Universidad de Valladolid

La gestión del riesgo empresarial: marco teórico, desafíos contemporáneos y enfoque estratégico

Pablo Olivas Del Saz

MÁSTER EN DIRECCIÓN DE PROYECTOS
Departamento De Organización De Empresas Y C.I.M.
Universidad De Valladolid
España

INSISOC
SOCIAL SYSTEMS ENGINEERING CENTRE
2025

La gestión del riesgo empresarial: marco teórico, desafíos contemporáneos y enfoque estratégico

Pablo Olivas Del Saz

MÁSTER EN DIRECCIÓN DE PROYECTOS
Departamento De Organización De Empresas Y C.I.M.
Universidad De Valladolid

Valladolid, julio 2025

Tutor
Fernando Acebes Senovilla

AGRADECIMIENTOS

A mi madre y a mis hermanos.

RESUMEN

Este trabajo presenta un análisis teórico y estructurado sobre la gestión del riesgo en el ámbito empresarial. Parte de la definición y comprensión de la corporación como entidad jurídica y organizativa, para luego introducir el concepto de riesgo desde una doble perspectiva: como posibilidad de pérdida y como incertidumbre. Se desarrolla una tipología amplia que abarca riesgos operativos, financieros y de mercado, analizando su impacto potencial sobre la actividad y el valor de la empresa. A través del modelo de valoración por flujos de caja descontados, se examina cómo la gestión del riesgo puede influir tanto directa como indirectamente en la creación de valor. Posteriormente, se estudia el enfoque de gestión integral del riesgo, con especial énfasis en el marco COSO, detallando sus componentes, principios y proceso de implementación. El trabajo también aborda riesgos clave contemporáneos, como los relacionados con criterios de medioambiente, el fraude y la corrupción. Finalmente, se analizan los procesos de toma de decisiones bajo condiciones de riesgo e incertidumbre, incluyendo los aspectos psicológicos y estratégicos que influyen en la racionalidad de las decisiones empresariales. En conjunto, el documento proporciona una visión completa y actualizada del conocimiento teórico en torno al riesgo corporativo como elemento estratégico central.

Palabras clave

Gestión del riesgo; Incertidumbre; Empresa; ERM; COSO.

ABSTRACT

This paper presents a theoretical and structured analysis of risk management in the business environment. It begins by defining and understanding the corporation as a legal and organizational entity, before introducing the concept of risk from a dual perspective: as the possibility of loss and as uncertainty. A broad typology is developed, covering operational, financial, and market risks, analyzing their potential impact on business activity and firm value. Using the discounted cash flow valuation model, the study explores how risk management can influence value creation both directly and indirectly. The work then examines the enterprise risk management approach, with special emphasis on the COSO framework, detailing its components, principles, and implementation process. Key contemporary risks are also addressed, including those related to environmental criteria, fraud, and corruption. Finally, the paper analyzes decision-making processes under risk and uncertainty, considering the psychological and strategic aspects that influence rational corporate behavior. Overall, the document provides a comprehensive and up-to-date theoretical overview of corporate risk as a central strategic element.

Keywords

Risk management; Uncertainty, Enterprise; ERM; COSO.

INDICE

INDICE DE FIGURAS

INTRODUCCIÓN

En el actual entorno económico, caracterizado por su creciente complejidad, globalización e incertidumbre, la gestión del riesgo se ha convertido en un componente estratégico esencial para la sostenibilidad de las organizaciones. Desde la crisis financiera de 2008 hasta eventos más recientes como la pandemia de COVID-19 o los conflictos geopolíticos que afectan las cadenas de suministro globales, las empresas han tenido que enfrentar amenazas de naturaleza diversa, algunas de ellas sin precedentes en su impacto. Este contexto ha obligado a replantear los modelos tradicionales de gestión del riesgo, dando paso a enfoques más integrales y transversales que permiten anticipar, mitigar y gestionar riesgos de forma estructurada y alineada con la estrategia corporativa.

La literatura académica ha respondido a esta necesidad mediante el desarrollo de marcos teóricos que abordan el riesgo no solo desde una perspectiva financiera, sino también organizativa, operativa y ética. Entre ellos, el modelo COSO de *Enterprise Risk Management* (ERM) se ha consolidado como una referencia ampliamente aceptada tanto en el ámbito académico como profesional. Sin embargo, pese a los avances en la conceptualización y formalización de estos marcos, persisten importantes lagunas. Por un lado, la implementación real de estos sistemas en las organizaciones es desigual y, en muchos casos, limitada a un cumplimiento superficial. Por otro, el conocimiento general sobre el impacto real del riesgo en la generación de valor sigue siendo fragmentario, especialmente en lo relativo a sus efectos indirectos o psicológicos en la toma de decisiones empresariales.

Este trabajo pretende contribuir a cerrar parte de esa brecha, ofreciendo un recorrido teórico completo y actualizado sobre la gestión del riesgo empresarial. Comienza por definir el marco estructural en el que operan las corporaciones modernas, para luego analizar el concepto de riesgo desde una doble perspectiva: como posibilidad de pérdida y como incertidumbre. A partir de esta base, se construye una clasificación detallada de los tipos de riesgos a los que se enfrentan las empresas, examinando su impacto tanto desde una lógica de pérdidas tangibles como desde la óptica de la variabilidad y la volatilidad. El análisis se complementa con la introducción del modelo de flujos de caja descontados (DCF) como herramienta para comprender el papel del riesgo en la creación de valor.

Dentro de este enfoque, es importante delimitar el alcance del trabajo. No se pretende realizar una cobertura exhaustiva de todos los riesgos posibles, y algunos elementos relevantes pueden no estar incluidos en el análisis. Tampoco se abordan escenarios excepcionales cuya singularidad los hace poco representativos desde una óptica teórica general, como es el caso de la pandemia de 2020. El objetivo no es ofrecer soluciones completas ni un inventario cerrado de herramientas, sino presentar los marcos conceptuales más sólidos para comprender y estructurar la gestión del riesgo.

El cuerpo central del trabajo está dedicado a explorar el modelo COSO ERM, sus componentes clave y el proceso de implementación en las organizaciones. También se realiza una revisión específica de riesgos contemporáneos con creciente relevancia, como los relacionados con criterios ESG (ambientales, sociales y de gobernanza), el fraude corporativo o la corrupción. Finalmente, se aborda la dimensión conductual del riesgo, a través del estudio de los procesos de toma de decisiones bajo condiciones de incertidumbre, incluyendo los sesgos y limitaciones cognitivas que afectan a los ejecutivos y altos directivos.

En conjunto, el trabajo se sitúa en la intersección entre teoría, estrategia y cultura organizacional, con el objetivo de ofrecer un mapa conceptual sólido que permita comprender la gestión del riesgo como una disciplina integrada, estratégica y esencial para el éxito empresarial a largo plazo.

Objetivo del Proyecto

El presente trabajo tiene como finalidad realizar un recorrido estructurado por el conocimiento teórico más relevante en torno a la gestión del riesgo empresarial. A través de un enfoque analítico y descriptivo, se examinan los fundamentos conceptuales, los tipos de riesgo, su influencia en la creación de valor, así como los principales marcos de gestión integrados, entre ellos el modelo COSO. Además, se abordan riesgos contemporáneos de gran impacto y se analizan los enfoques actuales para la toma de decisiones en entornos inciertos. En este contexto, se plantean los siguientes objetivos que orientan y delimitan el alcance del análisis desarrollado a lo largo del documento.

- Comprender la naturaleza jurídica, organizacional y de gobernanza de las corporaciones para establecer el contexto en el que se gestiona el riesgo empresarial.
- Definir el concepto de riesgo en el entorno empresarial y clasificar sus distintas tipologías con sus componentes clave.
- Analizar cómo la gestión del riesgo influye directamente en la generación de valor de la empresa.
- Describir los marcos teóricos existentes para la gestión integral del riesgo (ERM), con especial atención al marco COSO, analizando sus componentes, principios y etapas de implementación en el contexto empresarial.
- Examinar los principales riesgos contemporáneos identificados en la literatura, con especial atención a los relacionados con criterios ESG, fraude y corrupción, y su impacto potencial en las organizaciones.
- Analizar los enfoques teóricos existentes sobre la toma de decisiones basada en el riesgo, incluyendo modelos psicológicos y estratégicos que explican cómo las empresas enfrentan la incertidumbre.

Alcance del Proyecto

Este trabajo se centra en la exposición y análisis del conocimiento teórico existente sobre la gestión del riesgo en el contexto empresarial. Su contenido abarca la definición y clasificación de los distintos tipos de riesgo, así como la comprensión de su impacto sobre el valor de las organizaciones y su capacidad para alcanzar sus objetivos estratégicos. Se revisan los principales marcos de gestión integral del riesgo, con especial atención al modelo COSO, ampliamente adoptados tanto en la literatura académica como en la práctica profesional. Asimismo, se examinan riesgos contemporáneos relevantes como los vinculados a criterios medioambientales, el fraude y la corrupción, que han adquirido una creciente importancia en la agenda empresarial actual. Además, se analiza el papel que desempeña el riesgo en los procesos de toma de decisiones estratégicas, considerando no solo aspectos cuantitativos sino también elementos conductuales y organizativos. El estudio se basa en fuentes reconocidas del ámbito académico y técnico, sin abordar la aplicación empírica de casos concretos ni el desarrollo de herramientas propias. Por tanto, su alcance es eminentemente teórico y tiene como objetivo principal proporcionar una visión clara, estructurada y actualizada del estado del conocimiento en esta materia.

Motivación del Proyecto

En un entorno empresarial caracterizado por una creciente complejidad, volatilidad y exposición a riesgos de diversa índole, la necesidad de comprender en profundidad los marcos teóricos que sustentan la gestión del riesgo se ha vuelto más relevante que nunca. Las organizaciones ya no pueden limitarse a abordar el riesgo de manera reactiva o fragmentada; se requiere una visión integral que permita anticipar amenazas, minimizar impactos y, en última instancia, contribuir a la sostenibilidad y el valor a largo plazo de la empresa. Este trabajo nace del interés por explorar cómo el riesgo ha evolucionado como concepto y como herramienta estratégica, así como por sistematizar el conocimiento existente sobre los modelos y enfoques que guían su tratamiento. Asimismo, responde

a la inquietud de analizar cómo la teoría ha intentado dar respuesta a los riesgos que afectan a las empresas, el impacto de factores diversos o las decisiones en condiciones de incertidumbre, cuestiones que hoy ocupan un lugar central en la agenda directiva de muchas organizaciones.

En este contexto, este TFM se encuadra dentro de una de las líneas de investigación de INSISOC, Grupo de Investigación Reconocido (GIR) de la Universidad de Valladolid. En concreto, dentro de la línea que tiene como objetivo la gestión del riesgo y la incertidumbre en los proyectos, cuyo objetivo es adaptar y diseñar estándares y metodologías de dirección de proyectos, así como analizar la complejidad que rodea la gestión del riesgo y, por ende, la propia dirección de proyectos. Esta investigación se alinea con trabajos previos realizados por Acebes, Curto, et al., (2024), Acebes, González-Varona, et al., (2024), Pajares, Acebes, et al., (2024) o Pajares, Acebes, et al., (2022), entre otros.

Estructura del Documento

El documento se estructura en seis capítulos alineados con los objetivos del trabajo.

- El primer capítulo introduce el concepto de la compañía y la define. Este tipo de organizaciones son conocidas superficialmente por el grueso de la población, gracias a su importancia en la sociedad actual, pero poseen una serie de particularidades cuya naturaleza no está tan entendida. Se describe un modelo genérico de estructura empresarial, y se desarrollan las obligaciones de la dirección y la junta directiva. Esto, permite construir un boceto de los riesgos que pueden afectar a la empresa y de las herramientas de priorización que pueden tener los ejecutivos ante dichos riesgos, que, en la mayoría de los casos, serán preservar o aumentar el valor de la compañía. Finalmente, se presenta un rol en la empresa recomendado para la gestión de riesgos.

- El segundo capítulo profundiza en la noción de riesgo. Una vez comprendida la estructura y naturaleza de la compañía, el siguiente paso lógico es definir con precisión qué se entiende por riesgo en este contexto. Se establece una definición clara y operativa del concepto, y se presenta una clasificación de los distintos tipos de riesgo a los que puede enfrentarse una empresa. A continuación, se analiza cómo cada uno de estos riesgos puede incidir en la actividad empresarial, ya sea afectando sus objetivos estratégicos, su operativa diaria o su sostenibilidad a largo plazo. Este capítulo sienta así las bases para entender la relevancia del riesgo como elemento central en la toma de decisiones corporativas.

- El tercer capítulo combina los temas de los dos anteriores en uno. Primero, se ha tratado la compañía y el objetivo principal de esta, que es generar valor. Segundo, se presentan los riesgos, y cómo estos pueden afectar negativamente a la empresa. En este capítulo, se describe usando un modelo matemático y ambas definiciones de riesgo cómo este último afecta negativamente al valor de la empresa y, por lo tanto, por qué es importante que se gestione a nivel ejecutivo de forma adecuada. Se desarrollarán los efectos directos e indirectos del riesgo, los costes adicionales que suponen su desestimación y las posibilidades de transferirlos a otras entidades aseguradoras.

- En el cuarto capítulo se propone una solución para la gestión del riesgo en la empresa. Esta es la más extendida en la literatura y sobre la que se han formado esquemas internacionales como el marco COSO, del que se hablará. En este punto, se indica cómo crear un sistema en la compañía que permita la gestión integral de los riesgos que la afectan, incluyendo un punto en el que se habla de cómo esto sirve para incrementar el valor.

- El quinto capítulo trata sobre riesgos clave actualmente en la gestión de la empresa. Se abordan las aristas sociales y medioambientales, de creciente importancia en la historia reciente, y las actividades delictivas producidas en el seno de la empresa como son el fraude y la corrupción.

Estos riesgos son importantes en todas las compañías, y todos tienen un reflejo en el valor de estas, sea desde un punto de vista reputacional, regulatorio, legal y de negocio.

- El sexto y último capítulo trata sobre la toma de decisiones en la empresa. Una vez que se entiende la importancia de gestionar los riesgos, se propone una solución para ello y se destacan riesgos clave, es importante tomar las decisiones correctas y tomarlas con la gestión del riesgo en mente. En este capítulo se desarrollan los patrones psicológicos existentes a la hora de decidir, incluyendo los sesgos. Además, se muestra un sistema de decisión que explica cómo se decide y se proponen soluciones para tomar las mejores decisiones en base a este sistema.

- El trabajo finaliza con las conclusiones de este. Esto constituye el final del texto y se recopilan las lecciones aprendidas durante los capítulos y su relación con los objetivos que motivaron el TFM en un primer momento.

Capítulo 1 La compañía

Previo a entrar en materia, propiamente dicha, conviene hacer una pequeña introducción sobre la compañía. En un trabajo en el que se busca hablar de riesgos empresariales, es relevante hablar, en primer lugar, de las corporaciones, ya que son las afectadas por dichos riesgos. En este capítulo se definirá lo que es la corporación y sus diferencias y similitudes con los individuos que la conforman, se hablará de estructuras típicas y de cómo se gestionan. Este punto es importante, puesto que ayudará más adelante a entender las condiciones en las que se gestionan los riesgos que tienen un impacto posible en la empresa.

1.1 Definiciones e implicaciones

Según Merna (2012), se ha realizado muy poca investigación sobre cómo se gestionan los riesgos a nivel corporativo, quién se encarga y las funciones generales del cuerpo corporativo en relación con la gestión de riesgos. Para poder empezar a hablar de riesgos, primero hay que entender lo que es la corporación, cómo funciona habitualmente y cómo se estructura, para así prever las amenazas y oportunidades que pueden afectarla.

