forma puntual

5 El “Marco” se refiere colectivamente a los cinco componentes introducidos en el Capítulo 5 y cubiertos individualmente en los Capítulos 6 a 10.

6 *Control Interno—Marco Integrado* se puede obtener desde www.coso.org.

para su uso en la producción, corre el riesgo de sufrir sanciones por no entregarlas a tiempo. En respuesta a este riesgo, la empresa evaluó sus procesos internos de envío revisando la hora del día de las entregas, rutas de entrega típicas y reparaciones no programadas en la flota de entrega. Utilizó las conclusiones obtenidas para establecer programas de mantenimiento para su flota, programar entregas fuera de los períodos de urgencia y diseñar alternativas a las rutas clave. Reconociendo que no todos los retrasos de tráfico pueden evitarse, también se desarrollaron protocolos para alertar a los clientes de posibles retrasos. En este caso, la dirección mejoró el desempeño al influir en el riesgo dentro de lo que es capaz de gestionar internamente (producción y programación) y adaptarse a los riesgos externos en los que la capacidad de influir es limitada (retrasos en el tráfico).

- *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. Por ejemplo, cuando un banco se dio cuenta de que se enfrentaba a distintos riesgos en sus actividades de *trading*, el equipo de dirección respondió desarrollando un sistema para analizar información interna sobre transacciones e información del mercado respaldada por información externa relevante. El sistema proporcionó una visión global de los riesgos en todas las actividades de *trading*, lo cual permitió una mayor capacidad de información para los departamentos, clientes y operadores. También permitió al banco cuantificar los riesgos relativos. El sistema cumplió los requisitos de gestión del riesgo empresarial de la entidad y permitió al banco recabar datos previamente dispares para responder con mayor eficacia a los riesgos.
- *Reducir la variabilidad del desempeño:* Para algunas organizaciones, el verdadero desafío no tiene 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 tantos problemas como unos resultados inferiores a las expectativas. Por ejemplo, en un sistema de transporte público, los pasajeros estarán igual de molestos cuando un autobús o tren salga diez minutos antes de tiempo que cuando llegue diez minutos tarde. Ambos eventos pueden hacer que los pasajeros pierdan sus conexiones con otros medios de transporte. Para gestionar dicha variabilidad, los programadores de tránsito del transporte público incorporaron determinadas pausas en el horario. Así, los conductores esperan en paradas designadas hasta una hora determinada, independientemente de cuándo lleguen. Esto ayuda a suavizar la variabilidad de los tiempos de desplazamiento y mejora el desempeño global y las opiniones de los pasajeros con respecto al sistema. La gestión del riesgo empresarial permite a las organizaciones anticiparse a los riesgos que afectarían al desempeño e implantar las medidas necesarias para minimizar los trastornos.
- *Mejorar la implantación de recursos:* La obtención de información sólida sobre los riesgos permite a la dirección evaluar las necesidades generales de recursos y ayuda a optimizar la asignación de los mismos. Por ejemplo, una empresa de distribución de gas reconoció que su anticuada infraestructura aumentaba el riesgo de fuga de gas. Al examinar las tendencias de los datos relacionados con las fugas de gas, la organización pudo evaluar el riesgo en toda su red de distribución. Posteriormente, la dirección elaboró un plan para reemplazar la infraestructura obsoleta y reparar aquellas secciones que aún tuvieran una vida útil. Este enfoque permitió a la empresa mantener la integridad de la infraestructura y asignar recursos adicionales durante un período de tiempo más largo.

Es importante tener presente que los beneficios de integrar las técnicas de gestión del riesgo empresarial con las prácticas de definición de estrategias y gestión del desempeño variarán según la entidad. No existe un enfoque único aplicable a todas las entidades. Sin embargo, las técnicas aplicadas de gestión del riesgo empresarial generalmente ayudarán a las organizaciones a alcanzar sus objetivos de desempeño y rentabilidad y a prevenir o reducir la pérdida de recursos.

La gestión del riesgo empresarial y la capacidad para adaptarse, sobrevivir y prosperar

Cada entidad se propone lograr la estrategia y los objetivos de negocio en un entorno de continuo cambio. La globalización de los mercados, los avances tecnológicos, las fusiones y adquisiciones, las fluctuaciones de los mercados de capitales, la competencia, la inestabilidad política, las capacidades de la fuerza laboral y la regulación, entre otros factores, hacen que resulte difícil conocer todos los riesgos posibles para lograr la estrategia y los objetivos de negocio.

Dado que el riesgo siempre está presente y siempre está cambiando, perseguir y alcanzar las metas puede resultar difícil. Si bien las organizaciones no pueden gestionar todos los resultados potenciales de un riesgo, sí que pueden mejorar la forma en que se adaptan a las cambiantes circunstancias. Esto a veces se conoce como sostenibilidad organizacional, resiliencia y agilidad. El Marco incorpora este concepto en el amplio contexto de crear, preservar y materializar el valor.

La gestión del riesgo empresarial se centra en gestionar los riesgos para reducir la probabilidad de que se produzca un evento y en gestionar el impacto cuando este se produzca. “Gestionar el impacto” puede requerir que una organización se adapte a las circunstancias imperantes. En algunos casos extremos, esto puede incluir la aplicación de un plan de gestión de crisis. El Ejemplo 1.1 muestra dicho plan en la práctica.

En ocasiones una organización no es capaz de retomar sus actividades ordinarias en el corto plazo cuando se produce un evento de esas características. En estos casos, la organización debe adoptar una solución a más largo plazo. Tomemos como ejemplo el caso de un crucero que se vea afectado por un incendio en alta mar. A diferencia del escenario de un brote viral observado en el Ejemplo 1.1., que afecta sólo a unos pocos pasajeros, el incendio afecta a todos. Puede haber necesidades inmediatas de asistencia médica, comida, agua y cobijo para los pasajeros, o incluso la necesidad de evacuar a todos los pasajeros. Dado que los buques están constantemente en movimiento, la planificación de una respuesta común a las crisis puede ser menos eficaz, ya que cada lugar y cada tipo de incidente pueden presentar desafíos diferentes. Sin embargo, al programar la ubicación de su flota y los horarios escalonados de salida, la compañía puede mantener un itinerario en el que los buques estén siempre a pocas horas de un puerto o de otro crucero. Este solapamiento permite a la compañía reubicar rápidamente buques y tripulaciones que puedan ayudar en caso de emergencia.

La dirección estará en mejor posición de actuar si se toma su tiempo para prever los posibles escenarios que podrían producirse — tanto los probables, como los posibles y también los improbables. La capacidad de adaptación al cambio hace que una organización sea más resiliente y más capaz de evolucionar ante las limitaciones del mercado y de los recursos. Esta capacidad también puede dar a la dirección la confianza necesaria para aumentar el nivel de riesgo que la organización esté dispuesta a aceptar y, en última instancia, acelerar el crecimiento y crear valor.

Ejemplo 1.1: Plan de gestión de crisis

Un operador de cruceros está preocupado por la posibilidad de que se produzcan brotes virales mientras sus buques están en el mar. Un crucero no tiene la capacidad de poner en cuarentena a los pasajeros durante un brote, pero puede llevar a cabo procedimientos para minimizar la propagación de gérmenes. Sin embargo, a pesar de la instalación de estaciones de desinfección manual en todo el barco, de instalaciones de lavandería y de la desinfección diaria de los pasamanos, lavabos y otras áreas comunes, los brotes virales todavía pueden ocurrir y ocurren. La organización responde implantando prácticas específicas. En primer lugar, se aumentan los niveles de limpieza y desinfección rutinarias a bordo. Una vez que el buque está en puerto, todos los pasajeros deben desembarcar para permitir que los empleados especialmente capacitados desinfecten todo el buque. A continuación, se actualizan los protocolos de limpieza basados en la cepa de virus encontrada. El próximo crucero de salida se retrasa hasta que se completen todos los protocolos de limpieza. En la mayoría de los casos, el retraso es inferior a 48 horas. Al contar con sólidas técnicas de gestión del riesgo empresarial para responder inmediatamente y adaptarse a cada situación única, la compañía es capaz de minimizar el impacto manteniendo la confianza de los pasajeros en la línea de cruceros.

2. Comprensión de los términos: riesgo y gestión del riesgo empresarial

Definición de riesgo e incertidumbre

La estrategia y los objetivos de negocio de una entidad pueden verse afectados por potenciales eventos. La falta de previsibilidad completa existente en torno a que se materialice (o no) un evento y su impacto relacionado generan incertidumbre para cualquier organización. Existirá incertidumbre para cualquier entidad⁷ que se proponga alcanzar futuras estrategias y objetivos de negocio. En este contexto, el riesgo se define como:

La posibilidad de que ocurran eventos y afecten a la consecución de la estrategia y a los objetivos de negocio.

El recuadro de esta página contiene términos que amplían y respaldan la definición de riesgo. El Marco hace hincapié en que el riesgo hace referencia a potenciales eventos, que a menudo se consideran en términos de gravedad. En algunos casos, el riesgo puede hacer referencia a la anticipación de un evento esperado que no se llegue a materializar.

En el contexto del riesgo, los eventos van más allá de las transacciones rutinarias; incluyen asuntos empresariales más amplios como cambios en la estructura de gobierno y la estructura operativa, influencias geopolíticas y sociales, y negociaciones contractuales, entre otros factores. Algunos eventos que pueden afectar a la estrategia y los objetivos de negocio son fácilmente discernibles: un cambio en los tipos de interés, un competidor que lanza un nuevo producto o la jubilación de un empleado clave. Otros son menos evidentes, particularmente cuando múltiples eventos pequeños se combinan para crear una tendencia o condición más amplia. Por ejemplo, puede ser difícil identificar eventos específicos relacionados con el calentamiento global, si bien se trata de una condición generalmente aceptada. En algunos casos, es posible que las organizaciones ni siquiera sepan o sean capaces de identificar qué eventos pueden ocurrir.

Por lo general, las organizaciones se centran en aquellos riesgos que pueden dar lugar a un resultado negativo, como los daños causados por un incendio, la pérdida de un cliente clave o la aparición de un nuevo competidor. Sin embargo, los eventos también pueden tener resultados⁸ positivos, tales como un clima mejor de lo previsto, tendencias más fuertes en la retención de los empleados o mejores tipos impositivos, siendo aspectos que también deben tenerse en cuenta. Asimismo, los eventos que son beneficiosos para el logro de un objetivo pueden plantear al mismo tiempo un desafío para la consecución de otros objetivos. Por ejemplo, el lanzamiento de un producto con una demanda superior a la prevista tiene un efecto positivo en los resultados económicos. Sin embargo, también puede aumentar el riesgo para la cadena de suministro, lo que puede dar lugar a clientes insatisfechos si la empresa no puede suministrar el producto.

Algunos riesgos tienen un impacto mínimo en una entidad y otros un impacto mayor. Las técnicas de gestión del riesgo empresarial ayudan a la organización a identificar, priorizar y concentrarse en aquellos riesgos que pueden impedir la creación, preservación y materialización del valor, o que pueden erosionar el valor existente. Sin embargo, y lo que es igualmente importante, también ayuda a la organización a buscar oportunidades potenciales.

- **Evento:** Acto o conjunto de actos que se materializan.
- **Incertidumbre:** El estado de no saber si los eventos potenciales pueden manifestarse o cómo pueden hacerlo.
- **Gravedad:** Medida que valora consideraciones tales como la probabilidad y el impacto generado por determinados eventos o el tiempo que se tarda en recuperarse de ellos.

7 "Entidad" es un término amplio que puede abarcar una amplia variedad de estructuras jurídicas, entre las que se incluyen entidades públicas, entidades con ánimo de lucro y entidades sin ánimo de lucro.

8 El presente Marco distingue entre resultados positivos y oportunidades. Los resultados positivos se refieren a aquellos casos en los que el desempeño supera el objetivo original. Las oportunidades hacen referencia a una acción o potencial acción que cree o altere metas o enfoques para crear, preservar y materializar valor.

Definición de la gestión del riesgo empresarial

La gestión del riesgo empresarial se define en la presente publicación como:

La cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo de cara a la creación, preservación y materialización de valor.

Una mirada más en profundidad a la definición de la gestión del riesgo empresarial hace hincapié en su enfoque en la gestión del riesgo a través de:

- El reconocimiento de la cultura.
- El desarrollo de las capacidades.
- Las técnicas aplicadas.
- La integración de la estrategia establecida y el desempeño.
- La gestión del riesgo y su alineación con la estrategia y los objetivos de negocio.
- La relación con el valor.

Reconocimiento de la cultura

Son las personas quienes desarrollan y dan forma a la cultura a todos los niveles de la entidad, a través de lo que dicen y hacen. Son las personas quienes establecen la misión, la estrategia y los objetivos de negocio de la entidad, y ponen en marcha las técnicas de gestión del riesgo empresarial. Del mismo modo, la gestión del riesgo empresarial afecta a las decisiones y acciones de las personas. Cada persona tiene un punto de referencia único que influye en la forma en que identifica, evalúa y responde al riesgo. La gestión del riesgo empresarial ayuda a las personas a tomar decisiones, al tiempo que comprende que la cultura desempeña un papel importante en la toma de decisiones.

Desarrollo de capacidades

Las organizaciones persiguen varias ventajas competitivas para crear valor para la entidad. La gestión del riesgo empresarial se suma a las aptitudes necesarias para llevar a cabo la misión y la visión de la entidad y para prever los desafíos que pueden impedir el éxito de la organización. Una organización que tiene la capacidad de adaptarse al cambio es más resiliente y está en mejores condiciones para evolucionar frente a las limitaciones y oportunidades del mercado y los recursos.

Aplicación de técnicas

La gestión del riesgo empresarial no es estática, ni es un complemento del negocio. Más bien se aplica de manera continuada a todo el alcance de sus actividades, así como a proyectos especiales y nuevas iniciativas. Es parte de las decisiones adoptadas por la dirección a todos los niveles de la entidad.

Las técnicas utilizadas en la gestión del riesgo empresarial se aplican desde los niveles más altos de una entidad y fluyen a través de divisiones, unidades de negocio y funciones. El objetivo de estas técnicas es ayudar a las personas de la entidad a comprender mejor su estrategia, los objetivos de negocio que se han fijado, los riesgos existentes, lo que constituye un nivel aceptable de riesgo, la forma en que el riesgo impacta en el desempeño y el modo en que se espera que ayuden a gestionar el riesgo. A su vez, este entendimiento facilita la toma de decisiones a todos los niveles y ayuda a reducir el sesgo organizacional.

Integración de la estrategia establecida y el desempeño

Una organización establece una estrategia que apoye su misión y visión y que esté alineada con ellas. Además, establece objetivos de negocio que se derivan de la estrategia, y los traslada a las unidades de negocio, las divisiones y las funciones de la entidad. Al más alto nivel, la gestión del riesgo empresarial se integra con el establecimiento de la estrategia, de modo que la dirección comprenda el perfil de riesgo general de la entidad y las consecuencias de las estrategias alternativas con respecto a dicho perfil de riesgo. La dirección tiene en cuenta específicamente cualquier nueva oportunidad que surja a través de la innovación y las actividades emergentes.

Pero la gestión del riesgo empresarial no se detiene ahí, sino que continúa en las tareas del día a día de la entidad y, al hacerlo, puede generar importantes beneficios. Una organización que integra la gestión del riesgo empresarial en las tareas diarias tiene más probabilidades de tener unos costes más bajos en comparación con otra organización que se limite a aplicar “capas” de procedimientos de gestión del riesgo empresarial. En un mercado altamente competitivo, este ahorro de costes puede ser crucial para el éxito de un negocio. Asimismo, al incorporar la gestión del riesgo empresarial a las actividades clave de la entidad, la dirección puede identificar nuevas oportunidades para hacer crecer el negocio.

La gestión del riesgo empresarial también se integra con otros procesos de gestión. Es necesario adoptar acciones específicas para tareas específicas, tales como la planificación empresarial, las operaciones y la gestión financiera. Una organización que tiene en cuenta los riesgos de crédito y de cambio, por ejemplo, puede que necesite desarrollar modelos y capturar grandes cantidades de datos necesarios para poder llevar a cabo un adecuado análisis. Al integrar las técnicas de gestión del riesgo empresarial con las actividades operativas de una entidad y comprender cómo el riesgo puede afectar a la entidad en su conjunto (y no sólo a un área de la misma) la gestión del riesgo empresarial puede resultar más eficaz.

Gestión del riesgo y su alineación con la estrategia y los objetivos de negocio

La gestión del riesgo empresarial es esencial para lograr la estrategia y los objetivos de negocio. Unas prácticas bien diseñadas de gestión del riesgo empresarial proporcionan a la dirección y al consejo de administración una expectativa razonable de que pueden lograr la estrategia global y los objetivos de negocio de la entidad. Tener una expectativa razonable significa que el nivel de riesgo para lograr la estrategia y los objetivos de negocio es apropiado para esa entidad, reconociendo que nadie puede predecir el riesgo con absoluta precisión.

Pero incluso cuando se hayan adoptado expectativas razonables, las entidades pueden experimentar desafíos imprevistos, razón por la cual es importante revisar periódicamente las técnicas de gestión del riesgo empresarial. Su examen —y consiguiente revisión cuando sea necesario— ayuda a mantener prácticas sólidas que aumentan la confianza de la dirección en la capacidad de la entidad para responder con éxito a lo inesperado y lograr la estrategia y los objetivos de negocio.

Relación con el valor

Una organización debe gestionar el riesgo de acuerdo con la estrategia y los objetivos del negocio en relación con su apetito al riesgo, es decir, el tipo y nivel de riesgo de forma amplia, que está dispuesta a aceptar en su búsqueda del valor. La primera expresión del apetito al riesgo es la misión y visión de una entidad. Diferentes estrategias expondrán a una entidad a diferentes riesgos o diferentes niveles de riesgos similares.

El apetito al riesgo proporciona orientación sobre las prácticas que una organización debe seguir o no seguir. Establece una gama de técnicas adecuadas y orienta la toma de decisiones basadas en el riesgo en lugar de especificar un límite.

El apetito al riesgo no es estático; puede cambiar entre productos o unidades de negocio y también con el tiempo, en línea con la cambiante capacidad de la organización para gestionar el riesgo. Los tipos y el nivel de riesgo que una organización puede considerar aceptable pueden variar. Por ejemplo, durante una coyuntura óptima de la economía, una empresa de éxito y en crecimiento puede estar más dispuesta a aceptar ciertos riesgos considerables que cuando la coyuntura económica empeore y las perspectivas del negocio se deterioren. El apetito al riesgo debe ser lo suficientemente flexible como para adaptarse a las cambiantes condiciones empresariales, según sea necesario, sin esperar a revisiones y aprobaciones periódicas de la dirección.

Si bien se introduce aquí el apetito al riesgo⁹, el Marco establece numerosos casos en los que se aplica como parte de la gestión del riesgo empresarial. Algunas de las aplicaciones más importantes del apetito al riesgo son las siguientes:

- Uso por parte de la organización en la toma de decisiones que aumentan el valor.
- Ayuda a alinear el nivel aceptable de riesgo con la capacidad de la organización para gestionar el riesgo y las oportunidades.
- Relevancia al establecer la estrategia y los objetivos de negocio, ayudando a la dirección a considerar si los objetivos de desempeño están alineados con un nivel aceptable de riesgo.
- Asistencia en la comunicación del perfil de riesgo deseado por el consejo.
- Relevancia y alineación con la capacidad del riesgo.
- Uso a la hora de evaluar el riesgo agregado a nivel de cartera.

La gestión del riesgo empresarial ayuda a la dirección a seleccionar una estrategia que alinea la creación de valor anticipado con el apetito al riesgo de la entidad y sus capacidades para gestionar el riesgo con mayor frecuencia y de manera más sistemática a lo largo del tiempo. La gestión del riesgo conforme al apetito al riesgo mejora la capacidad de una organización para crear, preservar y materializar el valor.

9 El apetito al riesgo se analiza en mayor profundidad en el Marco en el Principio 7: Define el Apetito al riesgo

3. Estrategia, objetivos de negocio y desempeño

Estrategia y gestión del riesgo empresarial

La gestión del riesgo empresarial ayuda a una organización a comprender mejor:

- Cómo la misión, la visión y los valores clave forman la expresión inicial de qué tipo y nivel de riesgo es aceptable considerar al establecer la estrategia.
- La posibilidad de que la estrategia y los objetivos de negocio no estén alineados con la misión, visión y valores clave.
- El tipo y nivel de riesgo al que la organización se expone potencialmente al elegir una estrategia en particular.
- El tipo y el nivel de riesgo inherente a la ejecución de su estrategia y al logro de los objetivos de negocio y a la aceptabilidad de este nivel de riesgo, y en última instancia, del valor.

La Figura 3.1 ilustra la estrategia en el contexto de la misión, la visión y los valores clave, y como palanca de la dirección y el desempeño general de una entidad.

Figura 3.1: Contexto estratégico



Posible desalineación estratégica con los objetivos de negocio

Tanto la misión como la visión proporcionan una perspectiva de alto nivel sobre el tipo y el nivel de riesgo aceptable para la entidad. Ayudan a la organización a establecer límites y estar pendientes de cómo las decisiones pueden afectar a la estrategia. Una organización que entiende su misión y visión puede establecer estrategias que generen el perfil de riesgo deseado. Las declaraciones de una organización de atención médica incluidas en el Ejemplo 3.1. guían a la organización en la determinación de los tipos y el nivel de riesgo que es probable que se enfrente y acepte. La organización considerará los riesgos asociados a la prestación de atención médica de alta calidad (misión), el acceso conveniente y oportuno al servicio (misión), y el ser un lugar excelente para practicar la medicina (visión). Teniendo en cuenta su alta consideración por la calidad, el servicio y la amplitud de sus habilidades, es probable que la organización busque una estrategia que tenga un perfil de menor riesgo relacionado con la calidad de la atención y el servicio al paciente. Esto puede significar que se ofrezcan servicios para pacientes hospitalizados y/o ambulatorios, pero sin que exista una presencia online destacada. Por otra parte, si la organización hubiera centrado su misión

en la innovación de los enfoques de atención al paciente o en canales avanzados de prestación de servicios, seguramente habría adoptado una estrategia con un perfil de riesgo diferente.

La gestión del riesgo empresarial puede ayudar a una entidad a evitar que la estrategia esté desalineada. Puede proporcionar a una organización una visión adecuada para asegurar que la estrategia elegida, apoye la misión y visión más amplia de la entidad, para que pueda ser considerada por la dirección y el consejo de administración.

Evaluación de la estrategia seleccionada

La gestión del riesgo empresarial no crea la estrategia de la entidad, sino que informa a la organización sobre los riesgos asociados a las estrategias alternativas consideradas y, en última instancia, a la estrategia adoptada. La organización debe evaluar cómo la estrategia elegida ha podido afectar al perfil de riesgo de la entidad, y en especial a los tipos y al nivel de riesgo a los que la organización está potencialmente expuesta.

Al evaluar los riesgos potenciales que pueden surgir de la estrategia, la dirección también considera cualquier hipótesis clave que subyace a la estrategia elegida. Estos supuestos son una parte importante de la estrategia y pueden referirse a cualquiera de las consideraciones que forman parte del contexto de negocio de la entidad. La gestión del riesgo empresarial proporciona una valiosa información sobre la sensibilidad de los cambios en las hipótesis: es decir, si tendrían poco o gran efecto de cara a la consecución de la estrategia.

El Ejemplo 3.2 tiene en cuenta la misión y la visión de la organización de atención médica analizado, anteriormente, y cómo la entidad traslada esta información a su estrategia. Tomando como muestra el ejemplo mostrado, la organización puede considerar qué riesgos pueden derivarse de la estrategia elegida. Por ejemplo, los riesgos relacionados con la innovación médica pueden ser más pronunciados, los riesgos para la capacidad de prestar una atención de alta calidad pueden aumentar a raíz de las iniciativas de gestión de costes, y los riesgos relacionados con la gestión de nuevas alianzas estratégicas pueden ser un enfoque en el que la organización no se haya centrado anteriormente. Estos y muchos otros riesgos provienen de la elección de la estrategia. Sin embargo, sigue pendiente la pregunta de si es probable que la entidad logre su misión y visión con esta estrategia, o si existe un riesgo elevado con respecto a la materialización de los objetivos establecidos.

Ejemplo 3.1: Misión, visión y valores clave en la práctica

Misión: Mejorar la salud de las personas a las que prestamos nuestros servicios proporcionándoles una atención de alta calidad, una amplia gama de servicios y un acceso rápido y oportuno con un servicio excepcional de atención al paciente.

Visión: Nuestro hospital será el centro de atención médica preferido por médicos y pacientes, y será conocido por proporcionar una calidad sin igual, ofrecer un servicio excelente y ser un lugar ejemplar en el que practicar la medicina.

Valores clave: Nuestros valores sirven de base para todo lo que pensamos, decimos y hacemos. Trataremos a nuestros médicos, pacientes y colegas con respeto, honestidad y compasión, al tiempo que los hacemos responsables de estos valores.

Ejemplo 3.2: Misión, visión y valores clave en la práctica

Nuestra Estrategia:

- Maximizar el valor para nuestros pacientes mejorando la calidad en un amplio espectro de servicios.
- Reducir la tendencia al aumento de costes.
- Integrar la eficiencia operativa y las iniciativas de gestión de costes.
- Alinear médicos e integración clínica.
- Aprovechar la innovación en los programas clínicos.
- Desarrollar alianzas estratégicas.
- Gestionar la prestación de servicios al paciente y reducir los tiempos de espera donde sea posible.

Riesgo para la implantación de la estrategia y los objetivos de negocio

Siempre existen riesgos a la hora de llevar a cabo una estrategia, los cuales deben ser analizados por las organizaciones. En este caso, la atención se centra en comprender la estrategia establecida y los riesgos que existen con respecto a su relevancia y viabilidad. En ocasiones, los riesgos adquieren suficiente importancia como para que una organización desee volver a examinar su estrategia y considerar la posibilidad de revisarla o de seleccionar otra estrategia con un perfil de riesgo más adecuado.

El riesgo de llevar a cabo la estrategia también puede verse desde el punto de vista de los objetivos de negocio. Una organización puede utilizar diversas técnicas para evaluar los riesgos utilizando algún tipo de parámetro común. Siempre que sea posible, la organización debe utilizar unidades similares para medir el riesgo con respecto a cada objetivo. De este modo, se contribuirá a alinear la gravedad del riesgo con las medidas de desempeño establecidas

Gestión del riesgo empresarial y desempeño

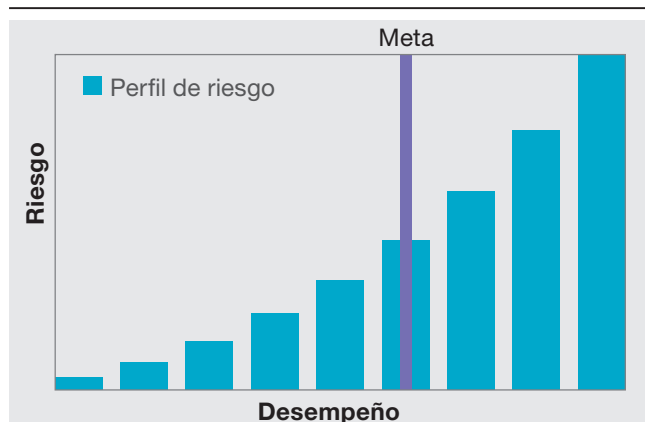
La evaluación del riesgo con respecto a la estrategia y los objetivos de negocio requiere que una organización comprenda la relación entre el riesgo y el desempeño — lo que en este Marco se denomina “perfil de riesgo”. El perfil de riesgo de una entidad proporciona una visión global de los riesgos en relación con un nivel específico de la entidad (por ejemplo, a nivel corporativo, a nivel de unidad de negocio, a nivel funcional) o un aspecto del modelo de negocio (por ejemplo, producto, servicio, geografía).

Esta visión global permite a la dirección considerar el tipo, gravedad e interdependencias de los riesgos y cómo éstos pueden afectar al desempeño. La organización deberá entender inicialmente el perfil de riesgo potencial cuando evalúe estrategias alternativas. Una vez que se elija una estrategia, el enfoque cambiará para comprender el perfil de riesgo actual de la estrategia elegida y los objetivos de negocio relacionados.

Esta relación entre riesgo y desempeño rara vez es lineal. Los cambios incrementales en los objetivos de desempeño no siempre dan lugar a cambios correspondientes en el riesgo (o viceversa). En consecuencia, una representación útil y dinámica, en ocasiones representada gráficamente, ilustrará el nivel global de riesgo asociado a los diferentes niveles de desempeño. Tal representación considera el riesgo como una continuación de resultados potenciales a lo largo del cual la organización debe sopesar el nivel de riesgo para la entidad y su desempeño deseado.

Existen varios métodos para representar un perfil de riesgo. El Marco utiliza un enfoque, que se muestra aquí, para ilustrar la relación entre los diversos aspectos de la gestión del riesgo empresarial. Esto ayuda a mejorar las conversaciones sobre el riesgo, el apetito al riesgo, la tolerancia y la relación general con los objetivos de desempeño.

Figura 3.2: Riesgo relativo al desempeño



En la Figura 3.2, cada barra representa el nivel global de riesgo con respecto a un nivel específico de desempeño para un objetivo de negocio. La línea de meta representa el nivel de desempeño escogido por la organización como parte de la definición de la estrategia establecida, que se comunica a través de un objetivo y una meta. Las organizaciones pueden desarrollar enfoques diferentes para conceptualizar y describir el perfil de riesgo de la entidad.

Los perfiles de riesgo que tienen una tendencia al alza, tal y como se muestra en la Figura 3.2, son típicos (pero sin limitarse a ellos) de objetivos de negocio tales como:

- *Exploración de petróleo y gas:* A medida que los esfuerzos de exploración de nuevas reservas de petróleo y gas apuntan a zonas cada vez más remotas e inaccesibles, es probable que las compañías de petróleo y de gas se enfrenten a mayores riesgos en un esfuerzo por localizar recursos.
- *Reclutamiento de recursos especializados:* A medida que las entidades persiguen productos o mercados cada vez más especializados, aumentan los riesgos asociados con la atracción y retención de conocimientos y experiencia en sus equipos de trabajo.
- *Transporte y logística:* A medida que aumenta el número de lugares o el volumen de mercancías, se incrementa el tamaño de la flota de transporte y la complejidad de las operaciones, lo cual deriva en un mayor nivel de riesgo.
- *Financiación para proyectos y mejoras:* En los mercados con escasa liquidez, o en los que la confianza del consumidor es baja, aumenta el nivel de riesgo asociado a la capacidad de una entidad para obtener financiación para proyectos o iniciativas.

Sin embargo, no existe un perfil de riesgo, modelo o tendencia universal. El perfil de riesgo de cada entidad será diferente según la estrategia y los objetivos de negocio. Las organizaciones pueden utilizar sus perfiles de riesgo para comprender mejor la relación intrínseca entre el riesgo, el desempeño al que aspiran y el desempeño real.

Los perfiles de riesgo ayudan a la dirección a determinar qué nivel de riesgo es aceptable y manejable en la búsqueda de la estrategia y los objetivos de negocio. Los perfiles de riesgo¹⁰ pueden ayudar a la dirección a:

- Comprender el nivel de desempeño en el contexto del apetito al riesgo de la entidad (véase el Principio 7: *Define el Apetito al riesgo*).
- Encontrar el nivel óptimo de desempeño dada la capacidad de la organización para gestionar el riesgo (ver Principio 9: *Formula Objetivos de Negocio*).
- Determinar la tolerancia con respecto a la variación del desempeño y en relación con el objetivo establecido (véase el Principio 9: *Formula Objetivos de Negocio*).
- Evaluar el impacto potencial del riesgo sobre los objetivos predeterminados (véase el Principio 11: *Evalúa la Gravedad del Riesgo* y Principio 14: *Desarrolla una visión a nivel cartera*).

Si bien el perfil de riesgo que se muestra aquí implica la necesidad de un nivel específico de precisión, y tal vez de datos, debe tenerse en cuenta que también se puede desarrollar utilizando información cualitativa.

10 Remítase al Apéndice D del Volumen II para acceder a un análisis más detallado sobre perfiles de riesgo.

4. Integración de la gestión del riesgo empresarial

La importancia de la integración

El éxito de una entidad es el resultado de innumerables decisiones tomadas cada día por la organización que afectan al desempeño y, en última instancia, a la consecución de la estrategia o de los objetivos de negocio. La mayoría de esas decisiones requieren la selección de un enfoque a partir de múltiples alternativas. Muchas de las decisiones no serán simplemente “correctas” o “incorrectas”, sino que incluirán pros y contras: tiempo frente a calidad; eficiencia frente a costes; riesgo frente a recompensa.

Al tomar tales decisiones, la dirección y el consejo de administración deben gestionar continuamente un contexto empresarial dinámico, el cual requiere integrar en todo momento los enfoques de gestión del riesgo empresarial en todos los ámbitos de la entidad. Por lo tanto, el Marco concibe de esta manera la gestión del riesgo empresarial. No es simplemente una función o departamento dentro de una entidad, ni algo que se puede sencillamente “añadir” a la entidad. Más bien, la cultura, las técnicas y las capacidades están juntas, integradas y se aplican a todos los niveles de la entidad.

La integración de la gestión del riesgo empresarial con las actividades y procesos del negocio se traduce en una mejor información que respalda la toma de decisiones y conduce a un mejor desempeño. Además, ayuda a las organizaciones a:

- Anticiparse a los riesgos antes o de manera más explícita, abriendo más opciones para gestionar los riesgos y minimizar el potencial de desviaciones en el desempeño, pérdidas, incidentes o fallos.
- Identificar y perseguir las oportunidades existentes y nuevas de acuerdo con el apetito al riesgo y la estrategia de la entidad.
- Comprender y responder a las desviaciones en el desempeño de manera más rápida y coherente.
- Desarrollar y reportar una visión más integrada y coherente del riesgo a nivel de cartera, permitiendo así que la organización asigne mejor los recursos limitados.
- Mejorar la colaboración, la confianza y el intercambio de información en toda la organización.

La integración permite a la organización tomar decisiones que están mejor alineadas con la velocidad y disrupciones potenciales provocadas por los distintos riesgos y con la búsqueda de nuevas oportunidades. Es posible que las entidades con un perfil de riesgo agresivo deban obtener rápidamente información relacionada con el riesgo y hayan racionalizado los procesos de toma de decisiones para aprovechar las oportunidades que se presentan con rapidez. Por ejemplo, una firma de inversión que tenga la oportunidad de presentar una oferta para cerrar una nueva operación pero que está obligada a responder en el plazo de unas horas. Las técnicas de gestión de riesgos de la firma están bien integradas con las capacidades del proceso de licitación, lo que le permite recopilar y revisar la información disponible y tomar una decisión en el plazo requerido.

Cuando las técnicas y capacidades de gestión de riesgos están separadas, la recopilación de información adecuada, la identificación de las partes interesadas y la toma de decisiones tarda más tiempo, lo que puede poner en peligro la capacidad de una entidad para cumplir plazos urgentes. En definitiva, cuanto más agresivo es el perfil de riesgo de una entidad, mayor es el valor de la integración.



Hacia la integración plena

Para la mayoría de las entidades, integrar la gestión del riesgo empresarial es un esfuerzo continuo. Los factores que influyen en la integración son la cultura de las entidades, el tamaño, la complejidad y el tiempo en que se ha adoptado una cultura consciente del riesgo.

Una entidad que está comenzando a desarrollar la gestión del riesgo empresarial tendrá unas prácticas y capacidades limitadas en las que confiar. Pero, a medida que la entidad madura, implanta prácticas y capacidades más especializadas que mejoran la toma de decisiones (como la identificación, evaluación y respuesta ante los riesgos). Una vez que las organizaciones integran sistemáticamente las consideraciones de riesgos, se vuelven menos dependientes de las técnicas e infraestructuras aisladas y formalizadas. Por ejemplo, en una entidad totalmente integrada, los empleados identificarán desviaciones con respecto al desempeño y comprenderán el efecto potencial sobre el perfil de riesgo sin depender de un programa de evaluación independiente.

El tiempo no es el único factor que afecta a la capacidad de una entidad para integrar plenamente la gestión del riesgo empresarial. El tamaño y el tipo también influyen (es decir, si la entidad tiene ánimo de lucro o no, si está fuertemente regulada, etc.). Por ejemplo, una gran empresa farmacéutica puede tener una cultura consciente del riesgo muy desarrollada, pero puede que sus reguladores le obliguen a mantener algunas prácticas de vigilancia y la presentación de informes independientes. Por el contrario, las entidades no reguladas de menor tamaño pueden centrarse más en desarrollar la conciencia sobre el riesgo y el concepto de riesgo integrado mientras informan sobre el desempeño.

En una entidad plenamente integrada, las técnicas de gestión del riesgo empresarial también afectarán a la estructura operativa. En este punto, la conciencia y la responsabilidad con respecto al riesgo se distribuyen más uniformemente en toda la estructura operativa, que a menudo se caracteriza por el entendimiento de que “todos somos gestores de riesgos”. Los silos de conocimiento se descomponen para permitir una mejor toma de decisiones en toda la entidad.

Las listas mostradas más adelante proporcionan ejemplos de cómo las organizaciones pueden fomentar la plena integración de la gestión del riesgo empresarial en toda la cultura, capacidades y prácticas de la entidad, con el resultado de una mejor toma de decisiones.

Cultura

Inculcar una mayor transparencia y conciencia del riesgo en la cultura de una entidad requiere acciones tales como:

- Implantar foros u otros mecanismos para compartir información, tomar decisiones e identificar oportunidades.
- Alentar a la gente a trasladar los problemas y preocupaciones a los jefes y superiores sin temor a represalias.
- Aclarar y comunicar las funciones y responsabilidades para el logro de la estrategia y los objetivos de negocio, incluidas las responsabilidades con respecto a la gestión de riesgos.
- Alinear los valores clave, los comportamientos y la toma de decisiones con incentivos y modelos de remuneración.
- Desarrollar y compartir una fuerte comprensión del contexto empresarial y las palancas necesarias para la creación de valor.