En "*The Dictionary of Management*" (French y Saward, 1983) se define "corporación" como:

"Una asociación de personas que se contempla a nivel legal como una entidad separada que puede establecer relaciones legales (como poseer una propiedad, ser parte de un contrato o algún otro procedimiento legal) y que continúa existiendo hasta que su disolución de acuerdo con la ley".

"Una corporación es una sucesión de personas o cuerpo de personas autorizados por ley para actuar como una persona, teniendo derechos y responsabilidades distintas de las que poseen los individuos que conforman la corporación".

Las corporaciones son empresas que buscan beneficio, y poseen otros objetivos como el crecimiento, la eficiencia y maximizar las ganancias. Dentro de esos objetivos, y del grupo de personas que conforman la compañía, hay que realizar funciones de gestión. Se puede definir esta gestión corporativa como la gestión de las actividades llevadas a cabo por el cuerpo corporativo y aquellas organizaciones que forman parte de la corporación que utiliza las herramientas y técnicas para ayudar en el proceso de toma de decisiones (Merna, 2012).

La historia de la empresa es extensa, la organización de personas con un objetivo común es un fenómeno que se viene dando desde hace siglos, dándose incluso las asociaciones entre empresas independientes como fue la formación de los gremios en la baja edad media. Las corporaciones gremiales trabajaban en conjunto y regulaban el mercado, aunque no compartiesen beneficios. La relación de dichas empresas y el Estado era directa, de forma que los primeros dependían por completo del segundo. Cualquier grupo de personas que buscase actividad comercial debían tener el beneplácito de la Corona para llevar a cabo su función, o de la parte de la nobleza y clero designada en caso de menores empresas. Se puede extraer del tipo de relación presentada que la clase dominante de la sociedad de la época tenía capacidad total para hacer desaparecer las organizaciones cuando considerase, así como adjuntarle las responsabilidades que se considerasen oportunas, según el modelo de gobierno y ley que hubiese en cada momento y lugar (Ogilvie, 2014).

Hoy en día, la relación del Estado con las empresas ha evolucionado y según el trabajo de Monbiot (2000), empieza a producirse un desfase significativo entre los derechos que la empresa ha ido

adquiriendo y las responsabilidades que ha ido esquivando por no tratarse de un individuo. En su obra, "*Captive State: The Corporate Takeover of Britain*" del año 2000, analiza una serie de casos en los que las empresas consiguen no hacerse responsables de acciones y decisiones que se realizan a nivel corporativo. Entre los ejemplos que presenta, en 1999 el tribunal de apelación prohibió a 3000 sudafricanos denunciar a "*Cape plc*" por envenenamiento de amianto producido por su trabajo. Esto acusa que las corporaciones no solo parecen estar exentas de ciertas responsabilidades a nivel nacional, sino que la ley internacional protege de igual manera a las multinacionales. Por el contrario, las empresas pueden denunciar, recurrir a la policía si lo necesitasen o declarar un interdicto contra los trabajadores. Pueden usar la ley como si fuesen seres humanos, pero en aspectos clave no están afectadas por ella (Monbiot, 2000).

Los directores de compañías son responsables individualmente de mantener el precio de las acciones lo más alto posible. Si se percibe negligencia en estos deberes financieros se les puede procesar a nivel judicial e incluso, encarcelar. Si en cambio, se percibe negligencia a la hora de proteger a sus empleados, incluso si ello conllevase la pérdida de vidas, permanecerían inmunes a nivel judicial. A lo sumo, la compañía podría sufrir una multa de variable cuantía, a la que la dirección no tendría que afrontar con sus fondos. Debido a los avances en previsión de riesgos laborales (PRL) y a los requerimientos legales en ese ámbito, se intenta mantener el daño realizado a los trabajadores al mínimo. Sin embargo, los accidentes de trabajo mortales en 2023 fueron 619 (Figura 1.1). Un ejemplo reciente de fallecimiento en el trabajo fue el caso de los mineros de León (Fernández, 2025), en el que, tras la pérdida de 4 empleados, se obtuvo unas condolencias muy sentidas de los directores de la compañía para la que trabajaban. Este caso, aparte de por lo tremendamente trágico, generó un cierto revuelo nacional con mirada al cuerpo empresarial por lo similar que es la lista de dueños y directivos del Grupo Cerredo y Blue Solving, empresas supuestamente distintas que operaban en la mina y que, insatisfechas con su gestión, solicitan reabrir otra mina para obtener beneficios (J. I. Fernández, 2025). Lo que ocurre es que, a nivel judicial, la firma será inocente si la responsabilidad de la muerte o el accidente es compartida, y la Fiscalía habitualmente no tiene la capacidad de demostrar la responsabilidad individual de cada director. La mayor penalización esperada será el despido o descualificación para desempeñar funciones similares.

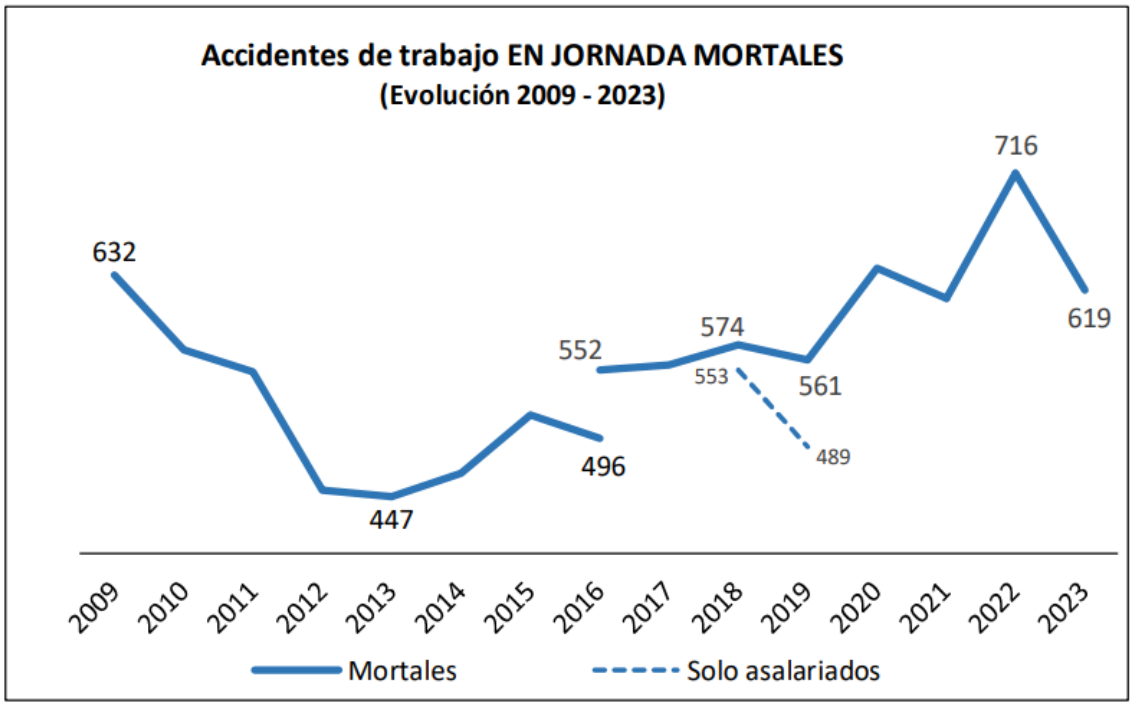

Figura 1.1: Gráfico con los datos de accidentes de trabajo mortales desde 2009 hasta 2023. Fuente: Ministerio de Trabajo y Economía Social, Gobierno de España (2024)

1.2 Estructura

Una estructura tradicional de la compañía es la multidivisional, en la que se presentan diferentes divisiones organizadas por funciones y que reportan a un responsable o *head office* (Figura 1.2).

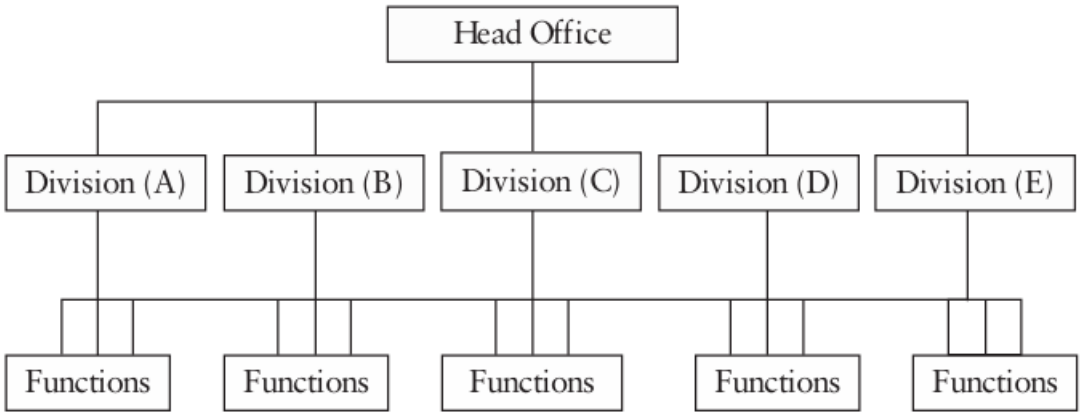

Figura 1.2: Estructura multidivisional. Fuente: Johnson y Scholes (1999)

Merna (2012) adaptó esta estructura para crear una versión actualizada (Figura 1.3) en la que encontramos la entidad corporativa arriba bajo la que se extienden el resto de las entidades empresariales. Estas son las responsables de la toma de decisiones, hasta las SBUs (*Strategic Business Unit*). Estas son divisiones originadas para cumplir con la visión estratégica de la firma, pueden ser producción, ventas, servicios, … Al nivel más bajo están los proyectos, que son los que generarán beneficios.

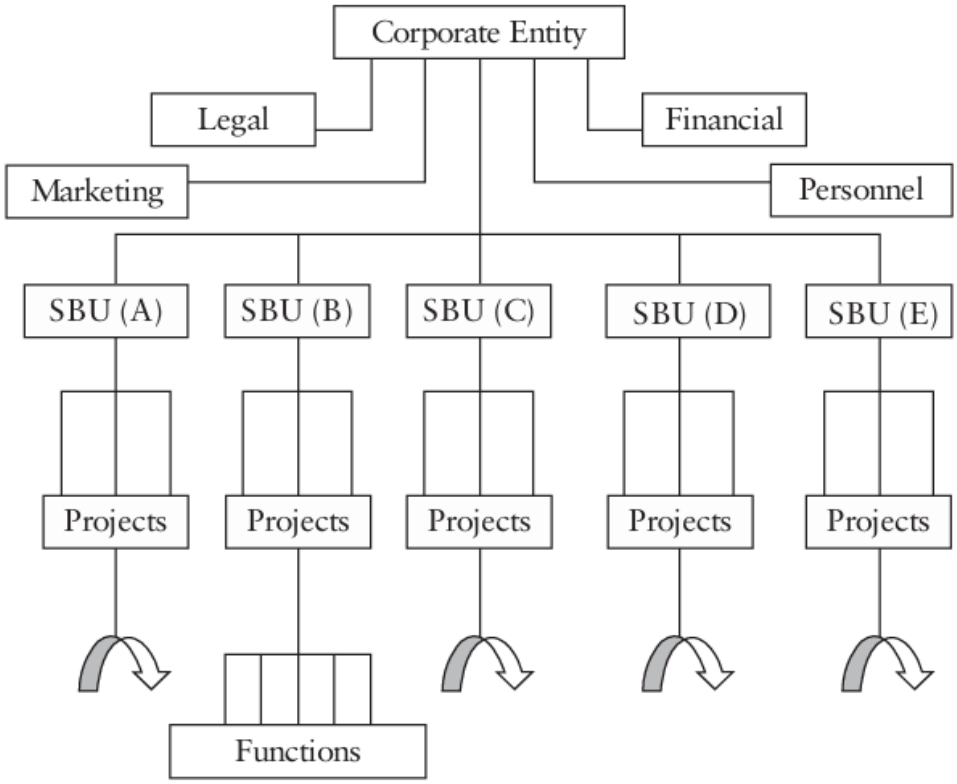

Figura 1.3: Estructura típica empresarial. Fuente: Merna (2012)

1.3 Gestión corporativa

La gestión corporativa, también referida habitualmente como estrategia corporativa, trata de asegurar la supervivencia de la corporación e incrementar su valor no solo a nivel financiero, sino de mercado y reputacional también. El alcance de esto y de la consecuente gestión de riesgos es amplio y variable según la estrategia. Normalmente, cubrirá los mercados actuales en los que la firma opera y las carteras de proyectos que cada SBU maneje, de los que se extraerán resultados que se evaluarán usando diferentes fuentes de información:

- Información interna
- Plan estratégico
- Reportes financieros
- Reportes financieros de cada *business unit*
- *Feedback* del monitoreo de riesgos
- Información pública
- Reportes financieros de competidores, clientes, proveedores y socios
- *Benchmarking*
- Artículos de investigación científica
- Estadísticas económicas
- Tendencias de consumo
- Consultas externas
- Previsiones tecnológicas
- Información de proyectos pasados y presentes

A la hora de gestionar la corporación, sus carteras de proyectos y los riesgos que la afectan, es indispensable conocer el plan estratégico de la empresa. Este es un portafolio de estrategias que portan la intención corporativa y son consecuentes con las inversiones financieras. Sus objetivos son:

- Crear y mantener una estrategia para lograr las intenciones de la empresa
- Incorporar y mantener los compromisos de los SBUs que apoyen la dirección estratégica
- Comunicar el plan
- Gestionar el cambio estratégico para mantener o ganar la ventaja competitiva

A nivel corporativo prácticamente toda la responsabilidad de la estrategia pertenece a los ejecutivos, aunque la última responsable sea la junta. La responsabilidad está alineada con los objetivos que cualquier firma trata de conseguir:

- Primario: Beneficio, como se ha mencionado, ese es el objetivo principal. Sin embargo, no todas las compañías están dispuestas a hacer lo que sea para conseguirlo, cada vez hay más concienciación con otros aspectos igualmente prioritarios, como el bienestar de los empleados.
- Secundario: Este depende del tipo de negocio que se haga. Determina la dirección que debe seguir la empresa.
- Corporativo: Estos son objetivos cuantificables que permitan determinar si el CEO (*Chief Executive Officer*) ha cumplido con las estrategias que se seleccionaron. Son más difíciles de enunciar, pero dan información directa de la estrategia

1.3.1. **Obligaciones de la dirección**

A la hora de gestionar la empresa y las personas que la integran, los directores son responsables de manera individual y conjunta de la viabilidad y futuro éxito de la compañía. Esta responsabilidad está debida a la propia compañía y no a los accionistas. Estos, en caso no estar de acuerdo con las decisiones tomadas no pueden tomar acción directa libremente y reconducir la decisión según su voluntad. De

forma similar, no tienen poderes para ordenar ninguna acción específica por parte de los empleados. Su poder real consiste en su capacidad para despedir a los directores y reemplazarlos por otros (Mrabure & Abhulimhen-Iyoha, 2020).

1.3.2. **La junta directiva**

La junta debe dirigir la compañía, convocar al director, delegar los poderes adecuados, monitorizar su rendimiento y tomar acciones correctivas si fuese necesario. El resto de los temas relativos a la junta son su estructura, su membresía y sus tareas. Todos ellos varían mucho entre países y empresas, ya que hay estructuras de lo más variopintas, juntas con rotación variable de sus miembros y tareas que a veces se asumen, y otras no. Lo importante es tener en cuenta que el futuro de la compañía depende en gran medida de la junta y del ejecutivo, debido a que portan la responsabilidad de gestión a alto nivel. Esto aplica, sin dudarlo, a la gestión de riesgos empresariales, que puede ser desarrollada al máximo gracias a la colaboración de la junta o destruida por completo (Naim & Rahman, 2022).

1.4 Riesgos a nivel corporativo y CRO

En el mundo real las empresas afrontan una competición feroz, que hace que reducir la gestión de las amenazas con seguros sea insuficiente o ineficiente desde el punto de vista económico. La vulnerabilidad a la volatilidad del mercado es demasiado grande, lo que ha hecho inevitable el ascenso de la gestión de riesgos en el ambiente corporativo. La dirección senior está cada vez más concienciada, tanto de la importancia de considerar los riesgos como de la importancia que tienen a la hora de hacerlo posible, pero en algunos casos existe la amenaza intrínseca de que esta vigilancia se quede en algo superficial. No es raro encontrar casos en los que se designa una persona dedicada a los riesgos que al final realiza un trabajo de gestión de seguros, y eso no es suficiente. La lista de riesgos que afectan a la empresa es larga, sea regulatorio o legal, político, fraude o de evento (se hablará en el próximo capítulo de los tipos de riesgos), emparejado con que la complejidad de estos está aumentando de igual manera. El éxito corporativo depende de la gestión integral de los riesgos, a través de una estructura completa y actualizada; lo que en la literatura nombran como ERM (*Enterprise Risk Management* - Gestión de Riesgos Corporativos) (Merna, 2012).

Un rol que está sugerido ampliamente en la literatura es el de *Chief Risk Officer* o CRO. Se busca poder gestionar los riesgos de forma efectiva a través de dedicar una persona a ello que esté a nivel ejecutivo y tenga el poder concedido por la junta para llevar a cabo sus ideas. A pesar de que, en efecto, se sugiere considerar esta posición, la aceptación e implementación a nivel empresarial es más limitada. Se presenta una cierta resistencia por parte de las empresas para incorporar este puesto debido, principalmente a que se entiende que la tarea de gestionar los riesgos debería caer en el CFO (*Chief Financial Officer*) debido a que, en la mayoría de los casos, los riesgos evaluados son financieros (Ojeka *et al*., 2019). Además de recaer la responsabilidad en el CFO, también suele hacerlo sobre el CEO quien es el responsable último de que la compañía cumpla con su obligación principal, generar beneficio (Safiullah *et al*., 2025).

1.5 Conclusiones del capítulo

Comprender la naturaleza y estructura de la compañía es un paso esencial para cualquier análisis riguroso de la gestión del riesgo empresarial. A lo largo de este capítulo se ha demostrado que, aunque la figura de la corporación es ampliamente reconocida en su dimensión económica y legal, sus particularidades estructurales y de gobierno interno siguen siendo, en muchos casos, poco

comprendidas. Esta falta de comprensión constituye una limitación real a la hora de identificar, evaluar y gestionar los riesgos a los que se enfrentan las organizaciones en el contexto contemporáneo.

La corporación, como entidad jurídica separada de las personas que la componen, acumula derechos y capacidades que no siempre van acompañados de responsabilidades proporcionales. Este desequilibrio, evidenciado en múltiples casos históricos y recientes, configura un entorno en el que los riesgos laborales, sociales y legales no solo existen, sino que pueden quedar diluidos en una estructura que dificulta la atribución de responsabilidades concretas. Así, la relación entre empresa, Estado y sociedad aparece como un factor clave que influye directamente en la manera en que se perciben y se gestionan ciertos tipos de riesgo.

Además, se ha analizado la organización interna de las compañías, especialmente en torno a estructuras como la multidivisional o las unidades estratégicas de negocio, que establecen niveles diferenciados de toma de decisiones y exposición al riesgo. A nivel corporativo, la gestión del riesgo no puede disociarse de la estrategia global ni del plan directivo, ya que los riesgos se manifiestan en la práctica a través de decisiones concretas, flujos de información y objetivos definidos. En este sentido, la implicación de la alta dirección y, sobre todo, de la junta directiva, resulta decisiva. Su papel no se limita a supervisar, sino que implica orientar y facilitar la gestión de riesgos con una visión estratégica.

Finalmente, el capítulo subraya la necesidad de contar con un enfoque estructurado y profesional en la gestión del riesgo a nivel corporativo. La aparición del rol de *Chief Risk Officer* (CRO) se presenta como una solución potencialmente eficaz, aunque su implantación todavía es limitada. La resistencia a su adopción revela, en parte, una visión todavía reduccionista del riesgo, vinculado exclusivamente a la esfera financiera y delegado a otras figuras ejecutivas como el CEO. Este punto refleja una de las tensiones clave que atraviesan la gestión moderna del riesgo: la necesidad de evolucionar desde enfoques funcionales hacia modelos verdaderamente integrales y estratégicos.

Capítulo 2 El riesgo en la empresa y sus tipos

La palabra "riesgo" es un término de uso cotidiano que se puede encontrar con cierta frecuencia en cualquier situación rutinaria. No obstante, en el ámbito empresarial, el concepto de riesgo adquiere matices distintos y puede ser interpretado desde diversas perspectivas. El objetivo primero de este capítulo será definir bien lo que se entenderá en este trabajo por riesgo, para así establecer una base común sobre la que se irá construyendo el sistema de gestión de riesgos empresariales. En contraste con el uso casual que se le da al riesgo en nuestro día a día, en este capítulo se explorarán las diferentes posibilidades y tipos que se pueden identificar, generando un criterio claro para su categorización.

2.1 ¿Qué significa "riesgo"?

Debido al uso cotidiano del término, puede no resultar inmediato el significado que adopta en el ámbito de la gestión de proyectos y en concreto, en la gestión del riesgo. No obstante, el uso que se le da en estos contextos dista del absoluto rigor científico, en el que el término tiene una denotación definida y compartida por todos los que la usan. En cierta medida, irremediablemente está "contaminado" por el uso que se le da a diario, que no es el que se define estrictamente para él. En la vigésimo tercera edición del diccionario de la Real Academia Española (2014) se define riesgo como: Contingencia o proximidad de un daño (Diccionario de la Real Academia Española de la Lengua, 2014). En este trabajo se le darán dos definiciones distintas.

La primera de ellas hará referencia al uso común de riesgo entendido como una situación posible de que algo malo ocurra. Es importante destacar de esta noción que se trata de una posibilidad, que puede no ocurrir. Además, se habla de "algo malo", aspecto que depende de la situación que se evalúa, pero conlleva una pérdida relativa de lo que se tiene. Este es el sentido más expandido del término en el habla coloquial. Ejemplos de esto serían:

- Los fumadores tienen un mayor riesgo de sufrir un cáncer de pulmón
- En los Pirineos hay mayor riesgo de tormenta que en la Mancha conquense
- En el rugby hay mayor riesgo de lesiones que en el tenis de mesa

En cualquiera de los ejemplos, la situación más arriesgada supone la que tiene una mayor probabilidad de pérdida o mayor magnitud de pérdida. De esta manera, una forma de medir el riesgo es calcular la pérdida esperada operando con la probabilidad y la magnitud de pérdida. Esto se puede traducir a términos económicos que serán los que interesen para nuestro modelo empresarial. Un ejemplo sería: Maribel y Rocío tienen un coche cada una que usan para ir a trabajar. Habitualmente, no incurrirían en ningún gasto al hacer el camino (en lo relativo al coche), pero para ambas existe riesgo de avería, que para simplificar diremos que costaría mil euros. Por el tipo de coche que tienen, la probabilidad de avería en un periodo de tiempo determinado en el caso de Rocío es del 5% , mientras que en el caso de Maribel es del 20%. Por lo tanto, la pérdida esperada de Rocío sería de 50€, mientras que la pérdida de Maribel sería de 200€. Se puede decir, por lo tanto, que Maribel tiene un mayor riesgo de avería que Rocío.

La otra definición por tratar entiende el riesgo como la impredecibilidad de una situación o la incertidumbre asociada a los resultados. Esta es la que los profesionales en la gestión de proyectos utilizan. De hecho, como referencia la definición del PMBOK (*Project Management Body of*

Knowledge)[1] es: "*hecho o condición incierta que, si ocurriese, tendría un efecto positivo o negativo sobre al menos un objetivo del proyecto*" (*Project Management Institute* - PMI, 2017). Mientras que asociar riesgo con pérdida o daño es más habitual en el lenguaje coloquial, es importante señalar que en el ámbito profesional la incertidumbre no tiene por qué derivar en efectos indeseables para la organización, pudiendo resultar en beneficios. Es más sencillo de entender usando un ejemplo, y en concreto, uno financiero. Al decir que invertir en la compañía A conlleva más riesgo que invertir en la compañía B hacemos uso de esta segunda definición. Que la inversión en una compañía u otra sea más arriesgada depende de que sea más difícil de predecir, por lo tanto, sea más volátil. Para medir esta noción de riesgo se pueden usar la desviación estándar o la varianza. Desarrollando el ejemplo, la inversión en la compañía A puede generar entre 0 y 1000€, mientras que la inversión en la compañía B puede generar entre 400 y 600€. En ambos casos, el resultado esperado de la inversión es 500€. Sin embargo, la varianza en la compañía A es mayor, por lo que el riesgo de la inversión es mayor en este caso. Mientras que se podría obtener un valor menor al mínimo que se obtendría en la B, también se puede obtener un valor mayor y, por lo tanto, ganar más dinero. En este caso un mayor riesgo puede entrañar un mayor beneficio, no solo una mayor pérdida.

En el párrafo anterior se hace referencia a la varianza y la desviación estándar, dos términos estadísticos que pueden no ser inmediatamente transparentes para todos los lectores. La varianza y la desviación estándar son medidas estadísticas fundamentales para cuantificar la dispersión o variabilidad dentro de un conjunto de datos, proporcionando información crucial sobre la variabilidad inherente en los datos. Estas medidas son herramientas indispensables en diversos campos, ya que permiten a los investigadores y analistas comprender hasta qué punto los datos individuales se desvían del valor promedio, ofreciendo así una visión más completa de la distribución de los datos. La varianza, definida matemáticamente como el promedio de las diferencias al cuadrado respecto a la media, capta la dispersión general de los datos. Una varianza alta indica que los datos están ampliamente dispersos alrededor de la media, mientras que una varianza baja sugiere que los datos están agrupados cerca de la media. Sin embargo, debido a que la varianza se expresa en unidades al cuadrado, a menudo resulta menos intuitiva para su interpretación directa, lo que ha llevado al uso generalizado de la desviación estándar. La desviación estándar, al ser la raíz cuadrada de la varianza, proporciona una medida de variabilidad más interpretable, ya que se expresa en las mismas unidades que los datos originales. En cualquier caso, ambas medidas pueden y son utilizadas para evaluar la dispersión de una serie de datos (Woolson & Clarke, 2002).

Habiendo explicado esto, se puede definir la gestión del riesgo como la gestión de las pérdidas esperadas y la gestión de la incertidumbre. Ambas nociones confluyen en un mismo punto y deben ser consideradas por los profesionales que trabajen en el mundo del riesgo, puesto que según el contexto convendrá adoptar una o la otra.

2.2 Tipos de riesgo

Una vez definido el concepto de riesgo en términos abstractos, resulta pertinente abordar su manifestación concreta y el modo en que incide en la dinámica empresarial. La incertidumbre respecto a determinados escenarios y la posibilidad de pérdidas representan factores que afectan a la organización tanto a nivel global como en sus distintas áreas funcionales.

[1] PMBOK: El PMI (2017) define los fundamentos para la dirección de proyectos (PMBOK) como un término que describe los conocimientos de la profesión de dirección de proyectos. Los fundamentos para la dirección de proyectos incluyen prácticas tradicionales comprobadas y ampliamente utilizadas, así como prácticas innovadoras emergentes para la profesión.

Con el fin de profundizar en la comprensión del riesgo, en este apartado se expondrán las tipologías más comunes que pueden identificarse en el entorno empresarial. En particular, se analizarán los distintos tipos de riesgos operativos, aunque es preciso subrayar previamente la relevancia de su adecuada identificación y clasificación, condición indispensable para una gestión eficaz.

La literatura especializada coincide en señalar que las empresas deben enfrentar los distintos tipos de riesgos mediante el desarrollo de programas específicos orientados a su tratamiento. En aquellos casos de mayor complejidad, se requiere una aproximación más detallada que contemple metodologías estructuradas, procesos definidos y análisis estadísticos rigurosos. Finalmente, la correcta integración de estos programas en el sistema general de gestión de la empresa constituye un elemento clave para asegurar una gestión integral del riesgo corporativo.

2.2.1. **Riesgo operativo**

A pesar de que las compañías han tenido que lidiar con fallo humano, procesos defectuosos o dificultades tecnológicas desde siempre, introducir el riesgo operativo en el lenguaje y sistema empresarial es algo relativamente nuevo, especialmente si comparamos con otros tipos de riesgos como el financiero (Lam, 2014). Esto se debe a que tradicionalmente, este tipo de riesgo se ha gestionado de forma informal, especialmente por los *managers* afectados como parte de su carpeta de responsabilidades. Además, también se tratan en la preparación previa de auditorías, sean rutinarias por requisito legal o asociadas a certificaciones externas. Esta aproximación episódica de los riesgos operativos cada vez que anualmente hay auditoría o cada vez que algún error invita al equipo a mejorar el proceso no sería la forma óptima de trabajar, aunque sí la más representativa de la tendencia en la industria.

En el caso de los riesgos operativos, el punto de vista que gobierna su gestión habitualmente es el que hace referencia a la pérdida. Mientras que no son completamente libres de entenderse como incertidumbre que puede generar beneficio, desde un punto de vista empresarial su desestimación puede conllevar grandes pérdidas para la empresa, por lo que es la visión que se adopta habitualmente. Errores en el proceso o de naturaleza humana pueden generar pérdidas para la compañía que, al acumularse, se tornan significativas. Además, existe la posibilidad de que algún riesgo operativo notable tenga una magnitud muy grande para la empresa, aunque es menos probable (Lam, 2014).

A parte de las pérdidas monetarias o de flujo de dinero que la empresa pueda incurrir por una mala o nula gestión de los riesgos operativos, existen también otros tipos de pérdidas como daño reputacional o de marca, cuestionamiento financiero, rechazo de clientes o proveedores, entre otros.

Se ha hablado de la naturaleza de los riesgos operativos, pero su definición está todavía pendiente. Tradicionalmente se los ha definido de forma negativa, como los riesgos que no son financieros ni de mercado. Actualmente, se ha convergido en una nueva versión común: el riesgo operacional es el riesgo de pérdida por procesos, personas y sistemas inadecuados o fallidos, y por eventos (Basel Committee, 2011). Esta definición está bien, pero se observa la falta de riesgos de negocio (márgenes, competición) y riesgos de reputación (confianza, marca), que podrían ser integrados como riesgos operacionales (especialmente considerando que al tratarse de riesgos importantes es necesario gestionarlos). En cualquier caso, cada empresa puede definir qué considera dentro de este grupo, y qué queda fuera.