Capacidades

Las capacidades de gestión del riesgo empresarial se integran en la entidad cuando:

- La dirección es capaz de tomar decisiones que están alineadas con su apetito, el perfil de riesgo de la entidad y los cambios en dicho perfil que se producen a lo largo del tiempo.
- La organización contrata a personas capacitadas con experiencia relevante que pueden ejercer juicios de valor y supervisión de acuerdo con sus responsabilidades.
- La organización tiene acceso a profesionales capaces, expertos en la materia u otros recursos técnicos para facilitar la toma de decisiones.
- Cuando se realizan las inversiones necesarias en tecnología u otras infraestructuras, la dirección puede considerar las herramientas necesarias para desempeñar las responsabilidades de gestión del riesgo empresarial.
- Los vendedores, contratistas y otras terceras partes se incorporan a las discusiones sobre riesgos y desempeño.

Prácticas

Las técnicas de gestión del riesgo empresarial se consideran integradas cuando:

- Al definir la estrategia se considera explícitamente el riesgo al evaluar las distintas opciones.
- La dirección aborda activamente el riesgo en la búsqueda de sus objetivos de desempeño.
- Se desarrollan actividades para realizar un seguimiento regular y constante de los resultados del desempeño y los cambios en el perfil de riesgo en toda la entidad.
- La dirección es capaz de tomar decisiones que sean coherentes con la velocidad y el alcance de los cambios en la entidad.

Ejemplo 4.1: Integración Práctica

La gestión de un gran departamento público integra las técnicas de gestión del riesgo empresarial en las reuniones mensuales de gestión del desempeño. En estas reuniones, analizan el desempeño y discuten los riesgos nuevos, emergentes y cambiantes que afectan a su capacidad de servir eficazmente al público. Esto promueve una mayor transparencia y una mayor capacidad de respuesta ante los riesgos más importantes, comparando ideas sobre la mejor manera de abordar el riesgo, y una mayor coherencia en el despliegue de las respuestas ante el riesgo en todas las operaciones del departamento.

El ejemplo 4.1 describe la integración del riesgo en la práctica empresarial.

Abordar la integración en el Marco

Cada componente de la gestión del riesgo empresarial incluye principios (se exponen en el capítulo siguiente), que se aplican para crear, preservar y materializar el valor en una organización con independencia de su tamaño, tipo o ubicación. Los principios y sus componentes no representan conceptos aislados e independientes. Cada uno de ellos destaca la importancia de integrar la gestión del riesgo empresarial y su rol en la toma de decisiones.

Para cada principio, el Marco define una serie de consideraciones para integrar plenamente la cultura, las técnicas y las capacidades en la entidad. Estas consideraciones no son integrales, sino que ponen de manifiesto una gama de aportaciones de cara a la toma de decisiones y la adopción del juicio profesional por parte de los empleados, del equipo de dirección y del consejo de administración.

5. Componentes y principios

Componentes y principios de la gestión del riesgo empresarial

El Marco consta de los cinco componentes interrelacionados de la gestión del riesgo empresarial. La Figura 5.1 muestra estos componentes y su relación con la misión, visión y valores clave de la entidad. Las tres cintas del diagrama de Establecimiento de la Estrategia y de los Objetivos, Desempeño, y Revisión y Monitorización representan los procesos más habituales que fluyen a través de la entidad. Las otras dos cintas, Gobierno y Cultura, e Información, Comunicación y Reporte, representan aspectos de apoyo a la gestión del riesgo empresarial.

La figura ilustra además que cuando la gestión del riesgo empresarial se integra en el desarrollo de la estrategia, la formulación de objetivos de negocio y la ejecución y el desempeño, puede aumentar el valor. La gestión del riesgo empresarial no es estática. Se integra en el desarrollo de la estrategia, la formulación de objetivos de negocio y la implantación de esos objetivos a través de la toma de decisiones diarias

Figura 5.1: Componentes de gestión de riesgos



Los cinco componentes¹¹ son:

- **Gobierno y Cultura:** El gobierno y la cultura juntos forman una base para todos los demás componentes de la gestión del riesgo empresarial. 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 se refleja en la toma de decisiones.
- **Establecimiento de la estrategia y de los objetivos:** La gestión del riesgo empresarial se integra en el plan estratégico de la entidad a través del proceso de establecimiento de la estrategia y de los objetivos de negocio. Con un conocimiento profundo del contexto empresarial, la organización puede comprender mejor los factores internos y externos y sus efectos en el riesgo. Una organización fija su apetito al riesgo en conjunción con la definición de estrategias. Los objetivos de negocio permiten poner en práctica la estrategia y configurar las operaciones y prioridades diarias de la entidad.
- **Desempeño:** Una organización identifica y evalúa los riesgos que pueden afectar a la capacidad de una entidad para alcanzar la estrategia y los objetivos de negocio. Como parte de esa búsqueda, la organización identifica y evalúa los riesgos que pueden afectar a la consecución de dicha estrategia y los objetivos de negocio.

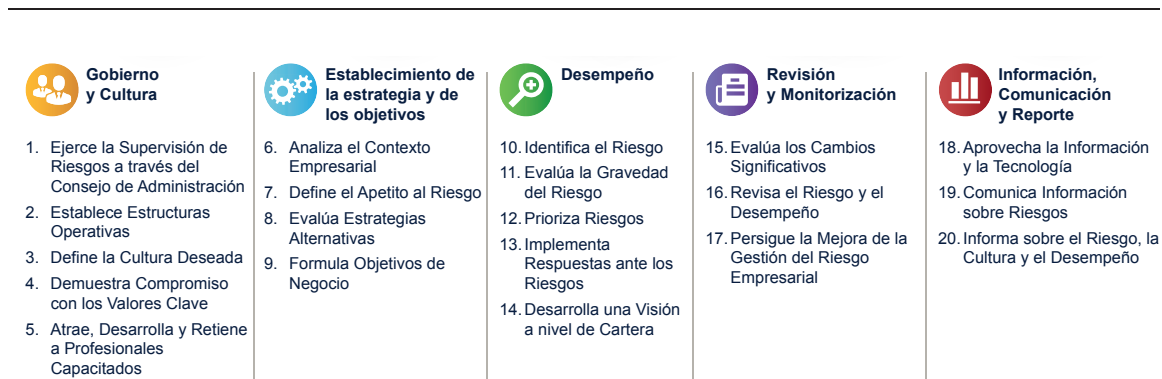
¹¹ Los componentes se analizan en detalle en los capítulos 6 al 10.

Prioriza los riesgos en función de su gravedad y teniendo en cuenta el apetito al riesgo de la entidad. La organización entonces selecciona las respuestas al riesgo y efectúa un seguimiento del desempeño considerando posibles cambios. De esta forma, desarrolla una visión de cartera sobre el nivel de riesgo que la entidad ha asumido para cumplir con su estrategia y conseguir los objetivos de negocio a nivel de entidad.

- **Revisión y Monitorización:** Al examinar las capacidades y técnicas de gestión del riesgo empresarial, y el desempeño de la entidad en relación con sus objetivos, una organización puede considerar en qué medida las capacidades y técnicas de gestión del riesgo empresarial han creado valor a lo largo del tiempo y seguirán haciéndolo cuando se produzcan cambios sustanciales.
- **Información, Comunicación y Reporte:** La comunicación es el proceso continuo e iterativo de obtener y compartir información en toda la entidad. La dirección utiliza información pertinente de fuentes internas y externas para facilitar la gestión del riesgo empresarial. La organización aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Al utilizar información que se aplica a todos los componentes, la organización informa sobre el riesgo, la cultura y el desempeño.

Dentro de estos cinco componentes hay una serie de principios, como se ilustra en la Figura 5.2. Los principios representan los conceptos fundamentales asociados a cada componente, y están redactados de la misma manera que lo harían las organizaciones como parte de las técnicas de gestión del riesgo empresarial de la entidad. Si bien estos principios son universales y forman parte de cualquier iniciativa eficaz de gestión del riesgo empresarial, la dirección debe hacer valer su criterio al aplicarlos. Cada principio se analiza detalladamente en los respectivos capítulos sobre los componentes.

Figura 5.2: Principios de gestión de riesgos



Evaluación de la gestión del riesgo empresarial

Una organización debe contar con medios adecuados para proporcionar a las partes interesadas de la entidad una expectativa razonable de que es capaz de gestionar el riesgo hasta un mínimo aceptable. Esto se logra evaluando las prácticas implantadas para la gestión del riesgo empresarial. Este tipo de evaluación es voluntario, a menos que la legislación o regulación lo establezca de otro modo.

El Marco proporciona criterios para llevar a cabo una evaluación y determinar si la cultura, las capacidades y las técnicas de gestión del riesgo empresarial abordan conjuntamente el riesgo de no lograr la estrategia de la entidad y los objetivos de negocio asociados. Durante la evaluación, la organización considera si:

- Los componentes y principios relativos a la gestión del riesgo empresarial están presentes y en funcionamiento.
- Los componentes relativos a la gestión del riesgo empresarial funcionan juntos de forma integrada.
- Los controles necesarios para poner en práctica los principios relevantes están presentes y en funcionamiento.¹²

¹² En *Control Interno—Marco Integrado* se incluye un análisis adicional sobre los controles para la aplicación de los

En estas tres consideraciones, “estar presente” significa que los componentes, principios y controles existen en el diseño e implantación de la gestión del riesgo empresarial para lograr la estrategia y los objetivos de negocio. “En funcionamiento” significa que están operando para lograr la estrategia y los objetivos de negocio. “De forma integrada” se refiere a las interdependencias de los componentes y a su funcionamiento conjunto. Las organizaciones pueden poner un énfasis diferente en principios específicos y aplicarlos de manera diferente, dependiendo de los beneficios que una organización busque obtener a través de la gestión del riesgo empresarial¹³. Cuando estos componentes, principios y controles de apoyo están presentes y en funcionamiento, la organización puede esperar dentro de lo razonable que la gestión del riesgo empresarial ayude a la entidad a crear, preservar y materializar valor.

Existen diferentes enfoques disponibles para evaluar la gestión del riesgo empresarial. Cuando la evaluación se realice para comunicarse con las partes interesadas externas, se realizará teniendo en cuenta los principios establecidos en el Marco. Al evaluar la gestión del riesgo empresarial con fines internos, algunas organizaciones pueden optar por utilizar algún tipo de modelo de madurez para completar esta evaluación, reconociendo que el modelo debe adaptarse a la complejidad del negocio. Los factores que añaden complejidad pueden incluir, entre otros aspectos, la geografía, industria, naturaleza, alcance y frecuencia de los cambios dentro de la entidad, el desempeño histórico y la variación en el desempeño, la dependencia de la tecnología y el grado de supervisión regulatoria.

Durante una evaluación, la dirección también puede examinar la idoneidad de esas capacidades y prácticas, teniendo en cuenta la complejidad de la entidad y los beneficios que la organización procura obtener mediante la gestión del riesgo empresarial.

principios.

13 En el Capítulo 1: *Introducción* se exponen los beneficios potenciales relacionados con la gestión del riesgo empresarial

Marco

Marco

6. Gobierno y cultura



Principios relacionados con el gobierno y la cultura

GESTIÓN DEL RIESGO EMPRESARIAL



GOBIERNO Y CULTURA

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 la estrategia y los objetivos de negocio.

2. Establece Estructuras Operativas:

La organización establece estructuras operativas con el fin de lograr la estrategia y los objetivos 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 el desarrollo de capital humano que esté alineado con la estrategia y los objetivos de negocio.

Introducción

El consejo de administración de una entidad desempeña un importante papel en el gobierno e influye de manera significativa en la gestión del riesgo empresarial. El presente 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 o los propietarios.

Cuando el consejo es independiente de la dirección y está compuesto por miembros experimentados, capacitados y con un elevado talento, puede ofrecer un adecuado grado de aportación sectorial, empresarial y técnica mientras desempeña sus responsabilidades de supervisión. Estas aportaciones incluyen el análisis pormenorizado de las actividades de la dirección cuando sea necesario, la presentación de puntos de vista alternativos, el análisis crítico de los sesgos de la organización y la actuación frente a conductas irregulares. Y lo que es aún más importante, en el desempeño de su función de supervisión de riesgos, el consejo de administración analiza de manera crítica al equipo de dirección sin intervenir en las funciones desempeñadas por ella.

Otra influencia crítica en la gestión del riesgo empresarial es la cultura. Con independencia de si la entidad es una pequeña empresa privada familiar, una multinacional grande y compleja, una administración pública o una ONG, su cultura refleja los valores clave de la entidad: las creencias, actitudes, comportamientos deseados e importancia de comprender el riesgo. La cultura facilita la consecución de la misión y visión de la entidad. Una entidad con una cultura consciente del riesgo destacará la importancia de gestionar el riesgo y fomentará un flujo transparente y oportuno de información sobre riesgos. Y lo hará sin atribuir culpabilidades, pero con una actitud de comprensión, responsabilidad y mejora continua.





Principio 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 la estrategia y los objetivos de negocio.

Rendición de cuentas y responsabilidad

El consejo de administración tiene la responsabilidad principal de la supervisión del riesgo en la entidad, y en muchos países tiene una responsabilidad fiduciaria para con las partes interesadas de la entidad, incluida la realización de revisiones de las técnicas de gestión del riesgo empresarial. Normalmente, es el consejo en pleno quien es responsable de la supervisión del riesgo, dejando las responsabilidades diarias de la gestión del riesgo a la dirección. Algunos consejos en pleno son quienes mantienen la propiedad de la responsabilidad mientras que otros delegan las responsabilidades en una comisión del consejo, como puede ser la comisión de riesgos. Independientemente de la estructura, es habitual crear una declaración que defina las responsabilidades respectivas del consejo y de la dirección.

Habilidades, experiencia y conocimientos de negocio

El consejo de administración está bien posicionado para supervisar la gestión del riesgo empresarial a través de sus habilidades colectivas, su experiencia y sus conocimientos del negocio. Esto incluye, por ejemplo, hacer las preguntas apropiadas para desafiar a la dirección cuando sea necesario acerca de la estrategia, los objetivos de negocio y las metas de desempeño. También incluye interactuar con las partes interesadas y presentar opiniones y acciones alternativas.

La supervisión de riesgos sólo es posible cuando el consejo de administración comprende la estrategia y el sector en el que opera la entidad y se mantiene informado sobre los asuntos relevantes. A medida que el contexto del negocio cambia, también lo hace el riesgo con respecto a la estrategia y los objetivos de negocio. En consecuencia, las cualificaciones requeridas para ser miembro del consejo pueden cambiar con el tiempo. Cada consejo de administración debe determinar por sí solo y revisar periódicamente si tiene las habilidades, la experiencia y la composición adecuadas para proporcionar una supervisión efectiva. Por ejemplo, es posible que las entidades expuestas al riesgo de ciberseguridad necesiten contar con miembros del consejo de administración que tengan experiencia en tecnologías de la información o tengan acceso a los conocimientos especializados necesarios a través de asesores independientes.

Ejemplo 6.1: Factores que impiden la independencia del consejo de administración

La independencia de un miembro del consejo puede verse obstaculizada si él o ella:

- Tiene un interés financiero sustancial en la entidad.
- Actualmente o recientemente ha desempeñado un cargo ejecutivo en la organización.
- Ha asesorado recientemente al consejo de administración sobre aspectos relevantes.
- Tiene una relación comercial con la entidad, como pueda ser de proveedor, cliente o proveedor de servicios subcontratados.
- Tiene una relación contractual existente con la organización.
- Ha donado una cantidad económica significativa a la entidad.
- Tiene relaciones de negocios o personales con partes interesadas clave de una organización.
- Es miembro del consejo de otras organizaciones que representan un posible conflicto de intereses.
- Ha ocupado el mismo cargo durante un período prolongado de tiempo.

Independencia

El consejo, en general, debe ser independiente. La independencia mejora la capacidad de los consejeros para ser objetivos y evaluar el desempeño y buen estado de la entidad sin ningún conflicto de interés o influencia indebida de las partes interesadas. El consejo de administración demuestra su independencia cuando cada uno de sus miembros es capaz de mostrar su capacidad individual para ser objetivo (ver Ejemplo 6.1).

Un consejo de administración independiente sirve como control y equilibrio de la dirección, y garantiza que la entidad se está gestionando en beneficio de las partes interesadas y no de un selecto número de consejeros o directivos.

Si bien la independencia a menudo requiere un enfoque mayor dentro de las empresas cotizadas, se pueden aplicar consideraciones similares a entidades privadas, organismos públicos y entidades sin ánimo de lucro.

Idoneidad de la gestión del riesgo empresarial

Es importante que el consejo de administración comprenda la complejidad de la entidad y cómo la integración de las capacidades y técnicas de gestión del riesgo empresarial aumentará el valor. El consejo mantiene conversaciones con la dirección para determinar si la gestión del riesgo empresarial está adecuadamente diseñada para aumentar el valor.

Por ejemplo, algunas organizaciones pueden aprovechar la comprensión de los riesgos y su alineación con la estrategia. En este caso, la dirección centraría la gestión del riesgo empresarial en las prácticas para lograr la estrategia y los objetivos de negocio – tal vez a través de distintas maneras de reducir las sorpresas y las pérdidas, o de reducir la variabilidad del desempeño. Otros pueden ganar valor al alinear la misión, la visión y los valores clave y las implicaciones de la estrategia elegida en su perfil de riesgo. En este caso, la gestión se centraría más en el establecimiento de la estrategia y el aumento del rango de oportunidades en línea con la estrategia elegida.

Sesgo de la organización

El sesgo en la toma de decisiones siempre ha existido y siempre existirá. No es inusual encontrar en una entidad personalidades dominantes, dependencia excesiva de los números, falta de consideración sobre la información contraria, ponderación desproporcionada de los acontecimientos recientes y tendencia a evitar o asumir riesgos. Por lo tanto, la cuestión no es si existe el sesgo, sino más bien cómo se puede gestionar el sesgo que afecta a las decisiones relacionadas con la gestión del riesgo empresarial. Se espera que el consejo comprenda los posibles sesgos existentes en la organización y que desafíe a la dirección para evitarlos.



Principio 2: Establece estructuras operativas

La organización establece estructuras operativas con el fin de lograr la estrategia y los objetivos de negocio.

Una estructura operativa describe la forma en que la entidad organiza y lleva a cabo sus operaciones diarias. A través de la estructura operativa, los empleados son responsables del desarrollo e implantación de prácticas para gestionar el riesgo y mantenerse alineado con los valores clave de la entidad. De esta forma, una estructura operativa contribuye a la gestión del riesgo alineada con la estrategia y los objetivos de negocio.

La estructura operativa suele estar alineada con la estructura jurídica y la estructura de gestión. La estructura jurídica influye en la forma en que opera una entidad y la estructura de gestión establece las líneas de rendición de cuentas, las funciones y responsabilidades para la gestión y operación continua del negocio.

Las diferentes estructuras jurídicas pueden ser más o menos adecuadas dependiendo del tamaño de la entidad y de cualquier estructura reguladora, fiscal o accionarial relevante. Es probable que una pequeña entidad opere como una sola entidad jurídica. Las entidades grandes pueden estar compuestas por varias entidades jurídicas distintas, en cuyo caso las decisiones pueden quedar separadas si la información sobre riesgos no se agrega a través de las estructuras jurídicas.

Bajo la estructura de gestión, el reporte suele trascender a las estructuras legales de la entidad. Por ejemplo, una sociedad que tiene tres divisiones jurídicas separadas informa como una sociedad consolidada.

Estructuras de la organización y líneas de reporte

La organización establece una estructura operativa y diseña líneas de reporte para llevar a cabo la estrategia y los objetivos de negocio. Es importante que la organización defina claramente las responsabilidades cuando diseñe las líneas jerárquicas. La organización también puede entablar relaciones con terceros externos que pueden influir en las líneas jerárquicas (por ejemplo, alianzas estratégicas de negocios, externalización o negocios conjuntos).

Diferentes estructuras operativas pueden dar lugar a diferentes perspectivas de un perfil de riesgo, lo que puede afectar a las técnicas de gestión del riesgo empresarial. Por ejemplo, la evaluación del riesgo dentro de una estructura operativa descentralizada puede indicar pocos riesgos, mientras que la visión dentro de un modelo centralizado puede indicar una concentración del riesgo – quizás relacionado con ciertos tipos de clientes, divisas o exposición fiscal.

Los factores que se deben tener en cuenta a la hora de establecer y evaluar las estructuras operativas pueden incluir las siguientes:

- Estrategia y objetivos de negocio de la entidad.
- Naturaleza, tamaño y distribución geográfica del negocio de la entidad.
- Los riesgos relacionados con la estrategia de la entidad y con los objetivos del negocio.
- La asignación de la autoridad, asunción de responsabilidades y responsabilidad a todos los niveles de la entidad.
- Tipología de líneas de reporte (por ejemplo, líneas directas/continuas vs. líneas secundarias) y canales de comunicación.
- Requisitos financieros, fiscales, regulatorios y otro tipo de requisitos de información.

La organización considera estos y otros factores a la hora de decidir qué estructura operativa adoptar. Por ejemplo, el consejo determinará qué funciones de la dirección tendrán al menos una “línea discontinua” de rendición de cuentas ante el consejo de administración para permitir una comunicación abierta con el consejo sobre todas las cuestiones de importancia. De igual manera, se definirán las líneas de reporte directas y las líneas meramente informativas a todos los niveles de la organización.

Estructuras de gestión del riesgo empresarial

La dirección planifica, organiza y lleva a cabo la estrategia y los objetivos de negocio de la entidad de acuerdo con su misión, visión y valores clave. En consecuencia, la dirección necesita información sobre cómo ocurren los riesgos asociados a la estrategia en toda la entidad. Un ejemplo de un método comúnmente utilizado para recopilar tal información es delegar la responsabilidad a un comité.

Los miembros de este comité son normalmente ejecutivos o altos directivos nombrados o elegidos por la dirección, y cada uno aporta sus habilidades, conocimientos y experiencia.

Las entidades con estructuras complejas pueden tener varios comités, cada una de los cuales estará integrado por diferentes miembros de la dirección, pero que se superponen. Esta estructura de múltiples comités se alinea entonces con la estructura operativa y las líneas de reporte, lo que permite a la dirección tomar decisiones de negocio según sea necesario, con una comprensión completa de los riesgos inherentes a esas decisiones.

Independientemente de la estructura particular del comité de gestión establecida, es habitual establecer claramente la autoridad del comité, los miembros de la dirección que forman parte de ella, la frecuencia con la que se reúnen y las responsabilidades específicas y los principios operativos. En algunas entidades pequeñas, la supervisión de la gestión del riesgo empresarial puede ser menos formal, y la dirección estará mucho más involucrada en las decisiones del día a día.

Facultades y responsabilidades

En una entidad que tenga un único consejo de administración, el consejo delega en la dirección la facultad para diseñar e implantar prácticas que faciliten la consecución de la estrategia y los objetivos de negocio. A su vez, la dirección define las funciones y responsabilidades de la entidad en general y de sus unidades operativas.

La dirección también define funciones, responsabilidades y líneas de rendición de cuentas de profesionales, equipos, divisiones y funciones alineadas con la estrategia y los objetivos de negocio.

En una entidad con una estructura de dos o más consejos de administración, se creará un consejo de supervisión de cara a las decisiones y estrategias a largo plazo que afecten al negocio en su conjunto. El consejo de administración se encarga de supervisar las operaciones del día a día, incluida la supervisión y la delegación de autoridad en la alta dirección. Al igual que con una estructura de gobierno de un solo consejo de administración, la alta dirección define las funciones y responsabilidades de la entidad en general y de sus unidades operativas.

Entre las funciones clave se suelen incluir las siguientes:

- Profesionales en un puesto de gestión que tienen la autoridad y responsabilidad de tomar decisiones y supervisar las prácticas de negocio para alcanzar la estrategia y los objetivos de negocio. Dentro del equipo de dirección, el responsable de riesgos¹⁴ suele encargarse de proporcionar conocimientos especializados y coordinar la gestión del riesgo.

14 El responsable de riesgos es la persona a quien se delega la autoridad sobre la gestión del riesgo empresarial; otros nombres para esta función o cargo pueden ser “responsable de la gestión del riesgo empresarial”, “responsable principal de riesgos”, “director de la gestión del riesgo empresarial” o “director de riesgos”.

- Los empleados que entienden tanto las normas de conducta de la entidad como los objetivos de negocio en relación con sus áreas de responsabilidad y las técnicas de gestión del riesgo empresarial relacionadas, en sus respectivos niveles de la entidad.

La dirección delega responsabilidades y tareas para que los empleados puedan tomar decisiones. Periódicamente, la dirección puede revisar sus estructuras reduciendo o añadiendo niveles de gestión, delegando más o menos responsabilidades y tareas a niveles inferiores, o asociándose con otras entidades.

Definir claramente la responsabilidad es importante, ya que faculta a las personas a actuar como sea necesario en una determinada función, pero también pone límites a su autoridad. Las decisiones basadas en el riesgo mejoran cuando la dirección:

- Delega solamente responsabilidad en la medida necesaria para conseguir la estrategia y los objetivos de negocio de la entidad (por ejemplo, revisión y aprobación de nuevos productos que implique a las funciones de negocio y de soporte necesarias, separadas del equipo de desarrollo de ventas).
- Especifica las operaciones que requieran revisión y aprobación (por ejemplo, la dirección tiene la facultad para aprobar adquisiciones).
- Tiene en cuenta aquellos riesgos nuevos y emergentes, en el marco de la toma de decisiones (por ejemplo, no se establece una alianza estratégica con un nuevo socio comercial si no se ha realizado antes la pertinente revisión del cumplimiento de la diligencia debida en la gestión de la entidad).

Gestión del riesgo empresarial en una entidad en continuo cambio

A medida que cambia una entidad, las capacidades y el valor procedente de la gestión del riesgo empresarial también pueden cambiar. La gestión del riesgo empresarial debe adaptarse a las capacidades de la entidad, considerando tanto lo que la organización busca alcanzar como la forma en que gestiona el riesgo. Es natural que la estructura operativa cambie a medida que evoluciona la naturaleza del negocio y su estrategia. Por lo tanto, la dirección evaluará regularmente la estructura operativa y las líneas de reporte asociadas.

En el mundo actual, caracterizado por unas tecnologías de la información en continua evolución, surgen nuevas estructuras operativas. Puede ser que las estructuras operativas habituales pronto se conviertan en estructuras de naturaleza “virtual”, que se basen mucho menos en ubicaciones físicas y más en interconexiones tecnológicas. Esto implicará examinar cómo cambiará el riesgo como respuesta a ello: ¿En qué momento de la toma de decisiones se considerará el riesgo? ¿Cómo afectará esto a la consecución de la estrategia y los objetivos de negocio? La dirección debe estar preparada para abordar estas cuestiones bajo una nueva estructura operativa y comprender cómo los cambios motivados por la innovación influirán en las técnicas de gestión del riesgo empresarial.



Principio 3: Define la cultura deseada

La organización define los comportamientos deseados que caracterizan la cultura a la que aspira la entidad.

Cultura y comportamientos deseados

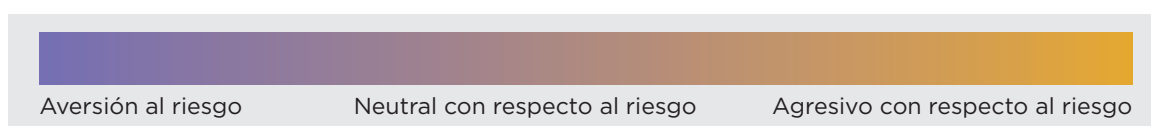
La cultura de una organización refleja sus valores, comportamientos y decisiones fundamentales. Las decisiones dependen a su vez de la información, juicios de valor, capacidades y experiencia disponibles. La cultura de una entidad influye en la forma en que la organización aplica este Marco: cómo identifica el riesgo, qué tipos de riesgo acepta y cómo lo gestiona.

Le corresponde al consejo de administración y a la dirección definir la cultura deseada de la entidad en su conjunto y de los individuos que la integran. Los valores clave impulsan los comportamientos esperados en la toma de decisiones del día a día para satisfacer las expectativas de las distintas partes interesadas. El establecimiento de una cultura que abarque a todas las personas –donde la gente haga lo correcto en el momento oportuno– es fundamental para que la organización sea capaz de aprovechar las oportunidades y gestionar el riesgo para lograr la estrategia y los objetivos de negocio.

Muchos factores conforman la cultura de las entidades. Los factores internos incluyen, entre otros, el nivel de juicios de valor y de autonomía que se proporciona al personal, la forma en que los empleados de la entidad interactúan entre sí y con sus jefes, las normas y reglas, la disposición física del lugar de trabajo y el sistema de recompensas establecido. Los factores externos incluyen requisitos regulatorios y expectativas de los clientes, inversores y otros elementos.

Todos estos factores influyen cuando la entidad se posiciona en el entorno cultural, que va desde la aversión al riesgo hasta la agresividad con respecto al riesgo (véase la Figura 6.1). Cuanto más se acerca una entidad al extremo de agresividad con respecto al entorno de riesgo, mayor será su propensión de aceptar tipos y niveles de riesgo mayores para lograr la estrategia y los objetivos de negocio (véase el Ejemplo 6.2).

Figure 6.1: Entorno cultural



Una cultura bien definida no implica que se tenga que adoptar un enfoque estándar con respecto a la gestión del riesgo empresarial. Es decir, los responsables de algunas unidades operativas pueden estar dispuestos a asumir más riesgos, mientras que otros pueden ser más conservadores. Por ejemplo, una unidad comercial agresiva puede centrar su atención en cerrar una venta sin prestar mayor atención al cumplimiento de las regulaciones más allá del apetito al riesgo deseado, mientras que los empleados de la unidad contratante puede centrarse en mantener el cumplimiento total dentro del apetito al riesgo deseado. Trabajando por separado, estas dos unidades podrían afectar negativamente a la entidad, pero si tienen una comprensión compartida de las decisiones de riesgo aceptables, pueden responder adecuadamente dentro del apetito al riesgo definido para lograr la estrategia y los objetivos de negocio.

El Juicio profesional

El juicio profesional tiene un papel importante que desempeñar en la definición de la cultura deseada y en la gestión del riesgo en todo el entorno cultural. A menudo se confía en los juicios de valor:

- Cuando existe información o datos disponibles limitados para apoyar una decisión.
- Cuando se producen cambios sin precedentes en la estrategia, objetivos de negocio, desempeño o perfil de riesgo de la organización.
- En tiempos de grandes cambios y transformaciones.

El juicio profesional depende de las experiencias personales, el apetito al riesgo, las capacidades y el nivel de información disponible y el sesgo organizacional. El juicio profesional por parte del equipo de dirección es susceptible de sesgo siempre que exista un exceso o un déficit de confianza, por ejemplo, en las habilidades de la organización, o cuando las hipótesis o las correlaciones en las que se basen dependan de una información limitada. Los comportamientos de la entidad también pueden derivar en un sesgo organizacional que afecte al juicio profesional. Las dinámicas de grupo en reuniones, los estilos de comunicación por parte de la dirección, y el reconocimiento de los empleados pueden afectar a la capacidad de la dirección para adoptar un juicio profesional óptimo.

El juicio profesional influye en la capacidad de una organización para gestionar períodos de crisis y retomar sus operaciones del día a día de una manera más eficiente. Durante los períodos de grandes transformaciones, puede verse frenada la capacidad de una organización para funcionar de acuerdo con las políticas o procedimientos existentes, exigiendo a la organización que dependa en mayor medida del juicio profesional y los comportamientos de la dirección y del consejo de administración. Las acciones emprendidas por la organización para sacar a la entidad de una crisis dependen de la responsabilización, los comportamientos y las acciones adoptadas por los empleados. Las organizaciones con equipos de dirección que tienen una amplia experiencia, capacidades sólidamente establecidas y un apetito al riesgo claramente definido probablemente ejercerán su juicio profesional con mayor claridad. A su vez, es probable que los partes interesadas tengan mayor confianza en que la organización se recuperará con éxito cuando el juicio profesional demostrado esté en línea con los valores clave de la entidad.

El juicio profesional también afecta a la medida en que se fomentan la innovación y la identificación de oportunidades dentro de una entidad. Cuando la entidad se caracteriza por contar con unas prácticas muy prescriptivas y una delegación de facultades limitada, puede ahogarse su potencial de innovación. Una organización que hace un mayor hincapié en desarrollar una cultura consciente del riesgo, puede confiar en mayor medida en el juicio profesional adoptado por la dirección cuando toma decisiones que aportan valor y buscan nuevas oportunidades en línea con el apetito al riesgo de la entidad.

Ejemplo 6.2: Dos ejemplos del entorno cultural

Una central nuclear probablemente tendrá una cultura de aversión al riesgo en sus operaciones diarias. Tanto la dirección como las partes interesadas externas esperan que las decisiones relativas a las nuevas tecnologías y sistemas se tomen cuidadosamente y con gran atención a los detalles y a la seguridad, a fin de proporcionar una expectativa razonable de la fiabilidad de la planta. No es deseable que las centrales nucleares inviertan fuertemente en tecnologías innovadoras y no probadas que son críticas para la gestión de las operaciones.

En cambio, es más probable que un gestor de capital riesgo sea una entidad agresiva con respecto al riesgo. La dirección y los inversores externos tendrán grandes expectativas de desempeño que requieren asumir riesgos potencialmente graves, sin dejar de estar dentro del apetito al riesgo definido por la entidad.

Influencia Cultural

La cultura de una organización afecta a cómo se identifica, evalúa y responde al riesgo desde el momento en que se establece la estrategia hasta la ejecución y el desempeño. Ejemplos de ello son aspectos como:

- *Determinar el alcance de del establecimiento de la estrategia y los objetivos de negocio:* La cultura de una organización puede afectar al tipo de alternativas estratégicas que se estén

valorando. Por ejemplo, a pesar de que se disponga de unos prometedores estudios de viabilidad, una organización con aversión al riesgo puede optar por no expandir sus operaciones mineras y de perforación en nuevas geografías.

- *Aplicar rigor a los procesos de identificación y evaluación de riesgos:* Dependiendo de la posición que ocupe una organización en el entorno cultural, puede que varíen la naturaleza y el tipo de riesgos y oportunidades. Lo que una entidad con aversión al riesgo considera riesgos potenciales puede que sean oportunidades dignas de ser aprovechadas para otra. Por ejemplo, la creciente demanda de pedidos online puede ser un riesgo para un fabricante tradicional pero una oportunidad para un minorista que quiera aumentar sus ventas y cuota de mercado.
- *Seleccionar las respuestas al riesgo y asignar recursos limitados:* Una entidad con aversión al riesgo puede adoptar respuestas al riesgo o asignar recursos adicionales para obtener una mayor confianza en el logro de un objetivo de negocio específico. Los costes y beneficios asociados a las respuestas incrementales al riesgo pueden ser interpretados de manera menos favorable por otras entidades más agresivas con respecto al riesgo. Por ejemplo, la contratación de un seguro adicional puede ser vista con buenos ojos por las entidades con aversión al riesgo o ser considerada un uso ineficiente de los recursos por parte de otra entidad.
- *Revisar el desempeño:* Las tendencias en el perfil de riesgo o en el contexto empresarial pueden ser abordadas de manera diferente por entidades en diferentes puntos del entorno cultural. Una entidad con aversión al riesgo puede hacer cambios más rápidamente en las respuestas a los riesgos a medida que se identifican desviaciones en el desempeño. Las entidades más agresivas con respecto al riesgo esperarán más tiempo antes de hacer cambios o harán cambios menores. Por ejemplo, las compañías aéreas pueden ajustar los horarios de vuelo con mayor rapidez en respuesta a los cambios adversos de las condiciones meteorológicas que las compañías ferroviarias o de autobuses, que pueden seguir operando sin interrupción durante más tiempo.

Alineación de valores clave, toma de decisiones y comportamientos

La capacidad de una organización para lograr con éxito la estrategia y los objetivos de negocio se verá obstaculizada cuando los comportamientos y decisiones de dicha organización no estén alineados con sus valores clave. Esta desalineación puede derivar en una pérdida de confianza de las partes interesadas, enfoques incoherentes y un desempeño inferior al previsto.

Cuando no se respetan los valores clave, generalmente es por una de las siguientes razones:

- El consejo y la alta dirección no establecen o actúan con una cultura adecuada.
- El consejo no supervisa el cumplimiento de las normas (internas y externas) por parte de la dirección.
- Los mandos intermedios y la gerencia no están alineados con la misión, visión y estrategia de la entidad.
- El riesgo se analiza después de haber establecido la estrategia o realizado la planificación empresarial.
- Los objetivos de desempeño generan incentivos o presiones que favorecen un comportamiento contrario a los valores clave.
- No existe una política clara de comunicación para escalar riesgos y aspectos clave relacionados con el desempeño.

- La investigación y resolución de la toma de riesgos excesivos es inadecuada.
- La dirección o los empleados actúan deliberadamente en contra de los valores clave.

En un entorno cultural consciente del riesgo, los empleados saben lo que la entidad establece y los límites con respecto a los cuales puede operar. Pueden analizar abiertamente y debatir qué riesgos se deben tomar para lograr la estrategia y los objetivos de negocio de la entidad, de manera que los comportamientos de los empleados y de la dirección estén más alineados con el apetito al riesgo de dicha entidad.

Evolución de la cultura

La cultura no se mantiene estática en el tiempo (ver Ejemplo 6.3). Los cambios dentro de la organización y las influencias externas pueden hacer que la cultura de una entidad evolucione. Un nuevo equipo de dirección puede tener una actitud y filosofía diferentes sobre la gestión del riesgo empresarial. Asimismo, una adquisición podría alterar la misión y visión de una entidad y afectar a la toma de decisiones. Las fusiones y adquisiciones también pueden dar lugar a cambios en la cultura. Estos cambios afectarán a la forma en que la organización ve el riesgo e influirán en la forma en que se tomen las decisiones.

Ejemplo 6.3: Cuando se producen desviaciones con respecto a las normas de conducta

Una *start-up* tecnológica está desarrollando un nuevo algoritmo que mejora la precisión del seguimiento de los cambios en el comportamiento de los clientes y sus preferencias de compra. En sus primeras etapas de desarrollo, esta empresa tuvo una cultura muy agresiva con respecto al riesgo, mientras se centraba en las fases iniciales de establecimiento de las operaciones comerciales e identificación de posibles socios comerciales, clientes y oportunidades de mercado. A medida que la organización fue madurando, formó alianzas más formales con clientes más grandes. La nueva empresa decidió finalmente salir a bolsa para acceder a un grupo más grande de inversores. Con este cambio, la empresa se desplazó hacia la izquierda en el entorno cultural, lo cual refleja el apetito al riesgo de la empresa y los cambios correspondientes en las prácticas y capacidades de gestión del riesgo empresarial de la entidad.