2.2.1.1 Proceso

El origen de estos riesgos está en procesos inefectivos o ineficientes. Los primeros se pueden definir como aquellos que no logran sus objetivos mientras que los segundos sí los consiguen, pero acarreando un coste excesivo. En algunos casos, existe un conflicto natural entre ambos. Por ejemplo, a la hora de optimizar el coste de un proceso se pueden eliminar parte de las comprobaciones o vías redundantes, lo que puede devenir en un proceso más propenso al fallo y, por lo tanto, más inefectivo. Por lo tanto, en este tipo de riesgos es importante alcanzar un balance entre la efectividad y la eficiencia.

Uno de los riesgos de proceso más comunes es el riesgo transaccional, relacionado con el procesado de transacciones. Esto se refiere al error potencial en cualquiera de las fases de las transacciones de un negocio, sea la venta, el precio, la documentación, la confirmación o la resolución. La compañía está expuesta a la posibilidad de pérdida sea financiera, de cliente o reputacional. Por ejemplo, un error en el precio puede tener impacto en las finanzas, o un error en la confirmación puede provocar que un cliente no quiera seguir trabajando con la empresa.

Otro riesgo común es lo relativo al conjunto de procesos de documentación. Lo más típico es que la insuficiencia o ineficiencia en la producción de documentos acarree riesgos innecesarios en caso de que haya alguna disputa. Cuando se trabaja con otras empresas, incluso, en temas transaccionales este riesgo se puede mitigar realizando un contrato marco, aprovechando su efecto a nivel legal. Sin embargo, aunque los estados cuentan con mecanismos como este para apoyar las interacciones entre empresas desde un punto de vista jurídico, existe el riesgo de fracasar en la documentación adecuada, especialmente en empresas mayores en las que se manejan muchos contratos con muchas versiones. El caos documental genera una situación de riesgo para la empresa (Fishkin, 2000).

Entre las propuestas para gestionar los riesgos de proceso, la más habitual en la literatura es la de automatización. El punto de inflexión en este punto de vista de minimizar la interacción humana para evitar errores tiene su origen en Toyota y su visión *Lean* de la manufactura de vehículos (Paladugu & Grau, 2020). De hecho, han incorporado esta visión vanguardista en su imagen de marca, dándole nombre: TPS (Toyota *Production System*) que definen como “filosofía de fabricación original de Toyota, diseñada para eliminar desperdicios y lograr la máxima eficiencia” (Toyota, s.f.).

2.2.1.2 Personas

Los riesgos de personas suelen estar originados en restricciones de la plantilla, incompetencia, deshonestidad o cultura corporativa que no promueve la conciencia sobre sobre los riesgos. Las restricciones de plantilla hacen referencia a cuando la empresa no es capaz de cubrir las vacantes que tiene por ausencia de mano de obra o porque las condiciones e incentivos que ofrecen no resultan atractivos para los candidatos al empleo. La incompetencia, a pesar de lo acusativo del término, refiere a la incapacidad de los empleados para desempeñar sus funciones por la ausencia de la formación adecuada. La deshonestidad de los empleados está relacionada con actividades fraudulentas que puedan desempeñar, como el robo de material, o el uso/distribución de información clasificada. Sobre la cultura de la empresa, afecta tanto a los empleados, que pueden no preocuparse por los riesgos, pero también sobre *management* y la junta (Becker & Smidt, 2016). Especialmente importante si la empresa retribuye a los empleados según los resultados sin castigar las pérdidas, como se ha visto en el Capítulo 1.

Todos los empleados son una fuente de riesgos, y según los que se identifiquen como importantes para la empresa, se deberán tomar medidas adecuadas. Por ejemplo, el riesgo (tanto en magnitud como en probabilidad) de robo por parte de los empleados en una empresa harinera es significativamente menor

que en una empresa de extracción de oro. Por lo tanto, y enlazando con el anterior punto; poner procesos exhaustivos de control en el primer caso puede resultar ineficiente por el sobrecoste, mientras que en el segundo casi cualquier punto de control extra hará el proceso menos inefectivo, ofreciendo beneficios para la empresa. Ocurre de forma similar con el filtrado de información sensible o crítica, que será menor en una empresa con buena ética y buen nivel de *compliance* que en una que incurra en prácticas no permitidas según la regulación que aplique. Por lo tanto, el riesgo que todos los empleados naturalmente suponen puede ser aceptado por la empresa si así se estima adecuado o en cambio, controlado de cerca.

Continuando con este hilo, se ha presentado a los empleados como un agente activo a la hora de provocar un daño posible a la empresa, pero hay casos en las que experimentan las consecuencias de una gestión inadecuada generando otro tipo de riesgos, los asociados a los accidentes y a la inhabilitación laboral. En el anterior capítulo se ha mencionado cómo el riesgo de enjuiciamiento penal al ejecutivo de la compañía por poner en riesgo a sus empleados es limitado y significativamente improbable, pero la empresa en conjunto sí puede experimentar las consecuencias de una inhabilitación laboral por razones médicas. Sea un aumento de la carga de trabajo para los compañeros o tener que arrancar procesos de *recruiting* (término en inglés para referirse a la selección de personal), la empresa acarrearía una situación de pérdidas por descuidar cómo trabaja su plantilla. Mientras que se puede mitigar con una correcta prevención de riesgos laborales, en algunos casos, no se puede prevenir y es inevitable, por lo que se puede considerar también.

Otra posibilidad, que tiene un impacto indirecto en la empresa y, por lo tanto, debemos mencionar, aunque la compañía no sea la principal afectada, se da en las empresas en los que los empleados trabajan de cara al público. Por la naturaleza de este tipo de puestos de trabajo los empleados están expuestos a una gran variedad de situaciones, y estas son una fuente de riesgo clara para la compañía. Puede ocurrir que se den situaciones tipificadas en el código penal como agresión, acoso o vulneración del honor en el que el empleado forma parte de la parte perpetuadora de la acción o de la víctima. El segundo de los casos desde un punto de vista puramente analítico puede suponer a la empresa un riesgo de baja o incluso una denuncia si así lo considera el afectado (en este caso, que forma parte de la plantilla). El primero en cambio puede tener un efecto importante a nivel reputacional y de imagen, debido a que se haya perpetuado un delito por parte de un trabajador en su horario laboral. Al final, indiscutiblemente, la víctima (sea quien sea) es la verdadera sufridora de que se cometiese ese supuesto crimen, pero no podemos dejar de señalar que la empresa también puede estar entre los elementos indirectamente afectados. Una de las propuestas para mitigar este riesgo, muy al estilo de Estados Unidos, es realizar lo que llaman *background checks*, o revisiones del historial previo del candidato. Mientras que hay trabajos que exigen probar estar libre de crímenes, especialmente de naturaleza sexual, no está tan extendido a nivel legal el obligar a las empresas a realizar este tipo de comprobaciones. Sin embargo, aunque hay profesiones en los que resulta evidente esta necesidad, como cuerpos de seguridad, trabajo con niños o sanidad por distintas razones, por lo general, un breve *check* para cualquier puesto de cara al público puede ser suficiente para mitigar este riesgo (Lam, 2014).

2.2.1.3 Sistema

A medida que la tecnología tiene un mayor peso en los puestos de trabajo, la importancia de considerar los riesgos asociados a un fallo del sistema se ha convertido en más relevante, sean sistemas generales compartidos por cualquier empresa (como cualquier herramienta de ofimática) o programas específicamente diseñados para apoyar el funcionamiento de la empresa en concreto. A parte del riesgo de fallo, también existe un riesgo de que la infraestructura tecnológica y de sistemas de la empresa no crezca acorde al negocio y, por lo tanto, no sea capaz de alimentar dicho negocio según se va generando, provocando otros riesgos como documentación y comunicación. Además de estos,

encontramos otros como disponibilidad del sistema, integridad de datos, capacidad, acceso y/o uso no autorizado y recuperación de negocio tras contingencias (Lam, 2014).

Otro riesgo, quizá menos inmediato, que podemos incluir aquí es el riesgo de pérdida asociado a modelos financieros defectuosos. A la hora de proyectar sus finanzas, las compañías recurren a modelos financieros que pueden usar metodologías inadecuadas, suposiciones antiguas o parámetros incorrectos, provocando que no se pueda evaluar de forma correcta el riesgo que se toma en cada decisión estratégica.

Finalmente, uno de los riesgos más importantes sería el de seguridad, especialmente siguiendo el auge del comercio electrónico. Se ha convertido en una tendencia casi habitual escuchar hablar de ciberataques, que pueden provocar el filtrado de cantidades masivas de datos, tanto de clientes como de la propia empresa. De hecho, la frecuencia con la que ocurren es alarmante y constituye una de las preocupaciones principales de las empresas (Toussaint *et al*., 2024), que trabajan para aumentar la concienciación en temas de seguridad cibernética en su plantilla. Este tipo de riesgo reviste una complejidad particular, ya que la mera capacidad de un *hacker* para acceder al sistema es suficiente para que se materialicen consecuencias negativas derivadas de dicha intrusión. Sin embargo, se puede trabajar en reforzar todo el sistema para hacerlo lo más resistente posible a ataques, aparte de formar a los empleados para evitar el *phishing*. Este último término, se refiere a la forma en la que cibercriminales obtienen información confidencial a través de suplantar una fuente de confianza y establecer comunicación electrónica con un individuo. Incluso, se puede localizar más la atención para prevenir el *whaling*. Este término, que proviene de la palabra inglesa *whale* hace referencia a un tipo de *phishing* específico realizado sobre individuos de alto valor para la empresa, como puede ser el CEO, algún miembro de la junta u otro ejecutivo de alto nivel. Solo en Estados Unidos, en 2017 el FBI atribuyó una pérdida de 675 millones de dólares al *whaling* y en 2018 el FBI estimó en 12 mil millones de dólares las pérdidas asociadas al *phishing* en más de 150 países desde 2013. Esto indica que la prevención contra los ataques sea a empleados o altos directivos, es crucial, y siempre existirá el riesgo de filtración por este tipo de estafas (Pienta *et al*., 2020).

2.2.1.4 Evento

El riesgo por evento se refiere a la pérdida debida a eventos singulares que son improbables, pero tienen consecuencias graves de ocurrir, lo que se puede conocer como cisnes negros. Estos pueden ser internos o externos, y pueden consistir en fraude, caídas de sistema, desastres naturales o humanos… Este tipo de riesgos suelen tener implicaciones que afectan a todos los tipos de riesgo, no exclusivamente a los operativos. Sin embargo, siguiendo la descripción del comité de Basilea, los incluyen como operativos debido a que impactan de forma inmediata en las operaciones de la empresa (Basel Committee, 2011). A pesar del carácter aleatorio e inesperado de estos riesgos, se pueden controlar con un *planning* y gestión adecuados. Un ejemplo puede ser un apagón que afecte a todo el suroeste europeo, en el que se pueden producir errores en los procesos (transacciones), imposibilidad de hacer negocio (cierre forzoso) y en el peor de los casos, daños personales.

Lo que en cierta medida puede parecer contraintuitivo es la frecuencia con la que estos eventos acontecen. Desde hace tiempo se viene estimando en la literatura que ocurre un fenómeno de gran impacto cada relativamente poco tiempo, tendencia que ya se acusaba en el año 2000 (*London Risk Books*). Con los años recientes, esta dinámica no ha hecho sino acrecentarse, o en cierta medida, recrudecerse. Los eventos imprevisibles crecen en importancia, por lo que saber gestionarlos se torna crítico. Desde 2020 se ha vivido una pandemia mundial de COVID-19, y a nivel nacional la borrasca Filomena, la erupción del volcán de Cumbre Vieja en La Palma y la DANA de Valencia, además del ya sutilmente mencionado apagón europeo. Sin embargo, todos estos eventos se presentan como naturales, incluido el tan propenso a la teoría de la conspiración COVID y el reciente apagón (2025)

cuyas causas permanecen indeterminadas. Pero, el evento que más está condicionando la gestión de riesgos a todos los niveles de todas las empresas del mundo es la guerra de aranceles promovida por la administración Trump durante su presidencia de los Estados Unidos (2025). Realizar un análisis del alcance y las implicaciones es casi imposible en este momento, pues todo se está desarrollando en tiempo presente, pero se pueden realizar estimaciones, que es lo que están haciendo las empresas, para aprovisionar las previsibles pérdidas y prepararse para el mayor evento en el mundo mercantil internacional de la historia reciente.

2.2.1.5 Negocio y reputación

El riesgo de negocio es aquel que se corresponde con cambios inesperados en el ambiente competitivo, o en las tendencias que dañan la franquicia y su economía. Incluye temas como estrategia, gestión de clientes, desarrollo de producto, precios y ventas. El más habitual es el riesgo de que los beneficios de la empresa no superen los costes, pero otro ejemplo puede ser el riesgo que entraña el desarrollo de nuevos productos. A nivel empresarial, el desarrollo de novedades e inversión en I+D constituye una parte indispensable para la supervivencia de la empresa. Los clientes demandan nuevas opciones, la innovación ofrece posibilidades nuevas para optimizar el servicio/producción… En este caso el riesgo se entiende como incertidumbre, puesto que la inversión en I+D+i sea del tipo que sea (producto o proceso) conlleva potencialmente pérdidas o ganancias para el negocio. Un último ejemplo de esto es cuando alguna compañía es capaz de adaptarse a algún cambio y modificar su modelo de negocio. Cualquier cambio de este tipo entraña una serie de riesgos asociadas a abrirse hueco en un nuevo mercado, y los riesgos asociados a tener un negocio nuevo.

También mencionado en este punto está el riesgo reputacional, según la propuesta de Lam (2014), por el impacto tan directo que tiene la imagen de una empresa sobre sus posibilidades de negocio, aunque también reconoce que se pueden separar.

2.2.2. **Riesgo financiero**

Los riesgos financieros o de crédito han sido los que más han acaparado la atención de las empresas de un tiempo a esta parte. No obstante, aunque estos riesgos han sido objeto de una amplia producción académica y profesional, la creciente complejidad del entorno financiero global evidencia que los esfuerzos realizados hasta la fecha resultan insuficientes. Además, este tipo de riesgos también es víctima de una ausencia significativa de interés por parte del grueso empresarial, lo que dificulta el desarrollo en su gestión y el avance efectivo. Las finanzas permiten recolectar y redistribuir capital privado de manera eficaz. A través de actividades financieras, las empresas pueden obtener fondos para expandirse y generar ganancias, mejorando la eficiencia económica. La gestión de las finanzas en la empresa es indispensable, hasta el punto de que existe el puesto de CFO (*chief finance officer*) como representación en el alto ejecutivo de la empresa para asegurar que esta parte de la gestión de la compañía se realiza de forma óptima (Zhao, 2023).

Las finanzas están expuestas al riesgo y a la variabilidad también. De hecho, en los ejemplos de riesgo como incertidumbre hay un caso puramente financiero. Más adelante, en el capítulo 3 se desarrollará cómo la gestión de riesgos tiene un efecto en el valor de la empresa y, por lo tanto, en su contabilidad y finanzas. Retornando al tema, a pesar de que este tipo de riesgos son particularmente relevantes en entidades bancarias, las instituciones no financieras también experimentan este tipo de riesgo, especialmente asociado a préstamos y a la obtención de capital. Algo que aún está pendiente es definir "riesgo financiero o crediticio", que puede ser la pérdida económica debido al fallo de una contraparte

prestataria o la incertidumbre asociada a un movimiento financiero. El fallo no tiene por qué ser la bancarrota, pero sí la incapacidad para cumplir con las obligaciones contractuales (Lam, 2014).