Principio 4: Demuestra compromiso con los valores clave

La organización demuestra su compromiso con los valores clave de la entidad.

Trasladar los valores clave a toda la organización

Comprender los valores clave de la entidad es fundamental para la gestión del riesgo empresarial. Los valores clave se reflejan en las acciones y decisiones tomadas a lo largo de toda la entidad. Sin una comprensión y un compromiso firme y positivo con respecto a los valores comunicados desde el consejo y la alta dirección de la organización, la conciencia del riesgo puede verse socavada y las decisiones relacionadas con el riesgo pueden ser incompatibles con estos valores. La forma en que los valores se comunican a través de la organización a menudo se describe como “el tono” que se marca en la organización.

Este tono ha de ser coherente y estar alineado con los valores clave, las palancas del negocio y el comportamiento deseado de los empleados y los socios comerciales. La coherencia contribuye a unir a la organización en sus esfuerzos por lograr la estrategia y los objetivos de negocio de la entidad. Pero no siempre es fácil marcar el tono de un modo coherente. Por ejemplo, diferentes mercados pueden requerir diferentes enfoques de motivación, evaluación y servicio al cliente. De vez en cuando, estos factores pueden ejercer presión sobre los diferentes niveles de la entidad, lo que provocará cambios en esa pauta (en las entidades más grandes, esta visión se conoce a veces como “marcar el tono en los mandos intermedios”). Sin embargo, cuanto más coherente sea el tono marcado en toda la entidad, más coherente será el desempeño de las responsabilidades en materia de gestión del riesgo empresarial de cara a lograr la estrategia y los objetivos de negocio de la entidad.

Alinear la cultura y el tono de la organización da confianza a las distintas partes interesadas en que la entidad cumple sus valores clave y persigue su misión y visión. Por ejemplo, en una entidad en la que la “seguridad ante todo” es un valor clave, la dirección demuestra su compromiso alentando activamente a todas las personas en todos los niveles a que identifiquen y amplíen las prácticas de seguridad, independientemente de su función dentro de la organización. Las partes interesadas externas, como los inspectores de seguridad que observan el contenido y el tono que se marca en los cursos de formación, las comunicaciones internas y los informes, tendrán la confianza de que la organización está adoptando su cultura y sus valores clave.

Adopción de una cultura consciente del riesgo

La dirección define las características necesarias para lograr la cultura deseada en el tiempo, con el enfoque y la supervisión del consejo de administración. Una organización puede entonces adoptar una cultura consciente del riesgo:

- *Manteniendo un liderazgo fuerte:* El consejo de administración y la dirección le dan importancia a la creación de una correcta toma de conciencia del riesgo y de un tono adecuado en toda la entidad. La cultura y, por tanto, la conciencia del riesgo no se puede cambiar únicamente a través de las funciones de los equipos o departamentos de la segunda línea de defensa por sí solos; la dirección de la organización (la primera línea de defensa) debe ser el verdadero motor del cambio.
- *Empleando un estilo de dirección participativo:* La dirección anima al personal a participar en la toma de decisiones y a analizar los riesgos para la consecución de la estrategia y los objetivos de negocio.



- *Asumiendo responsabilidades por todas las acciones realizadas:* La dirección documenta las políticas de las que es responsable y las cumple, demostrando al personal que la falta de asunción de responsabilidades no se tolera y que las responsabilidades se remuneran y re-compensan de forma oportuna.
- *Alineando los comportamientos relacionados con el riesgo y la toma de decisiones con el desempeño:* Los programas de remuneración e incentivos están alineados con los valores clave de la organización, incluidos los comportamientos esperados, el cumplimiento de los códigos de conducta y la promoción de la asunción de responsabilidades de cara a la toma de decisiones relacionadas con el riesgo y la adopción del juicio profesional.
- *Integrando el riesgo en la toma de decisiones:* La dirección aborda el riesgo de forma coherente al tomar decisiones clave de negocio, lo cual incluye analizar y revisar escenarios de riesgo que pueden ayudar a todos a entender la interrelación y los impactos de los riesgos antes de tomar las decisiones.
- *Llevando a cabo conversaciones abiertas y honestas sobre los riesgos que afronta la entidad:* La dirección no considera que el riesgo sea negativo y entiende que la gestión del riesgo es clave para alcanzar la estrategia y los objetivos de negocio.
- *Fomentar la conciencia del riesgo en toda la entidad:* La dirección envía continuamente mensajes al personal indicando que la gestión del riesgo es parte de sus responsabilidades diarias, y que no sólo se valora, sino que también es clave para el éxito y la supervivencia de la entidad.

Alinear el comportamiento individual con la cultura organizacional es fundamental. La influencia más poderosa procede del equipo de dirección que define y sostiene las prioridades de la organización. La organización desarrolla políticas, procedimientos y normas de conducta de forma explícita. De manera implícita, la organización debe dar ejemplo sobre sus valores clave y sus normas de conducta. La clave es que la dirección predique con el ejemplo de esos valores, reconociendo que las actuaciones relacionadas y alineadas con los valores clave son los que establecen la cultura más eficazmente aunque estas sean sutiles y se sobreentienda que están consideradas en los procesos de la entidad.

Refuerza la asunción de responsabilidades

El consejo de administración insta al director general¹⁵ a que asuma la responsabilidad última de gestionar los riesgos a los que se enfrenta la entidad y de establecer las técnicas y capacidades de gestión del riesgo empresarial necesarias para respaldar la consecución de la estrategia y los objetivos de negocio de la entidad. El director general y otros miembros de la dirección, en su conjunto, son responsables últimos de todos los aspectos relacionados— desde el diseño inicial hasta la evaluación periódica de la cultura y las capacidades de gestión del riesgo empresarial. En el caso de la gestión del riesgo empresarial, la asunción de responsabilidades se demuestra en cada estructura utilizada por la entidad.

La dirección proporciona orientación a los empleados para que entienda los conceptos relacionados con los riesgos. La dirección también demuestra liderazgo al comunicar las expectativas de conducta para todos los aspectos relacionados con la gestión del riesgo empresarial. Ese liderazgo mostrado desde el consejo y la alta dirección ayuda a establecer y a cumplir con las responsabilidades.

La asunción de responsabilidades se evidencia a través de las siguientes maneras:

- La dirección y el consejo de administración comunican claramente las expectativas (por ejemplo, desarrollando y haciendo cumplir las normas de conducta).
- La dirección se asegura de que la información sobre riesgos fluye por toda la entidad (por ejemplo, comunicando cómo se toman las decisiones y cómo se considera el riesgo en el marco de la toma de decisiones).
- Los empleados se comprometen con objetivos de negocio colectivos (por ejemplo, alineando los objetivos y el desempeño individual con los objetivos de negocio de la entidad).

15 El Marco hace referencia al "director general". Otros términos que describen este puesto de liderazgo en la alta dirección y que se pueden utilizar incluyen "director ejecutivo", "presidente", "consejero delegado" o "vicepresidente".

- La dirección analiza las desviaciones con respecto a las normas y comportamientos (por ejemplo, poniendo fin a la relación laboral o tomando otras acciones correctivas por no haber cumplido con las normas de la organización; llevando a cabo evaluaciones del desempeño).

Asunción de responsabilidades propias

En algunas estructuras de gobierno, los objetivos de desempeño recaen de manera descendente desde el consejo de administración hacia el director general, la dirección y el resto de los empleados, y la evaluación del desempeño se lleva a cabo para cada uno de estos niveles organizativos. El consejo de administración evalúa el desempeño del director general, que a su vez evalúa al equipo de la alta dirección, y así sucesivamente. En cada nivel, se evalúa el cumplimiento de los valores clave y las conductas esperadas, al tiempo que se asignan las correspondientes recompensas o medidas disciplinarias en caso oportuno. El consejo también puede llevar a cabo una autoevaluación para evaluar sus propias fortalezas e identificar oportunidades para mejorar la gestión del riesgo empresarial.

En otras estructuras de gobierno, como en las estructuras de dos o más consejos, el consejo de supervisión evalúa el desempeño del consejo ejecutivo en su conjunto y de sus miembros individuales; el consejo ejecutivo evalúa al equipo de la alta dirección que depende directamente del consejo ejecutivo.

Mantener la comunicación abierta y exenta de represalias

Es responsabilidad de la dirección cultivar una comunicación abierta y transparente sobre el riesgo y las expectativas de asunción de riesgos. La dirección ha de demostrar que el riesgo no es una cuestión que deba dejarse para el consejo de administración. Lo hace enviando mensajes claros y coherentes a los empleados de que la gestión del riesgo forma parte de las responsabilidades diarias de todos, y que no sólo se valora, sino que también es fundamental para el éxito y la supervivencia de la entidad. La comunicación abierta y la transparencia sobre los riesgos de la organización permiten a la dirección y a los empleados trabajar juntos de forma continua para compartir la información sobre riesgos en toda la entidad.

La información es compartida y trasladada al nivel pertinente dentro de la entidad. La transparencia de la información puede hacer referencia a:

- Cambios en la comprensión de las hipótesis que sustentan la elección de una estrategia u objetivos de negocio.
- Adecuación continua de la respuesta al riesgo.
- Incidentes, fallos, errores o pérdidas inesperadas.
- Desviaciones en el desempeño, incluido un desempeño excesivo o llevado a cabo por terceros.
- Cambios en el perfil de riesgo o visión del riesgo de la entidad a nivel de cartera.
- Desviaciones en los comportamientos esperados en comparación con los valores clave establecidos en la organización.

Además, la dirección proporciona al consejo de administración un nivel adecuado de información sobre los riesgos para evaluar si las prácticas actuales de gestión del riesgo empresarial son apropiadas. El consejo sólo puede aportar su supervisión de riesgos si se le proporciona información oportuna y completa, y cuando las líneas de comunicación están abiertas para analizar cualquier asunto con la dirección.

La entidad que demuestra una comunicación abierta y transparente ofrece diversos canales para que tanto la dirección como los empleados comuniquen sus preocupaciones sobre la asunción de riesgos, conductas empresariales o comportamientos potencialmente inapropiados o asunciones de riesgos excesivos, sin temor a represalias o intimidaciones. La entidad también prohíbe cualquier forma de represalia frente a cualquier empleado que participe de buena fe en cualquier investigación de comportamiento que no se ajuste a los estándares de conducta y al apetito al riesgo. Los empleados que lleven a cabo represalias o intimidaciones inapropiadas o ilegales estarán sujetos a medidas disciplinarias.

Responder ante conductas inadecuadas e incumplimiento de los valores clave

Si el establecimiento de una cultura en la que la dirección y los empleados actúen de acuerdo con los comportamientos deseados es clave para la gestión del riesgo empresarial, entonces ¿por qué a veces las cosas no salen según lo previsto? Incluso en aquellas entidades que demuestran un compromiso sólido con sus valores clave, en ocasiones se producen fallos operativos, escándalos y crisis que dañan la reputación, impidiendo a la organización alcanzar la estrategia y los objetivos de negocio.

Las conductas irregulares se producen por tres razones: porque la gente comete errores (por confusión o desconocimiento), tiene un momento de debilidad, o que opta por hacerlo de mala fe. Sabiendo que se puede dar cualquiera de estas tres situaciones, una organización debe alinear los comportamientos y valores clave para ayudar a las personas a evitar cometer errores e identificar a potenciales delincuentes, ya sean individuos o grupos. Para ello es necesario evaluar y priorizar adecuadamente los riesgos y elaborar respuestas detalladas para los mismos.

La organización envía un mensaje claro de lo que es un comportamiento aceptable e inaceptable cuando se tiene conocimiento de que se han producido desviaciones. Las desviaciones de las normas de conducta deben abordarse de manera oportuna y consistente (véase el ejemplo 6.4).

La respuesta a una conducta inadecuada dependerá de su magnitud, la cual es determinada por la dirección de acuerdo con la legislación y norma de conducta pertinente. La respuesta podrá variar desde que un empleado reciba una advertencia hasta que sea puesto a prueba o incluso pueda ser despedido. En todos los casos, las expectativas de comportamiento, adopción del juicio profesional y toma de decisiones ante el riesgo deben ser consistentes. La consistencia garantiza que la cultura de la entidad no se vea socavada.

Ejemplo 6.4: Cuando se producen incumplimientos de los valores clave

Para una compañía farmacéutica global, el área de investigación y el desarrollo (I+D) suele ser uno de los principales centros de costes, ya que los productos pueden tardar entre diez y veinte años en desarrollarse y comercializarse, y requieren una inversión financiera significativa. Durante la fase de investigación, es habitual que se identifiquen muchos efectos secundarios de un producto. Pero si la investigación y el desarrollo no revelaran todos los efectos secundarios potenciales al equipo de dirección (impidiendo así que la dirección tome una decisión informada sobre el paso de la fase de ensayos clínicos a la producción) y finalmente se lanzara el medicamento, podría tener consecuencias graves para la entidad si los pacientes que usan el medicamento presentaran efectos secundarios adversos. Por otra parte, el hecho de que la fase de I+D no revelara ninguna información al respecto, probablemente constituiría un claro incumplimiento del comportamiento deseado de la empresa.



Principio 5: Atrae, desarrolla y retiene a profesionales capacitados

La organización está comprometida con contar con un capital humano que esté alineado con la estrategia y los objetivos de negocio.

Establecimiento y evaluación de competencias

La Dirección, con la supervisión del consejo de administración, define los perfiles profesionales necesarios para lograr la estrategia y los objetivos de negocio. La identificación de las competencias necesarias ayuda a establecer cómo se deben llevar a cabo los diversos procesos de negocio y qué habilidades se deben considerar. Esta labor comienza con el consejo de administración, decidiendo cuáles son las competencias que se buscan en el director general, y el director general decidirá a su vez las competencias del equipo de dirección y los empleados de cada una de las divisiones, unidades operativas y funciones de la entidad. Es decir, el consejo de administración evalúa las competencias del director general y, a su vez, la dirección evalúa las competencias a todos los niveles de la entidad, identificando las posibles deficiencias o excesos cuando sea necesario.

La función de recursos humanos ayuda a identificar y definir las competencias necesarias al ayudar a la dirección a desarrollar las descripciones de puestos, funciones y responsabilidades, proporcionando formación y evaluando el desempeño individual en materia de gestión del riesgo. La dirección considera los siguientes factores a la hora de desarrollar los requisitos de competencias:

- Conocimiento, habilidades y experiencia en la gestión del riesgo empresarial.
- La naturaleza y el grado de criterio profesional que debe aplicarse, así como las limitaciones que deben establecerse en las facultades y responsabilidades asignadas a un puesto en particular.
- Los costes y beneficios de diferentes niveles de competencias y experiencia.

Atraer, desarrollar y retener profesionales

El compromiso permanente con las competencias se apoya en los procesos de gestión de los recursos humanos y se integra en ellos. El equipo de dirección, en sus diferentes niveles, establece la estructura y el proceso a seguir para:

- *Atraer:* Buscar el número necesario de candidatos que se ajusten a la cultura de riesgo de la entidad, a las conductas deseadas, estilo operativo y necesidades organizacionales, y que tengan las competencias adecuadas para los puestos propuestos.
- *Desarrollar:* Capacitar a los profesionales para desarrollar y mantener las competencias en gestión de riesgos apropiadas para las funciones y responsabilidades asignadas, reforzar las normas de conducta y los niveles esperados de competencia de cara al desarrollo de determinadas funciones asignadas, adaptar la formación en función de los puestos y las necesidades, y tener en cuenta un adecuado mix de técnicas de formación, que incluirá modalidades de formación presencial, autoestudio y formación en el propio puesto de trabajo.
- *Tutelar:* Guiar al profesional sobre el desempeño en lo relativo a las normas de conducta y competencias que se esperan del mismo, alinear las habilidades y conocimientos especializados del profesional con la estrategia y los objetivos de la entidad y ayudarlo a adaptarse a un entorno en constante evolución.



- *Evaluar*: Medir el desempeño de las personas en relación con la consecución de los objetivos de negocio y las competencias en materia de gestión del riesgo empresarial, considerando las normas y procedimientos aprobados en la entidad.
- *Retener*: Proporcionar incentivos para motivar a los profesionales y reforzar el nivel deseado de desempeño y conducta. Esto incluye ofrecer formación y posibles certificaciones en caso de considerarse necesario.

Mediante este proceso, cualquier comportamiento que incumpla con las normas de conducta, las políticas y expectativas de desempeño, y las responsabilidades de gestión del riesgo empresarial será identificado, evaluado y corregido de manera oportuna.

Además, las organizaciones deben identificar y evaluar continuamente aquellos puestos que sean claves para alcanzar la estrategia y los objetivos de negocio. La decisión de si un cargo o función es clave se tomará evaluando las consecuencias de tener ese cargo o función temporal o permanentemente sin ocupar. La pregunta que debe hacerse es: ¿Cómo se logrará la estrategia y los objetivos de negocio si, por ejemplo, se deja sin cubrir el puesto de director general?

Recompensar el desempeño

El desempeño se ve influido en gran medida por el grado en el que los profesionales asumen sus responsabilidades y cómo se ven recompensados al respecto. La dirección y el consejo de administración establecen incentivos y otras recompensas adecuadas a los distintos niveles de la entidad, teniendo en cuenta la consecución de los objetivos de negocio a corto y largo plazo. Para establecer estos incentivos y recompensar es necesario evaluar y priorizar adecuadamente los riesgos y elaborar respuestas detalladas a los mismos. Por el contrario, con arreglo a un programa de incentivos, aquellos profesionales que no cumplan las normas de conducta de la entidad, serán sancionados y no se les ascenderá ni recompensará de ningún otro modo.

Los aumentos de sueldos y las primas son incentivos habituales, pero las recompensas no monetarias como la asignación de mayores responsabilidades, mayor visibilidad y reconocimiento también son efectivas. La dirección establece y revisa regularmente las estructuras de medición y comparación de la entidad junto con sus comportamientos deseados. Al hacerlo, se revisa el desempeño de los individuos y equipos en relación con los parámetros definidos, los cuales incluyen factores de desempeño del negocio, así como de competencias demostradas (véase Ejemplo 6.5).

Ejemplo 6.5: Desempeño, incentivos y recompensas

Un negocio familiar dedicado a la fabricación de muebles está tratando de conseguir una mayor fidelización entre sus clientes a través de su gama de muebles de alta calidad. Para ello, quiere involucrar a su plantilla para que reduzcan los ratios de defectos de producción y alineen sus parámetros de desempeño, incentivos y recompensas con los objetivos de producción de su unidad operativa y con las expectativas de cumplir todas las normas de calidad y de seguridad de los productos, leyes de seguridad en el trabajo, programas de fidelización de clientes y mediante una precisa comunicación de revisión de productos defectuosos. Una vez que se alinearon los objetivos de negocio con los incentivos y las recompensas, la compañía percibió un mayor nivel de asunción de responsabilidades entre sus empleados y una mayor disposición a trabajar en equipo para abordar desafíos y, en último término, un descenso palpable en el número de productos defectuosos.

Abordar la presión

Una organización se enfrenta a distintas presiones que proceden de muy diversas fuentes. Las metas que la dirección establece para alcanzar la estrategia y los objetivos de negocio, por su propia naturaleza, generan presión. La presión también puede surgir durante tareas específicas (por ejemplo, durante la negociación de un contrato comercial), y a veces pueden ser autoimpuestas. Los cambios inesperados en el contexto empresarial, como pueda ser una repentina ralentización de la economía, también pueden aumentar la presión.

La presión puede motivar a los profesionales a cumplir sus expectativas o hacer que teman las consecuencias de no lograr la estrategia y los objetivos de negocio. En este último caso, las personas pueden eludir determinados procesos o llevar a cabo actividades fraudulentas. Las organizaciones pueden influir positivamente en la presión generada, reequilibrando las cargas de trabajo o aumentando los recursos, según proceda, y seguir comunicando la importancia de aplicar comportamientos éticos.

La presión excesiva se suele asociar a:

- Objetivos de desempeño poco realistas, en especial cuando se exigen resultados a corto plazo.
- Conflictos derivados de los distintos objetivos de negocio que tienen las partes interesadas.
- Desequilibrio entre la compensación por objetivos financieros a corto plazo y a los de a largo plazo centrados en atender a las partes interesadas, como los objetivos de sostenibilidad (véase Ejemplo 6.6).

La presión también está motivada por los cambios: los cambios en la estrategia, en la estructura operativa, en las actividades de adquisición o desinversión, y en el contexto empresarial, que a menudo es externo a la organización, como es el caso de las actuaciones de la competencia en el mercado. La dirección y el consejo de administración deben estar preparados para establecer y ajustar, según corresponda, la presión al asignar responsabilidades, diseñar medidas de desempeño y al evaluar el propio desempeño. Es responsabilidad de la dirección guiar a aquellas personas en quienes hayan delegado facultades para que estas adopten las decisiones adecuadas en el curso ordinario del negocio.

Ejemplo 6.6: El precio de la presión

Deben tenerse en cuenta las posibles reacciones negativas a las presiones al establecer la retribución y los incentivos. Por ejemplo, los gestores de inversiones asumen riesgos en nombre de sus clientes, y el rendimiento de esas carteras de inversión puede afectar significativamente a la remuneración de la entidad. Unos honorarios basados en la rentabilidad del fondo pueden provocar un comportamiento muy diferente en comparación con unos honorarios basados en el valor del fondo. Alinear la retribución de los profesionales con las conductas esperadas puede ayudar a reforzar la cultura deseada. Por el contrario, las estructuras de incentivos que no consideran adecuadamente los riesgos asociados a la generación de presión pueden crear comportamientos inapropiados.

Preparación de la sucesión

Para preparar la sucesión dentro de una organización, el consejo de administración y la dirección deben desarrollar planes de contingencia para asignar responsabilidades clave en materia de gestión del riesgo empresarial. En particular, es necesario definir planes de sucesión para los principales directivos, y los candidatos a la sucesión deben ser formados, dirigidos y asesorados por mentores para asumir ese papel. Por lo general, las entidades más grandes identifican a más de una persona que podría desempeñar un papel clave en la organización.

7. Estrategia y establecimiento de objetivos



Principios relacionados con la estrategia y el establecimiento de objetivos



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 riesgo.
9. **Formula Objetivos de Negocio:**
La organización considera el riesgo al tiempo que establece objetivos de negocio en los distintos niveles, alineados y apoyados en la estrategia.

Introducción

Cada entidad tiene una estrategia para llevar a cabo su misión, visión y para conservar y mejorar el valor. Puede resultar complicado evaluar si la estrategia se alinearán con la misión, la visión y los valores clave, pero es un desafío que debe ser asumido. Al integrar la gestión del riesgo empresarial con el establecimiento de la estrategia, la organización obtiene una mejor comprensión del perfil de riesgo asociado a con la estrategia y los objetivos de negocio. Realizar este ejercicio, orienta a la organización de cara a perfilar su estrategia considerando las tareas necesarias para llevarla a cabo.



⚙️ Principio 6: Analiza el contexto empresarial

La organización considera los efectos potenciales del contexto empresarial sobre el perfil de riesgo.

Entendiendo el contexto empresarial

Una organización considera el contexto empresarial cuando desarrolla una estrategia que apoye su misión, visión y valores clave. Se entiende por “contexto empresarial” las tendencias, relaciones y demás factores que influyen en la estrategia actual y futura de una organización y en sus objetivos de negocio. El contexto empresarial puede ser:

- Dinámico, donde pueden surgir nuevos riesgos en cualquier momento que interrumpen el status quo (por ejemplo, un nuevo competidor que haga que las ventas de productos disminuyan o incluso que el producto quede obsoleto).
- Complejo, con muchas interconexiones e interdependencias (por ejemplo, una entidad que tenga muchas unidades operativas en todo el mundo, cada una con sus propios regímenes políticos, políticas regulatorias y leyes fiscales).
- Impredecible, donde se sucedan cambios a gran velocidad y de manera imprevista (por ejemplo, fluctuaciones monetarias e inestabilidad política).

El entorno externo y las partes interesadas

El entorno externo forma parte del contexto empresarial. Se trata de todo aquello que, estando fuera de la entidad, puede influir en la capacidad de la entidad para alcanzar la estrategia y los objetivos de negocio, incluidas las partes interesadas externas.

Un ejemplo de partes interesadas externas es un organismo regulador que otorga a una entidad una licencia para operar, pero también tiene autoridad para multarla u obligarla a cerrar temporal o permanentemente sus actividades. Otro ejemplo es el caso de un inversor que aporta capital a la entidad, pero que puede decidir llevar esa inversión a otro lugar si no está de acuerdo con la dirección estratégica de la entidad o con su nivel de desempeño. Una organización que identifique su entorno externo y las partes interesadas, así como su grado de influencia en el negocio, podrá estar en mejor posición para anticiparse y adaptarse a los cambios.

Las partes interesadas externas no participan directamente en las operaciones de la entidad, pero sí:

- Se ven afectadas por la entidad (clientes, proveedores, competidores, etc.).
- Influyen directamente en el entorno empresarial de la entidad (gobierno, reguladores, etc.).

Ejemplo 7.1: Influencia del entorno externo

Dos compañías tecnológicas globales que compiten la una con la otra tratan de aumentar sus ingresos. La primera empresa está considerando el lanzamiento de un producto en los países en desarrollo, mientras que la otra empresa está desarrollando un nuevo producto que ampliaría su actual base de consumidores. A medida que cada empresa evalúa estrategias alternativas, considera diferentes categorías del entorno externo. La primera empresa se ve influida por factores políticos, legales y económicos a medida que gestiona las leyes específicas de cada país, los reglamentos públicos y las consideraciones relativas a la cadena de suministro. Por el contrario, la segunda empresa se centra en factores sociales y tecnológicos para entender las cambiantes necesidades de los clientes. Aunque ambas empresas pertenecen al mismo sector, tienen diferentes entornos externos que influyen en sus perfiles de riesgo específicos y en la estrategia elegida.

- Influyen en la reputación, marca y confianza de la entidad (comunidades, grupos de interés, etc.).

El entorno externo comprende varios factores que pueden ser categorizados por el acrónimo PESTEL: político, económico, social, tecnológico, medioambiental y legal (véase Figura 7.1). El ejemplo 7.1 ofrece un escenario que ilustra este concepto.

Figura 7.1: Categorías y características de entorno externo¹⁶

Categorías	Características del entorno externo
Políticas	La naturaleza y alcance de las intervenciones y de la influencia del gobierno, incluidas las políticas fiscales, leyes laborales, leyes medioambientales, restricciones comerciales, aranceles y estabilidad política.
Económicas	Tipos de interés, inflación, tipos de cambio, disponibilidad de crédito, crecimiento del PIB, etc.
Sociales	Necesidades o expectativas de clientes; demografía de la población (distribución de la pirámide demográfica por edades), niveles educativos, distribución de la riqueza.
Tecnológicas	Actividades de I+D, automatización e incentivos tecnológicos; tasa de cambios tecnológicos o grandes transformaciones y disrupciones.
Medioambientales	Catástrofes naturales o provocadas por el hombre, cambio climático, cambios en el consumo de energía, actitudes hacia el medio ambiente.
Legales	Leyes (por ejemplo, relativas al empleo, consumo, salud y seguridad), regulaciones, y/o normativas industriales.

El entorno interno¹⁷ y las partes interesadas

El entorno interno de una entidad es todo aquello dentro de la entidad que puede afectar a su capacidad para alcanzar la estrategia y los objetivos de negocio (Figura 7.2). Las partes interesadas internas son aquellas personas que trabajan dentro de la entidad y que influyen directamente en la organización (miembros del consejo, directivos y otro personal involucrado). Dado que las entidades varían enormemente en tamaño y estructura, las partes interesadas internas pueden afectar a la organización de manera diferente en su conjunto que a nivel de división, unidad operativa o función específica.

Figure 7.2: Categorías y características del entorno interno

Categorías	Características del entorno interno
Capital	Activos, incluido dinero en efectivo, equipos, bienes, patentes.
Personas	Conocimientos, habilidades, actitudes, relaciones, valores y cultura.
Procesos	Actividades, tareas, políticas o procedimientos; cambios en procesos de gestión, operativos y de soporte.
Tecnologías	Tecnologías nuevas, modificadas y/o adoptadas por la entidad.

¹⁶ Las categorías de entorno externo también pueden considerarse como posibles categorías de riesgo a la hora de identificar y evaluar los riesgos.

¹⁷ El entorno interno se analiza en más detalle en el componente Gobierno y Cultura (capítulo 6).

Cómo afecta el contexto empresarial al perfil de riesgo

El efecto que el contexto empresarial tiene sobre el perfil de riesgo de la entidad puede verse en tres fases: pasado, presente y futuro. Al analizar el desempeño conseguido en el pasado, la organización puede obtener información valiosa de cara a la definición de su perfil de riesgo. Al observar el desempeño actual, se puede identificar cómo las tendencias, relaciones y otros factores actuales están afectando al perfil de riesgo. Y al pensar en cómo serán todos estos factores en el futuro, la organización puede considerar cómo podría evolucionar su perfil de riesgo en función de hacia dónde se dirija o quiera dirigirse la organización. El ejemplo 7.2 muestra cómo una organización puede considerar el contexto empresarial dentro de los componentes de la gestión del riesgo empresarial.

Ejemplo 7.2: Considerar el contexto empresarial en cada uno de los componentes del Marco

La gestión de una empresa minorista integra la comprensión del contexto empresarial con otras técnicas de gestión del riesgo empresarial, tal y como se indica a continuación:

- **Gobierno y Cultura:** La organización desarrolla un entendimiento del gobierno corporativo y las tendencias regulatorias asociadas. El consejo incorpora esta comprensión de las expectativas emergentes a su supervisión de las técnicas de gestión del riesgo empresarial.
- **Estrategia y Establecimiento de Objetivos:** La dirección realiza un análisis detallado de las tendencias sociales, comerciales y los niveles de confianza de los consumidores que impulsan el comportamiento de su base de clientes e incorpora los hallazgos en su ciclo de establecimiento de la estrategia a largo plazo para conseguir el éxito empresarial.
- **Desempeño:** La dirección incorpora las tendencias medioambientales y cómo éstas pueden afectar a la evaluación de los riesgos relacionados con el objetivo de reducir los envases en un 50%, en línea con sus valores clave.
- **Revisión y Monitorización:** La dirección considera cómo los cambios en el mercado laboral, es decir, la aparición de la movilidad laboral, también puede afectar a la cultura de la entidad y a las técnicas de gestión del riesgo empresarial, incluyendo oportunidades para mejorar las prácticas actuales.
- **Información, Comunicación y Reporte:** La dirección considera que la legislación relativa a la privacidad de la información puede afectar a la forma en que la entidad captura, comunica y reporta la información sobre el riesgo.

⚙️ Principio 7: Define el apetito al riesgo

La organización define el apetito al riesgo en el contexto de la creación, preservación y materialización del valor.

Aplicación del apetito al riesgo

Las decisiones que se toman al seleccionar la estrategia y desarrollar el apetito al riesgo no son lineales, es decir, una decisión no siempre precede a la otra. Tampoco existe un apetito al riesgo universal que sea aplicable a todas las entidades.

Muchas organizaciones desarrollan estrategias y su apetito al riesgo en paralelo, reajustando cada uno de ellos a lo largo de la fase de definición de estrategias. Algunos consejos de administración proporcionarán información y pueden desafiar a la dirección por su elección con respecto al apetito al riesgo, mientras que otros estarán de acuerdo con la dirección y aprobarán el apetito al riesgo adoptado. Independientemente de cómo se tomen las decisiones, la organización tendrá un entendimiento preliminar de su apetito al riesgo basado en la misión y visión establecidas y en estrategias previas. Se trata de elementos importantes de cualquier apetito al riesgo, que se reajusta cada vez que una organización valora estrategias alternativas y selecciona la estrategia deseada.

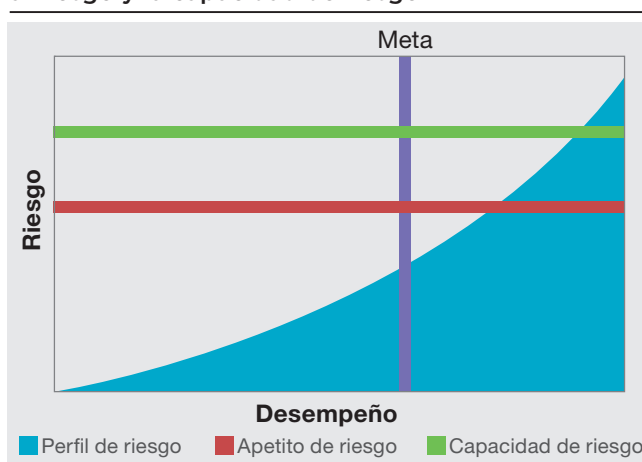
Algunas entidades consideran el apetito al riesgo en términos cualitativos mientras que otras prefieren utilizar términos cuantitativos, centrándose a menudo en equilibrar crecimiento, rentabilidad y riesgo. Cualquiera que sea el enfoque para describir el apetito al riesgo, este debe reflejar la cultura de la entidad. Además, si la organización quiere cambiar algún aspecto de la cultura, el definir un fuerte apetito al riesgo puede ayudar a crear y reforzar la cultura deseada.

El mejor enfoque para una entidad es aquel que se alinea con el análisis utilizado para evaluar el riesgo en general, ya sea cualitativo o cuantitativo. Desarrollar las bases oportunas en relación con el apetito al riesgo es un ejercicio que sirve para buscar el equilibrio óptimo entre riesgo y oportunidad.

En conjunto, estas consideraciones ayudan a enmarcar el apetito al riesgo de la entidad y proporcionan mayor precisión que una sola declaración de mayor nivel. La Figura 7.3 representa el perfil de riesgo como una zona sólida (en color azul), ocupando el espacio entre el eje de desempeño y las barras individuales del perfil de riesgo (de la ilustración anterior de la Figura 3.2). También se ha añadido una línea que muestra el apetito al riesgo.

En cualquier representación del perfil de riesgo, las organizaciones también pueden trazar la capacidad de riesgo (como en la Figura 7.3), que es la cantidad máxima de riesgo que una entidad puede asumir en la búsqueda del logro de la estrategia y los objetivos de negocio. La capacidad de riesgo debe tenerse en cuenta al establecer el apetito al riesgo, ya que generalmente una organización se esfuerza por mantener el apetito al riesgo dentro de la capacidad. Por lo general, una organización no fijará su apetito al riesgo por encima de su capacidad de riesgo, pero en situaciones poco habituales puede que una organización decida hacerlo así. Esta situación podría darse, por ejemplo, en el caso de que una organización que acepte

Figura 7.3 Perfil de riesgos que muestra el apetito al riesgo y la capacidad de riesgo



la amenaza de insolvencia, porque entienda que el éxito puede crear un valor considerable. Cuando la organización gestiona los riesgos por encima de su apetito al riesgo, por lo general la dirección deberá modificar sus prácticas para operar dentro de su apetito al riesgo o aceptar formalmente este nuevo nivel de asunción de riesgos. Algunas organizaciones también tratarán de obtener la aprobación del consejo de administración en estos casos (en el Anexo D se incluye un análisis adicional sobre los perfiles de riesgo en el Volumen II).

Definición del apetito al riesgo

No existe un apetito al riesgo “correcto” que sea aplicable a todas las entidades. La dirección y el consejo de administración eligen un apetito al riesgo con un entendimiento y conocimiento de los pros y los contras que conlleva dicho apetito. El apetito al riesgo puede conllevar una sola representación o varias representaciones que se alineen y especifiquen colectivamente al tipo y el nivel de riesgo aceptables.

Existen varios enfoques disponibles para determinar el apetito al riesgo, incluido el desarrollo de análisis, la revisión de objetivos de desempeño pasado y actual, y las modelizaciones. Para determinar el apetito al riesgo, las organizaciones pueden tener en cuenta a las partes interesadas como se indica en el análisis sobre el contexto empresarial. Le corresponde a la dirección comunicar el apetito al riesgo acordado con distintos niveles de detalle a lo largo de toda la entidad. Con el apoyo del consejo de administración, la dirección también revisa y refuerza el apetito al riesgo con el paso del tiempo a la luz de nuevas consideraciones emergentes.

Para algunas entidades, el uso de términos generales como “bajo apetito” o “elevado apetito” será suficiente. Otras entidades pueden considerar que tales afirmaciones son demasiado vagas para comunicarlas y aplicarlas eficazmente, y pueden buscar medidas más cuantitativas. A menudo, a medida que las organizaciones adquieren más experiencia en la gestión del riesgo empresarial, su descripción del apetito al riesgo se vuelve más precisa. En algunos casos, las organizaciones pueden desarrollar medidas cuantitativas que se vinculen con su declaración del apetito al riesgo. Por lo general, estas medidas se alinearán con la estrategia y los objetivos de negocio. Por ejemplo, una entidad que centre sus técnicas de gestión del riesgo empresarial en reducir la variabilidad del desempeño puede expresar su apetito al riesgo utilizando los resultados financieros o la beta de sus acciones.

El apetito al riesgo debe posicionarse y percibirse como un enfoque dinámico para configurar el perfil de riesgo de la entidad y no como una limitación adicional del desempeño. Por esta razón, algunas entidades desarrollarán una serie de expresiones del apetito al riesgo que hagan referencia a “objetivos”, “rangos”, “techos” o “suelos” (ver Ejemplo 7.3). Otras utilizarán otros términos cuantitativos específicos para aumentar la precisión.

Ejemplo 7.3: Expresiones de apetito al riesgo

Meta: Una cooperativa de crédito con un menor apetito al riesgo para sus pérdidas en préstamos traslada este mensaje a su organización estableciendo una meta de pérdidas para préstamos del 0,50% de la cartera total de préstamos.

Rango: Una compañía de suministros médicos opera con arreglo a un rango de riesgo general bajo. Su menor apetito al riesgo se debe a sus objetivos de seguridad y cumplimiento, lo cual incluye aspectos como la salud y seguridad de los empleados, con un apetito al riesgo marginalmente más alto para sus objetivos estratégicos de información y de operaciones. Esto significa que reduce a un volumen razonablemente viable los riesgos originados por los diversos sistemas médicos, productos, equipos y el entorno de trabajo, al tiempo que cumple sus obligaciones legales, las cuales tienen prioridad sobre otros objetivos de negocio.

Techo: Una universidad acepta un apetito al riesgo moderado al tiempo que busca ampliar el alcance de su oferta de estudios mientras mantiene un enfoque financiero prudente y explora sus posibilidades para atraer a nuevos estudiantes. La universidad favorecerá la incorporación de nuevos programas en aquellas áreas en las que tenga o pueda alcanzar fácilmente las capacidades necesarias para impartirlos. Sin embargo, la universidad no aceptará programas que presenten un riesgo grave para la misión y visión de la misma, estableciendo así un techo en materia de decisiones aceptables.

Suelo: Una empresa tecnológica fija una serie de objetivos agresivos de crecimiento en su sector y reconoce que tal crecimiento requiere una inversión de capital significativa. Si bien no acepta invertir capital de forma imprudente, la dirección considera que, como mínimo, el 25% del presupuesto operativo (es decir, se establece este porcentaje como “suelo”) debe asignarse a la búsqueda de innovación tecnológica.

Una organización puede considerar cualquier número de parámetros para ayudar a enmarcar su apetito al riesgo y proporcionar mayor precisión. Por ejemplo, la organización puede incluir:

- *Parámetros estratégicos*, como puedan ser nuevos productos a desarrollar o a evitar, inversión en capital, y fusiones y adquisiciones.
- *Parámetros financieros*, tales como variación máxima aceptable en el desempeño financiero, rentabilidad sobre activos o rentabilidad del capital ajustado al riesgo, calificación de deuda objetivo y ratio objetivo de deuda/patrimonio.
- *Parámetros operativos*, como requisitos ambientales, objetivos de seguridad, objetivos de calidad y concentración de clientes.

La dirección también puede considerar el perfil de riesgo de la entidad, la capacidad de riesgo, la capacidad de gestión del riesgo empresarial y la madurez, entre otros factores, al determinar el apetito al riesgo.

- *El perfil de riesgo* proporciona información sobre el nivel actual de riesgo de la entidad y cómo se distribuye el riesgo por la propia entidad, así como sobre las diferentes categorías de riesgo para la entidad. Las nuevas organizaciones no tendrán un perfil de riesgo existente previo del que puedan valerse, pero pueden obtener información valiosa de su sector y sus competidores.
- *La capacidad de riesgo* es el nivel máximo de riesgo que la entidad puede asumir en la búsqueda de la estrategia y los objetivos de negocio. Si el apetito al riesgo es muy alto, pero su capacidad de riesgo no es lo suficientemente grande como para soportar el impacto potencial de los riesgos relacionados, la entidad podría fracasar. Por otra parte, si la capacidad de riesgo de la entidad supera significativamente su apetito al riesgo, la organización puede perder oportunidades para aportar valor a las distintas partes interesadas.
- *La capacidad y madurez de la gestión del riesgo empresarial* proporcionan información sobre el buen funcionamiento de la gestión del riesgo empresarial. Una organización madura suele ser capaz de definir las capacidades de gestión del riesgo empresarial que le permiten comprender mejor su actual apetito al riesgo y los factores que influyen en su capacidad de riesgo. Una organización menos madura que tenga una capacidad de gestión del riesgo empresarial sin definir, puede no tener la misma comprensión del riesgo, lo que puede dar lugar a una declaración más amplia del apetito al riesgo o bien tendrá que redefinirla más pronto. La capacidad y madurez de gestión del riesgo empresarial también influye en la forma en que la organización cumple con su apetito al riesgo y opera dentro de sus límites.

Articular el apetito al riesgo

Algunas organizaciones articulan el apetito al riesgo como un solo punto, mientras que otras lo expresan como algo continuo (véase el ejemplo 7.4).

Una organización puede articular formulaciones detalladas del apetito al riesgo en el contexto de:

- La estrategia y los objetivos de negocio y su alineación con la misión, visión y valores clave.
- Las categorías de objetivos¹⁸ de negocio.
- Las metas de desempeño de la entidad.

Algunas organizaciones desarrollarán y articularán el apetito al riesgo utilizando otros enfoques, como puedan ser las categorías de riesgo. Estos enfoques son a veces más fáciles de gestionar

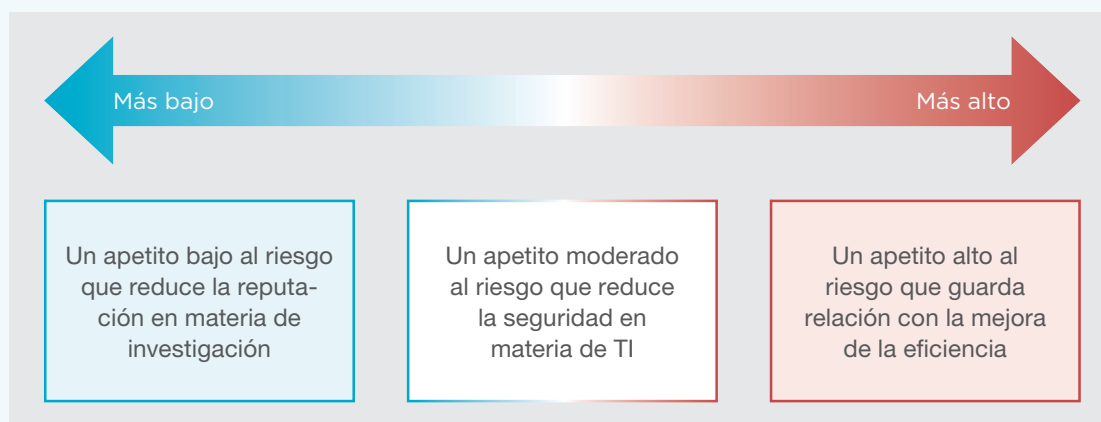
18 En el Principio 9 se analiza la formulación de los objetivos del negocio. Se incluyen a continuación para ilustrar mejor cómo el apetito al riesgo se traslada desde la estrategia hasta los objetivos de negocio.

y evaluar. Sin embargo, también pueden dar lugar a que las organizaciones gestionen el riesgo de manera aislada (en silos) en lugar de adoptar una visión integrada de la gestión del riesgo empresarial.

El equipo de dirección es quien comunica el apetito al riesgo, avalado por el consejo, y lo difunde por toda la entidad. Trasladar el apetito al riesgo es importante, ya que el objetivo es que todos los responsables de la toma de decisiones comprendan el apetito al riesgo con arreglo al cual deben operar, especialmente aquellos que lleven a cabo tareas para alcanzar sus objetivos de negocio (por ejemplo, equipos de venta locales y responsables de países).

La mayoría de las organizaciones optarán por comunicar el apetito al riesgo por toda la entidad de forma amplia. Algunos pueden optar por centrarse en las funciones directivas, que son quienes tienen la responsabilidad directa de gestionar el desempeño. Esto puede ocurrir, por ejemplo, cuando exista cierta sensibilidad con respecto a las actividades de la competencia, acceso a información privada o confidencial o si existe la posibilidad de que el apetito al riesgo impida el cumplimiento de las obligaciones. En algunos casos, las organizaciones también pueden optar por comunicar el apetito al riesgo a las partes interesadas externas, ya sea en su totalidad o de forma abreviada.

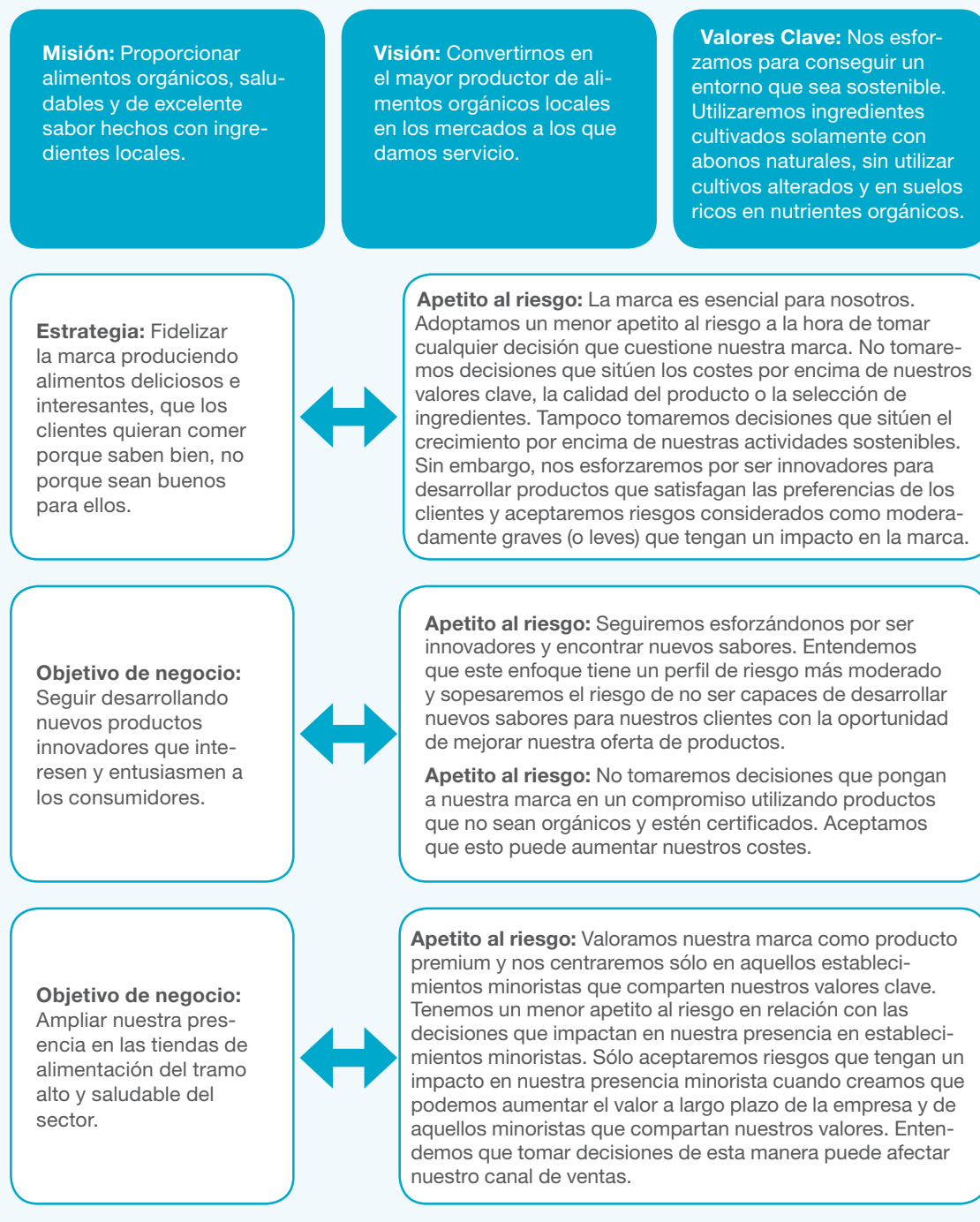
Ejemplo 7.4: Ilustración del apetito al riesgo



Una universidad ha fijado su estrategia centrándose en su papel como universidad preeminente en docencia e investigación que atrae a estudiantes sobresalientes y como un excelente lugar de trabajo para los mejores profesores. Las declaraciones del apetito al riesgo de la universidad reconocen que el riesgo está presente en todas sus actividades. La cuestión decisiva para establecer el apetito al riesgo es la disposición de la universidad a aceptar los riesgos relacionados con cada área. Para responder a esta pregunta, la dirección utiliza un espectro continuo, en el que se expresa el apetito al riesgo de los principales objetivos de negocio de la universidad (enseñanza, investigación, servicio, seguridad de los estudiantes y eficiencia operativa). Se colocan los distintos riesgos a lo largo del espectro continuo como base para su posterior análisis al más alto nivel.

El Ejemplo 7.5 muestra cómo una organización traslada el apetito al riesgo mediante declaraciones alineadas con los objetivos de negocio de alto nivel que, a su vez, se alinean con la estrategia general de la entidad.

Ejemplo 7.5: Comunicación del apetito al riesgo



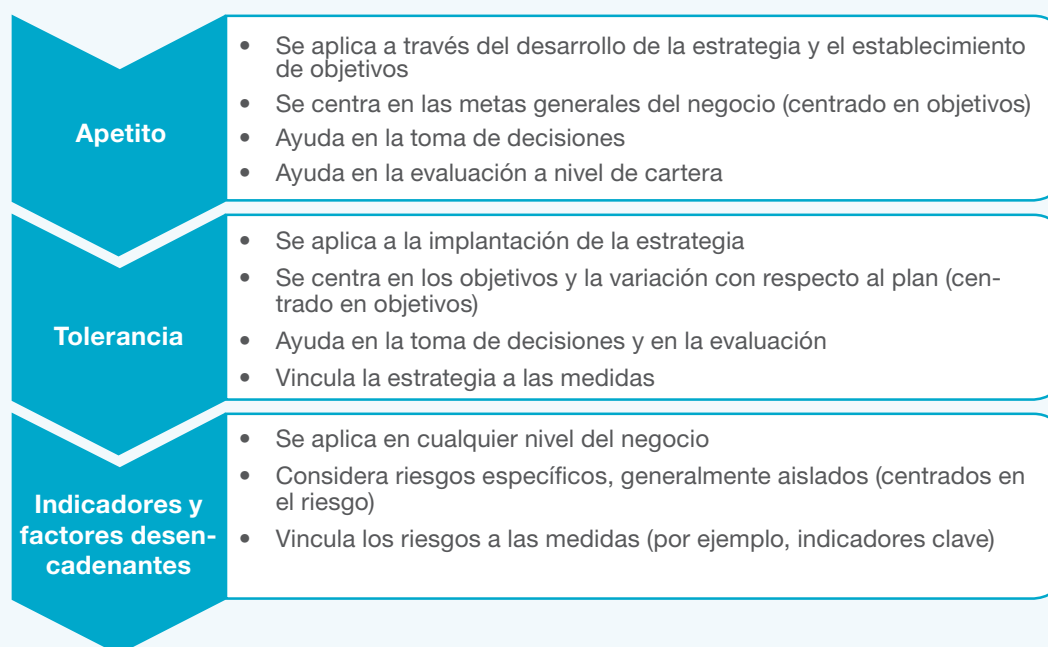
Uso del apetito al riesgo

El apetito al riesgo guía la forma en que una organización asigna los recursos, tanto a través de toda la entidad como en unidades operativas individuales. El objetivo es alinear la asignación de recursos con la misión, la visión y los valores clave de la entidad. Por lo tanto, cuando la dirección asigne recursos entre las unidades operativas, considerará el apetito al riesgo de la entidad y los planes de creación de valor de las distintas unidades operativas. Por ejemplo, la dirección puede optar por asignar una mayor parte de los recursos a aquellos objetivos de negocio con menor apetito al riesgo frente a aquellos objetivos de negocio que tengan un mayor apetito al riesgo. La organización busca alinear a las personas, los procesos y la infraestructura para implantar con éxito la estrategia y los objetivos de negocio, con un apetito al riesgo estable.

El apetito al riesgo se incorpora a las decisiones operativas de la organización. La dirección, con supervisión del consejo de administración, realiza un seguimiento continuo del apetito al riesgo a todos los niveles y se adapta al cambio cuando es necesario. De esta manera, la dirección crea una cultura que hace hincapié en la importancia del apetito al riesgo y responsabiliza a los encargados de implantar la gestión del riesgo empresarial dentro de los parámetros de apetito al riesgo.

Pero el apetito al riesgo es sólo una parte del enfoque. Para incorporar plenamente el apetito al riesgo en la toma de decisiones a distintos niveles, es necesario que se adapte y alinee con otras prácticas. La Figura 7.4 representa esta importante relación y la aplicación del apetito al riesgo, la tolerancia¹⁹ y los indicadores y factores desencadenantes²⁰ a medida que se trasladan a todos los niveles de una entidad.

Figura 7.4 Apetito al riesgo, tolerancia, límites y factores desencadenantes



¹⁹ La tolerancia se analiza más adelante en este capítulo en el Principio 9.

²⁰ Los límites y los factores desencadenantes se analizan en el componente Desempeño.



Principio 8: Evalúa estrategias alternativas

La organización evalúa las estrategias alternativas y el impacto potencial en el perfil de riesgo.

Una organización debe evaluar las estrategias alternativas como parte del establecimiento de la estrategia y evaluar el riesgo y las oportunidades de cada opción. Las estrategias alternativas se evalúan en el contexto de los recursos y capacidades de la organización para crear, preservar y materializar el valor. Una parte de la gestión del riesgo empresarial incluye la evaluación de estrategias desde dos perspectivas diferentes: (1) la posibilidad de que la estrategia no se alinee con la misión, visión y valores clave de la entidad, y (2) las consecuencias resultantes de la estrategia elegida.

La importancia de alinear la estrategia

La estrategia debe apoyar la misión, la visión y alinearse con los valores clave de la entidad y el apetito al riesgo. Si no lo hace, la entidad puede no lograr su misión y visión.

Además, una estrategia mal alineada aumenta el riesgo para las partes interesadas porque el valor de la organización y su reputación pueden verse afectados. Por ejemplo, veamos el caso de una empresa de telecomunicaciones que está considerando una estrategia para limitar las áreas en las que sus productos y servicios estén disponibles en aras de mejorar su desempeño financiero. Pero esta estrategia no concuerda con su misión de ser un proveedor de servicios críticos y un importante actor social en la comunidad local. Si bien la mejora prevista en los resultados financieros tiene por objeto aumentar el atractivo para los accionistas e inversores, esta mejora puede verse socavada por un efecto negativo en su reputación entre las comunidades y los reguladores que insistan en el mantenimiento de los servicios.

Comprender las consecuencias resultantes de la estrategia elegida

Al evaluar las estrategias alternativas, la organización busca identificar y comprender los riesgos y oportunidades potenciales de cada estrategia considerada. Los riesgos identificados forman en conjunto un perfil de riesgo para cada opción, es decir, diferentes estrategias dan lugar a diferentes perfiles de riesgo. La dirección y el consejo de administración utilizan estos perfiles de riesgo a la hora de decidir la mejor estrategia a adoptar, teniendo en cuenta el apetito al riesgo de la entidad. En algunos casos, esta evaluación puede requerir que se consideren múltiples estrategias para comprender la dependencia potencial de una estrategia con respecto a otra.

Otra consideración a la hora de evaluar estrategias alternativas son las hipótesis en relación con el contexto empresarial, los recursos y las capacidades. Estas hipótesis son una parte importante de la estrategia. Pueden hacer referencia a cualquiera de las consideraciones internas y externas que formen parte del contexto empresarial de la entidad. Cuando las hipótesis no están probadas, a menudo existe un mayor riesgo de efectos disruptivos que si la organización tuviera mayor certeza de que no se van a producir dichos efectos asociados a una estrategia. El nivel de confianza de la dirección y del consejo asociado a cada hipótesis afectará al perfil de riesgo de cada una de las estrategias. Además, una estrategia suele tener un perfil de riesgo más alto cuando se adopta un número significativo de hipótesis o cuando las hipótesis no están ampliamente probadas.

Una vez que se ha determinado un perfil de riesgo para la estrategia elegida, la dirección está en mejores condiciones para considerar el tipo y el nivel de riesgo que afrontará al llevar a cabo esa estrategia. En particular, el hecho de conocer el perfil de riesgo permite a la dirección determinar qué recursos se requerirán y asignarán para apoyar la ejecución de la estrategia mientras se



mantiene dentro del apetito al riesgo. Las necesidades de recursos incluirán aspectos como infraestructura, experiencia técnica y capital circulante.

La cantidad de esfuerzo invertido y el nivel de precisión requerido para evaluar las estrategias alternativas variarán según la importancia y complejidad de la decisión, los recursos y capacidades disponibles y el número de estrategias que se evalúen. Cuanto más significativa o compleja sea la decisión, más detallada será la evaluación, utilizando quizá varios enfoques.

Los enfoques más habituales para evaluar estrategias alternativas son el análisis DAFO²¹, la modelización, las valoraciones, las previsiones de ingresos, el análisis de la competencia y el análisis de escenarios. Normalmente es la dirección quien lleva a cabo la evaluación, ya que tiene una visión del riesgo a nivel de toda la entidad y entiende cómo la estrategia afecta al desempeño. Es decir, la dirección entiende a nivel de la entidad cómo la estrategia elegida puede afectar al desempeño a través de las distintas divisiones, funciones y geografías.

Cuando se desarrollan estrategias alternativas, la dirección adopta determinadas hipótesis. Estas hipótesis subyacentes pueden ser sensibles a los cambios, y dicha propensión al cambio puede afectar en gran medida al perfil de riesgo. Una vez que se ha elegido una estrategia, y al comprender la propensión de las hipótesis a los cambios, la organización es capaz de desarrollar los mecanismos de supervisión necesarios en relación con dichas hipótesis cambiantes.

El Ejemplo 7.6 ilustra el enfoque de una organización para evaluar la posibilidad de que las estrategias alternativas no estén alineadas con la misión, la visión y las consecuencias resultantes de las estrategias alternativas en el perfil de riesgo de la entidad. Este ejemplo también ilustra la necesidad de entender las distintas prioridades que llevan aparejadas los clientes, empleados y accionistas.

Alineación de la estrategia con el apetito al riesgo

Una organización debe esperar que la estrategia que seleccione pueda llevarse a cabo dentro del apetito al riesgo de la entidad; es decir, que la estrategia debe alinearse con el apetito al riesgo. Si el riesgo asociado a una estrategia específica no es coherente con el apetito al riesgo o la capacidad de riesgo de la entidad, será necesario revisarla, seleccionar una estrategia alternativa o revisar el apetito al riesgo.

Por ejemplo, un fabricante de material deportivo contaba con la siguiente estrategia: “Hacer crecer el negocio a través de la expansión de nuestras fábricas por todo el mundo.” Sin embargo, cuando se puso de manifiesto que algunas ubicaciones presentaban riesgos que superaban el apetito al riesgo del fabricante, tuvo que actualizarse la estrategia: “Hacer crecer el negocio a través de la expansión de nuestras fábricas por todo el mundo dentro de los requisitos de infraestructura establecidos y las regulaciones públicas.”

El desarrollo del apetito al riesgo debe alinearse con el desarrollo de la estrategia y los planes de negocio; de lo contrario puede parecer que los objetivos y prioridades estén en conflicto, o incluso creen tensiones sobre el tipo y el nivel de riesgo reflejado en la toma de decisiones.

21 DAFO es un acrónimo de Debilidades, Amenazas, Fortalezas y Oportunidades. Un análisis DAFO es un método de planificación estructurado que evalúa esos cuatro elementos

Ejemplo 7.6: Consideración de estrategias alternativas

A un proveedor de servicios logísticos globales le gustaría ampliar sus operaciones para satisfacer su demanda internacional, y para ello necesita un nuevo centro de distribución. Durante el proceso de establecimiento de la estrategia, se evalúan varias alternativas.

- La alternativa 1 consiste en abrir un centro de distribución en un país lejano en vías de desarrollo. Esta es la menos costosa de las ubicaciones que se barajan, tanto en costes de construcción como de mano de obra, pero aumentaría los tiempos de entrega en un promedio del 30%. La ubicación en este país en vías de desarrollo también presenta riesgos geopolíticos y económicos.
- La alternativa 2 consiste en abrir un centro de distribución ubicado en una ciudad de mediano tamaño más cercana. Este emplazamiento es un poco más caro de construir que la alternativa 1, pero la oferta de mano de obra es sólida. Sin embargo, los inviernos son severos en esta zona, lo que aumenta el riesgo de que los acontecimientos climáticos interrumpan el transporte.
- La alternativa 3 es una ubicación también cercana en una ciudad más grande. Esta ubicación es la más cara de construir y tiene el mercado laboral más competitivo, lo que puede derivar en mayores costes operativos. Sin embargo, el clima es templado durante todo el año.

A continuación se resumen las posibilidades de que la estrategia no se ajuste a la misión y la visión y las consecuencias resultantes de la estrategia en el perfil de riesgo.

Misión: Proporcionar servicios de transporte de la más alta calidad a los clientes dando prioridad a la seguridad en materia de operaciones, al tiempo que se mantiene una rentabilidad financiera sólida para los accionistas.

Visión: Potenciar nuestra marca para ser el proveedor de transporte internacional por excelencia.

	Objetivo de negocio	Medida de desempeño y meta
Alternativa 1	• Posibilidad de operar de tal manera que la calidad y la seguridad no estén alineadas con los valores clave de la entidad.	• Riesgo de que la variabilidad adicional de las operaciones pueda afectar a la satisfacción del cliente y erosionar el valor. • Riesgo de que el aumento de la complejidad de las operaciones (p. ej. regulaciones, leyes tributarias y tipos de cambio) pueda afectar a la eficiencia de las operaciones.
Alternativa 2	• Posibilidad de operar de tal manera que el tiempo pueda implicar unas difíciles condiciones de trabajo para los empleados y para los equipos, e impacte en la seguridad de las operaciones.	• Riesgo de que la entidad no pueda mantener unos servicios de transporte de alta calidad durante todo el año, lo cual significa que la satisfacción para los empleados se vería afectada.
Alternativa 3	• Posibilidad de operar de tal manera que los costes más elevados puedan erosionar las rentabilidades de los accionistas.	• El riesgo de operar mediante una elevada inversión en transporte de alta calidad incrementa los costes y puede impactar en la rentabilidad para los accionistas.

Cambios en la estrategia

Por lo general, las organizaciones celebran reuniones periódicas para definir la estrategia y esbozar estrategias a corto y largo plazo. Un cambio en la estrategia se justifica si la organización decide que la estrategia actual no logra crear, preservar o materializar el valor; o si un cambio en el contexto del negocio hace que la entidad se acerque demasiado al límite de riesgo que está dispuesta a aceptar, o bien requiere recursos y capacidades que no están disponibles para la organización. Por último, la evolución del contexto empresarial puede dar lugar a que la organización deje de tener expectativas razonables de que pueda lograr la estrategia (véase el Ejemplo 7.7).

Ejemplo 7.7: Cambios en la estrategia

Un fabricante mundial de cámaras fotográficas solía vender cámaras de cine, pero a medida que las cámaras digitales crecieron en popularidad, la empresa comenzó a experimentar un descenso de las ventas. Como respuesta a esta situación, la empresa modificó su estrategia adaptándose a las cambiantes necesidades de los consumidores y a las nuevas tecnologías. Ahora desarrolla cámaras digitales y reduce el riesgo de que sus productos se queden obsoletos. Estos cambios en la estrategia están respaldados por cambios en los objetivos de negocio y en las metas de desempeño relevantes.

Mitigar el sesgo

Es imposible evitar los sesgos, pero una organización debe tratar de ser imparcial –o mitigar cualquier sesgo– cuando esté valorando estrategias alternativas. El primer paso es identificar cualquier sesgo que pueda existir durante la definición de la estrategia. Cuando exista tal sesgo, la organización debería adoptar medidas para mitigarlo. El sesgo puede impedir que una organización elija la mejor estrategia para apoyar la misión, visión y valores clave de la entidad, y para reflejar el apetito al riesgo de la entidad.

Principio 9: Establece 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.

Establecimiento de objetivos de negocio

La organización desarrolla objetivos de negocio que son específicos, medibles u observables, alcanzables y relevantes. Los objetivos de negocio proporcionan un vínculo con las prácticas de la entidad para apoyar la consecución de la estrategia. Por ejemplo, los objetivos de negocio pueden hacer referencia a:

- *Desempeño financiero*: Mantener operaciones rentables para todos los negocios.
- *Aspiraciones de clientes*: Establecer centros de atención al cliente en lugares convenientes a los que los clientes puedan tener acceso.
- *Excelencia operativa*: Negociar contratos laborales competitivos para atraer y retener a los empleados.
- *Obligaciones de cumplimiento*: Cumplir las leyes de salud y seguridad aplicables en todos los sitios de trabajo.
- *Aumentos de la eficiencia*: Operar en un entorno energéticamente eficiente.
- *Liderazgo en innovación*: Liderar la innovación en el mercado con frecuentes lanzamientos de nuevos productos.

Los objetivos de negocio se pueden trasladar a todos los niveles de la entidad (divisiones, unidades operativas, funciones) o pueden aplicarse de forma selectiva. El traslado de los objetivos requiere un mayor nivel de detalle dado que se aplican progresivamente desde las altas esferas de la entidad hacia abajo. Por ejemplo, los objetivos de desempeño financiero se trasladan desde las metas de las divisiones hasta las unidades operativas individuales. Alternativamente, muchos objetivos de negocio serán específicos de una dimensión operacional, geográfica, por producto o servicio.

Alineación de objetivos de negocio

Los objetivos individuales se alinean con la estrategia, independientemente de cómo se estructure el objetivo y dónde se aplique. La alineación de los objetivos de negocio con la estrategia ayuda a la entidad a lograr su misión y visión.

Los objetivos de negocio que no se alineen, o sólo parcialmente, con la estrategia no apoyarán la consecución de la misión y la visión y pueden introducir riesgos innecesarios para el perfil de riesgo de la entidad. Es decir, la organización puede consumir recursos que se utilizarían más eficazmente de otro modo en la consecución de otros objetivos de negocio.

Los objetivos de negocio también deben alinearse con el apetito al riesgo de la entidad. Si no están alineados, la organización podría estar aceptando un riesgo demasiado elevado o demasiado bajo. Por lo tanto, cuando una organización evalúa un objetivo de negocio propuesto, debe considerar los riesgos potenciales que pueden ocurrir y determinar el efecto sobre el perfil de riesgo. Si un objetivo de negocio hace que la organización exceda el apetito al riesgo, este objetivo podrá ser modificado o, incluso, descartado.

Si una organización descubre que no puede definir unos objetivos de negocio alineados con la estrategia al tiempo que se mantienen dentro de su apetito o capacidades de riesgo, en ese caso deberá revisar la estrategia o el perfil de riesgo.

Comprender las implicaciones a la hora de seleccionar los objetivos de negocio

Una organización tiene muchas opciones a la hora de decidir los objetivos de negocio. Véase el caso, por ejemplo, de una organización que tenga la oportunidad de actualizar sus sistemas operativos principales y rediseñar su infraestructura de TI existente. Una opción es perseguir el objetivo de negocio de identificar a un proveedor adecuado y firmar un acuerdo de colaboración con él para desarrollar un sistema de TI personalizado. Otra opción es que la organización desarrolle su propio sistema internamente invirtiendo significativamente en sus capacidades de TI y aumentando el número de personal. Ambos objetivos se alinean con la estrategia general y, por tanto, la dirección debe evaluarlos y determinar el curso de acción apropiado, dadas las posibles consecuencias de cara al perfil de riesgo, los recursos y las capacidades de la entidad.

Tal y como sucede con la definición de la estrategia, la organización debe contar con una expectativa razonable de que el objetivo de negocio sea alcanzable dentro del apetito al riesgo o de los recursos disponibles por la entidad. La expectativa se basa en las capacidades y recursos de la entidad. Cuando no existe esta expectativa razonable, la organización debe elegir entre superar el apetito al riesgo, obtener más recursos o modificar el objetivo de negocio. Dependiendo de la importancia del objetivo de negocio para la estrategia, también puede ser necesario revisar la estrategia (véase el Ejemplo 7.8).

Ejemplo 7.8: Determinar las consecuencias de seleccionar un objetivo de negocio

Como parte de su estrategia a 5 años, un productor agrícola opta por cultivar productos orgánicos como diferenciador con respecto a la competencia. La compañía analiza el coste de la transición a un entorno orgánico y determina que se requerirá una inversión significativa, lo cual puede amenazar sus objetivos de desempeño financiero. Dada la importancia de mantener los resultados financieros, la organización opta por abandonar los objetivos de negocio seleccionados.

Categorización de los objetivos de negocio

Muchas organizaciones agrupan los objetivos de negocio más habituales en categorías comunes. Algunas organizaciones categorizarán o agruparán los objetivos de negocio para alinearlos con aspectos específicos de la estrategia, tales como la cuota de mercado, el enfoque al cliente o la responsabilidad corporativa. Las organizaciones también pueden alinear los objetivos de negocio con varios grupos de negocio de la entidad, tales como operaciones, recursos humanos u otras áreas funcionales definidas. Independientemente de cómo se clasifiquen, deben alinearse con las prácticas de negocio, productos, geografías u otras dimensiones de la organización. La dirección decide la forma en que una organización categoriza sus objetivos de negocio.

En algunos casos, las organizaciones deben cumplir requisitos externos que establecen la forma en que se clasifican los objetivos de negocio con fines informativos. Por ejemplo, si una organización está obligada a informar sobre su evaluación del riesgo ambiental, deberá indicar específicamente si incluye esos requisitos dentro de sus objetivos de negocio y en su reporte de información.

Las organizaciones deben tener cuidado y no confundir las categorías de objetivos de negocio con las categorías de riesgos. Las categorías de riesgos hacen referencia a los grupos de riesgos compartidos o comunes que pueden afectar a dichos objetivos de negocio.

Establecimiento de medidas de desempeño y metas

La organización establece metas para realizar un seguimiento del desempeño de la entidad y favorecer la consecución de los objetivos de negocio. Por ejemplo:

- Una sociedad de gestión de activos busca obtener un retorno sobre de la inversión del 5% anual en su cartera.
- Un restaurante se especializa en los pedidos online de comida para su entrega a domicilio en un plazo de 40 minutos.
- Un call center se esfuerza por minimizar las llamadas perdidas al 2% del total de llamadas recibidas.

Al establecer estas metas, la organización puede influir en el perfil de riesgo de la entidad. Una meta agresiva puede provocar un mayor riesgo para ese objetivo de negocio. Por ejemplo, una organización puede fijar unas metas de crecimiento agresivas que aumenten los riesgos de cara a esa búsqueda de crecimiento adicional. Por el contrario, una organización puede fijar una meta de crecimiento más conservadora que reduzca el riesgo de no alcanzar esa meta, pero también puede dar lugar a que la meta deje de estar alineada con el logro del objetivo de negocio.

Otro ejemplo sería de nuevo el caso de la sociedad de gestión de activos indicada anteriormente, que entiende que un ROI del 5% le permitirá alcanzar sus objetivos financieros. Si aspira a una rentabilidad del 7%, incurriría en un mayor riesgo en su desempeño. Si se esfuerza por alcanzar el 3%, lo que le permite un perfil de riesgo menos agresivo, no logrará sus objetivos financieros más amplios (en el Capítulo 8 se analiza con mayor detenimiento la identificación y evaluación de los riesgos para el logro de los objetivos de negocio, así como la revisión de la idoneidad de las medidas y metas de desempeño).

El Ejemplo 7.9 muestra un caso más completo de los objetivos de negocio considerados a nivel de entidad, división, unidad operativa y función, junto con las metas asociadas. El ejemplo muestra cómo los objetivos de negocio aumentan en especificidad a medida que se van trasladando a todos los niveles de la entidad.

Ejemplo 7.9: Objetivo de negocio (de muestra) por nivel

	Objetivo de negocio	Medida de desempeño y meta
Objetivos de negocio (entidad)	• Seguir desarrollando productos innovadores que interesen y entusiasmen a los consumidores. • Expandir la presencia minorista en el sector de la alimentación saludable.	• 8 productos en I+D en todo momento. • 5% de crecimiento año tras año.
Objetivos de negocio para Norteamérica (división)	• Incremento del espacio asignado en principales establecimientos que compartan nuestros valores clave. • Seguir abasteciéndose de productos de los mercados locales.	• 7% de crecimiento del espacio asignado. • 92% de tasa de abastecimiento local.
Objetivos de negocio para Pastelería (unidad operativa)	• Desarrollar <i>snacks</i> saludables y de alta calidad que superen las expectativas de los clientes.	• 4,8 sobre 5 en encuesta de satisfacción de clientes.
Objetivos de negocio para Recursos Humanos (función)	• Mantener una tasa de rotación de empleados adecuada. • Contratar y formar a responsables de ventas de productos durante el próximo año.	• Rotación inferior al 10%. • Contratar 50 responsables de ventas. • 95% de tasa de formación de personal de ventas.

Entender la tolerancia

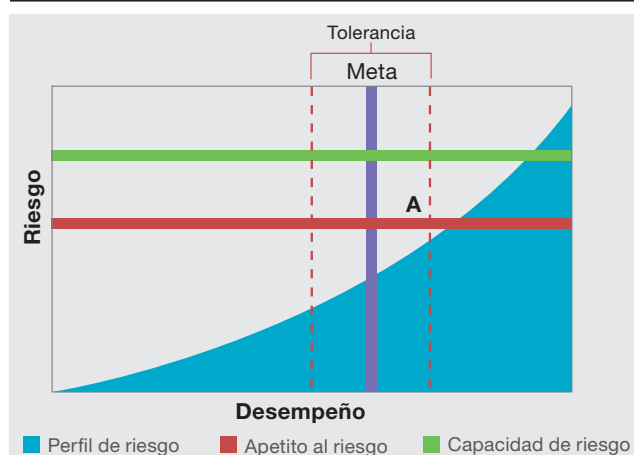
La tolerancia está estrechamente ligada al apetito al riesgo, esto es, la variación aceptable en el desempeño. Describe la gama de resultados aceptables en relación con el logro de un objetivo de negocio dentro del apetito al riesgo. También proporciona un enfoque para medir si los riesgos para la consecución de la estrategia y de los objetivos de negocio son aceptables o inaceptables.

Tener un entendimiento claro de la tolerancia a las variaciones del desempeño permite a la dirección mejorar el valor para la entidad. Por ejemplo, el límite adecuado de la variación aceptable no debería superar en general el punto en el que el perfil de riesgo se cruza con el apetito al riesgo. Sin embargo, cuando el límite adecuado se sitúa por debajo del apetito al riesgo, la dirección puede cambiar sus metas y aun así estar dentro de su apetito al riesgo general. El punto máximo en el que se puede establecer la meta de desempeño es donde el límite correcto de tolerancia se cruza con el apetito al riesgo ("A" en la Figura 7.5).

A diferencia del apetito al riesgo, que es general, la tolerancia es táctica y concentrada. Es decir, debe expresarse en unidades medibles (preferiblemente en las mismas unidades que los objetivos de negocio), aplicarse a todos los objetivos de negocio e implantarse en toda la entidad. Al establecer la tolerancia, la organización considera la importancia relativa de cada objetivo de negocio y la estrategia. Por ejemplo, para aquellos objetivos que se consideran de gran importancia para lograr la estrategia de la entidad, o en los casos en que una estrategia es de gran importancia para su misión y visión, la organización tal vez desee establecer un margen de tolerancia más bajo. La tolerancia se centra en los objetivos y el desempeño, no en riesgos específicos.

Operar dentro de la tolerancia definida proporciona a la dirección una mayor seguridad de que la entidad se mantiene dentro de su apetito al riesgo, lo cual a su vez proporciona una confianza adicional de que la entidad logrará sus objetivos de negocio.