2.2.2.1 Subtipos de riesgos financieros

Riesgo de tasas de interés y cambio

Debido a la integración internacional, las fluctuaciones en tasas de interés y tipos de cambio afectan las inversiones a largo plazo y pueden desencadenar crisis financieras. Aunque el mercado internacional no incurra en incumplimientos, grandes fluctuaciones pueden afectar severamente el valor de las inversiones a largo plazo.

Riesgo de productos financieros

El auge de las finanzas en internet ha disminuido la barrera de entrada al sector. La falta de evaluación adecuada de los productos financieros genera inversiones ciegas y posibles pérdidas.

Riesgo de gestión interna del sistema financiero

La competencia entre bancos e instituciones financieras puede derivar en conflictos y prácticas nocivas. La emisión de bonos como estrategia para atraer inversión y enfrentar crisis financieras puede funcionar a corto plazo, pero también introduce riesgos que podrían afectar negativamente al sistema financiero en el futuro.

Riesgo de flujo de capital

La interrupción en el flujo de capital dentro de una empresa puede generar un riesgo de liquidez severo. Esta situación no solo afecta sus operaciones actuales, sino que también perjudica su calificación crediticia, limitando su capacidad de financiamiento futuro. Las medidas tradicionales de gestión no son suficientes para resolver este tipo de riesgo.

Riesgo de crédito financiero

Se refiere al incumplimiento unilateral en actividades financieras, como los préstamos personales o a pymes. La falta de transparencia y de sistemas de supervisión ha provocado muchas deudas incobrables. El riesgo de crédito, comúnmente asociado a pérdidas de préstamos, ha sido protagonista en múltiples crisis financieras (hipotecas subprime, bonos rusos, etc.). Sin embargo, este riesgo no solo afecta a bancos, sino a cualquier empresa que haga transacciones con terceros. Además, muchas de las exposiciones más serias al riesgo de crédito provienen de instrumentos financieros fuera del balance contable, como swaps, opciones y garantías.

Riesgo de opciones financieras

Las opciones de compra exponen al comprador, no al vendedor, al riesgo de crédito, ya que el vendedor debe cumplir si la opción se vuelve rentable. Esta exposición equivale al valor de la opción en el momento, y persiste hasta que la opción vence. El modelo de *Black-Scholes* ayuda a cuantificar esta exposición de forma precisa.

Riesgo financiero de *swap*

Un *swap* es un acuerdo financiero en el que dos partes intercambian flujos de efectivo basados en uno o más índices de precios. Por ejemplo, en un *swap* de tasas de interés, las partes intercambian pagos de intereses, uno a tasa fija y otro a tasa variable, sobre un importe nominal. Sobre estos, hay dos dificultades principales a la hora de estimar los riesgos:

- Falta de información pública sobre la severidad en caso de impago: Hay pocos datos sobre lo que ocurre cuando una contraparte de *swap* incumple, ya que los impagos en estos contratos son poco frecuentes. Además, según la ley de quiebras de EE. UU., los acreedores de *swaps* suelen tener baja prioridad para reclamar los activos de la parte en quiebra. Sin embargo, esta desventaja suele compensarse con protecciones adicionales, como garantías o cláusulas que exigen aportar más colateral si baja la calificación crediticia de la contraparte.
- Dificultad para estimar la exposición al riesgo: El riesgo de crédito depende del valor de mercado del *swap*, que normalmente es cercano a cero al inicio, pero puede variar con el tiempo según los movimientos de los precios o tasas de interés. La exposición puede ser un activo o un pasivo, dependiendo de cómo evolucionen los mercados. Por ejemplo, si bajan las tasas, quien recibe tasa fija tiene un activo y, por tanto, exposición al riesgo de crédito de la contraparte; si suben, la situación se invierte.

Para estimar este riesgo el método más sencillo es sumar un porcentaje fijo del importe nominal al valor de mercado actual del *swap*, pero primero habría que estimar el porcentaje y solo sería útil para un *swap* individual, y no todos los que puedan afectar a la empresa. En el caso de las organizaciones con más recursos, suelen emplear simulaciones avanzadas que les dan esta información.

2.2.3. **Riesgo de mercado**

El riesgo de mercado se puede entender como la posibilidad de pérdidas derivadas de cambios en precios o tasas del mercado, como tasas de interés, tipos de cambio, precios de acciones o materias primas. También como la incertidumbre intrínseca de mercados concretos que no es diversificable (se desarrollará este punto en el capítulo 3). Todas las empresas enfrentan este riesgo, aunque la forma y magnitud varían según la industria. Instituciones financieras pueden verse afectadas por desajustes entre activos y pasivos, mientras que empresas multinacionales enfrentan riesgos cambiarios al operar en distintos mercados. Las empresas energéticas, por su parte, dependen de la estabilidad entre los precios de insumos y productos. Además, existen riesgos comunes a todas las organizaciones, como la dependencia del rendimiento de inversiones para cumplir obligaciones financieras, o los déficits en fondos de pensiones. Gestionar adecuadamente estos riesgos es esencial para mantener la estabilidad y solvencia empresarial.

Existen tres tipos de riesgo de mercado: riesgo de comercio, desajuste entre activos y pasivos, y riesgo de liquidez.

El **riesgo de comercio** abarca los riesgos que enfrenta una empresa en sus carteras de inversión y operaciones debido a cambios en tasas de interés, tipos de cambio, precios de acciones y de materias primas. Estas exposiciones suelen ser de corto plazo y, por lo general, pueden cerrarse o cubrirse en un plazo de varios días. Es el principal tipo de riesgo de mercado al que se enfrentan los bancos de inversión y los intermediarios. También afecta a empresas energéticas con actividades de creación de mercado y a corporaciones no financieras que poseen libros de negociación. Este riesgo se refiere habitualmente a la incertidumbre existente, pues según el estado en el que estén los mercados internacionales puede ser favorable para la empresa.

El **desajuste entre activos y pasivos** surge de las diferencias en la sensibilidad a las tasas de interés entre los activos y pasivos registrados en el balance general. Este tipo de riesgo se distingue del riesgo de negociación porque suele ser menos líquido y, por lo tanto, solo puede ajustarse o cerrarse ocasionalmente, aunque se puede cubrir y volver a cubrir con más frecuencia. Es el principal riesgo de mercado para los bancos comerciales y minoristas, aunque también afecta a aseguradoras y bancos de inversión. En el caso de las empresas energéticas, los desajustes entre los precios de insumos y productos también pueden analizarse dentro de este mismo marco. Lo mismo ocurre con el manejo del desfase entre los activos y pasivos de los fondos de pensiones.

El **riesgo de liquidez** es el riesgo de que una empresa no pueda obtener fondos para cumplir con sus obligaciones financieras a medida que vencen, ya sea aumentando sus pasivos o convirtiendo activos en efectivo sin incurrir en pérdidas significativas. Este riesgo es común a todas las empresas y se solapa con el riesgo financiero de flujo de capital. Puede presentarse incluso dentro de una cartera de negociación, por ejemplo, al intentar vender una posición grande en el mercado o al operar en mercados con poca liquidez (como ocurre frecuentemente en mercados emergentes).

2.3 Conclusiones del capítulo

El segundo capítulo establece los fundamentos conceptuales necesarios para comprender la gestión del riesgo empresarial desde una perspectiva estructurada. A partir de una doble definición, riesgo como posibilidad de pérdida y como incertidumbre en los resultados, se construye una base sólida que permite articular un enfoque analítico y cuantificable del riesgo en la organización. Esta distinción no es meramente teórica, sino que condiciona las herramientas utilizadas, las decisiones estratégicas adoptadas y el tipo de gestión requerida en cada caso.

La pérdida esperada y la variabilidad de los resultados representan dos dimensiones distintas pero complementarias del riesgo, ambas relevantes para la toma de decisiones. Se introduce así la lógica de la cuantificación del riesgo mediante medidas como la probabilidad, el impacto, la desviación estándar o la varianza. Esto permite no solo clasificar los riesgos, sino también priorizarlos y evaluarlos en términos económicos y estratégicos. Esta aproximación será fundamental para el desarrollo posterior del modelo de valoración y del marco ERM.

El capítulo también presenta una clasificación detallada de los tipos de riesgos que pueden afectar a una empresa: riesgos operativos, financieros y de mercado. Cada uno de ellos incluye subcategorías que abarcan desde fallos en procesos internos hasta factores macroeconómicos. La sección dedicada al riesgo operativo resulta especialmente reveladora, al mostrar cómo aspectos tradicionalmente considerados menores, como errores humanos, deficiencias en la documentación o una cultura corporativa poco consciente del riesgo, pueden generar pérdidas significativas o incluso comprometer la viabilidad de la empresa. En este contexto, se destaca la importancia de la automatización, la prevención y el diseño de sistemas resilientes.

Asimismo, se exponen los riesgos financieros con una profundidad técnica que pone de relieve su complejidad y su interdependencia con otras áreas. Subtipos como el riesgo de crédito, las tasas de interés, la liquidez o los derivados financieros son analizados desde una óptica crítica, revelando tanto su impacto potencial como las dificultades que existen para modelarlos con precisión. En paralelo, los riesgos de mercado completan el panorama y evidencian que la exposición de las empresas no se limita a su operación interna, sino que también está condicionada por factores externos que, en muchos casos, no pueden ser controlados ni eliminados mediante diversificación.

En conjunto, este capítulo sienta las bases conceptuales y tipológicas necesarias para abordar la gestión del riesgo desde una perspectiva integral. Al definir con claridad qué se entiende por riesgo, cómo se

manifiesta y de qué manera se puede categorizar, se establece el marco indispensable sobre el que se apoyará el análisis posterior de su relación con la generación de valor y las herramientas estructuradas para su tratamiento.

Capítulo 3 El papel del riesgo en la generación de valor

Después de hablar sobre la compañía y el riesgo, y antes de empezar a desarrollar cómo crear e implementar una ERM, en este capítulo se relacionará el riesgo con la generación de valor en la empresa. La corporación tiene como objetivo último el beneficio, aunque no sea el único criterio aplicable a la hora de diseñar la estrategia, por lo que es importante tener una visión de cómo el riesgo afecta a la capacidad que tiene de generar ese valor que le proporcionará el beneficio. Se puede inferir de esto que la generación de valor es un paso necesario para cumplir con la misión lucrativa de la empresa, y para poder estudiar el valor se hará uso de un modelo de valoración usado ampliamente en la literatura financiera, el DCF (*discounted cash flow*) o flujo de fondos descontados. Según este modelo, el valor está determinado por el flujo de fondos esperado descontado de la firma, en el que la ratio de descuento es el coste del capital. Además, se explican los efectos directos e indirectos del riesgo en costes derivados de situaciones financieras complicadas, ampliaciones de capital o impuestos. Se analiza el papel de la transferencia del riesgo a otras entidades, bien a través de mecanismos tradicionales como los seguros, o mediante fórmulas alternativas conocidas como *Alternative Risk Transfer* (ART). Todo ello permite comprender cómo una gestión adecuada del riesgo no solo protege a la empresa, sino que puede contribuir activamente a incrementar su valor.

3.1 El modelo de valoración

El primer paso del modelo DCF es proyectar el flujo de fondos futuro de la empresa. Como anotación, el flujo de fondos de un periodo concreto es igual a los fondos que entran menos los que salen. Es importante no confundir con los ingresos contables, debido a que, a nivel contable, hay que tener en cuenta valores como las amortizaciones que no suponen un flujo de dinero, y que quedan fuera del modelo (Kruschwitz y Löffler, 2006).

El flujo de fondos en un periodo de tiempo *t* se denominará CF_t . Su valor es desconocido, por lo que existe una incertidumbre. Si embargo, se puede hacer una estimación, que se llamará $E(CF_t)$, que representa el valor esperado y el más probable. Si se representasen todos los valores que puede tomar el flujo de caja se obtendría una curva determinada (Figura 3.1).

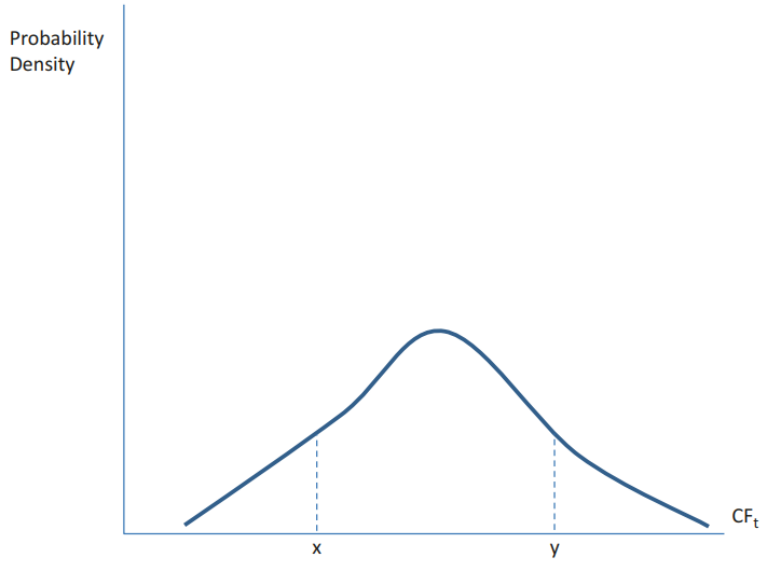

Figura 3.1: Ejemplo de curva con los valores posibles del flujo de caja. Fuente: Niehaus (2017)

En la Figura 3.1 se representa en el eje de abscisas los valores que puede tomar y en el eje de ordenadas la probabilidad de que los tome. El área bajo la curva tendría un valor de 1, puesto que el valor que se obtenga siempre estará entre los extremos de la propia curva.

Volviendo al modelo, habitualmente los periodos analizados son anuales, por lo que el primer periodo representará el próximo año; el segundo periodo, los dos próximos años… De esta manera, se pueden añadir periodos, habitualmente entre 5 y 10 en total, y después un último periodo terminal. Cada estimación está afectada por la ratio de descuento *r*, que es el coste del capital o la tasa de retorno requerida. Estas relaciones expresadas en Ecuación (1) quedarían:

$$Valor\ de\ la\ firma = \frac{E(CF_1)}{(1+r)^1} + \frac{E(CF_2)}{(1+r)^2} + \frac{E(CF_3)}{(1+r)^3} + \cdots \quad (1)$$

Cuando este valor de *r* es igual o superior a los retornos esperados de las inversiones es cuando los inversores pueden esperar beneficio. Por lo tanto, el coste del capital es igual ratio de retorno libre de riesgo más una prima de riesgo que refleja el riesgo de los flujos de caja (2)

$$r = retorno\ libre\ de\ riesgo + prima\ de\ riesgo \quad (2)$$

Uno de los puntos más importantes de todo esto es modelar correctamente la prima de riesgo.

3.2 El modelo para los riesgos como pérdidas

El modelo funciona para valorar el riesgo y cómo este impacta en el valor de la firma. A razón de esto, conviene recordar que hay dos definiciones de riesgo, siendo la primera la que se refiere a las pérdidas y la segunda a la incertidumbre. Por ejemplo, si una empresa tiene el riesgo de perder 50.000 € en un periodo determinado debido a compensaciones a los trabajadores, pero se gasta 20.000 € en equipamiento de seguridad y con ello mitiga ese riesgo por completo, se podría decir que el flujo de caja ha aumentado en 30.000 €. En este ejemplo queda claro que las decisiones orientadas a la prevención o al control de gastos tienen un efecto directo sobre la fórmula de valoración. El valor de estas decisiones viene dado por el hecho de que la reducción de las pérdidas estimadas es superior al coste de mitigarlas. En este contexto, se puede afirmar que una prevención efectiva en costes genera flujos de caja estimados (Niehaus, 2017).