Figura 7.5 Perfil de riesgo que muestra la tolerancia



Medidas de desempeño y tolerancias establecidas

Las medidas de desempeño relacionadas con un objetivo de negocio ayudan a confirmar que el desempeño real se encuentra dentro de la tolerancia establecida (véase el Ejemplo 7.10). Las medidas de desempeño pueden ser cuantitativas o cualitativas. La tolerancia también considera tanto la variación en exceso como por defecto, a veces denominada variación positiva o negativa. Obsérvese que la variación en exceso y por defecto no siempre se fija en distancias iguales a la meta.

La cantidad de variación en exceso y por defecto depende de varios factores. Una organización, por ejemplo, con una dilatada experiencia, se puede mover en los límites (por exceso y por defecto) más cerca de la meta deseada a medida

Ejemplo 7.10 Variación de la meta por defecto

Una gran planta embotelladora de bebidas se fija la meta de no tener más de 5 incidentes de tiempo perdido en un año y establece la tolerancia entre 0 y 7 incidentes. La variación en exceso entre 5 y 7 representa mayores incidentes y el potencial de pérdida de tiempo y de un aumento de reclamaciones de salud y seguridad, lo cual es un resultado negativo para la entidad. Por el contrario, la variación por defecto de hasta 5 incidentes representa un beneficio: menos incidentes de pérdidas de tiempo y menos reclamaciones de salud y seguridad. La organización también necesita considerar el coste de buscar un nivel 0 incidentes de tiempo perdido.

que gana experiencia gestionando a un nivel más bajo de variación. El apetito al riesgo de la entidad es otro factor: una entidad que tenga un apetito al riesgo más bajo puede preferir tener una variación del desempeño menor en comparación con una entidad que tenga un mayor apetito al riesgo.

Es habitual que las organizaciones asuman que una variación en exceso en el rendimiento sea un beneficio, y que una variación por defecto sea un riesgo. Exceder una meta u objetivo generalmente indica eficiencia o un buen desempeño, no simplemente que se está explotando una oportunidad. Pero quedarse por debajo de una meta no significa necesariamente un fracaso: depende de la meta de la organización y de cómo se defina la variación (ver Ejemplo 7.11).

Las organizaciones también deben comprender la relación entre el coste y la tolerancia para poder afrontar eficazmente los riesgos asociados. Por lo general, cuanto más estrecha sea la tolerancia, mayor será la cantidad de recursos requeridos para operar dentro de ese nivel de desempeño. Por ejemplo, veamos el caso de las compañías aéreas que efectúan un estrecho seguimiento de sus llegadas y salidas en hora. Una compañía aérea puede optar por abandonar una serie de rutas porque su desempeño (salidas y llegadas en hora) no se ajusta a la tolerancia revisada (o reducida) de la compañía aérea. La compañía entonces tendría que sopesar las consecuencias en términos de costes tras renunciar a los ingresos derivados de esas rutas a las que ha renunciado para conseguir una variación menor en su objetivo de desempeño.

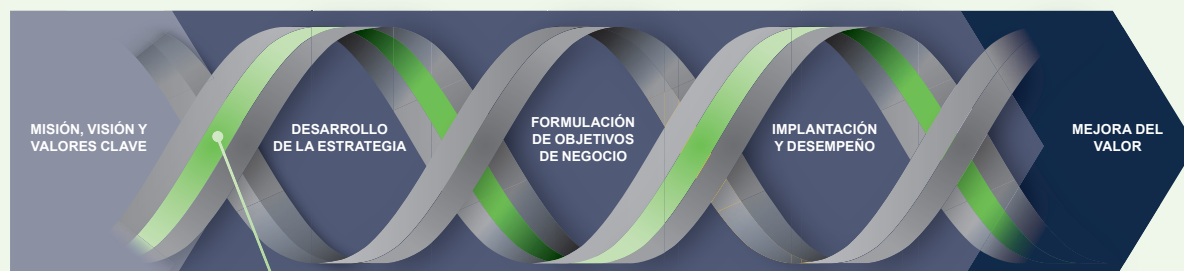
Ejemplo 7.11: Límites de Tolerancia

Objetivo de negocio	Meta	Tolerancia
Rentabilidad sobre la inversión (ROI) para una gestora de activos	Objetivo anual de rentabilidad del 5% sobre su cartera.	Rentabilidad anual del 3% a 7%.
Pedidos “online” para un restaurante en sus envíos a domicilio	Meta de entrega en un plazo de 40 minutos.	Plazo de entrega de 30 a 50 minutos.
Minimizar las llamadas perdidas para un “call center”	Objetivo del 2% sobre las llamadas totales.	Objetivo del 1% al 5% sobre las llamadas totales.

8. Desempeño

Principios relacionados con el desempeño

GESTIÓN DEL RIESGO EMPRESARIAL



DESEMPEÑO

10. **Identifica el Riesgo:**

La organización identifica el riesgo que impacta en la consecución de la estrategia y los objetivos de negocio.

11. **Evalúa la Gravedad del Riesgo:**

La organización evalúa la gravedad del riesgo.

12. **Prioriza Riesgos:**

La organización prioriza los riesgos como base para la selección de respuestas 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.

Introducción

La identificación, evaluación y respuesta a los riesgos que pueden afectar al logro de la estrategia y los objetivos de negocio de la entidad ayuda a crear, preservar, materializar y minimizar la erosión del valor de dicha entidad. Los riesgos originados a nivel transaccional pueden resultar tan disruptivos como los identificados a nivel de entidad. Los riesgos pueden afectar a una unidad operativa o a la entidad en su conjunto. Pueden estar altamente correlacionados con factores dentro del contexto del negocio o con otros riesgos. Además, las respuestas al riesgo pueden requerir inversiones significativas en infraestructura o ser aceptadas como parte de las actividades del negocio. Dado que el riesgo proviene de una amplia variedad de fuentes, es necesario contar con un rango de respuestas a todos los niveles de la entidad.

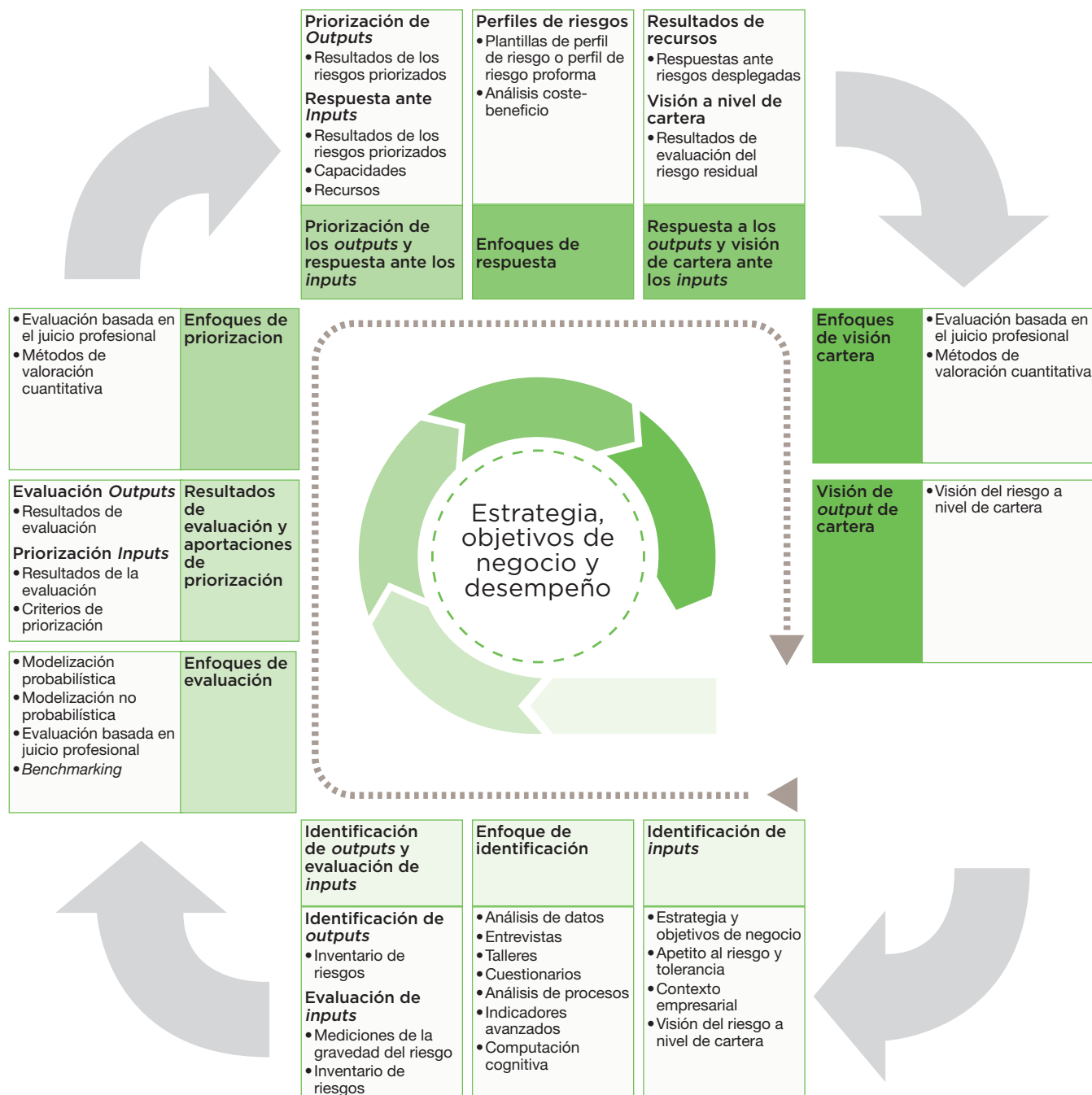
Este componente del Marco se centra en las prácticas que apoyan a la organización en la toma de decisiones y en la consecución de la estrategia y los objetivos de negocio. Con ese fin, las organizaciones utilizan su estructura operativa para desarrollar una técnica que:

- Identifica riesgos nuevos y emergentes para que la dirección pueda dar respuesta al riesgo de manera oportuna.
- Evalúa la gravedad del riesgo, con un entendimiento de cómo el riesgo puede cambiar dependiendo del nivel de la entidad.
- Prioriza los riesgos, permitiendo a la dirección optimizar la asignación de recursos en respuesta a dichos riesgos.
- Identifica y selecciona las respuestas al riesgo.
- Desarrolla una visión de cartera para mejorar la capacidad de la organización para articular el nivel de riesgo asumido en la búsqueda de la estrategia y los objetivos de negocio a nivel de entidad.



La Figura 8.1 ilustra que estas técnicas son iterativas, es decir, que las aportaciones de un paso del proceso suelen ser el resultado del paso anterior. Las técnicas se llevan a cabo a todos los niveles y con responsabilidades y rendición de cuentas para la adecuada gestión del riesgo empresarial, en línea con la gravedad del riesgo.

Figura 8.1: Relación entre el proceso de evaluación del riesgo, *inputs*, enfoques y *outputs*





Principio 10: Identifica el riesgo

La organización identifica el riesgo que impacta en la consecución de la estrategia y los objetivos de negocio.

Identificación del riesgo

La organización identifica riesgos nuevos, emergentes y cambiantes para lograr la estrategia y los objetivos de negocio de la entidad. Realiza actividades de identificación de riesgos para, en primer lugar, establecer un inventario de riesgos y, posteriormente, confirmar que los riesgos existentes siguen siendo aplicables y relevantes. A medida que las técnicas de gestión del riesgo empresarial se integran progresivamente en la entidad, el conocimiento y la conciencia de los riesgos se mantienen actualizados a través de las operaciones del día a día. Algunas entidades complementarán esas actividades de vez en cuando para confirmar la integridad del inventario de riesgos. La frecuencia con la que lo haga una organización dependerá de lo rápido que cambien los riesgos o surjan nuevos riesgos. Cuando es probable que los riesgos tarden meses o años en materializarse, la frecuencia con que se realice el ejercicio de identificación de riesgos será menor que cuando los riesgos sean menos predecibles u ocurran a mayor velocidad.

Los riesgos nuevos, emergentes y cambiantes incluyen aquellos que:

- Surgen de un cambio en los objetivos de negocio (por ejemplo, la entidad adopta una nueva estrategia basada en los objetivos de negocio o modifica un objetivo de negocio existente).
- Surgen de un cambio en el contexto empresarial (por ejemplo, cambios en las preferencias de los consumidores en favor de productos ecológicos u orgánicos que tienen un impacto potencialmente adverso en las ventas de los productos de la empresa).
- Hacen referencia a un cambio en el contexto empresarial que puede no haberse considerado previamente en la entidad (por ejemplo, un cambio en las regulaciones que resulte en nuevas obligaciones para la entidad).
- Se desconocían anteriormente (por ejemplo, el descubrimiento de una susceptibilidad a la corrosión en las materias primas utilizadas en las operaciones de fabricación de la empresa).
- Se identificaron previamente, pero desde entonces se han alterado debido a un cambio en el contexto empresarial, en el apetito al riesgo o en las hipótesis de partida (por ejemplo, un aumento positivo en las previsiones de ventas que afectan a la capacidad de producción).

Los riesgos emergentes surgen cuando cambia el contexto empresarial y estos pueden alterar el perfil de riesgo de la entidad en el futuro. Debe tenerse en cuenta que los riesgos emergentes pueden no ser lo suficientemente bien comprendidos como para identificarse y evaluarse con precisión desde un principio, y pueden requerir una nueva identificación con mayor frecuencia. Además, las organizaciones deben comunicar la información cambiante que dispongan sobre los riesgos emergentes.

La identificación de riesgos nuevos y emergentes, o de cambios en los riesgos existentes, permite a la organización mirar hacia el futuro y le da tiempo a evaluar la gravedad potencial de los riesgos, y aprovecharse de dichos cambios. A su vez, al disponer de tiempo para evaluar el riesgo, la organización puede anticiparse a la respuesta al riesgo, o revisar la estrategia de la entidad y los objetivos de negocio según sea necesario.

Algunos riesgos pueden seguir siendo desconocidos, como pueden ser los riesgos que la organización no tenía previsto considerar durante la identificación de riesgos. Esto normalmente se debe al hecho de que se produzcan cambios en el contexto empresarial. Por ejemplo, a menudo se desconocen las acciones o intenciones futuras de los competidores, pero estas pueden representar nuevos riesgos para el desempeño de la entidad.

Las organizaciones quieren identificar aquellos riesgos que probablemente generen efectos disruptivos en las operaciones y afecten a su expectativa razonable de lograr la estrategia y los objetivos de negocio. Dichos riesgos representan un cambio significativo en el perfil de riesgo y pueden ser acontecimientos específicos o circunstancias cambiantes. A continuación, se incluyen algunos ejemplos:



- *Tecnología emergente*: Avances tecnológicos que puedan afectar a la relevancia y longevidad de los productos y servicios existentes.
- *Ampliación del papel del big data y del análisis de datos*: La forma en que las organizaciones pueden acceder, transformar y analizar de manera efectiva y eficiente grandes volúmenes de fuentes de datos estructurados y sin estructurar.
- *Agotamiento de los recursos naturales*: La disminución de la disponibilidad y el aumento del coste de los recursos naturales que afectan a la oferta, la demanda y la ubicación de los productos y servicios.
- *Aumento de negocios virtuales*: El creciente protagonismo de los negocios virtuales que influyen en los canales de oferta, demanda y distribución de las estructuras tradicionales del mercado.
- *Movilidad de la mano de obra*: Trabajos a distancia y en remoto que introducen nuevas actividades en las operaciones diarias de una entidad.
- *Escasez de mano de obra*: Los desafíos de garantizar el trabajo con las habilidades y niveles de educación requeridos por las entidades para lograr el desempeño.
- *Cambios en el estilo de vida, la salud y la demografía*: Los hábitos y necesidades cambiantes de los clientes actuales y futuros a medida que cambian la demografía.
- *Entorno político*: Acciones del gobierno que alteran la forma de operar de un sector en un país.

La identificación de oportunidades está integrada en la identificación del riesgo²². Es decir, a veces las oportunidades surgen del riesgo. Por ejemplo, los cambios demográficos y el envejecimiento de la población pueden considerarse un riesgo para la estrategia actual de una entidad y una oportunidad para renovar la fuerza laboral con el fin de lograr un mejor crecimiento. Del mismo modo, los avances tecnológicos pueden representar un riesgo para los modelos de distribución y servicio para los establecimientos minoristas, así como una oportunidad de cambiar la forma en que los clientes obtienen sus productos (por ejemplo, a través de servicios online). Cuando se identifican oportunidades, éstas se comunican a través de la organización para que se tengan en cuenta de cara al establecimiento de la estrategia y los objetivos de negocio.

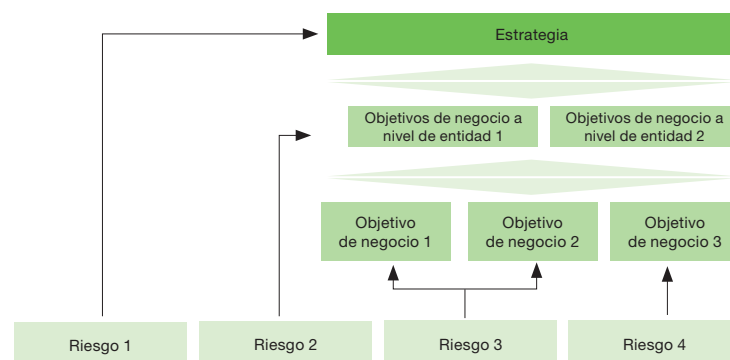
Uso del apetito al riesgo

Un inventario de riesgos es simplemente una lista o catálogo de los riesgos a los que se enfrenta la entidad. Dependiendo del número de riesgos individuales identificados, las organizaciones pueden estructurar el inventario de riesgos por categorías para proporcionar definiciones estándar sobre los diferentes riesgos. Esto permite agrupar riesgos similares, como los riesgos financieros, los comerciales o los de cumplimiento (o, más ampliamente, los riesgos de obligaciones). Dentro de cada categoría, las organizaciones pueden optar por definir los riesgos en subcategorías más detalladas. El inventario de riesgos puede actualizarse para reflejar los cambios identificados por la dirección.

La Figura 8.2 ilustra cómo los riesgos que impactan en diferentes niveles de la entidad forman parte del inventario de riesgos:

- El riesgo 1 tiene un impacto potencial directo en la estrategia.
- El riesgo 2 impacta en los objetivos de negocio de la entidad.
- El riesgo 3 impacta en dos objetivos de negocio que posteriormente se agregan e impactan en los objetivos de negocio a nivel de entidad.
- El riesgo 4 impacta en un único objetivo de negocio, así como en otros objetivos de negocio a nivel de entidad.

Figura 8.2: El riesgo impacta a diferentes niveles



²² El presente Marco distingue entre eventos positivos y oportunidades. Los eventos positivos hacen referencia a aquellos casos en los que el desempeño supera el objetivo original. Las oportunidades son acciones o potenciales acciones que crean o alteran metas o enfoques para crear, preservar y materializar la estrategia y los objetivos de negocio.

Dado que el impacto de los riesgos no puede limitarse a niveles o funciones específicas, las actividades de identificación deben captar todos los riesgos e, independientemente de dónde se identifiquen, todos los riesgos han de formar parte del inventario de riesgos de la entidad. Por ejemplo, una entidad que identifique riesgos a nivel de estrategia relacionados con el gobierno a nivel de consejo y el logro de las metas de diversidad también debe tener en cuenta estos riesgos a nivel de objetivos de negocio. O una organización que identifique el riesgo de no cumplir con el plazo de facturación de un cliente al nivel de objetivo de negocio también debe considerar el impacto de ese riesgo a nivel de entidad.

Para demostrar que se ha llevado a cabo una completa identificación de riesgos, la dirección identificará los riesgos y oportunidades en todas las funciones y niveles, aquellos riesgos que sean comunes a más de una función, así como aquellos que sean únicos a un producto, una oferta de servicios, una jurisdicción u otra función en particular.

Enfoques para identificar el riesgo

Existen diversos enfoques disponibles para identificar los riesgos. La organización puede identificar los riesgos como parte de las actividades diarias, tales como la presupuestación, la planificación empresarial, las revisiones del desempeño y las reuniones, como consideraciones en los procesos de aprobación de nuevos productos y diseños y en respuesta a las quejas de clientes, incidentes o pérdidas financieras. Las actividades de identificación integradas a través de la entidad pueden complementarse con actividades específicas adicionales tales como cuestionarios sencillos, talleres de trabajo y entrevistas. Algunos enfoques pueden ser factibles a través de la tecnología, como la trazabilidad del dato y el desarrollo de análisis complejos.

Dependiendo del tamaño, la extensión geográfica y la complejidad de una entidad, la dirección puede utilizar más de una técnica. Por ejemplo, una entidad puede recopilar datos internos sobre incidentes y pérdidas históricas y analizarlos para identificar riesgos nuevos, emergentes y cambiantes. Además, la naturaleza y el tipo de riesgo pueden determinar la técnica apropiada. Por ejemplo, la dirección puede utilizar enfoques más sofisticados para identificar los riesgos asociados con una adquisición. Algunas organizaciones pueden obtener información de otras organizaciones del mismo sector o región para obtener información sobre riesgos potenciales. La Figura 8.3 y la siguiente lista proporcionan información sobre enfoques útiles para identificar diferentes tipos de riesgos.

Figura 8.3: Enfoques para la identificación de riesgos

Tipo de riesgo	Computación Cognitiva	Seguimiento de Datos	Entrevistas	Indicadores Clave	Análisis de Procesos	Talleres de Trabajo
Existentes	✓	✓	✓	✓	✓	✓
Nuevos	✓	✓			✓	✓
Emergentes	✓		✓	✓		✓

- *La computación cognitiva* permite a las organizaciones recopilar y analizar grandes volúmenes de datos para detectar tendencias futuras y análisis de grandes volúmenes de información sobre riesgos nuevos y emergentes, así como cambios en los riesgos existentes de manera más eficiente que un ser humano.
- *El seguimiento de datos* relativos a eventos pasados puede ayudar a predecir sucesos futuros. Si bien los datos históricos se utilizan normalmente en la evaluación de riesgos –basándose en la experiencia real en relación con la gravedad– también se pueden utilizar para comprender las interdependencias y desarrollar modelos predictivos y causales. Las bases de datos desarrolladas y mantenidas por proveedores externos que recopilan información sobre incidentes y pérdidas incurridas por el sector o región pueden dotar de información a la organización sobre los riesgos potenciales. A menudo están disponibles bajo suscripción. En algunos sectores, se han formado consorcios para compartir datos internos.
- *Las entrevistas* indagan en el conocimiento del profesional acerca de eventos pasados y potenciales. Para sondear a grandes grupos de personas, se pueden utilizar cuestionarios o encuestas.

- *Los indicadores clave* son parámetros cualitativos o cuantitativos que ayudan a identificar cambios en los riesgos existentes. Los indicadores de riesgo no deben confundirse con las mediciones del desempeño, que normalmente son retrospectivas por naturaleza.
- *El análisis de procesos* implica desarrollar un diagrama de un proceso para comprender mejor las interrelaciones de sus inputs, tareas, outputs y responsabilidades. Una vez establecidas las correspondencias, se pueden identificar y considerar los riesgos en relación con los objetivos de negocio relevantes.
- *Los talleres de trabajo* reúnen a profesionales de diferentes funciones y niveles para aprovechar el conocimiento colectivo del grupo y desarrollar una lista de riesgos relacionados con la estrategia de la entidad o los objetivos de negocio.

Cualquiera que sea el enfoque que se elija, una organización debe tener en cuenta cómo los cambios en las hipótesis en las que se basa la estrategia y los objetivos de negocio pueden generar riesgos nuevos o emergentes. Sirva como ejemplo el caso de una empresa cuyo equipo de dirección asumió un tipo de cambio equivalente al de la moneda local para importar determinadas materias primas. Sin embargo, el tipo de cambio real cayó en más del 10%, lo que creó un nuevo riesgo para alcanzar los objetivos generales de rentabilidad. Asimismo, la dirección consideró el contexto empresarial – las perspectivas económicas previstas para la entidad, las preferencias cambiantes de los clientes y las tasas de crecimiento esperadas cuando llevó a cabo la identificación de riesgos.

Al identificar los riesgos, la organización debe tratar de describir con precisión el riesgo en sí mismo, en lugar de otras consideraciones relativas a ese riesgo, como sus causas originales, sus impactos potenciales o el efecto de que el riesgo se defina de manera deficiente. En la Figura 8.4 se comparan las descripciones de estas otras consideraciones, que son menos útiles, con las descripciones de riesgo más precisas, que son más aceptables

Figura 8.4: Descripción de los riesgos con precisión

Otras consideraciones	Descripciones imprecisas de riesgos	Descripciones aceptables de riesgos
Posibles causas raíz	• La falta de formación aumenta el riesgo de que se produzcan errores de procesamiento e incidencias. • El descenso de la motivación entre los empleados contribuye al riesgo de que los empleados clave dejen la organización, provocando una alta rotación.	• El riesgo de que los errores de procesamiento impacten en la calidad de las unidades de fabricación. • El riesgo de perder empleados clave y tener una alta rotación, que repercuta en los objetivos de retención de los empleados.
Impactos potenciales asociados a la materialización de un riesgo	• Un nuevo producto tiene más éxito de lo previsto, la capacidad de fabricación tiene dificultades para mantener el nivel exigido de producción por el aumento de la demanda, lo cual provoca retrasos en plazos de entrega, quejas de clientes y efectos negativos en la reputación de la empresa. • El riesgo de ataques de denegación de servicio debido a los sistemas tradicionales de TI que no han impedido que se produzcan fugas de datos de clientes, sanciones regulatorias, pérdida de clientes y reputación negativa.	• El riesgo de que la demanda supere los objetivos de producción y que impacte en el servicio al cliente. • El riesgo de ataques de denegación de servicio que afecte a la capacidad de la empresa para mantener la confidencialidad de los datos de clientes.
Efectos potenciales de respuestas a riesgos mal definidos	• El riesgo de que en las conciliaciones bancarias no se identifiquen los pagos incorrectos a clientes. • El riesgo de que las comprobaciones de calidad no detecten los defectos de productos antes de la distribución.	• El riesgo de que se produzcan pagos incorrectos a clientes que afecten a los resultados financieros de la entidad. • El riesgo de que los defectos de productos afecten a los objetivos de calidad y seguridad.

La identificación precisa del riesgo:

- Permite a la organización gestionar más eficazmente el inventario de riesgos y comprender su relación con la estrategia del negocio, los objetivos y el desempeño.
- Permite a la organización evaluar con mayor precisión la gravedad del riesgo en el contexto de los objetivos de negocio.
- Ayuda a la organización a identificar las causas raíz e impactos habituales, y así seleccionar y abordar las respuestas al riesgo más apropiadas.
- Permite a la organización comprender las interdependencias entre riesgos y objetivos de negocio.
- Ayuda a agregar los riesgos para obtener una visión de los mismos a nivel de cartera.

En consecuencia, se alienta a las organizaciones a describir los riesgos utilizando una estructura de frase estándar. A continuación, se incluyen dos enfoques posibles:

- La posibilidad de [describir la circunstancia o el acontecimiento potencial] y los impactos asociados sobre [describir los objetivos de negocio específicos establecidos por la organización].
 - **Ejemplo:** La posibilidad de que se produzca una variación en los tipos de cambio y los impactos asociados sobre los ingresos.
- El riesgo de [describir la categoría establecida por la organización] en relación con [describir la circunstancia o el acontecimiento potencial] y [describir el impacto relacionado].
 - **Ejemplo:** El riesgo para el desempeño financiero en relación con una posible variación de los tipos de cambio y su impacto en los ingresos.

Enmarcar el riesgo

La teoría prospectiva (o teoría de la expectativa), que explora la toma de decisiones humanas, indica que los individuos no son neutrales en cuanto al riesgo; por el contrario, la respuesta dada ante una pérdida tiende a ser más extrema que la respuesta dada a una ganancia. Y esto lleva aparejada una tendencia a malinterpretar las probabilidades y las mejores reacciones de resolución. Asimismo, la manera en que se enmarca un riesgo –enfocándose en el lado positivo (una ganancia potencial) o negativo (una pérdida potencial)– a menudo influye en la respuesta. Con esto en mente, debe tenerse en consideración la importancia de describir el riesgo con una estructura definida de forma coherente para reducir el sesgo a la hora de enmarcar el riesgo. El Ejemplo 8.1 presenta una ilustración de cómo enmarcar el riesgo.

Ejemplo 8.1: Enmarcar el riesgo

Un individuo se enfrenta a dos series de opciones:

1. Una ganancia segura de 240 dólares, o un 25% de probabilidad de ganar 1.000 dólares y un 75% de probabilidad de no ganar nada.
2. Una pérdida segura de 750 dólares, o un 75% de probabilidad de perder 1.000 dólares y un 25% de probabilidad de no perder nada.

En la primera serie de opciones, la mayoría de la gente elige “una ganancia segura de 240 dólares”, porque esa opción se enmarca en el ámbito positivo. En la segunda serie de opciones, la mayoría de las personas eligen una “probabilidad del 75% de perder 1.000 dólares”, porque en este caso es la pérdida la que es más segura. La teoría de la expectativa sostiene que las personas no quieren poner en riesgo lo que ya tienen o piensan que pueden tener, pero tendrán una mayor tolerancia al riesgo cuando piensan que pueden minimizar las pérdidas.



Principio 11: Evalúa la gravedad del riesgo

La organización evalúa la gravedad del riesgo.

Evaluación del riesgo

Los riesgos identificados e incluidos en un inventario de riesgos de la entidad se evalúan con el fin de comprender su gravedad de cara a lograr la estrategia y los objetivos de negocio de una entidad. Las evaluaciones de riesgos dan información sobre la selección de las respuestas al riesgo. Dada la gravedad de los riesgos identificados, la dirección decide los recursos y capacidades a utilizar para que el riesgo se mantenga dentro del apetito al riesgo de la entidad.

Evaluación de la gravedad a diferentes niveles de la entidad

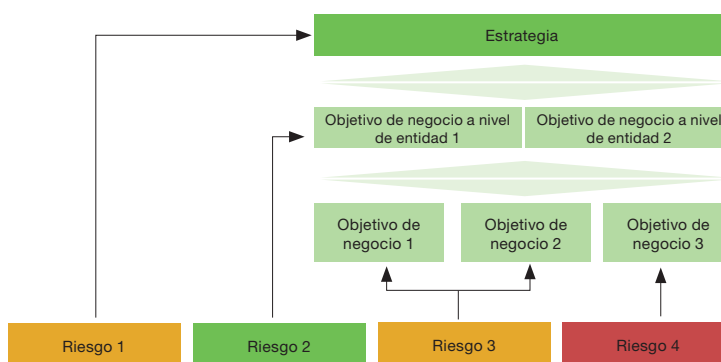
La gravedad de un riesgo se evalúa en múltiples niveles (divisiones, funciones y unidades operativas) de acuerdo con los objetivos de negocio a los que pueda afectar. Puede ser que los riesgos evaluados como importantes a nivel de unidad operativa, por ejemplo, sean menos importantes que los de nivel de división o entidad. En los niveles más altos de la entidad, es probable que los riesgos tengan un mayor impacto en la reputación, marca y fiabilidad.

El uso de una terminología y categorías de riesgo estandarizadas ayuda a evaluar los riesgos a todos los niveles de la organización. También se pueden agrupar los riesgos comunes entre las unidades de negocio, divisiones y funciones. Por ejemplo, el riesgo de las interrupciones tecnológicas identificadas por múltiples divisiones puede agruparse y evaluarse de forma colectiva. Del mismo modo, los riesgos medidos a niveles escalonados dentro de una entidad también pueden agruparse. Cuando se agrupan los riesgos comunes, la clasificación de gravedad puede cambiar. Los riesgos que son de baja gravedad individualmente pueden llegar a ser más o menos graves cuando se valoren conjuntamente en todas las unidades o divisiones de negocio.

La Figura 8.5 ilustra el inventario de riesgos asignado a la estrategia y los objetivos de negocio. En una evaluación del riesgo “descendente” a nivel de entidad, se puede estimar que el riesgo 4 tiene un nivel de gravedad bajo. En una evaluación a nivel de unidad de negocio, el riesgo 4 puede considerarse más significativo y, por lo tanto, tener una mayor gravedad.

Para que las prácticas de evaluación de riesgos sean completas, la evaluación descendente tendrá en cuenta los riesgos identificados y evaluados en los niveles más bajos. Por ejemplo, una evaluación a nivel de entidad evaluaría los riesgos a nivel de entidad, pero también debería tener en cuenta los riesgos graves identificados a nivel de objetivo de negocio de la entidad, como el riesgo 2, para determinar si, dada su gravedad, constituye una preocupación a nivel de entidad.

Figura 8.5: Evaluación del riesgo a diferentes niveles

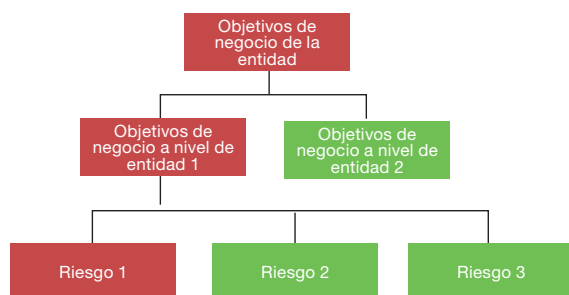


La Figura 8.6 ilustra cuatro escenarios habituales.

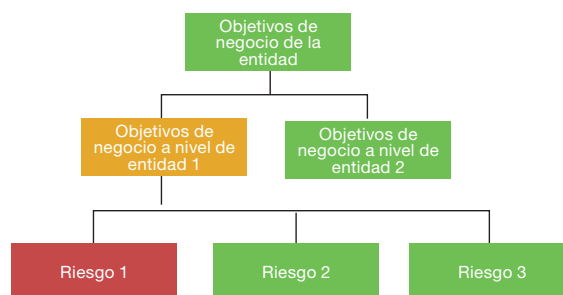
- En el escenario 1, la organización reconoce que el riesgo podría afectar tanto al objetivo de negocio a nivel unidad de negocio como al objetivo de negocio a nivel de entidad. Por ejemplo, un error de seguridad en un proceso de fabricación puede, dada su magnitud, afectar al conjunto de la entidad.
- En el escenario 2, un riesgo disminuye de gravedad en los niveles superiores de la entidad, lo cual indica que no representa el mismo impacto potencial para la entidad en su conjunto. Por ejemplo, un atraso en las transacciones puede representar un riesgo para la unidad operativa que gestiona el procesamiento, pero puede no tener un impacto significativo en el objetivo de negocio general, y a nivel de entidad puede tener poco o ningún impacto. Sin embargo, si el atraso aumenta, este riesgo podría pasar al escenario 3 o incluso al 1.
- En el escenario 3, dos riesgos tienen, a título individual, evaluaciones de gravedad moderada, pero juntos impactan en los objetivos de negocio y a nivel de entidad de manera más significativa, y por tanto se evalúan como más graves. Por ejemplo, la imposibilidad de contratar empleados para las funciones de soporte más habituales, como es el caso de profesionales legales, representa un riesgo bajo para cada unidad operativa, pero comienza a afectar a la entidad de forma más significativa a nivel de objetivo de negocio, ya que esta tendencia podría tener un impacto perjudicial en la capacidad para alcanzar un objetivo de negocio que dependa en gran medida del nivel de especialización de los profesionales legales. Sin embargo, a nivel de entidad, ese riesgo puede no ser tan significativo dada la importancia del objetivo de negocio y su alineación con la estrategia.
- En el escenario 4, determinados riesgos afectan a toda la entidad. Por ejemplo, el riesgo de adquisición por parte de competidores impacta en la estrategia de la entidad en su conjunto, pero puede no afectar individualmente a los objetivos de negocio.

Figura 8.6: Evaluación de la gravedad a diferentes niveles

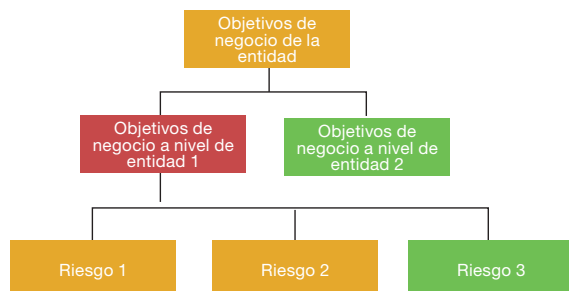
1) El riesgo a nivel de objetivo de negocio mantiene su gravedad en los niveles superiores



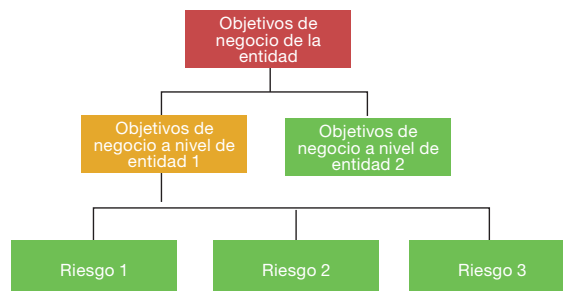
2) El riesgo a nivel de objetivo de negocio disminuye su gravedad en los niveles superiores



3) El riesgo a nivel de objetivo de negocio aumenta su gravedad en los niveles superiores



4) El riesgo a nivel de objetivo de negocio de la entidad disminuye su gravedad en los niveles inferiores



Selección de medidas de gravedad

La dirección selecciona medidas para evaluar la gravedad del riesgo. En general, estas medidas se alinean con el tamaño, naturaleza y complejidad de la entidad y su apetito al riesgo. También se pueden utilizar diferentes umbrales a distintos niveles de la entidad para la que se está evaluando un riesgo. Los umbrales utilizados para evaluar la gravedad de un riesgo se adaptan al nivel de evaluación –por entidad o unidad operativa. El nivel aceptable de riesgo para el desempeño financiero, por ejemplo, puede ser mayor a nivel de entidad que a nivel de unidad operativa.

La dirección determina la gravedad relativa de varios riesgos para seleccionar una respuesta adecuada al riesgo, asignar recursos y apoyar la toma de decisiones y el desempeño del equipo de dirección. Entre las medidas que se pueden utilizar se incluyen²³:

- **Impacto:** El resultado o efecto de un riesgo. Puede haber una serie de posibles impactos asociados a un riesgo. El impacto de un riesgo puede ser positivo o negativo en relación con la estrategia o los objetivos de negocio.
- **Probabilidad:** La posibilidad de que se materialice un riesgo. Esto puede expresarse en términos de probabilidad o frecuencia de ocurrencia. La probabilidad puede expresarse de diversas maneras, como lo demuestran los siguientes ejemplos:
 - **Cualitativa:** “La posibilidad de que se materialice un riesgo relacionado con un acontecimiento o circunstancia potencial y los impactos asociados sobre un objetivo específico de negocio [dentro del horizonte temporal previsto por el objetivo de negocio, por ejemplo, doce meses] es remota.”
 - **Cuantitativa:** “La posibilidad de que se materialice un riesgo relacionado con un acontecimiento o circunstancia potencial y los impactos asociados sobre un objetivo específico de negocio [dentro del horizonte temporal previsto por el objetivo de negocio, por ejemplo, doce meses] es del 80%.”
 - **Frecuencia:** “La posibilidad de que se materialice un riesgo relacionado con un acontecimiento o circunstancia potencial y los impactos asociados sobre un objetivo específico de negocio [dentro del horizonte temporal previsto por el objetivo de negocio, por ejemplo, doce meses] es de una vez cada doce meses.”

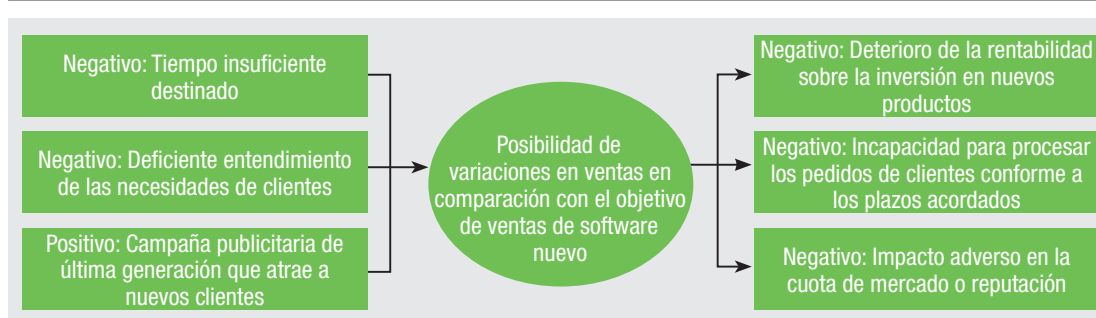
Como parte del proceso de evaluación, la dirección considera posibles combinaciones de probabilidad e impacto. Por ejemplo, puede haber un riesgo bajo de incidentes operativos que resulten en pérdidas superiores al 20% de los ingresos ordinarios de la entidad. Al mismo tiempo, puede haber una mayor probabilidad de que se produzcan incidentes operativos que provoquen pérdidas inferiores al 1% de los ingresos ordinarios de la entidad. Siempre que la dirección determine cuándo un riesgo puede generar efectos disruptivos o requerir un cambio en la respuesta al riesgo, ese riesgo se tendrá en cuenta en las actividades de evaluación.

El horizonte temporal utilizado para evaluar los riesgos debe ser el mismo que el utilizado para la estrategia y los objetivos de negocio relacionados. Por ejemplo, si los objetivos del negocio se centran en un horizonte temporal de tres años, la dirección considerará los riesgos dentro de ese plazo. Dado que la estrategia y los objetivos de negocio de muchas entidades se centran en horizontes temporales a corto y medio plazo, la dirección a menudo se centra en los riesgos asociados a dichos marcos temporales. Sin embargo, al evaluar los riesgos de la misión, visión o estrategia, el plazo puede ser más largo. La dirección necesita ser consciente de estos plazos más largos y no ignorar los riesgos que podrían surgir u ocurrir más allá del corto plazo.

Adicionalmente, el riesgo procede de múltiples fuentes y genera diferentes impactos. Las causas raíz pueden tener un impacto positivo o negativo en la evaluación de un riesgo. La Figura 8.7 ilustra los distintos resultados que pueden obtenerse de diversas fuentes.

23 En el Principio 14 se analizan medidas adicionales, incluida la persistencia, velocidad y complejidad.

Figure 8.7: Causas raíz e impactos del riesgo



Las medidas de gravedad deben alinearse con la estrategia y los objetivos de negocio. El Ejemplo 8.2 ilustra cómo una organización identifica los riesgos para sus objetivos de negocio y aplica las medidas adecuadas. Cuando se identifican diferentes impactos para un objetivo de negocio, la dirección proporciona orientación sobre cómo evaluar la gravedad del impacto. Cuando los impactos múltiples dan lugar a evaluaciones diferentes de la gravedad o bien requieren una respuesta diferente al riesgo, la dirección determina si es necesario identificar y evaluar por separado los riesgos adicionales.

Enfoques de evaluación

Los enfoques de evaluación del riesgo pueden ser cualitativos, cuantitativos o una combinación de ambos.

- Los enfoques de evaluación cualitativa, tales como entrevistas, talleres de trabajo, encuestas y análisis comparativos (benchmarking), se utilizan a menudo cuando no es factible ni rentable obtener suficientes datos para su cuantificación. Las evaluaciones cualitativas son más eficientes de completar; sin embargo, tienen limitaciones en su capacidad para identificar correlaciones o realizar un análisis de coste-beneficio.
- Los enfoques de evaluación cuantitativa, tales como la modelización, los árboles de decisión, las simulaciones de Monte Carlo, etc., permiten obtener un mayor detalle y precisión, y respaldan un análisis de coste-beneficio. En consecuencia, los enfoques cuantitativos se utilizan habitualmente en actividades más complejas y sofisticadas para complementar las técnicas cualitativas. Los enfoques cuantitativos incluyen:
 - Modelos probabilísticos (por ejemplo, valor en riesgo, flujo de efectivo en riesgo, distribución de pérdidas operacionales) que asocian una serie de eventos y el impacto resultante con la probabilidad de dichos eventos en base a ciertas hipótesis. Por ejemplo, al entender cómo cada factor de riesgo podría variar e impactar el flujo de caja, la dirección podrá medir y gestionar mejor el riesgo.
 - Los modelos no probabilísticos (por ejemplo, el análisis de sensibilidad, y el análisis de escenarios) utilizan hipótesis subjetivas para estimar el impacto de los eventos sin cuantificar la probabilidad asociada a un objetivo de negocio. Por ejemplo, el análisis de escenarios permite a la dirección entender el impacto en un objetivo de negocio para aumentar la rentabilidad bajo diferentes hipótesis, tales como un competidor que lanza al mercado un nuevo producto, una interrupción en la cadena de suministro o un aumento en los costes del producto.

Dependiendo de lo compleja y madura que sea la entidad, la dirección podrá confiar en un cierto grado de juicio profesional y en la experiencia al llevar a cabo la modelización. Independientemente del enfoque utilizado, cualquier hipótesis deberá ser expresada claramente.

Ejemplo 8.2: Alineación de objetivos de negocio, riesgo y medidas de gravedad

Tipo de Objetivo	Objetivo de negocio	Riesgo identificado	Meta y tolerancia	Medidas de gravedad	
				Calificación/ Tipo de impacto	Probabilidad
Objetivos de negocio para Snacks (unidad operativa)	Seguir desarrollando productos innovadores que que interesen y atraigan a los consumidores	La posibilidad de que la organización no sea capaz de desarrollar nuevos productos que superen las expectativas de los clientes	Objetivo: 8 productos en desarrollo en todo momento Tolerancia: número de nuevos productos en desarrollo entre 6 y 12 en todo momento	Impacto medio en la satisfacción del cliente	Posible
Objetivo de negocio para Recursos Humanos	Reclutar y formar a gerentes de venta de productos en el próximo año	La posibilidad de que la organización no pueda identificar de forma oportuna al personal adecuado para el puesto de responsable de ventas	Objetivo: Reclutar a 50 gerentes de ventas Tolerancia: La entidad recluta entre 35 y 50 gerentes de venta en el próximo año	Impacto menor en operaciones/ Recursos Humanos	Posible
		La posibilidad de que la organización no pueda programar la formación para los nuevos gerentes de ventas	Objetivo: Formar al 95% de los gerentes de ventas Tolerancia: La entidad forma a un mínimo del 85% de los gerentes de ventas de producto en el próximo año		Improbable

La gravedad prevista de un riesgo puede influir en el tipo de enfoque que se utilice. Al evaluar los riesgos que podrían tener impactos extremos, la dirección puede utilizar el análisis de escenarios, pero al evaluar los efectos de múltiples eventos, la dirección podrá encontrar más útiles las simulaciones (por ejemplo, las pruebas de estrés). Por el contrario, los riesgos de alta frecuencia y bajo impacto pueden ser más adecuados para el análisis de datos y la computación cognitiva. Para llegar a un consenso sobre la gravedad del riesgo, las organizaciones pueden emplear el mismo enfoque que utilizaron como parte del proceso de identificación de riesgos.

También es posible que sean diferentes equipos quienes lleven a cabo las evaluaciones toda lo largo de la entidad. En este caso, la organización establece un enfoque para revisar cualquier diferencia en los resultados de la evaluación. Por ejemplo, si un equipo califica unos riesgos específicos como “bajos”, pero otro equipo los califica como “medios”, la dirección revisará los resultados para determinar si hay incoherencias en el enfoque, hipótesis y perspectivas de los objetivos de negocio o riesgos.

Por último, una parte de la evaluación del riesgo trata de comprender las interdependencias que pueden existir entre los riesgos. Las interdependencias pueden producirse cuando múltiples riesgos afectan a un objetivo de negocio o cuando un riesgo desencadena otro. Los riesgos pueden producirse de manera simultánea o secuencial. Por ejemplo, para un innovador tecnológico, el retraso en el lanzamiento de nuevos productos conlleva una pérdida simultánea de cuota de mercado y una

dilución del valor de marca de la entidad. La forma en que la dirección entienda las interdependencias se reflejará en la evaluación de la gravedad.

Riesgo inherente, objetivo y residual

Como parte de la evaluación de riesgos, la dirección tendrá en cuenta el riesgo inherente, el riesgo residual objetivo y el riesgo residual real.

- *El riesgo inherente* es el riesgo que existe para una entidad siempre que no se produzcan acciones directas o definidas adoptadas por la dirección para alterar o modificar su gravedad.
- *El riesgo residual objetivo* es el nivel de riesgo que una entidad está dispuesta a asumir para lograr estrategia y objetivos de negocio, sabiendo que la dirección implantará, o ha implantado, acciones directas o definidas para alterar o modificar la gravedad del riesgo.
- *El riesgo residual real* es el riesgo remanente después de que la dirección haya tomado medidas para alterar su gravedad. El riesgo residual real debe ser igual o inferior al riesgo residual objetivo. Cuando el riesgo residual real supere el riesgo objetivo, deberán identificarse medidas adicionales que permitan a la dirección alterar o modificar aún más la gravedad del riesgo.

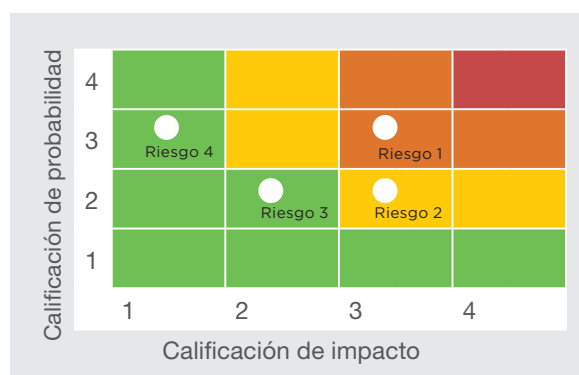
La dirección puede identificar riesgos para los cuales se hayan implantado respuestas innecesarias. Las respuestas de riesgo redundantes son aquellas que no dan lugar a un cambio medible en la gravedad del riesgo. La eliminación de dichas respuestas puede permitir a la dirección asignar los recursos destinados a esa respuesta en otro lugar.

Representación de resultados de evaluación

Los resultados de la evaluación a menudo se representan utilizando un “mapa de calor” u otro tipo de representación gráfica para resaltar la gravedad relativa de cada uno de los riesgos de cara al logro de una determinada estrategia u objetivo de negocio. Cada uno de los riesgos trazados en el mapa de calor asume un determinado nivel de desempeño para esa estrategia u objetivo de negocio.

Los riesgos evaluados para un objetivo de negocio determinado se trazan en el mapa de calor utilizando las medidas de gravedad seleccionadas por la entidad para un determinado nivel de desempeño. Las diversas combinaciones de probabilidad e impacto (medidas de gravedad), dado el apetito al riesgo, se codifican por colores para reflejar un nivel particular de gravedad. En la Figura 8.8, la entidad tiene cuatro grados de gravedad de riesgo que van desde el rojo al verde. La codificación por colores se alinea con un resultado de gravedad en particular y refleja el apetito al riesgo de la entidad. Las entidades con aversión al riesgo pueden codificar más cuadrados en color rojo en comparación con las entidades agresivas con respecto al riesgo.

Figura 8.8: Mapa de calor del objetivo de negocio



La Figura 8.9 ilustra el perfil de riesgo para un único objetivo de negocio y un determinado nivel de desempeño. Si el nivel de desempeño cambia, se capturan los cambios correspondientes en cada uno de los riesgos. Esto puede dar lugar a nuevos riesgos, riesgos que cambien de gravedad o que se eliminen riesgos.

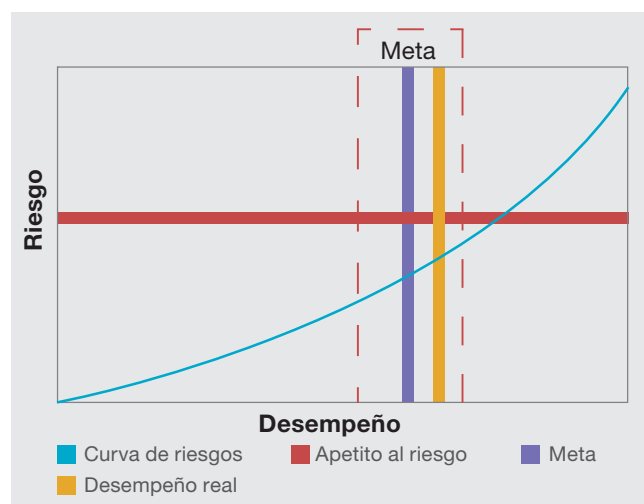
El inventario de riesgos constituye la base a partir de la cual una organización puede construir un perfil de riesgo (como se muestra en la Figura 8.9). Cada punto de datos de la curva de riesgos representa la combinación y gravedad de los riesgos para ese objetivo de negocio (tal como se ilustra de forma desagregada en el mapa de calor de la Figura 8.8). La dirección puede utilizar el perfil de riesgo en su evaluación para:

- Confirmar que el desempeño está dentro de la tolerancia.

- Confirmar que el riesgo está dentro del apetito al riesgo.
- Comparar la gravedad de un riesgo en varios puntos de la curva.
- Evaluar el punto de disrupción de la curva en el cual el nivel de riesgo supera con creces el apetito de la entidad e impacta en su desempeño o en el logro de la estrategia y los objetivos de negocio.

Además, la dirección considera cómo los diferentes riesgos pueden presentar diferentes impactos para el mismo objetivo de negocio. Por ejemplo, una franquicia de ferreterías identifica el riesgo de caída de ventas debido a que no dispone de una gama de productos diversificada que atraiga a un amplio grupo de clientes. La dirección también es consciente de que los cambios en las iniciativas de marketing y publicidad pueden afectar significativamente a las ventas. Al centrarse en el objetivo de negocio de las ventas, la dirección es capaz de comprender mejor los riesgos que afectan a las ventas. Al entender la gravedad de los diferentes riesgos para el mismo objetivo de negocio, la dirección puede tomar decisiones conscientes del riesgo sobre la diversidad de productos en stock y el presupuesto deseado para gastar en marketing y publicidad con el fin de gestionar el riesgo de la caída de ventas.

Figura 8.9: Perfil de riesgo objetivo del negocio



Identificación de desencadenantes para la reevaluación

La organización se esfuerza por identificar los factores desencadenantes que provocarán una reevaluación de la gravedad al riesgo en caso necesario. Los factores desencadenantes suelen ser los cambios en el contexto empresarial, pero también pueden deberse a cambios en el apetito al riesgo, y sirven como indicadores de alerta temprana sobre los cambios en las hipótesis que sustentan la evaluación de la gravedad. Un factor desencadenante puede ser un aumento en el número de reclamaciones de clientes, un cambio adverso en un índice económico, una caída de las ventas o un aumento en la rotación de empleados. Los desencadenantes también pueden proceder de un competidor (por ejemplo, un producto de un competidor que se retira del mercado porque tiene defectos).

La gravedad de los riesgos y la frecuencia con la que puedan cambiar la gravedad determinará la frecuencia con la que se puede desencadenar una reevaluación. Por ejemplo, los riesgos asociados a la variación de los precios de las materias primas pueden tener que evaluarse diariamente, pero los riesgos asociados a la evolución demográfica o a los gustos del mercado tal vez deban evaluarse sólo anualmente.

Sesgo en la evaluación

La dirección deberá identificar y mitigar el efecto del sesgo en la realización de prácticas de evaluación de riesgos. Por ejemplo, el sesgo resultante de la confianza puede respaldar una percepción preexistente de un riesgo conocido. Asimismo, la forma en que se enmarca un riesgo también puede afectar a la manera en que se interpretan y evalúan los riesgos. Por ejemplo, para un riesgo determinado, puede haber una gama de impactos potenciales, cada uno de ellos con una probabilidad distinta. Por tanto, un riesgo con una probabilidad baja pero un impacto alto podría tener el mismo resultado que el de una probabilidad alta con un impacto bajo; sin embargo, un riesgo puede ser aceptable para la organización y otro no. Como tal, la forma en que el riesgo se presenta y se enmarca será fundamental para mitigar cualquier sesgo.

El sesgo puede dar lugar a que se infravalore o sobreestime la gravedad de un riesgo y a que se limite la eficacia de la respuesta al riesgo seleccionada. Subestimar la gravedad puede resultar en una respuesta inadecuada, dejando a la entidad expuesta y potencialmente fuera del apetito al riesgo de la entidad. Por su parte, sobreestimar la gravedad de un riesgo puede dar lugar a que los recursos se desplieguen innecesariamente en respuesta a dicho riesgo, creando ineficiencias en la entidad. Además, puede obstaculizar el desempeño de la entidad o afectar a su capacidad para identificar nuevas oportunidades.

Principio 12: Prioriza riesgos

La organización prioriza los riesgos como base para la selección de respuestas ante los riesgos.

Establecimiento de criterios

Las organizaciones priorizan los riesgos para dotar la toma de decisiones de información adecuada sobre las respuestas al riesgo y para optimizar la asignación de recursos. A la vista de los recursos disponibles para una entidad, la dirección debe evaluar los pros y los contras de la asignación de recursos para mitigar un riesgo u otro. La priorización de los riesgos, dada su gravedad, la importancia del objetivo de negocio correspondiente y el apetito al riesgo de la entidad, ayudan a la dirección en la toma de decisiones.

Las prioridades se determinan mediante la aplicación de criterios acordados²⁴. Entre los ejemplos de dichos criterios se incluyen:

- **Adaptabilidad:** La capacidad de una entidad para adaptarse y responder ante los riesgos (por ejemplo, responder a cambios demográficos como la edad de la población y el impacto en los objetivos de negocio relacionados con la innovación de productos).
- **Complejidad:** El alcance y naturaleza de un riesgo para el éxito de la entidad. La interdependencia de los riesgos suele aumentar su complejidad (por ejemplo, los riesgos de obsolescencia de un producto y la caída de ventas con respecto al objetivo de una empresa de ser líder del mercado en tecnología y satisfacción del cliente).
- **Velocidad:** La rapidez a la que un riesgo afecta a una entidad. La velocidad puede alejar a la entidad de la variación aceptable en el desempeño (por ejemplo, el riesgo de interrupción de la actividad debido a las huelgas de los agentes portuarios y aduaneros que afecten al objetivo de conseguir una gestión eficaz de la cadena de suministro).
- **Persistencia:** Cuánto tiempo impacta un riesgo en una entidad (por ejemplo, la persistencia de la publicidad negativa realizada por los medios de comunicación y el impacto en los objetivos de ventas tras la identificación de posibles fallos en los frenos y la consiguiente retirada de vehículos en todo el mundo).
- **Recuperación:** La capacidad de una entidad para retornar a los niveles de tolerancia (por ejemplo, seguir funcionando después de una inundación grave u otra catástrofe natural). La recuperación no incluye el tiempo necesario para volver a los niveles de tolerancia, que se considera parte de la persistencia, no de la recuperación.

La priorización tiene en cuenta la gravedad del riesgo en comparación con el apetito al riesgo. Puede darse mayor prioridad a aquellos riesgos que probablemente se acerquen o superen el apetito al riesgo.

Priorización del riesgo

Los riesgos con evaluaciones similares de gravedad pueden priorizarse de manera diferente. Es decir, dos riesgos pueden ser evaluados como “medios”, pero la dirección puede dar una prioridad adicional a un riesgo sobre otro porque tiene mayor velocidad y persistencia (ver Ejemplo 8.3), o porque la respuesta al riesgo para uno de ellos proporciona una rentabilidad ajustada al riesgo más alta que para otros riesgos de similar gravedad.

Ejemplo 8.3: Priorización del riesgo

Para una gran cadena de restaurantes, la respuesta al riesgo de que las quejas de los clientes no se resuelvan y generen mala publicidad en las redes sociales se considera una prioridad mayor que la respuesta al riesgo de prolongar las negociaciones contractuales con vendedores y proveedores. Ambos riesgos son graves, pero la velocidad y el alcance de los comentarios online pueden tener un mayor impacto en el desempeño y la reputación de la cadena de restaurantes, lo que requiere una respuesta más rápida ante unos comentarios negativos.

²⁴ Los criterios también pueden tenerse en consideración al evaluar la gravedad de un riesgo, como se analiza en el Principio 11.

La forma en que se prioriza un riesgo suele dotar de información adecuada a las respuestas al riesgo que la dirección considera. Las respuestas más eficaces abordan tanto la gravedad (impacto y probabilidad) como la priorización de un riesgo (velocidad, complejidad, etc.).

Es más probable que los riesgos de mayor prioridad sean aquellos que afecten a la entidad en su conjunto o que surjan a nivel de entidad. Por ejemplo, el riesgo de que los nuevos competidores introduzcan nuevos productos y servicios en el mercado puede exigir una mayor adaptabilidad y una revisión de la estrategia y los objetivos de negocio de la entidad para que ésta siga siendo viable y relevante.

Uso del apetito al riesgo para priorizar los riesgos

La dirección también debe comparar el apetito al riesgo al priorizar los riesgos. Los riesgos que dan lugar a que la entidad se acerque al apetito al riesgo para un objetivo de negocio específico suelen tener mayor prioridad (véase el Ejemplo 8.4). Además, se puede dar prioridad a los niveles de desempeño que se aproximan a los límites exteriores de la tolerancia.

Al priorizar los riesgos, la dirección también reconoce que existen riesgos que la entidad opta por aceptar; es decir, algunos ya se consideran gestionados a un nivel aceptable para la entidad y para los cuales no se contemplará ninguna respuesta adicional al riesgo.

Ejemplo 8.4: Relación del perfil de riesgo con el apetito al riesgo

La misión de una compañía de servicios públicos es ser el proveedor de electricidad más fiable de su región. El aumento reciente de la frecuencia y la persistencia de los cortes de suministro eléctrico indica que la empresa se está acercando a su apetito al riesgo y es menos probable que logre su objetivo de negocio de prestar un servicio fiable. Esta situación desencadena una mayor prioridad con respecto a este riesgo. Un cambio de prioridad puede hacer que se revise la respuesta al riesgo, implantando respuestas adicionales y asignando más recursos para reducir la probabilidad de que el riesgo incumpla el apetito al riesgo de la organización.

Priorización a todos los niveles

La priorización del riesgo se produce en todos los niveles de una entidad, y se pueden asignar diferentes prioridades de riesgo a diferentes niveles. Por ejemplo, los riesgos de alta prioridad a nivel operativo pueden evaluarse como riesgos de baja prioridad a nivel de la entidad. La organización asigna una prioridad al nivel en el que se asumen la responsabilidad con respecto al riesgo y con respecto a aquellos que son responsables de su gestión.

Las organizaciones dan prioridad a los riesgos de forma agregada cuando se identifica a un único responsable del riesgo o es probable que se aplique una respuesta común al riesgo. Esto permite identificar y describir claramente los riesgos utilizando una categoría de riesgo estándar, lo que permite priorizar los riesgos comunes de forma coherente en toda la entidad. El resultado es una respuesta al riesgo más consistente y eficiente que la que se habría dado si cada riesgo se hubiera priorizado por separado.

Los responsables o dueños del riesgo se encargan de utilizar la prioridad asignada para seleccionar y aplicar respuestas al riesgo apropiadas en el contexto de los objetivos de negocio y de las metas de desempeño. En muchos casos, el responsable de la respuesta al riesgo y el responsable del riesgo pueden ser dos personas diferentes, o pueden estar a distintos niveles dentro de la entidad. Los responsables del riesgo deben tener suficiente autoridad para priorizar los riesgos en función de sus cometidos y capacidad para asumir sus responsabilidades para gestionar de forma eficaz el riesgo.

Sesgo en la priorización

La dirección debe esforzarse por priorizar los riesgos y gestionar sin sesgos los distintos objetivos de negocio que competirán entre sí de cara a la asignación de recursos. Los objetivos de negocio competirán entre sí por cuestiones como la asignación de recursos adicionales, conseguir medidas de desempeño específicas, cumplir criterios específicos para conseguir incentivos y recompensas personales u obtener otros resultados específicos.



Principio 13: Implementa respuestas ante los riesgos

La organización identifica y selecciona las respuestas ante los riesgos.

Elegir las respuestas ante los riesgos

Para todos los riesgos identificados, la dirección selecciona y da una respuesta al riesgo. La dirección considera la gravedad y priorización del riesgo, así como el contexto empresarial y los objetivos de negocio asociados. Por último, la respuesta al riesgo también tiene en cuenta las metas de desempeño de la organización. Las respuestas dadas ante el riesgo se enmarcan en las siguientes categorías:

- *Aceptar:* No se adoptan medidas para cambiar la gravedad del riesgo. Esta respuesta es apropiada cuando el riesgo para la estrategia y los objetivos de negocio ya está dentro del apetito al riesgo. El riesgo que está fuera del apetito al riesgo de la entidad y que la dirección desea aceptar requerirá generalmente la aprobación del consejo de administración u otros órganos de supervisión.
- *Evitar:* Se adoptan medidas para eliminar el riesgo, lo cual puede implicar la interrupción de una línea de productos, expandirse hacia un nuevo mercado geográfico o la venta de una división. Escoger la opción de “evitar” sugiere que la organización no es capaz de identificar una respuesta que reduzca el impacto del riesgo a un nivel de gravedad aceptable.
- *Perseguir:* Se toman medidas que aceptan un mayor riesgo para lograr un mayor desempeño. Esto puede implicar que se adopten estrategias de crecimiento más agresivas, que se amplíen las actividades o se desarrollen nuevos productos y servicios. Cuando se opta por perseguir el riesgo, la dirección entiende la naturaleza y el alcance de cualquier cambio requerido para lograr el desempeño deseado sin exceder los límites de tolerancia aceptable.
- *Reducir:* Se adoptan medidas para reducir la gravedad del riesgo. Esto implica cualquiera de las innumerables decisiones de negocio del día a día que reducen el riesgo a un nivel de gravedad alineado con el perfil de riesgo residual objetivo y el apetito al riesgo.
- *Compartir:* Se adoptan medidas para reducir la gravedad de un riesgo transfiriendo o compartiendo una parte del mismo. Las técnicas más habituales que se utilizan incluyen la subcontratación a proveedores de servicios especializados, la contratación de seguros y la contratación de operaciones de cobertura. Al igual que con la respuesta destinada a “reducir”, al compartir el riesgo se reduce el riesgo residual en coherencia con el apetito al riesgo.

Estas categorías de respuestas al riesgo requieren que el riesgo se gestione dentro del contexto empresarial, los objetivos de negocio, las metas de desempeño y el apetito al riesgo de la organización. En algunos casos, la dirección puede que tenga que considerar otro curso de acción, incluido lo siguiente:

- *Revisar los objetivos de negocio:* La organización opta por examinar y revisar los objetivos de negocio potenciales dada la gravedad de los riesgos identificados y la tolerancia. Esto puede ocurrir cuando las otras categorías de respuestas al riesgo no representen las actuaciones deseadas para la entidad.
- *Revisar la estrategia:* La organización opta por examinar y revisar la estrategia potencial dada la gravedad de los riesgos identificados y el apetito al riesgo de la entidad. Esto puede ocurrir cuando otras categorías de respuestas al riesgo no representan las actuaciones deseadas para la entidad.

Las organizaciones también pueden optar por superar el apetito al riesgo si el efecto de permanecer dentro del apetito se percibe como mayor que la exposición potencial por superarlo. Por ejemplo, la dirección puede aceptar el riesgo asociado a la aprobación rápida de un nuevo producto en favor de la oportunidad y la ventaja competitiva resultante de llevar esos productos al mercado lo más rápidamente posible. Cuando una entidad acepte repetidamente riesgos que se acerquen o superen el apetito como parte de sus operaciones habituales, podrá ser justificable que se realice una revisión y ajuste del apetito al riesgo.

Selección e implantación de respuestas al riesgo

La dirección selecciona e implanta las respuestas al riesgo considerando los siguientes factores:

- *Contexto empresarial:* Las respuestas al riesgo se seleccionan o adaptan al sector, geografía, entorno regulatorio, estructura operativa u otros factores.
- *Costes y beneficios:* Los costes y beneficios anticipados suelen ser proporcionales a la gravedad y priorización del riesgo.
- *Obligaciones y expectativas:* La respuesta al riesgo aborda las normas del sector generalmente aceptados, las expectativas de las partes interesadas y la alineación con la misión y visión de la entidad.
- *Priorización del riesgo:* La prioridad asignada al riesgo dota de información adecuada a la asignación de recursos. Las respuestas al riesgo que tienen grandes costes de implantación (por ejemplo, actualizaciones de sistemas, aumentos de personal) para riesgos de menor prioridad, deben considerarse cuidadosamente y pueden no ser apropiadas dada la prioridad evaluada.
- *Apetito al riesgo:* La respuesta al riesgo permite que la entidad asuma riesgos dentro del apetito al riesgo o mantenga su estado actual. La dirección identifica la respuesta que lleve el riesgo residual dentro del apetito. Esto se puede conseguir, por ejemplo, contratando un seguro e implantando respuestas a nivel interno para reducir el riesgo a un rango de tolerancia.
- *Gravedad del riesgo:* La respuesta al riesgo debe reflejar el tamaño, alcance y naturaleza del riesgo y su impacto en la entidad. Por ejemplo, en un entorno de transacciones o producción, donde los riesgos están motivados por los cambios de volumen, la respuesta propuesta se adapta para dar cabida al aumento de la actividad.

A menudo, cualquiera de las diversas respuestas al riesgo situarán el riesgo residual en línea con la tolerancia, y a veces una combinación de respuestas proporcionará el resultado óptimo. Por el contrario, a veces una respuesta afectará a múltiples riesgos, en cuyo caso la dirección podrá decidir que no se necesitan acciones adicionales para abordar un riesgo particular

La respuesta al riesgo puede cambiar el perfil de riesgo (véase el Ejemplo 8.5). Una vez que la dirección selecciona una respuesta al riesgo, se deben implantar actividades de control²⁵ para garantizar que esas respuestas al riesgo se lleven a cabo según lo previsto. La dirección debe ser consciente de que el riesgo se gestiona, pero no se elimina. Siempre existirá algún riesgo residual, no sólo porque los recursos sean limitados, sino también por las incertidumbres del futuro y las limitaciones inherentes a todas las actividades.

Ejemplo 8.5: Modificación de perfiles de riesgo

Una explotación agrícola de tamaño mediano está considerando contratar un seguro meteorológico frente a inundaciones o tormentas que compense cualquier disminución de la producción por debajo de un volumen mínimo determinado. El perfil de riesgo resultante para los niveles de producción tendría en cuenta los resultados potenciales de desempeño cubiertos por el seguro.

25 Las actividades de control se analizan en *Control Interno—Marco Integrado*.

Consideración de costes y beneficios de las respuestas al riesgo

La dirección debe tener en cuenta los costes y beneficios potenciales de las diferentes respuestas al riesgo. En general, los costes y beneficios previstos son proporcionales a la gravedad y la priorización del riesgo. Por ejemplo, un riesgo de alta prioridad y mayor gravedad puede justificar el aumento de costes en recursos, dados los beneficios previstos por la respuesta.

Las mediciones de coste y beneficio para seleccionar y desplegar las respuestas al riesgo se realizan con diferentes niveles de precisión. Los costes incluyen los gastos directos, indirectos (siempre que sea factible) y, en el caso de algunas entidades, los costes de oportunidad asociados al uso de los recursos. La medición de los beneficios puede ser más subjetiva, ya que generalmente son difíciles de cuantificar. En muchos casos, sin embargo, el beneficio de una respuesta al riesgo puede evaluarse en el contexto de la consecución de la estrategia y los objetivos de negocio. En algunos casos, dada la importancia de una estrategia u objetivo de negocio, puede que no haya una respuesta óptima al riesgo desde el punto de vista de los costes y beneficios. En tales casos, la organización puede elegir entre seleccionar una respuesta o volver a examinar la estrategia y los objetivos de negocio de la entidad.

La dirección también es responsable de las respuestas al riesgo que abordan cualquier obligación regulatoria, las cuales, de nuevo, puede que no sean óptimas desde el punto de vista de coste y beneficio, pero que cumplen las obligaciones legales o de otro tipo (ver Ejemplo 8.6). Al seleccionar la respuesta adecuada, la dirección debe tener en cuenta las expectativas de las distintas partes interesadas, como puedan ser los accionistas, reguladores y clientes.

Ejemplo 8.6: Relación del perfil de riesgo con el apetito al riesgo

Una compañía de seguros implanta una serie de respuestas al riesgo para abordar los nuevos requisitos regulatorios del sector asegurador. Estas respuestas requerirán que la empresa realice inversiones adicionales en su infraestructura tecnológica, modifique sus procesos actuales e incremente su personal para asistir en la implantación y lograr sus objetivos de cumplimiento normativo.

Consideraciones adicionales

La selección de una respuesta al riesgo puede introducir nuevos riesgos que no se habían identificado previamente o que puedan tener consecuencias involuntarias. Por ejemplo, para la explotación agrícola del Ejemplo 8.5, el riesgo de inundaciones que dañen los cultivos se redujo al contratar el seguro; sin embargo, la explotación puede correr ahora el riesgo de que se reduzca su flujo de caja.

En el caso de los riesgos recientemente identificados, la dirección debe evaluar la gravedad y la prioridad relacionada, y determinar la eficacia de la respuesta al riesgo propuesta. Por otra parte, la selección de una respuesta al riesgo puede presentar nuevas oportunidades no consideradas previamente. La dirección puede identificar respuestas innovadoras que, si bien se ajusten a las categorías de respuesta descritas anteriormente, pueden ser totalmente nuevas para la entidad o incluso para un sector. Estas oportunidades pueden surgir cuando las opciones de respuesta al riesgo existente alcancen el límite de eficacia y cuando sea probable que los nuevos ajustes sólo supongan cambios marginales en la gravedad de un riesgo. La dirección canaliza cualquier nueva oportunidad a través de la redefinición de la estrategia.



Principio 14: Desarrolla una visión a nivel de cartera

La organización desarrolla y evalúa una visión del riesgo a nivel de cartera.

Entendimiento de la visión a nivel de cartera

La gestión del riesgo empresarial permite a la organización considerar las posibles consecuencias para el perfil de riesgo desde la perspectiva de toda la entidad (o a nivel de cartera). La dirección primero considera el riesgo en lo que se refiere a cada división, unidad operativa o función. Cada gestor desarrolla una evaluación compuesta de riesgos que refleja el perfil de riesgo residual de la unidad en relación con sus objetivos de negocio y su tolerancia.

Una visión de cartera permite a la dirección y al consejo de administración considerar el tipo, la gravedad y las interdependencias de los riesgos y la forma en que éstos pueden afectar el desempeño. A través de la visión de cartera, la organización identifica los riesgos que son graves a nivel de entidad. Entre ellos, se pueden incluir los riesgos que surgen a nivel de entidad, así como los riesgos transaccionales y de procesamiento, que podrían generar efectos disruptivos en la entidad en su conjunto.

Con una visión a nivel de cartera, la dirección está bien posicionada para determinar si el perfil de riesgo residual de la entidad se alinea con el apetito al riesgo global. El mismo riesgo en diferentes unidades puede ser aceptable en el caso de las unidades operativas, pero, tomado en conjunto, puede ser muy diferente. En términos globales, el riesgo puede superar el apetito al riesgo de la entidad en su conjunto, en cuyo caso se requieren respuestas de riesgo adicionales o diferentes. Por el contrario, un riesgo puede no ser aceptable en una unidad, pero puede estar dentro del rango en otra. Por ejemplo, algunas unidades operativas tienen un riesgo más elevado que otras, pero el riesgo global se mantiene dentro del apetito al riesgo de la entidad. Y en los casos en que la visión a nivel de cartera muestre que los riesgos sean significativamente menores que el apetito al riesgo de la entidad, la dirección podrá optar por motivar a los gerentes de las unidades operativas individuales para que acepten un mayor riesgo en áreas específicas, esforzándose por aumentar el valor de la entidad.

Desarrollo de una visión a nivel de cartera

Se puede desarrollar una visión del riesgo a nivel de cartera de diversas maneras. Un método consiste en centrarse en las principales categorías de riesgo de las unidades operativas, o en el riesgo para la entidad en su conjunto, utilizando parámetros como el capital ajustado al riesgo o el capital en riesgo. Este método es especialmente útil cuando se evalúa el riesgo frente a los objetivos de negocio establecidos en términos de ingresos, crecimiento y otras medidas de desempeño, a veces en relación con el capital asignado o disponible. La información derivada puede resultar útil para redistribuir el capital entre las distintas unidades operativas y modificar la dirección estratégica (se pueden utilizar otros métodos cualitativos para desarrollar esta visión de cartera).