3.3 El modelo para los riesgos como incertidumbre

Cuando el riesgo se refiere a la variabilidad o incertidumbre, es ligeramente más complejo de entender. En un primer momento, se puede intuir que un flujo de caja más variable se traducirá en una disminución en el valor de la firma. Sin embargo, esta conclusión de que mayor incertidumbre siempre disminuirá el valor debe ser modificada para considerar un principio financiero básico: el que los inversores pueden diversificar el riesgo de sus carteras teniendo valores diversos. Es decir, la mayoría de los inversores no tendrán una acción sencilla, sino que poseerán un número de acciones diferentes. De esta manera, si se obtiene un resultado desfavorable por parte de alguna de las firmas se puede contrarrestar con los resultados favorables de las otras. La diversificación del portafolio supone la eliminación de parte de la incertidumbre de una forma similar a la que las aseguradoras son capaces de reducir la incertidumbre del pago que tendrán que hacer a sus clientes a base de incluir una lista larga y detallada de cláusulas en la póliza. Uno de los requisitos para esta diversificación sea efectiva es que los retornos de los diferentes valores de portafolio no estén correlacionados entre sí. Cuando se

ejecuta de forma correcta, el riesgo no se transfiere, sino que se elimina; lo que explica por qué se recomienda diversificar la cartera de valores (Fraser, 2010).

No obstante, no todos los riesgos pueden diversificarse. Hay casos en los que los valores están afectados por factores comunes, lo que provoca que estén correlacionados positivamente y reduce la capacidad en la que se puede eliminar el riesgo. Esto significa en una cartera variada habrá algunos riesgos que se hayan podido eliminar mientras que otros permanecerán. El riesgo que permanece debido a estar causado por factores comunes es lo que se llama sistemático o de mercado, como se ha visto en el capítulo anterior, y no puede eliminarse a través de la diversificación.

La asociación entre la diversificación del portafolio y la valoración según el modelo es profunda y no sencilla de escrutar. La prima de riesgo en la fórmula del coste del capital no dependerá del riesgo específico de la firma. Esto significa que las acciones tomadas por la empresa para reducir sus riesgos específicos improbablemente influirán en la ratio de descuento que aparece en el denominador (Ecuación 1). En otras palabras, no se reducirá la prima de riesgo. Cualquiera podría concluir que las reducciones en los riesgos específicos de la firma no incrementarán su valor, sin embargo, esto no está garantizado. En algunos casos, la mitigación de riesgos puede aumentar el valor, de forma indirecta aumentando los flujos de caja. Aunque pueda parecer anti-intuitivo, el riesgo se está entendiendo como incertidumbre que puede tener un efecto tanto positivo como negativo, no como daño, y de ahí esta deducción.

Tras este análisis se apunta que la única forma de reducir el coste del capital es reducir la cantidad de riesgo que no es diversificable, el sistemático o de mercado. Sobre cómo hacerlo, la duda existe puesto que la estrategia expuesta no sirve en este caso, por lo que queda un camino: transferirlo. El coste de remunerar la contraparte por la transferencia del riesgo sistemático se compensará con el incremento de valor asociado a reducir el coste de capital. O eso debería ser, porque puede darse el caso en el que tanto el coste como el incremento se compensen entre sí, no generando ningún tipo de valor. De hecho, la transferencia de riesgos sistemáticos es improbable que aumente el valor de la firma (Niehaus, 2017).

En resumen, para este tipo de riesgo, ni las reducciones en riesgos específicos de la firma ni en riesgos de mercado es probable que aumenten el valor de la firma disminuyendo el coste del capital.

3.4 Efecto indirecto de la reducción de riesgo en el flujo de caja estimado

Para generar valor para la empresa a través de la gestión del riesgo, entendido como incertidumbre, el enfoque debe centrarse en los numeradores de la fórmula de valoración, dado que las acciones emprendidas en este ámbito difícilmente tendrán un impacto significativo sobre los denominadores (Ecuación 1). Las reducciones en la incertidumbre sí pueden aumentar los flujos de caja esperados a través de "efectos indirectos" debido a que la disminución en variabilidad en dichos flujos los aumentará indirectamente.

Habitualmente, disminuir la variabilidad haciendo uso de un seguro o una cobertura supondrá una disminución en el flujo de fondos debido a que el coste de estas actividades es elevado. Casi siempre las primas de seguros exceden los pagos que se puedan hacer dado el riesgo, es decir, que se paga más al seguro de lo que se obtiene de vuelta. La cantidad por la que la prima excede los pagos se conoce como recargo de prima y es el coste del aseguramiento. Aunque el efecto inmediato de los seguros o las coberturas es de reducir el flujo de caja estimado, existen posibles efectos positivos indirectos al reducir la variabilidad. Por ejemplo (Niehaus, 2017): dos casos. El caso A tiene una alta variabilidad mientras que el caso B tiene una baja variabilidad. Las operaciones en ambos son (Ecuaciones 3 y 4):

Caso A:

$$FC = \begin{cases} 900€ & prob\ 0{,}5 \\ -100€ & prob\ 0{,}5 \end{cases} \quad (3)$$

Caso B:

$$FC = \begin{cases} 450€ & prob\ 0{,}5 \\ 350€ & prob\ 0{,}5 \end{cases} \quad (4)$$

En ambos casos el flujo de caja estimado es de 400€, pero la variabilidad (riesgo) del caso A es muy superior al caso B, por lo que es posible que se obtenga un retorno mejor de la inversión, generando de forma indirecta, un aumento del valor. También hay que tener en cuenta que si el caso B es diversificable ambos casos tendrían el mismo valor.

3.5 Coste de las dificultades financieras

Supóngase, que la firma obtiene un resultado muy malo en su flujo de caja, llegando a ser negativo, lo que le impide hacerse cargo de sus deudas y dicta que se renegocien, lo que resulta costoso. Un flujo de caja muy malo puede hacer que la empresa tenga problemas financieros, por lo que, si consideramos estos costes, es posible que se prefiera el caso A (3) al B (4). Esto se debe a que el peor de los resultados posibles del caso B no solo incluye un valor negativo, sino que habría que sumarle los costes que irremediablemente se producirán debido al estado de dificultades financieras en el que entraría la empresa. La variabilidad por lo tanto en este caso es incluso, superior a la que se anticipaba. Esto apunta que reducir la incertidumbre puede incrementar los flujos de caja estimados de forma indirecta evitando incurrir en estos costes mencionados.

Los costes asociados a los problemas financieros se extienden más allá de renegociar la deuda (Fraser, 2010). Las compañías en esta situación lo tienen más difícil para negociar con proveedores, empleados y clientes. Además, la relación con estos grupos ya de por sí puede ser complicada. Todos querrán tener la seguridad de que la organización permanecerá el máximo tiempo posible, y si no se diese, pueden reaccionar de maneras diferentes:

- Proveedores: Si algún proveedor quisiese hacer una inversión para algún cliente, querrá también seguridad de que su cliente seguirá haciendo negocio con él durante muchos años para así obtener un retorno de la inversión. Por lo tanto, el proveedor exigirá a su cliente que posea algún tipo de seguro.
- Empleados: Si los empleados tienen dudas de si su empresa seguirá operando en el futuro próximo es más probable que acepten empleo en otra firma.
- Clientes: Si los clientes no tienen claro la persistencia de la compañía exigirán descuentos o dejarán de consumir sus productos/servicios. Esto es particularmente importante cuando el producto que se vende debe durar años, puesto que se pone en duda la capacidad de la empresa de responder ante cualquier problema o avería.

La conclusión es la siguiente: si la variabilidad aumenta las posibilidades de problemas financieros, reducirla a través de la gestión de riesgos puede incrementar el valor.

3.6 Costes de la ampliación de capital

Está ampliamente detallado en la literatura que ampliar el capital con capital externo es costoso y las firmas habitualmente prefieren usar fondos propios para financiar sus inversiones (Niehaus, 2017). Para ilustrar cómo los costes de la ampliación de capital pueden tener un papel en la toma de decisiones: hay una empresa que quiere arrancar un proyecto de 10 millones de euros del que se espera un beneficio neto de 1 millón. Es decir, se invertirán 10 millones y se obtendrán 11. Además, la decisión tiene que tomarse ya, o desaparecerá la oportunidad de realizar el proyecto. Si la compañía pudiese obtener el capital sin coste, sin duda emprendería el proyecto. Sin embargo, si los costes asociados a obtener este capital fuesen de 2 millones, la empresa decidiría no invertir en el proyecto. Si fuese posible, se intentaría usar fondos propios.

Sin embargo, los fondos de los que dispone la empresa son estimados también y, por lo tanto, sujetos a variabilidad. Si la empresa adopta una estrategia de alto riesgo obtendrá un flujo de caja de 6 o 18 millones. En caso de que se dé el segundo resultado contaría con los fondos para iniciar el proyecto, pero si se diese el primero, no podría. En cambio, si se adopta una estrategia de bajo riesgo obtendrá un flujo de 10 o 14 millones, lo que le permite asegurar tener fondos para invertir en el proyecto, sea cual sea el resultado, obteniendo un millón de valor generado por el proyecto. En consecuencia, una menor incertidumbre ofrece más garantías para obtener beneficio y aumentar el valor.

3.7 Impuestos

Otro factor afectado por la volatilidad son los impuestos que debe pagar la firma, debido a que estos están ligados a los beneficios que obtenga. Reducir la incertidumbre en los ingresos de la compañía tendrá un efecto en la incertidumbre sobre los impuestos a pagar, provocando un aumento del flujo de caja estimado. Un ejemplo para entender esto (Niehaus, 2017): los ingresos esperados de una empresa sin impuestos son 15 millones o -5 millones, por lo que el estimado es 5 millones. Los impuestos aplicables son del 40% para valores positivos y 0% para negativos, lo que implica que después de aplicarlos el flujo sea de 9 millones (15 x 0,6) o -5 millones. Ahora, el estimado es de 2 millones. Si la misma empresa usa una cobertura y consigue reducir su volatibilidad obtendrá un flujo de caja estimado sin impuestos de 8 millones o 2 millones, que sigue dando un estimado final de 5 millones. Cuando se aplican los impuestos, se obtienen valores de 4,8 y 1,2 millones, lo que da finalmente un estimado de 3 millones. Al compararlo con el obtenido antes de la cobertura, que era de 2 millones, se observa cómo la reducción en variabilidad puede generar valor para la empresa en materia de impuestos.

En resumen, gracias a reducir la variabilidad la firma puede aumentar su valor, sea a través de mejorar su capacidad de financiación, reducir su pago de impuestos o evitar necesitar capital externo.

3.8 Transferencia del riesgo

A lo largo del capítulo se ha ido mencionando el impacto que tiene transferir el riesgo mediante aseguramiento y coberturas en el valor de la empresa, por lo que, este punto tratará de recopilar información sobre las formas "habituales" de transferir el riesgo y se introducirá lo que se conoce como ART o "*Alternative Risk Transfer"* (también llamado "*unconventional risk transfer"*), como una forma novedosa de gestionar el riesgo. Cabe decir que entre los objetivos de este trabajo no está desarrollar en detalle este último tema en particular, que necesitaría dedicación completa por sí mismo.

3.8.1. **Transferencia convencional**

Existen muchas formas de clasificar el negocio del reaseguro; para simplificar, es común distinguir entre dos categorías de contratos y dos métodos. Por un lado, se diferencian el reaseguro facultativo y el reaseguro por tratado; por otro lado, el reaseguro proporcional y el no proporcional (también llamado "exceso de pérdida") (Pompella, 2017).

En el primer caso, la diferencia radica en que un acuerdo facultativo implica que cada riesgo se trata individualmente, lo que significa que el cedente tiene la facultad de decidir si cede un riesgo al reasegurador, y cuál. A su vez, el reasegurador tiene derecho a aceptar o rechazar la propuesta. En cambio, en el reaseguro por tratado u "obligatorio", todos los riesgos pertenecientes a ciertas categorías se ceden al reasegurador como un conjunto. Por ejemplo, todos los riesgos de vida o enfermedad asociados a tipos específicos de pólizas, o todos los riesgos del sector automotriz. En este tipo de contrato no se pueden excluir riesgos individuales.

En el segundo caso, la diferencia es bastante intuitiva. En el reaseguro proporcional, un porcentaje acordado del riesgo, medido por el límite máximo de cobertura, se transfiere del asegurador al reasegurador, junto con el mismo porcentaje de las primas. Por otro lado, el reaseguro no proporcional o exceso de pérdida solo entra en acción cuando se supera un límite de retención previamente definido en un valor monetario (no en porcentaje). Naturalmente, cuanto más alto es el límite de retención, menores son los costos del reaseguro. Los riesgos en exceso se ceden a un primer reasegurador, quien puede compartir su exposición con otro reasegurador o con varios a la vez (lo que se conoce como "capas verticales" y "capas horizontales", respectivamente).

En las coberturas proporcionales, es importante distinguir dos subtipos: cuota parte y excedente de suma asegurada (*surplus share*). El reaseguro proporcional por cuota parte funciona, desde el punto de vista del reasegurador, como un exceso expresado en porcentaje, que solo se diferencia de la franquicia por estar definido como un porcentaje (Figura 3.2). Esto significa que el asegurador conserva la responsabilidad de cubrir el riesgo hasta un límite de retención predeterminado, por ejemplo, el 25 %, mientras que el 75 % restante se transfiere al reasegurador. En el reaseguro por excedente, también existe un límite de retención, pero su función es distinta. Las reclamaciones por debajo de ese límite son responsabilidad del cedente, mientras que las que superan ese monto se ajustan de manera proporcional, en función de la relación entre el monto del riesgo total y la parte retenida por el asegurador (Pompella, 2017).

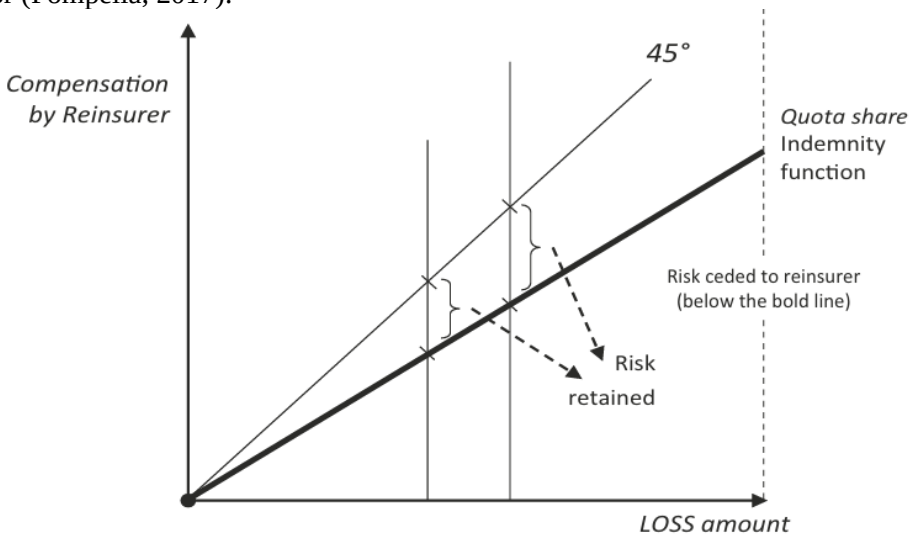

Figura 3.2: Reaseguro de cuota parte. Fuente: Pompella (2017)

3.8.2. *Alternative Risk Transfer* - ART

La transferencia alternativa de riesgos (*alternative risk transfer*, ART) no tiene una definición formal, pero puede entenderse en términos generales como un conjunto de productos de transferencia de riesgos no tradicionales. La mayoría de estos productos pueden clasificarse en dos categorías: vehículos no convencionales utilizados para cubrir riesgos tradicionales y vehículos basados en instrumentos de los mercados de capitales. El mercado de ART tiene sus raíces en una tendencia más profunda: la convergencia entre los mercados de capitales y la industria bancaria. Los productos de ART no pueden desarrollarse sin un alto grado de interacción entre la industria aseguradora y los mercados de capitales, interacción que tradicionalmente ha sido limitada (Lam, 2014).