También se puede representar gráficamente una visión de cartera indicando el tipo y el nivel de riesgo asumido en comparación con el apetito al riesgo de la entidad para cada función, estrategia y objetivo de negocio de la organización. La visión de cartera de la Figura 8.10 ilustra la alineación de los riesgos con los objetivos de negocio y la relación entre los diferentes objetivos.

Para desarrollar una visión del riesgo, existen cuatro niveles en orden ascendente de nivel de integración (de mínimo a máximo):

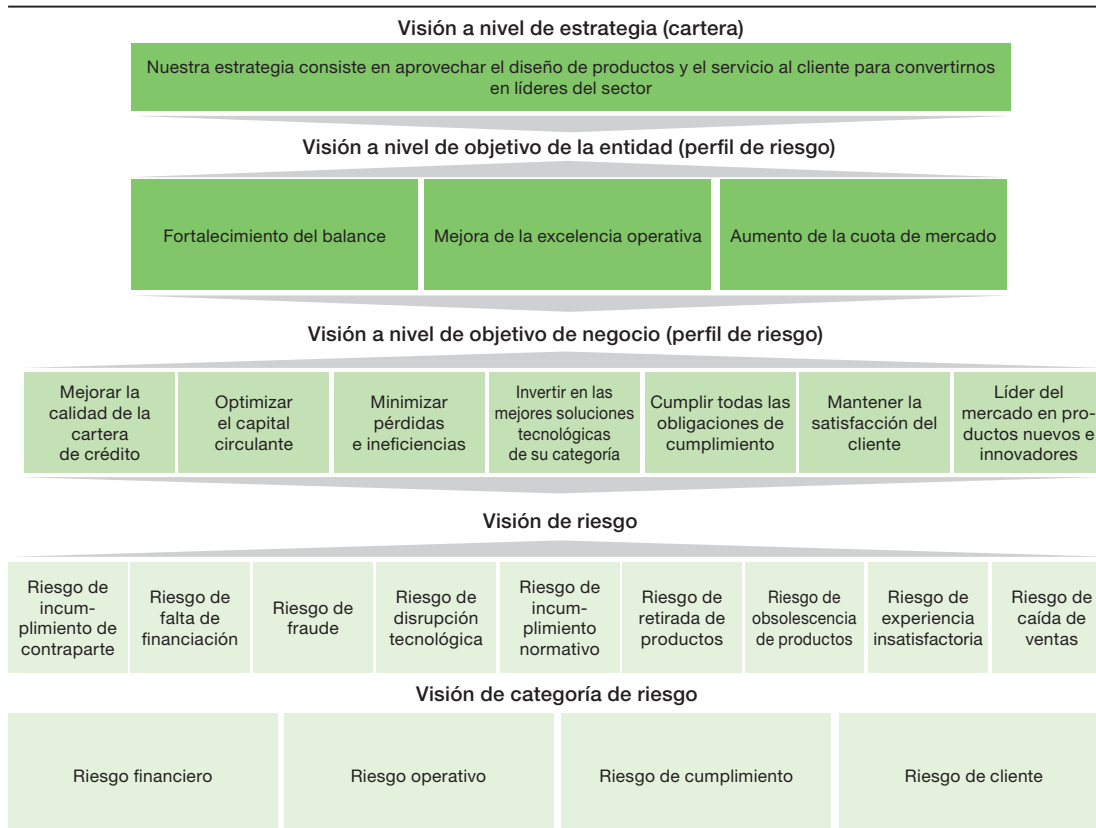
- *Integración mínima* — *Visión de riesgo*: Desde el punto de vista centrado en el riesgo, la entidad identifica y evalúa riesgos específicos. El enfoque predominante se centra en el evento de riesgo subyacente más que en el objetivo; por ejemplo, el riesgo de un incumplimiento que impacte en el cumplimiento de la entidad con las regulaciones locales.

- **Integración limitada — Visión de categoría de riesgo:** Esta vista utiliza información capturada en la vista del inventario de riesgos y organiza los riesgos con arreglo a categorías u otro esquema de clasificación. Las categorías de riesgos a menudo reflejan la estructura operativa de la entidad y dotan de información relevante a las funciones y responsabilidades. Un departamento de cumplimiento, por ejemplo, tendrá la responsabilidad de ayudar a la organización a gestionar sus riesgos relacionados con el cumplimiento.
- **Integración parcial — Visión de perfil de riesgo:** Adoptando una visión más integrada, una organización se centra en los objetivos de negocio y los riesgos que se alinean con esos objetivos (por ejemplo, todos los objetivos pueden verse potencialmente afectados por los riesgos relacionados con el cumplimiento). Además, se identifican y consideran las dependencias que pueden existir entre los objetivos de negocio. Por ejemplo, el objetivo de mejorar la excelencia operativa puede ser un requisito previo para reforzar el balance y aumentar la cuota de mercado. Esta visión se basa en la información utilizada para crear la visión centrada en el riesgo o en las categorías de riesgo.
- **Integración completa — Visión de cartera:** En este nivel, el enfoque se desplaza hacia la estrategia global de la entidad y los objetivos de negocio. El aumento de la integración facilita la identificación, evaluación, respuesta y revisión del riesgo en los niveles apropiados para la toma de decisiones. Los consejos de administración y la dirección se centran más en la consecución de la estrategia, mientras que la responsabilidad y la gestión de los objetivos de negocio y los riesgos individuales dentro del inventario de riesgos se trasladan a toda la entidad. Utilizando el mismo ejemplo, el consejo revisa y desafía a la dirección sobre cómo la entidad está mejorando su excelencia operativa, incluyendo la gestión de los riesgos relacionados con el cumplimiento.

Al desarrollar la visión de cartera, las organizaciones pueden observar riesgos que:

- Aumentan su gravedad a medida que se consolidan progresivamente a niveles superiores dentro de la entidad.

Figura 8.10 Visión del riesgo a nivel de cartera



- Disminuyen su gravedad a medida que se consolidan progresivamente.
- Compensan otros riesgos actuando como coberturas naturales.
- Demuestran una correlación positiva o negativa con los cambios que se producen en la gravedad de otros riesgos.

Utilizando la Figura 8.10 como ejemplo, una organización desarrolla su visión de cartera y observa las siguientes características:

- *La gravedad de las interrupciones tecnológicas* aumenta a medida que los riesgos se agregan progresivamente, reconociendo la dependencia que tienen múltiples organizaciones de los sistemas operativos y tecnologías comunes.
- *El riesgo de incumplimiento de contraparte* disminuye en gravedad a medida que la entidad no tiene un solo acreedor que se considere suficientemente grande como para afectar a la entidad en su conjunto.
- *El riesgo de caída de las ventas en múltiples unidades operativas* puede actuar como cobertura natural cuando la caída de ventas de una unidad operativa es compensada por el aumento de las ventas en otra.
- *El riesgo de fluctuaciones monetarias* también puede actuar como cobertura natural cuando la variación en los tipos de cambio en un país compensan las variaciones en otro.
- *La fuerte correlación positiva entre el riesgo de retirada de productos y el riesgo de incumplimiento normativo* aumenta la prioridad de las respuestas a ambos riesgos.
- *Una fuerte correlación positiva entre los objetivos de negocio* exige que se invierta en soluciones tecnológicas al más alto nivel y se minimicen las pérdidas e ineficiencias que se tienen en cuenta al seleccionar las respuestas al riesgo asociadas.

El desarrollo de una visión a nivel de cartera de los riesgos para la entidad permite la toma de decisiones basada en el riesgo y ayuda a establecer objetivos de desempeño y a gestionar los cambios en el desempeño o en el perfil de riesgo. Entre las consideraciones importantes a la hora de establecer objetivos y responder al cambio, cabe destacar la comprensión de los riesgos que es probable que aumenten o disminuyan, si se introducen nuevos riesgos y si los riesgos existentes pierden importancia. Al utilizar una visión de cartera para comprender la relación entre riesgo y desempeño, la organización puede evaluar los resultados de la estrategia y los objetivos de negocio de acuerdo con el apetito al riesgo de la entidad.

Análisis de la visión de cartera

Para evaluar la visión de cartera del riesgo, la organización deberá utilizar técnicas cualitativas y cuantitativas. Las técnicas cuantitativas incluyen la modelización de regresión y otros medios de análisis estadístico para determinar la sensibilidad de la cartera frente a cambios repentinos o significativos. Las técnicas cualitativas incluyen análisis de escenarios y comparativos.

Al hacer hincapié en la cartera, la dirección puede revisar:

- Hipótesis en los que se base la evaluación de la gravedad del riesgo.
- Comportamientos de riesgos individuales bajo condiciones de tensión.
- Interdependencias de riesgos dentro de la visión de cartera.
- Eficacia de las respuestas al riesgo existente.

Mediante el uso de tests de estrés, análisis de escenarios u otros ejercicios analíticos, una organización puede evitar o responder más eficazmente ante grandes sorpresas y pérdidas. La organización utiliza diferentes técnicas para evaluar el efecto de los cambios en el contexto empresarial u otras variables sobre un objetivo de negocio o la estrategia. Por ejemplo, una organización puede optar por analizar el efecto de una modificación de los tipos de interés en la visión de cartera. Alternativamente, la organización puede tratar de comprender el impacto de múltiples variables que

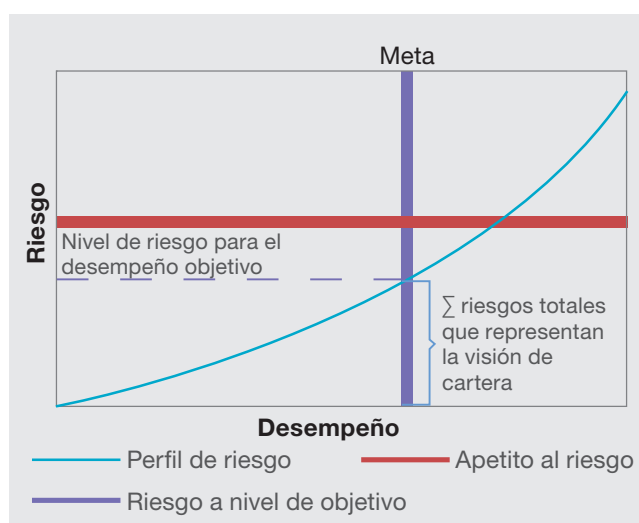
ocurren simultáneamente, tales como el cambio de los tipos de interés y un repunte en los precios de las materias primas que afectan a la rentabilidad de la entidad. Por último, la organización puede optar por evaluar el impacto de un evento a gran escala, como un incidente operativo o un fallo de un tercero. Al analizar el efecto de hipotéticos cambios en la visión de cartera, la organización identifica posibles riesgos nuevos, emergentes o cambiantes y evalúa la idoneidad de las respuestas al riesgo existentes.

Los test de estrés ayudan a una organización a comprender cómo la forma o la altura de la curva de riesgo pueden responder a los cambios potenciales. Por ejemplo:

- Validación de eventos que podría generar efectos disruptivos y hacer que la curva de riesgos supere el apetito al riesgo (esto es, la magnitud de una brecha de financiación potencial que impacta en la viabilidad del negocio, que podría representarse por la intersección de la curva de riesgos con el apetito al riesgo de la entidad).
- La medida en que la curva de riesgos puede cambiar hacia arriba o hacia abajo en respuesta a un cambio (por ejemplo, confirmando hasta qué punto los cambiantes indicadores de salud económica, como los niveles de desempleo y el producto interior bruto, representan un deterioro suficiente en el contexto empresarial y provocan que la curva de riesgos cambie hacia arriba).
- Las respuestas al riesgo que pueden hacer que determinadas secciones de la curva se vuelvan más planas (por ejemplo, diversificar productos formalizando nuevas estrategias de cobertura financiera o la contratación de seguros adicionales).
- La facilidad con la que la organización puede moverse a lo largo de la curva. La velocidad y agilidad de la organización para tomar decisiones y desplazarse a lo largo de la curva de riesgo hasta una nueva intersección deseada de riesgo y desempeño (por ejemplo, la velocidad de ajustar los volúmenes de producción en respuesta a los cambios en las ventas).

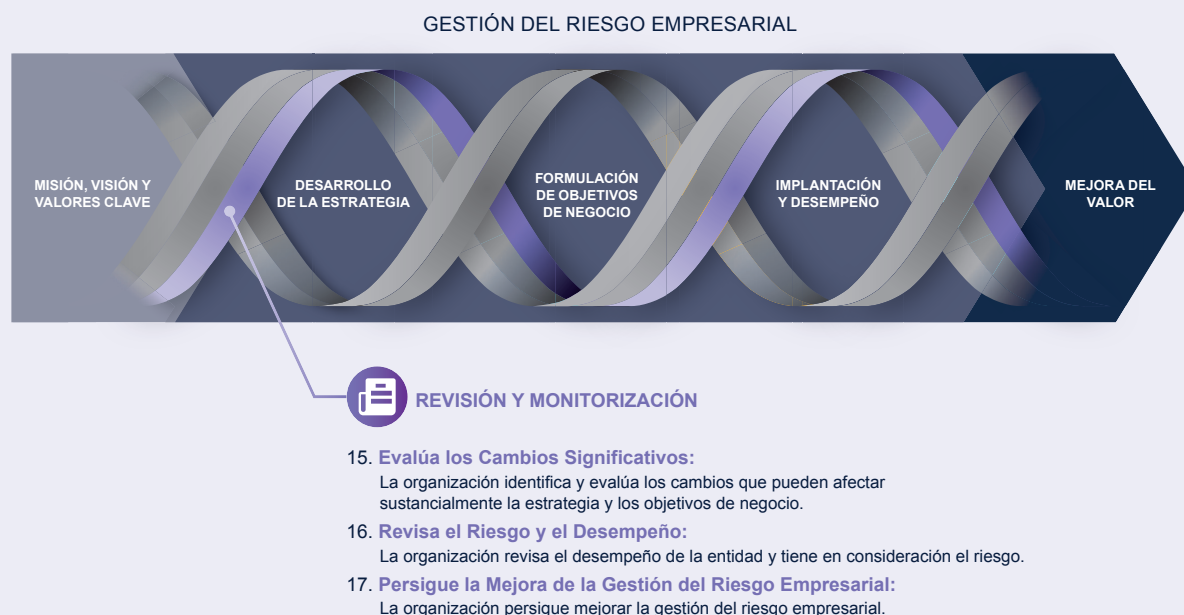
Estas prácticas ayudan a evaluar la capacidad de adaptación de la entidad. Asimismo, estos ejercicios ayudan a la dirección a cuestionar las hipótesis en las que se basa la selección de la estrategia de la entidad y la evaluación del perfil de riesgo. Por lo tanto, el análisis de la visión de cartera también puede formar parte de la evaluación de una organización al seleccionar una estrategia o establecer objetivos de negocio. La Figura 8.11 muestra la visión del riesgo a nivel de cartera.

Figura 8.11: El perfil de riesgo muestra el riesgo como visión de cartera



9. Revisión y Monitorización

Principios relacionados con la Revisión y Monitorización



Introducción

La estrategia o los objetivos de negocio de la entidad y las técnicas y capacidades de gestión del riesgo empresarial pueden cambiar con el tiempo, a medida que la entidad se adapta a un contexto de negocio cambiante. Además, el contexto empresarial en el que opera la entidad también puede cambiar, de manera que las prácticas actuales ya no sean aplicables o no sean suficientes para facilitar el logro de los objetivos de negocio actuales. Según sea necesario, la organización revisará sus prácticas o complementará sus capacidades.



Principio 15: Evalúa los cambios significativos

La organización identifica y evalúa los cambios que pueden afectar sustancialmente a la estrategia y los objetivos de negocio.

Integración de las revisiones en las técnicas de negocio

Por lo general, las organizaciones anticipan muchos cambios al establecer los la estrategia y los objetivos de negocio, y el desempeño, pero también deben ser conscientes de la posibilidad de que se produzcan cambios sustanciales de mayor envergadura que puedan tener un efecto más pronunciado. Un cambio sustancial puede dar lugar a riesgos nuevos o cambiantes y afectar a las hipótesis clave que sustentan la estrategia. Las prácticas para identificar tales cambios deben incorporarse a las actividades de negocio y llevarse a cabo de manera continua. Muchas técnicas de gestión pueden identificar cambios sustanciales en el curso ordinario de la gestión del negocio. Por ejemplo, la revisión del plan de integración de una empresa recién adquirida puede determinar la necesidad de mejoras futuras en el ámbito de las TI.

Los cambios sustanciales, como la adquisición de una entidad o la implantación de un nuevo sistema, podrían cambiar la visión del riesgo de la entidad a nivel de cartera o afectar al funcionamiento de la gestión del riesgo empresarial. En el caso de una adquisición, la integración de las operaciones de la empresa adquirida podría afectar a la cultura existente y a la responsabilidad sobre el riesgo. La implantación de un nuevo sistema podría presentar nuevas exposiciones relacionadas con la seguridad de la información, lo que podría influir en la forma en que se capturan y gestionan los datos.

Las organizaciones tienen en cuenta cómo los cambios pueden afectar a la gestión del riesgo empresarial y a la consecución de la estrategia y los objetivos de negocio. Esto requiere identificar los cambios en el entorno internos y externos relacionados con el contexto empresarial, así como los cambios en la cultura. A continuación, se incluyen algunos ejemplos de cambios sustanciales en el entorno interno y externo.

El entorno interno

- **Rápido crecimiento:** Cuando hay una rápida expansión en las operaciones, las estructuras existentes, las actividades de negocio, los sistemas de información o los recursos pueden verse afectados. Es posible que los sistemas de información no puedan cumplir eficazmente los requisitos de información sobre riesgos debido al aumento del volumen de transacciones. Es posible que sea necesario redefinir las funciones y responsabilidades de supervisión del riesgo a la luz de los cambios organizativos y geográficos resultantes de una adquisición. Los recursos pueden verse afectados hasta el punto de que las respuestas y acciones con respecto al riesgo dejen de funcionar. Por ejemplo, es posible que los supervisores no sepan adaptarse a los nuevos niveles de actividad resultante de añadir nuevos turnos de fabricación o de aumentar el personal.
- **Innovación:** Siempre que se introduzcan elementos de innovación, es probable que sea necesario modificar las respuestas a los riesgos y las acciones de la dirección. Por ejemplo, la introducción de nuevas capacidades de venta a través de dispositivos móviles puede exigir controles de acceso específicos para dicha tecnología. Es posible que los usuarios necesiten formación adicional. Las tecnologías de innovación también pueden mejorar la gestión del riesgo empresarial. Por ejemplo, un nuevo sistema de uso de dispositivos móviles que captura información de ventas previamente no disponible aporta a la dirección la capacidad de realizar un seguimiento del desempeño, realizar previsiones de ventas potenciales y tomar decisiones de inventario en tiempo real.

- *Cambios sustanciales en el equipo de dirección y los empleados:* Un cambio en la dirección puede afectar a la gestión del riesgo empresarial. Un recién llegado al equipo de dirección puede no comprender la cultura de la entidad y tener una filosofía diferente, o centrarse únicamente en el desempeño excluyendo el apetito al riesgo o la tolerancia.

El entorno externo

- *Cambios en el entorno regulatorio o económico:* Los cambios en las regulaciones o en la economía pueden derivar en un aumento de las presiones competitivas, cambios en los requisitos operativos y riesgos diferentes. Si se produce un fallo a gran escala en las operaciones, en el reporte y el cumplimiento en una sola entidad, los reguladores pueden introducir normativas que afecten a todas las entidades de un sector. Por ejemplo, si se produce un vertido de material tóxico en un área poblada o sensible al medio ambiente, puede que se introduzcan nuevas restricciones de transporte en todo el sector que afecten a la logística y el transporte de una entidad. Si se considera que una empresa que cotiza en bolsa tiene poca transparencia, puede que se introduzcan requisitos regulatorios de información más estrictos para todas las empresas cotizadas. Si se tiene conocimiento de que los pacientes de un centro sanitario reciben malos tratos puede que esto genere requisitos adicionales en todos los centros sanitarios de ese tipo. Y un entorno más competitivo puede provocar en determinadas personas la toma de decisiones que no estén alineadas con el apetito al riesgo de la entidad y que aumenten las exposiciones al riesgo de la entidad. Cada uno de estos cambios puede requerir que una organización examine minuciosamente el diseño y la aplicación de la gestión del riesgo empresarial.

Identificar cambios sustanciales, evaluar sus efectos y responder a los cambios son procesos iterativos que pueden afectar a varios componentes de la gestión del riesgo empresarial. Puede ser útil realizar un análisis a posteriori (después de que se haya producido un evento de riesgo) para revisar cómo respondió la organización y considerar qué lecciones aprendidas podrían aplicarse de cara a eventos futuros.



Principio 16: Revisa el riesgo y el desempeño

La organización revisa el desempeño de la entidad y tiene en consideración el riesgo.

Integración de las revisiones en las prácticas de negocio

Gran parte de la atención que se presta a la gestión del riesgo empresarial se dirige a gestionar el riesgo, ya sea reduciendo el tipo y el nivel de riesgo a niveles aceptables o aprovechando adecuadamente las nuevas oportunidades a medida que surgen. Con el paso del tiempo, puede que la entidad no pueda llevar a cabo sus prácticas de forma tan eficaz como querría, provocando así que el riesgo se manifieste y afecte al desempeño. De vez en cuando, la organización tal vez desee considerar sus capacidades y técnicas de gestión del riesgo empresarial. Las observaciones que pueda aplicar podrán hacer referencia a hipótesis incorrectas, prácticas implantadas, capacidades de la entidad o factores culturales. A veces, sin embargo, el desempeño se ve afectado debido a la naturaleza inherente del riesgo que una organización no puede predecir con total exactitud. Al revisar el desempeño, las organizaciones buscan respuestas a preguntas tales como:

- **¿El rendimiento de la organización ha sido acorde a lo esperado y ha alcanzado su objetivo?** La organización identifica las desviaciones que han ocurrido y considera lo que puede haber contribuido a ellas. Esto puede implicar el uso de medidas relacionadas con los objetivos u otras métricas clave. Por ejemplo, sirva el caso de una entidad que se ha comprometido a abrir cinco nuevas oficinas cada año para facilitar su estrategia de crecimiento a largo plazo y desarrollar así su presencia en todo el país. La organización ha decidido que podría seguir implantando su estrategia con la apertura de tan sólo tres oficinas, y que asumiría más riesgos de los deseados si abriera siete o más oficinas. Por lo tanto, la organización supervisa el desempeño y determina si la entidad ha abierto el número previsto de oficinas y cómo están funcionando esas nuevas oficinas. Si el crecimiento está por debajo del plan, es posible que la organización deba revisar la estrategia.
- **¿Qué riesgos están ocurriendo que puedan afectar al desempeño?** El seguimiento realizado del desempeño también confirma si se identificaron previamente los riesgos o si se han generado nuevos riesgos emergentes. La organización también examina si los niveles de riesgo reales se encuentran dentro de los límites de tolerancia establecidos. Por ejemplo, el examen del desempeño ayuda a confirmar si se materializó el riesgo de retrasos debido a los requisitos adicionales de permisos de construcción exigidos y si esto afectó al número de nuevas oficinas que se abrieron, y si el número de oficinas que se abrirá sigue estando dentro del rango de desempeño aceptable.
- **¿Estaba la entidad asumiendo el riesgo suficiente para alcanzar su meta?** Cuando una entidad no ha cumplido su meta, la organización trata de comprender si se han materializado riesgos que estén afectando a la consecución de la meta o si se han tomado riesgos insuficientes para el logro de dicha meta. Utilizando el mismo ejemplo, supongamos que la entidad abre sólo tres oficinas. En ese caso, la dirección observa que los equipos de planificación y logística funcionan por debajo de su capacidad y que no se han utilizado el resto de recursos asignados para la apertura de nuevas oficinas. La entidad asumió un riesgo insuficiente a pesar de haber asignado recursos.
- **¿Ha sido precisa la estimación del riesgo?** Cuando el riesgo no se ha evaluado con precisión, la organización se pregunta por qué ha sido así. Para responder a esta pregunta, la organización debe cuestionar la comprensión del contexto empresarial y los supuestos en los que se basa la evaluación inicial. También debe determinar si se dispone de nueva información que ayude a perfeccionar la evaluación. Por ejemplo, supongamos que la entidad del ejemplo abre cinco oficinas y observa que el nivel estimado de riesgo fue demasiado bajo en comparación con el tipo y el nivel de riesgo que se ha producido (por ejemplo, más problemas, retrasos e imprevistos de los inicialmente evaluados).

Si una organización determina que el desempeño no se sitúa dentro de su variación aceptable, o que la meta de desempeño provoca un perfil de riesgo diferente al esperado, puede ser necesario:

- *Revisar los objetivos de negocio:* Una organización puede optar por cambiar o abandonar un objetivo de negocio si no se logra el desempeño de la entidad dentro de una variación aceptable.
- *Revisar la estrategia:* Si el desempeño de la entidad resultara en una desviación sustancial del perfil de riesgo esperado, la organización puede optar por revisar su estrategia. En este caso, puede optar por reconsiderar estrategias alternativas que hayan sido evaluadas previamente, o identificar nuevas estrategias.
- *Revisar la cultura:* Una organización puede optar por revisar su cultura y determinar si está adoptando las acciones oportunas, siendo consciente de los riesgos. ¿Se siente cómoda la organización tomando el riesgo necesario para tener éxito, o es propensa a asumir demasiado riesgo del que se puedan derivar resultados adversos?
- *Reevaluar la meta de desempeño:* Una organización puede optar por reevaluar el nivel de desempeño objetivo para reflejar una mejor comprensión de la razonabilidad del desempeño potencial y la gravedad correspondiente de los riesgos con respecto al objetivo de negocio.
- *Reevaluar la gravedad de los resultados del riesgo:* Una organización puede volver a realizar la evaluación de riesgos con respecto a los riesgos pertinentes, y los resultados pueden variar en función de los cambios que se hayan producido en el entorno de negocio, la disponibilidad de nuevos datos o información que permita una evaluación más precisa, o que cuestione las hipótesis en las que se basó la evaluación inicial.
- *Revisar cómo se priorizan los riesgos:* Una organización puede optar por aumentar o disminuir la prioridad de los riesgos identificados para facilitar la reasignación de recursos. Los cambios serán resultado de la revisión de la evaluación con respecto a los criterios de priorización aplicados anteriormente.
- *Reevaluar las respuestas al riesgo:* Una organización puede considerar la posibilidad de modificar o añadir respuestas para ajustar el riesgo al desempeño y al perfil de riesgo deseado. En el caso de aquellos riesgos cuya gravedad se reduzca, una organización podrá reasignar recursos a otros riesgos u objetivos de negocio. En el caso de aquellos riesgos cuya gravedad aumente, la organización podrá reforzar las respuestas con procesos, personas, infraestructuras u otros recursos adicionales. En el marco de la revisión de las respuestas a los riesgos, la organización también puede considerar las actividades de seguimiento desarrolladas e implantadas como parte del control interno²⁶.
- *Reevaluar el apetito al riesgo:* Por lo general, las acciones correctivas se emprenden para mantener o restablecer la alineación del perfil de riesgo con el apetito al riesgo de la entidad, pero pueden extenderse a su reevaluación. Sin embargo, esta acción requiere la revisión y aprobación del consejo de administración u otro órgano de supervisión del riesgo.

El alcance de cualquier acción correctiva debe alinearse con la magnitud de la desviación en el desempeño, la importancia del objetivo de negocio y los costes y beneficios asociados a la alteración de las respuestas al riesgo. Por ejemplo, véase el caso de un pequeño establecimiento minorista que cuenta con una parte significativa de su inventario en productores locales. El establecimiento supervisa los resultados financieros de su tienda semanalmente y se da cuenta de que los bienes producidos localmente no son suficientemente rentables para alcanzar sus objetivos financieros. Por lo tanto, decide revisar su objetivo de negocio de abastecerse localmente y comienza a importar bienes menos costosos para mejorar su desempeño financiero. El establecimiento también reconoce que este cambio puede afectar a otros riesgos, como la logística, las fluctuaciones monetarias y el tiempo de salida al mercado.

26 En *Control Interno—Marco Integrado* se incluye un análisis adicional sobre las actividades de seguimiento

Cuando el examen del desempeño identifique repetidamente nuevos riesgos que no hayan sido identificados a través de las prácticas de identificación de riesgos de la organización, o cuando el riesgo real no sea coherente con las calificaciones de gravedad, la dirección deberá determinar si está justificado realizar una revisión de las técnicas de gestión del riesgo empresarial. En el Principio 17 se puede encontrar un análisis más detallado sobre la revisión de las prácticas de evaluación de riesgos.

Consideración de las capacidades de la entidad

Parte de la revisión del desempeño consiste en considerar las capacidades de la organización y su efecto en el desempeño. Si no se cumplen las metas de desempeño, ¿se debe a que las capacidades son insuficientes? Si se superan los objetivos, ¿se debe a que se requieren medidas correctivas? La organización debe responder a estas preguntas.

Las acciones correctivas pueden implicar reasignar recursos, reevaluar los objetivos del negocio o analizar estrategias alternativas (ver Ejemplo 9.1).

La capacidad de recursos de la entidad también informa de las decisiones para proponer medidas correctivas. Para los objetivos de negocio que afecten a la entidad en su conjunto, la organización puede optar por reevaluar el objetivo en lugar de incurrir en los costes de desarrollar respuestas al riesgo adicionales. Siempre que se produzcan desviaciones significativas de la tolerancia, o cuando el desempeño represente una interrupción en la consecución de la estrategia de la entidad, la organización puede reevaluar su estrategia.

Ejemplo 9.1: Consideración de las capacidades de la entidad

La administración pública local de una región es consciente de que la economía local se basa en gran medida en el turismo. Los funcionarios municipales entienden los niveles mínimos, objetivo y máximos de turismo requeridos para lograr sus objetivos financieros. En particular, han determinado el volumen de ingresos que se pueden generar a través del turismo en función de indicadores como las reservas de hoteles y tasas de ocupación. Han identificado que una tasa de ocupación del 50% (su objetivo) proporciona a la ciudad con suficientes ingresos para lograr su presupuesto operativo anual y financiar otros programas. Sin embargo, una tasa de ocupación superior al 85% aumenta los riesgos relacionados con el uso del sistema de transporte público, las exigencias de presencia de policía local y la gestión de los recursos naturales. La ciudad hace un seguimiento de los patrones del sector turístico para tomar decisiones más conscientes del riesgo sobre la agresividad necesaria en sus futuras campañas de marketing y gestionar activamente el riesgo influenciado por el turismo.



Principio 17: Persigue la mejora de la gestión del riesgo empresarial

La organización persigue mejorar la gestión del riesgo empresarial.

Buscando la mejora

Incluso las entidades que cuentan con una gestión adecuada del riesgo empresarial pueden mejorar aún más su eficiencia. Al integrar las evaluaciones continuas en sus prácticas empresariales, las organizaciones pueden actualizar sistemáticamente las mejoras potenciales de sus técnicas de gestión del riesgo empresarial. También pueden ser útiles las evaluaciones independientes.²⁷ La búsqueda de una mejor gestión del riesgo empresarial debe llevarse a cabo en toda la entidad (véase el Ejemplo 9.2).

La dirección trata de alcanzar la mejora continua en toda la entidad (funciones, unidades operativas y divisiones) para mejorar la eficiencia y utilidad de la gestión del riesgo empresarial a todos los niveles. Las oportunidades para revisar y mejorar la eficiencia y utilidad pueden darse en cualquiera de las siguientes áreas:

- **Nuevas tecnologías:** Las nuevas tecnologías pueden ofrecer una oportunidad para mejorar la eficiencia. Por ejemplo, una entidad que utiliza datos de satisfacción de clientes considera que el volumen de datos recabado es excesivo para poder procesarlos. Para mejorar la eficiencia, implanta una nueva tecnología de minería de datos que identifica los de datos clave de una forma rápida y precisa.
- **Deficiencias históricas:** La revisión del desempeño puede identificar deficiencias históricas o las causas de fallos anteriores, y esa información puede utilizarse posteriormente para mejorar la gestión del riesgo empresarial. Por ejemplo, la dirección de una entidad observa que hay deficiencias en la evaluación de riesgos a lo largo del tiempo. Aunque la dirección gestione esas deficiencias, la organización decide mejorar sus prácticas de evaluación de riesgos para reducir el número de deficiencias y mejorar la gestión del riesgo empresarial.
- **Cambios organizativos:** Al tratar de conseguir una mejora continua, la organización puede identificar la necesidad de implantar cambios organizativos, tales como cambios en la estructura de gobierno. Por ejemplo, una función de gestión del riesgo empresarial depende del director financiero, pero cuando la entidad rediseña su equipo estratégico, decide reasignar la responsabilidad de la gestión del riesgo empresarial a este equipo reorganizado.
- **Apetito al riesgo:** La revisión del desempeño proporciona claridad sobre los factores que afectan el apetito al riesgo de la entidad. También le da a la dirección una oportunidad para redefinir su apetito al riesgo. Por ejemplo, la dirección puede efectuar un seguimiento del desempeño de un nuevo producto durante un año y evaluar la volatilidad del mercado. Si la dirección determina que el mercado está funcionando bien y es menos volátil de lo que se

Ejemplo 9.2: Mejora continua

Una agencia pública tiene conocimiento de que cuenta con unas prácticas más rigurosas para establecer y poner en práctica las capacidades de gobierno y para inculcar la cultura deseada. Por el contrario, las prácticas de la organización para establecer e implantar mecanismos de información y comunicación son mejorables. Si bien la dirección supervisa las oportunidades de mejora para todos los componentes de la gestión del riesgo empresarial, se centra en el desarrollo de sus prácticas de información y comunicaciones.

²⁷ Los lectores pueden consultar también el análisis sobre las actividades de seguimiento en *Control Interno—Marco Integrado*



pensaba en un principio, la organización podrá responder incrementando su apetito al riesgo para iniciativas futuras similares.

- *Categorías de riesgo:* Una organización que aspira a conseguir una mejora continua puede identificar patrones a medida que evoluciona el negocio, lo que puede llevar a la entidad a reevaluar sus categorías de riesgo. Por ejemplo, las categorías de riesgo de una entidad no incluyen el riesgo de ciberseguridad, pero ahora que la entidad ha decidido ofrecer varios productos y servicios online, está revisando las categorías para incluir este riesgo, de manera que pueda mapear de forma precisa su estrategia.
- *Comunicaciones:* La revisión del desempeño puede identificar procesos de comunicación obsoletos o que funcionen de forma deficiente. Por ejemplo, al revisar el desempeño, una organización descubre que no se están comunicando con éxito sus iniciativas mediante correo electrónico. En respuesta, la organización decide destacar las iniciativas en un blog y una aplicación de mensajes instantáneos para conseguir un mayor atractivo ante el cambiante perfil de sus empleados.
- *Comparación con entidades análogas:* Llevar a cabo revisiones con respecto a entidades análogas del sector puede ayudar a una organización a determinar si está operando fuera de los límites del desempeño de su sector. Por ejemplo, un proveedor global de servicios de paquetería descubrió durante una revisión de entidades análogas que sus operaciones en Asia estaban consiguiendo unos resultados muy inferiores a los de uno de sus principales competidores. Por consiguiente, tiene previsto revisar y, en caso necesario, modificar su estrategia para aumentar su competitividad y su desempeño en Asia.
- *Ritmo de cambio:* La dirección tiene en cuenta el ritmo al que evoluciona o cambia el contexto empresarial. Por ejemplo, una entidad de un sector en el que la tecnología evoluciona rápidamente o en el que se producen cambios organizativos a menudo puede tener más oportunidades de mejorar la eficiencia y utilidad de la gestión del riesgo empresarial, pero una entidad que opere en un sector en el que el ritmo de cambio tecnológico sea más lento, probablemente tenga menos posibilidades.

10. Información, comunicación y reporte

Principios relacionados con Información, comunicación y reporte

GESTIÓN DEL RIESGO EMPRESARIAL



INFORMACIÓN, COMUNICACIÓN Y REPORTE

18. **Aprovecha la 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.

Introducción

Los avances tecnológicos y empresariales han dado lugar a un crecimiento exponencial del volumen de datos y de la atención prestada a los mismos. Las organizaciones se enfrentan hoy en día al reto de la enorme cantidad de datos disponible y a la rapidez con la que deben ser procesados, organizados y almacenados. Con tanta información disponible, las organizaciones pueden sentirse abrumadas por la “sobrecarga de información”. En este entorno, es importante que las organizaciones proporcionen la información correcta, en la forma apropiada, con el nivel adecuado de detalle, a las personas correctas y en el momento oportuno.

Las organizaciones transforman los datos en información sobre partes interesadas, productos, mercados y acciones de la competencia. A través de sus canales de comunicación, pueden proporcionar información oportuna y pertinente al público destinatario. Las organizaciones también pueden estructurar datos e información en categorías coherentes. De esta manera, pueden identificar riesgos que puedan afectar a la estrategia y los objetivos de negocio.





Principio 18: Aprovecha la información y la tecnología

La organización utiliza los sistemas de información y tecnología de la entidad como soporte a la gestión del riesgo empresarial.

Uso de información relevante

Las organizaciones aprovechan la información relevante disponible cuando aplican técnicas de gestión del riesgo empresarial. La “información relevante” es información simple que ayuda a las organizaciones a ser más ágil en la toma de decisiones, dándoles una ventaja competitiva. Las organizaciones utilizan la información para anticiparse a situaciones que pueden obstaculizar la materialización de la estrategia y los objetivos del negocio. La información sobre riesgos debe ser más que un repositorio de datos históricos sobre riesgos. Es necesario que ayude a la comprensión y el desarrollo de un perfil de riesgo completo, actual y en evolución.

Las organizaciones se plantean qué información ha de estar disponible para la dirección, qué sistemas y tecnología de información se utilizan para capturar esa información (que puede ser más de la que se necesita), y cuáles son los costes de obtener esa información. El equipo de dirección y el resto de los empleados puede entonces identificar en qué medida la información soporta las técnicas de gestión del riesgo empresarial, que pueden incluir cualquiera de las siguientes:

- Para las técnicas relacionadas con el gobierno y la cultura, la organización puede necesitar información sobre las normas de conducta y el desempeño individual en relación con esas normas. Por ejemplo, las empresas de servicios profesionales tienen normas de conducta específicas para poder desarrollar relaciones independientes con los clientes. La formación anual del personal está encaminada al refuerzo de esas normas, y la dirección recopila información al poner a prueba los conocimientos de los empleados para determinar si entienden lo que se espera de ellos.
- Para las prácticas relacionadas con el establecimiento de la estrategia y objetivos, la organización puede necesitar información sobre las expectativas de las partes interesadas en cuanto al apetito al riesgo. Las partes interesadas, como puedan ser los inversores y clientes, pueden expresar sus expectativas a través de foros de analistas, publicaciones en blogs, términos y condiciones contractuales, etc. Todas ellas proporcionan información relevante sobre el tipo y el nivel de riesgo que una entidad puede estar dispuesta a aceptar y la estrategia que persigue.
- Para las prácticas relacionadas con el desempeño, las organizaciones pueden necesitar información sobre sus competidores para evaluar los cambios en el nivel de riesgo. Por ejemplo, una gran inmobiliaria residencial puede evaluar el riesgo de perder cuota de mercado en favor de pequeñas firmas de perfil “boutique”. La información que necesitan son los modelos de precios por comisiones de sus competidores y los planes de marketing online. Si los niveles de comisiones de sus competidores son bajos y agresivos, y su presencia online está extendida, la empresa puede revisar su capacidad para alcanzar sus objetivos de ventas.
- Para las prácticas relacionadas con la revisión y la monitorización, las organizaciones pueden necesitar información sobre las tendencias emergentes en el ámbito de la gestión del riesgo empresarial. Las organizaciones pueden recopilar dicha información en conferencias de gestión del riesgo empresarial y en blogs específicos del sector.

Hoy en día, los datos se generan con tanta rapidez que a menudo es un reto para la dirección procesarlos y ajustarlos para convertirlos en información útil. Los sistemas de información pueden ayudar a las entidades a afrontar este reto. Sin embargo, el foco no debe ponerse en la creación de un sistema de información nuevo e independiente, o incluso en flujos independientes para la gestión del riesgo empresarial. Por lo general, es más eficiente para una organización aprovechar sus sistemas de información existentes para capturar lo que necesite de cara a comprender el riesgo, tomar

decisiones considerando el riesgo y cumplir con los requisitos de reporte.

Para que sea útil, la información deberá estar a disposición de quienes toman las decisiones cuando sea necesaria. También es esencial que la información sea de alta calidad. Si los datos subyacentes son inexactos o incompletos, es posible que la dirección no pueda emitir juicios profesionales, estimaciones o decisiones²⁸ sólidas. Para mantener una información de alta calidad, las organizaciones implantan sistemas de gestión de datos y establecen políticas de gestión de la información estableciendo líneas claras de responsabilidad y de rendición de cuentas.

Evolución de la información

Los datos transformados en información pueden proceder tanto de fuentes estructuradas como no estructuradas. Los datos estructurados generalmente se refieren a información que está altamente organizada y es fácil de buscar (por ejemplo, archivos de base de datos, índices públicos u hojas de cálculo). Por el contrario, los datos no estructurados no siguen un patrón de datos predefinido, ni tampoco están organizados (por ejemplo, mensajes de correo electrónico, fotos, vídeos y documentos de procesamiento de texto). Varios estudios de investigación han estimado que hoy en día los datos no estructurados superan a los estructurados en más de un 80%.

Históricamente, el análisis de datos se ha basado en patrones predefinidos al convertir datos en información. En la actualidad, los avances en computación cognitiva, como la inteligencia artificial²⁹, la minería de datos y el aprendizaje automático pueden recopilar, convertir y analizar grandes volúmenes de datos no estructurados en información que ayude a las organizaciones a tomar mejores decisiones empresariales. Estos avances, combinados con el análisis humano, permiten una mejor comprensión del dato y facilitan la gestión. El Ejemplo 10.1 ilustra la utilización de la información no estructurada.

En resumen, los avances en el análisis de datos pueden ayudar a las organizaciones a evitar la “sobrecarga de información” y utilizar la enorme cantidad de datos que ahora están disponibles en su beneficio. Pueden ser capaces de detectar correlaciones en el desempeño de la actividad de negocio que no serían fácilmente evidentes con un enfoque tradicional de análisis de datos. O pueden ser capaces de identificar las tendencias probables en el desempeño. Incluso pueden ser capaces de evaluar más a fondo las hipótesis clave, incorporadas en una estrategia, lo que a su vez proporciona una mayor comprensión de las decisiones sobre estrategias alternativas, objetivos de negocio y establecimiento de objetivos de desempeño. Tener más información pertinente para la toma de decisiones también reduce la dependencia de la experiencia individual y los juicios de valor en la toma de esas decisiones.

Ejemplo 10.1: Utilización de información no estructurada en la toma de decisiones

Una cadena de consumo utiliza la inteligencia artificial para obtener mejor información sobre cómo mejorar la experiencia del cliente. De esta manera, la dirección es capaz de recabar análisis sobre los consumidores a través de las redes sociales, tales como el comportamiento de compra, incluidos patrones históricos y preferencias. Los análisis obtenidos pueden utilizarse para reducir el riesgo de exceso o falta de inventario, ya que proporcionan a la dirección una mejor visión de los niveles de inventario correctos. Esta mejora en la gestión de inventario reduce los costes operativos y de recursos y mejora la experiencia del cliente.

Ejemplo 10.2: Definición de las necesidades de información

La estrategia de una compañía farmacéutica es ampliar su participación en el mercado desarrollando un nuevo medicamento dirigido a una población específica. Para recibir la aprobación de su nuevo producto, la organización debe proporcionar a los reguladores información que cumpla con requisitos específicos de cumplimiento, tales como las conclusiones sobre la seguridad del medicamento. Estas conclusiones se basan en diversos datos como la demografía de la población examinada, el número de efectos secundarios, la duración de los estudios y el tipo de aplicación. Los datos se capturan a partir de los comentarios recibidos internamente por el paciente y a través de conversaciones de seguimiento en redes sociales.

28 Para más información sobre la calidad de la información, véase el Principio 13 de *Control Interno—Marco Integrado*.

29 La inteligencia artificial puede definirse como la teoría y el desarrollo de sistemas informáticos que realizan tareas que normalmente requieren inteligencia humana, como el reconocimiento del habla, la toma de decisiones, la percepción visual y otros factores.

Fuentes de datos

Los datos que se transforman en información se convierten en conocimiento (por ejemplo, el análisis de los comentarios publicados en redes sociales identifica los riesgos potenciales para la marca de la entidad). Por lo tanto, los requisitos de datos deben basarse en requisitos de información. El Ejemplo 10.2 ilustra cómo una empresa determina que necesita datos para proporcionar información de cumplimiento a un grupo de interés externo.

Los datos pueden recogerse a partir de diversas fuentes y en diversas formas. La Figura 10.1 muestra ejemplos de datos estructurados y no estructurados.

Figura 10.1: Fuentes de datos internos

Fuentes	Ejemplos de datos	Estructurados	No estructurado
Reuniones del consejo y de la dirección	Actas de la reunión y notas sobre transacciones potenciales		✓
Encuesta de satisfacción del cliente	Opiniones de clientes prioritarios sobre las interacciones con los empleados	✓	✓
Actividades de <i>due diligence</i>	Aumentos y disminuciones de personal debido a acuerdos de reestructuración	✓	
Correo electrónico	Información relativa a la toma de decisiones y desempeño de la entidad		✓
Informes y estudios geopolíticos elaborados por el gobierno	Cambios demográficos en los mercados emergentes	✓	
Informes de fabricantes	Intereses emergentes en productos enviados de fabricantes competidores		✓
Informes de <i>marketing</i> sobre servicios de seguimiento <i>web</i>	Número de visitas al sitio web, duración por página, y conversiones a compras de clientes	✓	
Metadatos	Detalles sobre contenidos de archivos de vídeo, incluidos detalles técnicos y descripciones de texto de escenas	✓	✓
Índices públicos	Datos de índice de escasez de agua para fabricantes de bebidas o explotaciones agrícolas que consideren nuevas ubicaciones	✓	
Redes sociales y <i>blogs</i>	Recuentos de comentarios negativos y positivos sobre un nuevo producto de la compañía	✓	✓

Categorización de la información sobre riesgos

Las organizaciones pueden clasificar la información que capturan utilizando categorías de riesgo comunes³⁰. Estas categorías pueden organizarse por áreas funcionales, como auditoría interna, gestión de la información o gestión del riesgo operacional. También pueden basarse en el tamaño, escala y complejidad de la entidad.

El uso de un conjunto común de categorías ayuda a las organizaciones a agregar la información sobre riesgos para determinar si existe algún impacto potencial resultante de las concentraciones de riesgo en la entidad. Esta estructura de categorías también les ayuda a evaluar los riesgos que podrían afectar a la estrategia y los objetivos de negocio. También sirve de base para elaborar respuestas al riesgo empresarial e informes coherentes.

30 Algunas organizaciones se refieren a estas categorías comunes de riesgo como "taxonomía del riesgo".

Gestión de datos

Los datos deben ser bien gestionados para proporcionar la información adecuada que apoye decisiones conscientes del riesgo. Esto requiere capturar y preservar la calidad de los datos, al tiempo que permite que diferentes tecnologías puedan intercambiarlos y utilizarlos. La gestión eficaz de los datos considera tres elementos clave: el gobierno del dato e información, los procesos y controles, y la arquitectura.

- *El gobierno de datos e información* ayuda a proporcionar datos estandarizados y de alta calidad a los usuarios finales de manera oportuna, verificable y segura. También ayuda a estandarizar la arquitectura de datos, autorizar normas, asignar responsabilidades y mantener la calidad. Asimismo, define funciones y responsabilidades claras para los responsables de los datos y de la información sobre riesgos.
- *Los procesos y controles* ayudan a una entidad a reforzar la fiabilidad de los datos y permiten realizar las correcciones necesarias. Por ejemplo, las organizaciones pueden tener un proceso para identificar instancias y patrones de datos tanto de baja como de alta calidad, y si esos datos son relevantes para cumplir con los requisitos. O bien pueden permitir identificar la coherencia, redundancia, disponibilidad y precisión de los datos. Pero la gestión de los datos va más allá de utilizar procesos y controles para garantizar su calidad. También implica, en primer lugar, evitar que se produzcan problemas de calidad.
- *La arquitectura de gestión de datos* hace referencia al diseño fundamental de la tecnología. Está compuesto por modelos, políticas, reglas o normas que dictan qué datos se recopilan y cómo se almacenan, organizan, integran y utilizan en los sistemas y en la organización. Las organizaciones implantan normas y proporcionan reglas para estructurar la información de manera que los datos puedan ser leídos, ordenados, indexados, recuperados y compartidos de manera fiable con las partes interesadas internas y externas, protegiendo en última instancia su valor a largo plazo.

Uso de la tecnología para tratar la información

La tecnología se asocia a menudo con los sistemas de información. Sin embargo, la tecnología a menudo implica algo más que el procesamiento y la presentación de informes de datos; también puede ayudar a la organización a desarrollar actividades. La robótica utilizada en la fabricación, los electrodomésticos inteligentes que gestionan el uso de energía en edificios residenciales y comerciales, y la tecnología wearable son ejemplos de cómo la tecnología puede ayudar a una organización a gestionar riesgos específicos. El Ejemplo 10.3 ilustra cómo la tecnología está ayudando a gestionar el riesgo y a captar información que ayude en la toma de decisiones.

Sin embargo, la tecnología también puede introducir nuevos riesgos a una entidad, lo cual puede ser crítico para materializar la estrategia y objetivos de negocio. La decisión sobre qué tecnología implantar depende de muchos factores, incluidos objetivos de la organización, necesidades del mercado, requisitos competitivos, y los costes y beneficios asociados. Una organización utiliza estos factores para sopesar los beneficios de obtener y gestionar información contra los costes de selección o desarrollo de las tecnologías de apoyo.

Ejemplo 10.3: Sistemas de información

Una organización sanitaria trata de encontrar maneras de reducir el número de casos de personas mayores que no se toman los medicamentos recetados. La omisión de las dosis prescritas puede reducir los beneficios de los medicamentos y aumentar los riesgos para la salud del paciente. Como respuesta, la organización ha distribuido tecnología adaptable a los pacientes que identifica aquellos casos en los que se les olvida una dosis y supervisa la salud general de cada paciente. Esta información es comunicada al proveedor sanitario correspondiente.

Cambios de necesidades

La dirección aprovecha y diseña su tecnología para cumplir una amplia gama de requerimientos, incluidos aquellos debidos a cambios internos y externos. De la misma manera que las entidades responden a los cambios en el contexto empresarial en el que operan y adaptan su estrategia y objetivos de negocio, también deben revisar sus tecnologías. Por ejemplo, las cambiantes expectativas de los clientes pueden requerir que las organizaciones cambien su tecnología para poder obtener información más oportuna y una revisión más activa de los comentarios en las redes sociales.



Principio 19: Comunica información sobre riesgos

La organización utiliza canales de comunicación como soporte a la gestión del riesgo empresarial.

Comunicación con las partes interesadas

Existen varios canales a disposición de la organización para comunicar datos e información sobre riesgos a partes interesadas internas y externas. Estos canales permiten a las organizaciones proporcionar información relevante para su uso en la toma de decisiones.

A nivel interno, la dirección comunica claramente la estrategia y los objetivos de negocio de la entidad por toda la organización para que todos los empleados, a todos los niveles, entiendan sus funciones específicas. En particular, los canales de comunicación permiten a la dirección transmitir:

- La importancia, relevancia y valor de la gestión del riesgo empresarial.
- Las características, conductas deseadas y valores clave que definen la cultura de la entidad.
- La estrategia y objetivos de negocio de la entidad.
- El apetito al riesgo y la tolerancia.
- Las principales expectativas de la dirección y del personal en relación con el riesgo empresarial y la gestión del desempeño.
- Las expectativas de la organización sobre cualquier asunto importante relacionado con la gestión del riesgo empresarial, incluidos los casos de debilidad, pérdida o incumplimiento.

La dirección también comunica información sobre la estrategia y los objetivos de negocio de la entidad a accionistas y otras partes externas. La gestión del riesgo empresarial es un asunto clave en estas comunicaciones, de modo que las partes interesadas externas no sólo entienden el desempeño en relación con la estrategia, sino también las acciones adoptadas conscientemente para lograrla. La comunicación externa puede incluir la celebración de reuniones trimestrales con analistas para analizar el desempeño.

Una entidad con canales de comunicación abiertos puede ser receptora de información de las partes interesadas externas. Por ejemplo, los clientes y proveedores pueden aportar información sobre el diseño o la calidad de los productos o servicios, lo que permite a la organización abordar las cambiantes exigencias o preferencias de los clientes. O bien, las consultas de grupos preocupados por el medioambiente sobre enfoques de sostenibilidad podrían proporcionar a una organización un análisis de valor de los principales enfoques o identificar riesgos potenciales para su reputación.

Esta información puede llegar a través de comunicaciones por correo electrónico, foros públicos, blogs, líneas directas u otros canales.

Comunicación con el consejo

La comunicación eficaz entre el consejo de administración y la dirección es crítica para que las organizaciones puedan lograr la estrategia y los objetivos de negocio y aprovechar las oportunidades dentro del entorno empresarial. La comunicación sobre el riesgo comienza por definir claramente las responsabilidades en materia de riesgos: quién debe saber qué y cuándo debe actuar. Las organizaciones deberían examinar su estructura de gobierno para velar por que las responsabilidades se asignen y definan claramente en el consejo de administración y la dirección, y que la estructura favorezca el diálogo sobre el riesgo deseado. La responsabilidad del consejo es supervisar y velar por que se adopten las medidas apropiadas para que la dirección pueda identificar, evaluar, priorizar y dar respuesta al riesgo (ver Ejemplo 10.4).

Para comunicarse eficazmente, el consejo de administración y la dirección deben tener un entendimiento compartido del riesgo y su relación con la estrategia y los objetivos de negocio. Además, los consejeros deben desarrollar una comprensión profunda del negocio, las palancas de valor, los costes principales y la estrategia y los riesgos asociados. Muchos miembros del consejo utilizan las visitas presenciales como canal de comunicación para interactuar con la dirección y el personal para entender las operaciones y la gestión.

El consejo de administración y la dirección analizan continuamente el apetito al riesgo. Como parte de su función de supervisión, el consejo de administración garantiza que las comunicaciones relativas al apetito al riesgo son permanecen abiertas. Puede hacerlo manteniendo reuniones formales trimestrales del consejo, y convocando juntas extraordinarias para abordar cuestiones específicas, como el terrorismo cibernético, la sucesión del director general o la realización de fusiones. El consejo y la dirección pueden usar el apetito al riesgo como piedra angular, lo cual les permitirá identificar los riesgos que estén asociados o no a la estrategia, realizar un seguimiento del perfil de riesgo de la entidad, y supervisar la eficacia de los programas de gestión del riesgo empresarial. Dado el fuerte vínculo con la estrategia, el apetito al riesgo debería revisarse a medida que evolucionen la estrategia y los objetivos de negocio.

La dirección proporciona cualquier información que ayude al consejo a cumplir sus responsabilidades de supervisión con respecto al riesgo. No hay un único método correcto para comunicarse con el consejo, pero a continuación se muestran algunos enfoques comunes comúnmente utilizados:

- Abordar los riesgos según la estrategia y los objetivos de negocio establecidos por la entidad.
- Capturar y alinear la información a un nivel que sea coherente con las responsabilidades de supervisión del riesgo por parte de los consejeros y con los requisitos de información que determine el consejo.
- Garantizar que los informes presenten el perfil de riesgo de la entidad alineado con su declaración de apetito de riesgo, y vincular la información de riesgo reportada con las políticas de exposición y tolerancia al riesgo.
- Capturar casos en los que los niveles de desempeño actuales se aproximen a la tolerancia aceptable en la variación del desempeño y los planes establecidos para gestionar el propio desempeño.
- Proporcionar una perspectiva longitudinal de las exposiciones al riesgo que incluya datos históricos, explicaciones de tendencias e información prospectiva en relación con las posiciones actuales.
- Actualizar con una frecuencia coherente y alineada con el ritmo de evolución del riesgo y la gravedad del mismo.
- Utilizar plantillas estandarizadas para facilitar una presentación y estructura coherente de la información sobre riesgos a lo largo del tiempo.

La dirección no debe subestimar la importancia de una comunicación abierta y de calidad con el consejo de administración. Debe existir un diálogo dinámico y constructivo sobre los riesgos entre la dirección y el consejo de administración, incluida la voluntad de cuestionar cualquier hipótesis relativa a la estrategia y los objetivos de negocio. Los consejos de administración pueden fomentar

Ejemplo 10.4: Comunicación con el Consejo

Una empresa que aspira a mejorar la comunicación del riesgo optó por revisar su estructura de gobierno aumentando la relevancia del puesto de director de riesgos para garantizar que el riesgo se integre en todos los debates de la estrategia empresarial. Los temas de riesgos son analizados ahora por el pleno del consejo de administración. La empresa identificó que, ahora que el riesgo ya no recae en una comisión del consejo, sino que se incorpora a las responsabilidades de gestión del riesgo empresarial del equipo de dirección, se ha mejorado la integración de los análisis sobre riesgos y la estrategia, así como la claridad sobre el riesgo.

un entorno en el que la dirección se sienta cómoda para presentar información sobre riesgos al consejo, incluso si aún no tienen una respuesta definida, planificada o establecida para ese riesgo. La dirección puede sentirse incómoda al analizar riesgos emergentes con el consejo en un momento en que la gravedad de estos riesgos aún no esté clara. Al estar abierto a conversaciones en las que aún no se haya llegado a una resolución definitiva, el consejo de administración puede alentar a la dirección a entablar un diálogo más oportuno e incisivo, en lugar de esperar a que estos riesgos evolucionen dentro de la entidad.

Métodos de comunicación

Para que la información se reciba tal como está previsto, debe comunicarse claramente. Para asegurarse de que los métodos de comunicación funcionan, las organizaciones deben evaluarlos periódicamente. Esto se puede hacer a través de los procesos existentes, estableciendo las expectativas de la gestión del riesgo empresarial en los objetivos de desempeño de los empleados y las evaluaciones periódicas posteriores del desempeño.

Los métodos de comunicación varían ampliamente, desde la celebración de reuniones cara a cara, la publicación de mensajes en la intranet de la entidad o el anuncio de un nuevo producto en una convención del sector, hasta la difusión de información a los accionistas a nivel mundial a través de redes sociales y comunicaciones.

Los métodos de comunicación pueden adoptar la forma de:

- *Mensajes electrónicos* (por ejemplo, correos electrónicos, redes sociales, mensajes de texto y mensajería instantánea).
- *Materiales externos/de terceros* (por ejemplo, revistas sectoriales, comerciales y profesionales, informes de medios de comunicación, sitios web de empresas homólogas, índices internos y externos clave).
- *Comunicaciones informales/verbales* (por ejemplo, reuniones individuales y grupales).
- *Eventos públicos* (por ejemplo, exposiciones itinerantes, reuniones en ayuntamientos, conferencias sobre aspectos técnicos y sectoriales).
- *Formación y seminarios* (por ejemplo, formación en directo u online, difusión por Internet y otras formas de vídeo y talleres).
- *Documentos internos escritos* (por ejemplo, documentos informativos, cuadros de mando, evaluaciones del desempeño, presentaciones, cuestionarios y encuestas, políticas y procedimientos, preguntas frecuentes).

Además de la lista anterior, se necesitan líneas de comunicación independientes y separadas cuando los canales normales no funcionan o son insuficientes para comunicar asuntos que requieran mayor atención. Muchas organizaciones proporcionan un medio para comunicarse anónimamente con el consejo de administración o con un delegado del consejo –como un canal de denuncias de irregularidades. Muchas organizaciones también establecen protocolos y políticas de denuncia para facilitar la comunicación cuando se produzcan excepciones en las normas de conducta o comportamientos inapropiados.



Principio 20: Informa sobre el riesgo, la cultura y el desempeño

La organización informa sobre el riesgo, la cultura y el desempeño a múltiples niveles a través de toda la entidad.

Identificación de usuarios de la información y sus funciones

La elaboración y presentación de información ayuda al personal de todos los niveles a comprender la relación entre riesgo, cultura y desempeño y a mejorar la toma de decisiones de cara al establecimiento de la estrategia y los objetivos de negocio, el gobierno y las operaciones diarias. Los requisitos de reporte de información dependen de las necesidades de los usuarios. Entre los usuarios de los informes se pueden incluir:

- La dirección y el consejo de administración con responsabilidad sobre el gobierno y la supervisión de la entidad.
- Los responsables de riesgos encargados de la gestión eficaz de los riesgos identificados.
- Los proveedores de aseguramiento que buscan información sobre el desempeño de la entidad y la eficacia de las respuestas a los riesgos.
- Las partes interesadas externas (reguladores, agencias de calificación, grupos de interés y otros).
- Otras terceras partes que requieran informes de riesgos para poder cumplir con sus funciones y responsabilidades.

También es importante comprender las estructuras operativas y de gobierno de los respectivos usuarios de la información. Cada usuario requerirá diferentes niveles de detalle sobre la información de riesgos y el desempeño para cumplir sus responsabilidades en la entidad. La presentación y reporte de la información también debe dejar clara la interrelación entre los usuarios y el efecto relacionado en toda la entidad.

La información sobre riesgos presentada en los diferentes niveles de la organización se traslada por toda la entidad y fluye hacia arriba para lograr un mayor nivel de información. Por ejemplo, los informes presentados al consejo de administración respaldan las decisiones sobre el apetito al riesgo y la estrategia de la empresa. Los informes presentados a la alta dirección ofrecen un nivel más detallado y facilitan las decisiones de cara al establecimiento de la estrategia y la elaboración de la presupuestación, así como las decisiones adoptadas a nivel de división y/o función. El siguiente nivel de reporte es aún más detallado y facilita a los jefes de división y de funciones la planificación, la presupuestación y la ejecución de las operaciones de día a día. Este nivel de información debe alinearse con los informes de la alta dirección y del consejo de administración. En los niveles más altos, los informes sobre el riesgo consideran una visión de cartera.

Los informes sobre riesgos podrán ser elaborados por cualquier equipo dentro de la estructura operativa. Los equipos prepararán sus informes divulgando información de acuerdo con sus responsabilidades de gestión de riesgos. Por ejemplo, los equipos pueden preparar información sobre riesgos como parte de las presentaciones de planificación financiera y presupuestación para favorecer sus solicitudes de recursos adicionales a fin de mantener o evitar que el perfil de riesgo se deteriore.



Atributos de los informes

Los informes combinan información cuantitativa y cualitativa sobre el riesgo, y la presentación puede variar desde tipologías bastante simples hasta más complejas, dependiendo del tamaño, tipo y complejidad de la entidad. La información reportada sobre riesgos facilita a la dirección la toma de decisiones, aunque la dirección debe seguir adoptando su juicio profesional de cara a la consecución de la estrategia y los objetivos de negocio y dentro del entorno del negocio.

La información histórica puede aportar información útil y significativa para los informes, pero el énfasis en la información con vistas al futuro es más beneficiosa. Conocer los procesos integrales necesarios para cumplir la misión y visión de una entidad, así como el entorno empresarial en el que opera, puede ayudar a la dirección a conectar la información histórica con informaciones sobre posibles alertas tempranas (visión de futuro). Los análisis de alertas tempranas sobre tendencias clave, riesgos emergentes y cambios en el desempeño pueden requerir información tanto interna como externa.

Tipos de informes

La presentación de informes e información sobre riesgos puede incluir algunos de los elementos siguientes, o incluso todos ellos:

- *La visión del riesgo a nivel de cartera* presenta la gravedad de los riesgos a nivel de entidad que pueden afectar a la consecución de la estrategia y los objetivos de negocio. La presentación de información sobre la visión a nivel de cartera resalta los mayores riesgos para la entidad, las interdependencias entre los riesgos específicos y las oportunidades. La visión del riesgo a nivel de cartera se encuentra normalmente en los informes a la dirección y al consejo de administración.
- *La visión del perfil de riesgo* resulta similar a la visión de cartera, describe la gravedad de los riesgos, pero se centra en los diferentes niveles dentro de la entidad. Por ejemplo, el perfil de riesgo de una división o unidad operativa puede figurar en los informes de riesgos dirigidos a la dirección o a dichas áreas de la entidad.
- *El análisis de las causas raíz* facilita a los usuarios comprender las hipótesis y los cambios que sustentan la visión de cartera y de perfil de riesgo.
- *El análisis de sensibilidad* mide la sensibilidad ante los cambios en las hipótesis clave implícitas en la estrategia y el efecto potencial en la estrategia y los objetivos de negocio.
- *El análisis de los riesgos nuevos, emergentes y cambiantes* proporciona una visión prospectiva para anticipar los cambios en el inventario de riesgos, los efectos sobre las necesidades y asignación de recursos, y el desempeño previsto de la entidad.
- *Los principales indicadores y medidas de desempeño* marcan la tolerancia al riesgo de la entidad y el riesgo potencial para una estrategia u objetivo de negocio.
- *Los análisis de tendencias* muestran los movimientos y cambios en la visión del riesgo a nivel de cartera, el perfil de riesgo y el desempeño de la entidad.
- *La declaración de incidentes, brechas y pérdidas* proporciona información sobre la eficacia de las respuestas al riesgo.
- *El seguimiento de los planes e iniciativas de gestión del riesgo empresarial* proporciona un resumen del plan e iniciativas para establecer o mantener las técnicas de gestión del riesgo empresarial. La inversión en recursos y la urgencia con que se lleven a cabo las iniciativas también pueden reflejar el compromiso de los responsables de la organización con respecto a la gestión del riesgo empresarial y la cultura a la hora de responder a los riesgos.

Los informes de riesgos se complementan con comentarios y análisis por parte de especialistas en la materia. Por ejemplo, los expertos en cumplimiento, legal y tecnología a menudo aportan comentarios y análisis sobre la gravedad del riesgo, la eficacia de las respuestas al riesgo, las palancas de cambios que muestran los análisis de tendencias, y los desarrollos y oportunidades sectoriales que la entidad puede tener.

Informar sobre riesgos al consejo

A nivel de consejo de administración, es probable que exista un intercambio formal de informes y también un intercambio informal de información. Por ejemplo, el consejo puede mantener reuniones informales sobre la posibilidad de implantar una estrategia y las implicaciones de adoptar estrategias alternativas considerando el perfil de riesgo y otros análisis para la reflexión. La emisión formal de informes desempeña un papel más integral cuando el consejo ejerce otras responsabilidades, entre las cuales se incluye considerar los riesgos para la consecución y ejecución de la estrategia, revisar el apetito al riesgo, o supervisar las técnicas de gestión del riesgo empresarial implantadas por la dirección.

Existen varias maneras en que la dirección puede informar al consejo, pero es fundamental que el enfoque utilizado en la presentación de informes sea la trazabilidad entre la estrategia, los objetivos de negocio, el riesgo y el desempeño. Informar al consejo constituye el nivel más alto de reporte e incluirá la visión a nivel de cartera. La presentación de informes al consejo debe fomentar el análisis del desempeño de la entidad de cara a cumplir con la estrategia y los objetivos de negocio, así como el impacto del riesgo potencial para cumplir dichos objetivos.

Informar sobre la cultura

La cultura de una entidad se basa en el comportamiento y las actitudes, y su medición es a menudo una tarea muy compleja. El reporte sobre la cultura puede plasmarse en:

- Análisis de tendencias culturales.
- Análisis comparativo con otras entidades o normas.
- Esquemas de compensación y su influencia potencial en la toma de decisiones.
- Análisis de las lecciones aprendidas.
- Revisiones de tendencias de comportamiento.
- Encuestas de actitudes tomadas con respecto al riesgo y concienciación sobre los riesgos.

Indicadores clave

Los indicadores clave se utilizan para predecir la ocurrencia de un riesgo. Generalmente son de carácter cuantitativo, pero también pueden ser cualitativos. Los indicadores clave se comunican a los niveles de la entidad que están en mejor posición para gestionar el riesgo emergente cuando sea necesario. Deberían comunicarse junto con los indicadores clave del desempeño (KPIs) para demostrar la interrelación entre el riesgo y el desempeño. Los indicadores clave facilitan un enfoque proactivo de la gestión del desempeño (véase el Ejemplo 10.5).

Los indicadores y los indicadores clave del desempeño pueden reflejarse en una sola medida. Por ejemplo, en una empresa manufacturera, los volúmenes de producción y los umbrales que los rodean se pueden analizar desde la óptica del riesgo. Unos volúmenes de producción que superen los objetivos pueden considerarse como riesgos potenciales de calidad, mientras que unos volúmenes de producción por debajo del objetivo pueden sugerir riesgos potenciales de retrasos en las entregas, escasez de mano de obra o tiempo de inactividad de los equipos.

Ejemplo 10.5: Uso de los principales indicadores

Una agencia pública quiere retener en su plantilla a sus profesionales más competentes. El objetivo de negocio que persigue la retención de los empleados más competentes tiene como objetivo mantener unas tasas de rotación inferiores al 5% anual. Unos de los principales indicadores sería el porcentaje de los empleados con derecho a jubilarse en un plazo de cinco años. Cualquier resultado superior al 5% indicaría que el riesgo con respecto a este objetivo se estaría posiblemente manifestando. Un indicador clave del desempeño sería la tasa de rotación real. Los indicadores clave del desempeño se basan en el desempeño histórico, y aunque la comprensión de los resultados históricos puede fijar una serie de líneas de referencia, la tendencia al alza de esta tasa no necesariamente debería denotar una manifestación del riesgo.

Los indicadores clave se comunican junto con las correspondientes metas y desviaciones aceptables. Saber dónde se encuentra una entidad con respecto al entorno cultural, ya sea con aversión al riesgo o agresividad con respecto al riesgo, ayudará a determinar los indicadores clave y los indicadores clave del desempeño de los cuales se hará un seguimiento, así como la desviación aceptable de los mismos.

Frecuencia y calidad del informe

La dirección trabaja en estrecha colaboración con aquellos que utilizarán los informes para identificar qué información se requiere, con qué frecuencia se necesita y cuáles son sus preferencias en cuanto al formato de presentación de la información. La dirección es responsable de implantar los controles apropiados para que los informes sean precisos, claros y completos.

La frecuencia de los informes debe ser proporcional a la gravedad y prioridad del riesgo. Estos reportes deben permitir a la dirección determinar el tipo y el nivel del riesgo asumido por la organización, su pertinencia continuada y la idoneidad de las respuestas al riesgo existentes. Por ejemplo, los cambios en las cotizaciones bursátiles, o los precios de la competencia en el sector hotelero o aéreo, pueden comunicarse diariamente, de acuerdo con los cambios potenciales en el riesgo. En cambio, la presentación de informes sobre riesgos derivados del progreso de una organización con respecto a proyectos e iniciativas estratégicas a largo plazo podrá ser mensual o trimestral.

Glosario de Términos Principales

- **Contexto empresarial:** Las tendencias, eventos, relaciones y otros factores que pueden influir, aclarar o cambiar la estrategia actual y futura de la entidad y los objetivos de negocio.
- **Objetivos de negocio:** Las medidas que la organización toma para alcanzar su estrategia.
- **Valores clave:** Las creencias e ideales de la entidad sobre lo que es bueno o malo, aceptable o inaceptable, que influyen en el comportamiento de la organización.
- **Cultura:** Las actitudes, comportamientos y entendimiento del riesgo, tanto positivos como negativos, que influyen en las decisiones de la dirección y los empleados y reflejan la misión, visión y valores clave de la organización.
- **Datos:** Información concreta sobre hechos, elementos, etc. que pueden ser recopilados a nivel colectivo para ser analizados, utilizados o referenciados.
- **Gestión del Riesgo Empresarial:** La cultura, capacidades y técnicas, integradas con el establecimiento de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo en la creación, preservación y consecución del valor.
- **Entidad:** Cualquier forma de organización con ánimo de lucro, sin ánimo de lucro, u organismo gubernamental. Una entidad puede cotizar en bolsa, ser de propiedad privada, ser propiedad de una estructura cooperativa, o tener cualquier otra estructura legal.
- **Entorno externo:** Cualquier elemento ajeno a la entidad que influya en la capacidad para lograr la estrategia y los objetivos de negocio.
- **Partes interesadas externas:** Cualquier parte que no esté directamente involucrada en las operaciones de la entidad pero que esté afectada por ella, que influya directamente en el entorno empresarial de la entidad o que influya en la reputación, marca y confianza de la entidad.
- **Evento:** Acto o conjunto de actos que se materializan.
- **Marco de trabajo:** Los cinco componentes son (1) Gobierno y Cultura; (2) Estrategia y Establecimiento de Objetivos; (3) Estrategia y Desempeño de Objetivos; (4) Revisión y Monitorización; e (5) Información, Comunicación y Reporte.
- **Impacto:** El resultado o efecto de un riesgo. Puede haber una serie de posibles impactos asociados a un riesgo. El impacto de un riesgo puede ser positivo o negativo en relación con la estrategia u objetivos de negocio de la entidad.
- **Información:** Datos procesados, organizados y estructurados relativos a un hecho o circunstancia en particular.
- **Control interno:** Un proceso llevado a cabo por el consejo de administración, la dirección y el resto de los empleados de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos relativos a las operaciones, a la información y al cumplimiento (para más información, véase *Control Interno - Marco Integrado*).
- **Entorno interno:** Cualquier elemento de dentro de la entidad que influya en la capacidad para lograr la estrategia y los objetivos de negocio.
- **Partes interesadas internas:** Los profesionales que trabajan dentro de la entidad, como los empleados, la dirección y el consejo de administración.
- **Probabilidad:** La posibilidad de que se produzca un evento determinado.
- **Misión:** El propósito principal de la entidad, que establece lo que quiere lograr y su razón de ser.
- **Estructura operativa:** La forma en que la entidad organiza y lleva a cabo sus operaciones diarias.

- **Oportunidad:** Una acción o potencial acción que cree o altere metas o enfoques para crear, preservar y materializar valor.
- **Organización:** Término utilizado para describir colectivamente el consejo de administración, la dirección y el personal de una entidad.
- **Sostenibilidad organizacional:** La capacidad de una entidad para soportar el impacto de eventos a gran escala.
- **Gestión del desempeño:** La medición de esfuerzos para lograr o superar la estrategia y los objetivos de negocio.
- **Visión a nivel de cartera:** Una visión compuesta del riesgo al que se enfrenta la entidad, que posiciona a la dirección y al consejo de administración para que consideren el tipo, la gravedad y la interdependencia de los riesgos y cómo pueden afectar al desempeño de la entidad en relación con la estrategia y los objetivos de negocio.
- **Técnicas:** Los métodos y enfoques aplicados dentro de una entidad en relación con la gestión del riesgo.
- **Expectativa razonable:** El nivel de riesgo resultante de lograr la estrategia y los objetivos de negocio que es apropiado para una entidad, reconociendo que no se puede predecir el riesgo con precisión.
- **Riesgo:** La posibilidad de que ocurran eventos y afecten a la consecución de la estrategia y los objetivos de negocio. NOTA: “Riesgos” (plural) se refiere a uno o más eventos potenciales que pueden afectar a la consecución de los objetivos. “Riesgo” (singular) se refiere a todos los eventos potenciales (en términos colectivos) que pueden afectar a la consecución de los objetivos.
- **Apetito al riesgo:** Los tipos y el nivel de riesgo, en un sentido amplio, que una organización está dispuesta a aceptar en la búsqueda de valor.
- **Capacidad de riesgo:** Es el nivel máximo de riesgo que una entidad es capaz de absorber para lograr la estrategia y los objetivos de negocio.
- **Inventario de riesgos:** Todos los riesgos identificados que puedan afectar a una entidad.
- **Perfil de riesgo:** Una visión compuesta del riesgo asumido a un nivel particular de la entidad, o aspecto del negocio que se posiciona a la dirección de cara a considerar los tipos, la gravedad y las interdependencias de riesgos, y cómo éstos pueden afectar al desempeño en relación con la estrategia y los objetivos del negocio.
- **Gravedad:** Medida que valora consideraciones tales como la probabilidad y el impacto generado por determinados eventos o el tiempo que se tarda en recuperarse de ellos.
- **Partes interesadas:** Partes que tienen un interés genuino o adquirido en la entidad.
- **Estrategia:** El plan de la organización para lograr su misión y visión y aplicar sus valores clave.
- **Tolerancia:** Los límites de la desviación aceptable en el desempeño en relación con el logro de los objetivos de negocio.
- **Incertidumbre:** El estado de no saber si los eventos potenciales pueden manifestarse o cómo pueden hacerlo.
- **Visión:** Aspiraciones de la entidad de cara a su estado en el futuro o lo que la organización pretende lograr con el paso del tiempo.

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

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.