Las estimaciones del sector reasegurador han sido históricamente poco fiables cuando se trata de riesgos nuevos o catastróficos, debido tanto a bases técnicas débiles como a la falta de series temporales extensas que permitan calcular probabilidades con precisión. Esto se debe a la relación inversa entre la severidad y la frecuencia de los siniestros: cuanto más graves, menos frecuentes, lo que complica su modelización. En consecuencia, las primas suelen basarse en el daño estimado, no en la probabilidad, lo que vuelve al sector vulnerable ante concentraciones ocasionales de eventos extremos. Cuando esto ocurre, el sistema entra en una fase procíclica de dificultad para asumir grandes riesgos y necesita tiempo para recobrar su capacidad financiera.

Como respuesta, surgió la "securitización" del riesgo puro, una innovación financiera que permitió a las aseguradoras mantener niveles de cobertura estables incluso cuando los reaseguradores tradicionales restringían su participación. Esto se logró recurriendo directamente al mercado en busca de capital, especialmente en momentos de tensión, cuando las primas se elevaban por encima de lo razonable o se reducía la oferta disponible, todo ello en un intento de preservar la solvencia del cedente (Pompella, 2017).

Las razones para que haya surgido ART son muchas más, y las estrategias para poder transferir el riesgo efectivamente son variadas y complejas. Sin embargo, esto deberá servir como una breve introducción al mundo que hay detrás de la transferencia no convencional de riesgos, y no como el objetivo del trabajo.

3.9 Conclusiones del capítulo

Este capítulo ha permitido establecer un vínculo claro entre la noción de riesgo y su influencia directa e indirecta sobre el valor de la empresa. A través del modelo de valoración por flujos de caja descontados (DCF), se ha evidenciado cómo la gestión del riesgo puede modificar tanto el numerador (los flujos de caja esperados) como el denominador (el coste del capital) de dicha fórmula.

En particular, se ha demostrado que la gestión de riesgos como pérdidas permite aumentar el valor de la firma cuando los costes de mitigación son inferiores a las pérdidas evitadas. Por otro lado, el análisis del riesgo como incertidumbre ha permitido profundizar en el papel que juega la variabilidad de los flujos de caja y la importancia de la diversificación para los inversores. Aunque la reducción del riesgo específico de una firma no afecta directamente al coste del capital, sí puede generar efectos positivos indirectos en los flujos de caja, como la reducción de costes financieros, fiscales o reputacionales.

Además, se ha analizado cómo ciertas estrategias, como la transferencia del riesgo mediante seguros o mecanismos alternativos (ART), pueden proteger el valor de la firma en entornos inciertos, aunque su impacto neto sobre la valoración dependerá del equilibrio entre el coste de la cobertura y los beneficios esperados.

En conjunto, este capítulo refuerza la idea de que una gestión del riesgo bien estructurada y alineada con la estrategia financiera de la empresa no solo reduce la exposición a pérdidas, sino que puede ser una palanca clave en la creación y preservación de valor a largo plazo.

Capítulo 4 Desarrollo e implementación de ERM

En los anteriores capítulos se ha expuesto lo que es la compañía, qué son los riesgos y cómo estos afectan a su objetivo último, que es el beneficio lucrativo. Especialmente en el anterior capítulo se ha visto el por qué una gestión de riesgos adecuada puede generar valor y, por lo tanto, ser una justificación para una aproximación ERM. La premisa principal de ERM es que los riesgos deberían ser gestionados a nivel empresarial, es decir, considerando el agregado de riesgo que afecta a la empresa. Para reducir los costes de problemas financieros o los costes de obtener capital externo, la compañía debería gestionar la incertidumbre asociada a su propio flujo de caja y valor de las acciones. Para reducir los impuestos sobre el beneficio, la compañía debería gestionar el beneficio imponible (Niehaus, 2017). La perspectiva ERM surge como solución para estas necesidades y en este capítulo se explorará todo lo relativo a su desarrollo, implementación, monitoreo y control.

4.1 ¿Qué es ERM?

El estudio de la gestión de riesgos (RM, *risk management*) existe desde el final de la Segunda Guerra Mundial. Las organizaciones siempre han gestionado riesgos, aunque a veces lo han hecho de forma subconsciente, implícita o inconsistente. La Gestión de Riesgos Empresariales (ERM) simplemente organiza las prácticas de gestión de riesgos dentro de un marco que permite a las organizaciones gestionarlos de manera más coherente y coordinada. Es importante entender la "E" en ERM. La ERM no se limita a una visión financiera del riesgo ni a una visión del riesgo en IT, sino que abarca una visión empresarial o de toda la organización en cuanto a la gestión de riesgos. Involucra a todo el personal y a todas las áreas y procesos de la organización, y se enfoca en todos los riesgos críticos. No se trata de una gestión de riesgos improvisada ni puntual (Wesioly & Moeller, 2020).

Este enfoque puede parecer abrumador para organizaciones más pequeñas, pero no tiene por qué ser así. Cuando las organizaciones pequeñas planifican y revisan sus estrategias y objetivos generales, y durante su operación diaria, pueden utilizar el mismo enfoque de gestión de riesgos que emplean las organizaciones más grandes.

De hecho, las organizaciones pequeñas y medianas tienen la ventaja de poder aprovechar prácticas operativas existentes, menores costos de coordinación y redes de comunicación interna más eficientes al desarrollar o mejorar sus capacidades de gestión de riesgos.

Como se ha mencionado, las organizaciones siempre han gestionado riesgos, pero organizar y mejorar sus prácticas de gestión de riesgos les permite abordarlos de manera más eficiente y eficaz. En la Figura 4.1 se puede ver los elementos a considerar, que serán enumerados a continuación. A la hora de empezar a gestionar los riesgos de manera formal lo primero es establecer el contexto externo e interno. Comprender el entorno en el que opera la organización, junto con las dinámicas externas (por ejemplo, requisitos regulatorios de cumplimiento, expectativas de clientes y partes interesadas, presiones económicas y de la competencia) y las dinámicas internas (por ejemplo, estructura de gobierno, cultura, objetivos estratégicos). Tras ello, los siguientes pasos son:

Identificación de riesgos: Comprender todos los riesgos que podrían afectar a la organización y que podrían impedirle alcanzar sus objetivos estratégicos y operacionales.

Evaluación/priorización de riesgos: Determinar la criticidad de los riesgos identificados estimando el impacto y la probabilidad de que dichos riesgos ocurran.

Respuesta al riesgo: Determinar las respuestas apropiadas para los riesgos críticos utilizando el enfoque MATE:

- Mitigar el riesgo para minimizar su impacto o probabilidad
- Aceptar el riesgo
- Transferir el riesgo (por ejemplo, mediante un seguro)
- Evitar el riesgo al no perseguir los objetivos subyacentes

Monitoreo del riesgo: Revisar continuamente los riesgos críticos utilizando indicadores clave de riesgo (KRI) para asegurarse de que no aumenten a niveles inaceptables y que los controles funcionen como se espera. También revisar el entorno cambiante para detectar riesgos emergentes.

Informe de riesgos: Comunicar toda la información relevante sobre los riesgos (incluido el perfil de riesgo de la organización) a todas las partes interesadas clave de manera oportuna.

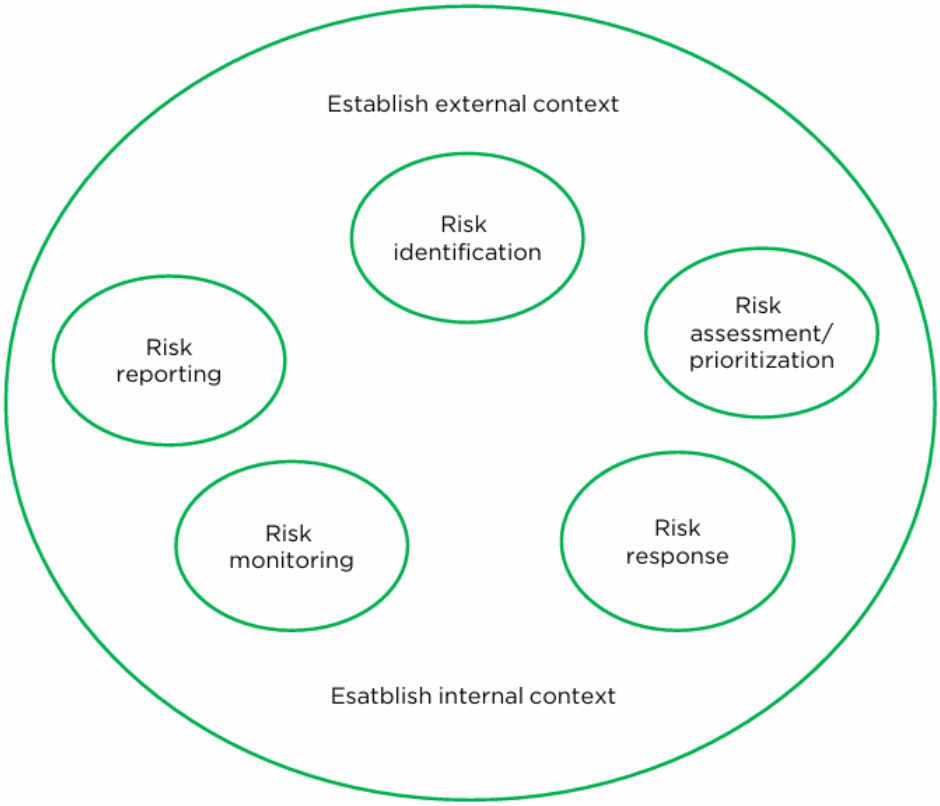

Figura 4.1: Representación de los elementos para una correcta gestión del riesgo, incluyendo una pequeña errata en el epígrafe de abajo "*establish internal context*". Fuente: Wesioly & Moeller (2020)

4.2 COSO ERM *framework*

El marco COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) constituye un modelo de referencia ampliamente reconocido en el ámbito de la gestión de riesgos empresariales y el control interno. Desde su formulación inicial en 1992 y su posterior actualización en 2017, este

marco ha proporcionado una estructura integral que permite a las organizaciones identificar, evaluar y gestionar eficazmente los riesgos que pueden afectar el logro de sus objetivos estratégicos y operativos.

La iniciativa COSO fue creada en 1985 por cinco organizaciones profesionales estadounidenses con el propósito de mejorar la calidad de la información financiera y mitigar el fraude corporativo. En 1992, se publicó el documento *Internal Control – Integrated Framework*, que se convirtió en el estándar predominante para la evaluación y mejora de los sistemas de control interno. En 2004, se introdujo el enfoque ampliado de ERM – *Integrated Framework* (COSO ERM), orientado a una gestión integral de riesgos. La versión más reciente, publicada en 2017, refuerza la necesidad de alinear la gestión de riesgos con la estrategia y el desempeño organizacional (GlobalSuite Solutions, 2023).

La versión 2017 del marco COSO ERM se estructura en torno a cinco componentes interrelacionados (Figura 4.2):

- Gobierno y cultura: Proporciona los fundamentos para una gestión de riesgos sólida, incluyendo la definición de valores, normas éticas, cultura organizacional y la asignación de roles y responsabilidades.
- Estrategia y establecimiento de objetivos: Asegura la integración de la gestión de riesgos en los procesos estratégicos, estableciendo el apetito de riesgo y formulando objetivos alineados con dicho umbral.
- Desempeño: Implica la identificación, evaluación y priorización de riesgos en función de su severidad, así como la selección de respuestas apropiadas para mitigar su impacto potencial.
- Revisión y monitoreo: Permite evaluar continuamente el entorno interno y externo, así como el desempeño de los controles implementados, ajustando las estrategias de gestión de riesgos conforme a los cambios identificados.
- Información, comunicación y reporte: Facilita el flujo efectivo de información relevante sobre los riesgos en todos los niveles organizacionales y hacia las partes interesadas clave, favoreciendo una toma de decisiones informada.

Este enfoque estructurado favorece una visión holística y proactiva de la gestión de riesgos, incrementando la capacidad organizacional para anticipar amenazas, aprovechar oportunidades y asegurar una mayor resiliencia frente a entornos cambiantes.

Figura 4.2: Componentes de la gestión de riesgos según COSO. Fuente: COSO (2017)

El marco COSO se ha consolidado como una herramienta esencial en la gestión de riesgos y control interno dentro del entorno empresarial actual. Su adopción ha sido impulsada por la creciente complejidad regulatoria y la necesidad de transparencia en la información no financiera. En España, muchas organizaciones han optado por implementar el marco COSO III, emitido en 2013, para garantizar que los cinco componentes de control interno operen de manera coordinada, especialmente en la supervisión de la información no financiera (Pérez & Contreras, 2021).

La presión regulatoria, como la Directiva sobre Información Corporativa en Materia de Sostenibilidad (CSRD) de la Unión Europea, ha llevado a que aproximadamente 6.000 empresas españolas estén obligadas a reportar sobre sus impactos ambientales, sociales y de gobernanza (ESG), lo que ha incrementado la necesidad de estructuras de control interno robustas como las que ofrece el marco COSO.

Además, la implementación del marco COSO facilita a las organizaciones la construcción de indicadores de medición y propicia la rendición de cuentas, aspectos fundamentales en la gestión de riesgos relacionados con factores ambientales, sociales y de gobernanza (ASG).

4.3 Componentes y principios COSO

El marco COSO se organiza en torno a 5 componentes, y estos a su vez se subdividen en principios (Figura 4.3). En esta sección se expondrán los principios incluidos en cada componente siguiendo la guía de *Committee of Sponsoring Organizations of the Treadway Commission* (2020).

4.3.1. Gobierno y cultura

Principio 1: Ejerce la supervisión de riesgos del Consejo.
El primer principio resalta la importancia de que el consejo de administración supervise activamente los riesgos de cumplimiento y el programa de ética y cumplimiento. Se recomienda que esta supervisión pueda ser delegada a un comité especializado que mantenga contacto directo y regular con el *Chief Risk Officer* (CRO). Este contacto debe incluir reuniones privadas entre el CRO y el consejo, sin la presencia de la alta dirección, garantizando independencia y transparencia. Además, se subraya la necesidad de contar con recursos adecuados, autoridad suficiente y experiencia específica dentro del consejo.

Figura 4.3: Componentes y principios del marco COSO. Fuente: COSO (2017)

Principio 2: Establece estructuras operativas.
El segundo principio aborda la necesidad de establecer estructuras operativas que permitan la autonomía y eficacia del programa de cumplimiento. El CRO debe tener un estatus organizativo equiparable al de otros líderes funcionales y contar con independencia funcional respecto a departamentos como legal o finanzas. Se aconseja que esta función reporte directamente al consejo, y que se establezcan políticas claras, procedimientos documentados, y protocolos para la escalada de eventos significativos de riesgo.

Principio 3: Define la cultura deseada.
El tercer principio se enfoca en la cultura organizacional, subrayando que el compromiso con el cumplimiento debe comenzar en los niveles más altos y permear toda la estructura empresarial. Se propone incorporar el cumplimiento en los códigos de conducta, la evaluación del desempeño y los sistemas de incentivos. Asimismo, se promueve la adopción de métricas de cumplimiento y la realización de evaluaciones culturales periódicas.

Principio 4: Demuestra compromiso con los valores fundamentales.
El cuarto principio detalla el compromiso con los valores fundamentales, que debe manifestarse en la conducta de los líderes, en la rendición de cuentas y en la gestión coherente de incidentes. El tono "desde arriba" debe traducirse en ejemplos concretos de integridad, y se deben adoptar mecanismos que protejan a los informantes de represalias, refuercen la justicia organizacional y apliquen sanciones proporcionales a las faltas.

Principio 5: Atrae, desarrolla y retiene a personas capaces.
Por último, el quinto principio trata sobre la atracción, desarrollo y retención de individuos capacitados. El marco subraya la importancia de contratar personas éticas y con conciencia de cumplimiento, realizar procesos de selección con diligencia, y desarrollar a los empleados mediante formación específica. También se destaca la necesidad de definir claramente las posiciones que implican "autoridad sustancial", para evitar designaciones inadecuadas que pongan en riesgo a la organización.

4.3.2. **Estrategia y establecimiento de objetivos**

Principio 6: Análisis del contexto empresarial.
La gestión eficaz del riesgo de cumplimiento comienza con una profunda comprensión del contexto interno y externo de la organización. El marco destaca que las decisiones estratégicas pueden generar nuevos riesgos de cumplimiento, modificar los existentes o incluso eliminarlos. Se recomienda la participación activa del CRO en el proceso de formulación de la estrategia, para anticipar y mitigar riesgos derivados de los cambios estratégicos. Entre los impulsores internos más relevantes se incluyen cambios en personas, procesos y tecnología, así como presiones de gestión mal alineadas con la ética. A nivel externo, destacan los marcos legales y regulatorios, las dinámicas económicas, la competencia y factores políticos o sociales, todos los cuales pueden alterar significativamente el perfil de riesgo de cumplimiento.

Principio 7: Definición del apetito de riesgo.
Este principio aborda la necesidad de discutir abiertamente el nivel de riesgo de cumplimiento que una organización está dispuesta a asumir. Aunque no se trata de aceptar infracciones deliberadas, se reconoce que eliminar completamente el riesgo es imposible. El apetito de riesgo debe considerarse de forma diferenciada por tipo de riesgo, unidad de negocio o región geográfica. La evaluación del apetito debe alinearse con los objetivos empresariales y revisarse periódicamente para adaptarse a cambios en el entorno de cumplimiento.

Principio 8: Evaluación de estrategias alternativas.
La toma de decisiones estratégicas; como fusiones, adquisiciones o expansiones, puede implicar riesgos significativos de cumplimiento. Por ello, se recomienda que el CRO tenga voz activa en la evaluación de estas alternativas. Esto permite realizar la debida diligencia con enfoque en el cumplimiento desde etapas tempranas, identificar riesgos heredados y preparar adecuadamente la integración del programa de cumplimiento. Asimismo, durante la implementación estratégica, se sugiere ajustar controles internos, planes de formación, monitoreo y auditoría, según los riesgos detectados.

Principio 9: Formulación de objetivos empresariales.
La fijación de objetivos medibles es esencial para alinear la estrategia con el cumplimiento. En este proceso, el área de cumplimiento debe estar involucrada para garantizar que los incentivos no fomenten conductas contrarias a la normativa. Se pone como ejemplo el riesgo de que metas agresivas de producción puedan llevar a omitir controles de calidad. Además, se recomienda establecer el cumplimiento como objetivo empresarial independiente, si no está ya integrado en otros. La función de cumplimiento también debe definir sus propios indicadores clave de desempeño (KPIs, *Key Performance Indicators*), tales como tasas de finalización de formación, tiempos de respuesta ante incidentes, o resultados de auditorías internas.

4.3.3. **Desempeño**

Principio 10: Identificación del riesgo.
Destaca la importancia de identificar sistemáticamente los riesgos de cumplimiento a los que está expuesta la organización. Dada la creciente complejidad normativa, es fundamental contar con procesos documentados que permitan rastrear riesgos nuevos, existentes y emergentes. Se recomiendan métodos como entrevistas con personal clave, análisis de procesos, uso de indicadores, y consultas con comités de cumplimiento. La identificación debe considerar tanto regulaciones vigentes como cambios esperados, implicaciones del uso de terceros, y señales derivadas de mecanismos de denuncia o investigaciones internas.

Principio 11: Evaluación de la severidad del riesgo.
En él se establece que cada riesgo debe analizarse en términos de probabilidad e impacto, tanto desde la perspectiva de cumplimiento legal como desde la ética organizacional. La severidad no solo se refiere a sanciones regulatorias, sino también al daño reputacional o a la pérdida de confianza por parte de los grupos de interés. Además, es importante valorar los controles existentes y su eficacia al momento de estimar el riesgo residual.

Principio 12: Priorización del riesgo.
Este establece la necesidad de clasificar los riesgos según su criticidad. Esto permite asignar recursos limitados de forma eficiente. Algunos riesgos, aunque no sean prioritarios a nivel global (ERM), pueden serlo para el programa de cumplimiento debido a su efecto en la cultura organizacional. La priorización debe facilitar la focalización de medidas correctivas, planes de formación y esfuerzos de supervisión.

Principio 13: Implementación de respuestas al riesgo.
En él se promueve una respuesta estructurada y alineada a cada riesgo identificado. Las respuestas pueden incluir mitigación, aceptación, transferencia o evitación. El documento subraya que la responsabilidad no debe recaer exclusivamente en la función de cumplimiento, sino que debe involucrar a los dueños del riesgo, auditoría interna y otras funciones. El plan de respuesta debe especificar responsables, métricas de éxito, y mecanismos de seguimiento.

Principio 14: Desarrollo de una visión de cartera.
Finalmente, este insiste en la importancia de observar los riesgos de forma integrada, considerando cómo interactúan entre sí. Por ejemplo, un control reforzado para reducir un riesgo de cumplimiento podría generar demoras operativas y afectar otros procesos. Esta visión holística ayuda a identificar conflictos o sinergias entre controles, y permite consolidar riesgos a nivel organizacional, evaluando su efecto agregado.

4.3.4. **Revisión y monitoreo**

Principio 15: Evaluar cambios significativos.
Este principio enfatiza que los cambios en la organización; como modificaciones en los objetivos estratégicos, transformaciones tecnológicas, cambios en la estructura de personal o en los procesos, pueden alterar rápidamente el perfil de riesgos de cumplimiento. Asimismo, factores externos como nuevas normativas, cambios regulatorios, presiones sociales o expectativas éticas emergentes también impactan significativamente. El CRO debe identificar de forma proactiva estos impulsores del cambio y adaptar el programa en consecuencia. Se recomienda utilizar herramientas tecnológicas para la gestión del cambio normativo, y establecer canales de monitoreo que permitan actuar con agilidad frente a estos cambios.

Principio 16: Revisión del riesgo y del desempeño.
Este principio destaca que la revisión de riesgos prioritarios y del desempeño del programa de cumplimiento no solo proporciona garantías al consejo directivo y a la alta dirección, sino que también constituye una vía de mejora continua. Las expectativas regulatorias establecen que los programas de cumplimiento deben evaluarse periódicamente. La revisión debe incluir tanto la evaluación de los riesgos con mayor probabilidad e impacto, como la revisión del desempeño general del programa. Para ello, se recomienda emplear auditorías internas, mecanismos de retroalimentación (como líneas de denuncia) y planes de monitoreo estructurados.

Principio 17: Impulsar la mejora continua.
La mejora del programa de cumplimiento debe ser un objetivo constante. La revisión periódica puede ser realizada por el propio equipo de cumplimiento, por auditoría interna o por consultores externos. En cualquier caso, el análisis debe verificar si el programa incorpora todos los elementos fundamentales de un sistema eficaz de cumplimiento y si estos están funcionando correctamente. También recomienda utilizar guías como la del Departamento de Justicia de EE.UU. (*Evaluation of Corporate Compliance Programs*) para valorar si el programa está bien diseñado, si se implementa de forma efectiva y si funciona en la práctica.

4.3.5. **Información, comunicación y reporte**

Principio 18: Aprovechamiento de la información y la tecnología.
Para que la función de cumplimiento sea efectiva, debe tener acceso oportuno a información relevante sobre cada elemento del programa de cumplimiento y ética. La tecnología cumple un rol esencial en múltiples aspectos del programa, incluyendo la formación en cumplimiento, que puede entregarse a través de métodos interactivos y flexibles que mejoran el aprendizaje. También es clave en el monitoreo y auditoría mediante análisis de datos, capaces de examinar la totalidad de las transacciones y detectar patrones de incumplimiento o fallos en los controles internos. Además, la tecnología facilita la evaluación preliminar de denuncias internas y permite a los gestores acceder a paneles de control adaptados a sus unidades de negocio, mejorando la capacidad de respuesta ante incidentes.

Principio 19: Comunicación de la información sobre riesgos.
La comunicación se presenta como la columna vertebral del programa de cumplimiento. La función de cumplimiento debe relacionarse con todas las áreas de la organización, actuando como socio estratégico en la identificación y gestión de riesgos éticos y regulatorios. Se enfatiza la necesidad de una comunicación bidireccional entre las unidades operativas y el área de cumplimiento, lo que garantiza soluciones prácticas y contextualizadas. Las comunicaciones deben adaptarse a los distintos niveles: desde mensajes generales emitidos por la alta dirección, hasta contenidos específicos transmitidos por supervisores. Estas pueden adoptar diversas formas como emails, reuniones, cartelería, eventos, y deben reforzar los contenidos de las formaciones formales. Se resalta la importancia de establecer un protocolo de escalado para denuncias, especialmente en casos graves o que involucren a personal directivo.

Principio 20: Reporte sobre riesgos, cultura y desempeño.
El reporte eficaz es esencial para demostrar la efectividad del programa de cumplimiento. Debe incluir evaluaciones de riesgo, métricas relevantes, incidentes investigados, asignación de recursos, y medidas adoptadas. El reporte dirigido al consejo debe enfocarse en la supervisión del programa global, mientras que el dirigido a gerentes operativos debe ser más detallado y funcional. También se deben abordar aspectos de la cultura organizacional, utilizando encuestas, entrevistas o grupos focales para identificar tendencias y percepciones. Además, se destaca la necesidad de generar informes sobre la gestión de riesgos con terceros (proveedores, agentes, etc.), detallando controles, visitas, auditorías y capacitaciones. Por último, la documentación rigurosa de investigaciones es imprescindible para garantizar la trazabilidad, especialmente ante potenciales acciones legales o investigaciones regulatorias.

4.4 Proceso

Cabe señalar que el marco COSO, con sus componentes estructurales y principios detallados, constituye una referencia de gran utilidad para la gestión del riesgo empresarial. Sin embargo, es importante subrayar que su adopción no es obligatoria. Se trata de una herramienta de carácter voluntario que orienta a las organizaciones en la construcción de un sistema ERM sólido y alineado con la estrategia corporativa. Su valor reside en proporcionar una estructura conceptual robusta que permite integrar el cumplimiento normativo, la ética y el desempeño organizacional bajo un enfoque transversal de gestión del riesgo. No obstante, cada empresa debe adaptar su aplicación a sus circunstancias particulares. A continuación, se presenta el proceso propuesto para desarrollar e implementar dicho sistema en el contexto específico de la organización objeto de este trabajo. Hay seis pasos para implementar (o mejorar) eficazmente un programa de gestión de riesgos. El tiempo para implementar el programa puede variar generalmente de uno a tres años, dependiendo de las prácticas existentes de gestión de riesgos de la organización, su cultura de riesgos, tamaño y complejidad (Wesioly & Moeller, 2020).

Estos pasos no tienen que seguirse secuencialmente. De hecho, puede haber momentos en los que el líder de gestión de riesgos de una organización pueda llevar a cabo dos o tres de estos pasos al mismo tiempo.

Paso 1
Involucrar a la junta directiva y/o alta dirección: Para que el programa de gestión de riesgos sea exitoso, es imprescindible que la junta directiva y/o la alta dirección comprendan su valor y estén comprometidos con él.

Paso 2
Establecer elementos de gobernanza de riesgos: Como en cualquier función organizacional, es importante proporcionar algunas directrices internas para gestionar los riesgos. Formalizar un apetito por el riesgo, una política de riesgos y responsabilidades proporciona dicha orientación.

Paso 3
Realizar una evaluación de riesgos y controles con la junta directiva y/o alta dirección: La dirección debe comprender los riesgos críticos de la organización y gestionarlos adecuadamente.

Paso 4
Involucrar al personal: Dado que "el riesgo es asunto de todos", es importante que todo el personal comprenda los riesgos. Comunicar las prioridades de riesgo y obtener retroalimentación es esencial para gestionarlos adecuadamente.

Paso 5
Aumentar el valor de la gestión de riesgos: Una vez que se han establecido o mejorado las prácticas fundamentales, las organizaciones deben seguir monitoreando los riesgos y considerar pasos adicionales de monitoreo y reporte.

Paso 6
Integrar las prácticas de gestión de riesgos: El verdadero valor de la gestión de riesgos está en mantener a los miembros de la organización involucrados en decisiones operativas y estratégicas clave. Alinear la gestión de riesgos con la planificación y la estrategia permite lograr esto.

4.4.1. **Compromiso de la dirección**

El primer paso para implementar un programa de gestión de riesgos es conseguir compromiso con el propio programa por parte de la junta y/o de la gerencia senior. No todas las empresas tienen que organizarse de la misma forma, como se explicó en el Capítulo 1. Por lo tanto, es indispensable adaptarse a la estructura ejecutiva para conseguir en primera instancia el apoyo de la dirección y en última, del resto de empleados.

En muchos casos, la junta y/o la gerencia senior no conocerán en profundidad los riesgos que afectan a la empresa y cómo gestionarlos. Es imperativo conseguir un lenguaje común para compartir entre todos. Una formación básica sobre riesgos asegurará que todas las partes tengan un entendimiento sólido sobre las prácticas de gestión de riesgos. En esta sesión formativa se deberían incluir los siguientes puntos (Wesioly & Moeller, 2020):

- Definiciones de riesgo y gestión de riesgos
- Beneficios del ERM
- Estado actual y ejemplos relevantes de riesgos y sus subsecuentes impactos en empresas similares o del mismo sector
- Buenas prácticas
- Responsabilidades y expectativas de gobierno de la junta, la dirección y el personal

Tras la formación, es importante asegurar el compromiso de la junta al programa de gestión de riesgos. Los participantes deberían salir de la sesión con un entendimiento básico de los conceptos y prácticas propios de dicha gestión. A continuación, hay que asegurar que la gestión de riesgos estará incluida en la agenda de la junta y es imperativo que esta permanezca en la agenda durante la implementación de un programa de gestión de riesgos y a medida que las operaciones retoman su estado estable.

4.4.2. **Establecer elementos de gobernanza de riesgos**

Puede parecer prematuro implementar un programa de gestión de riesgos, pero establecer ahora elementos de gobernanza como el apetito de riesgo, una política de riesgos y las responsabilidades de riesgo sentará las bases para el resto del proceso posteriormente. Estos elementos de gobernanza de riesgos pueden revisarse y desarrollarse a lo largo de la implementación (Wesioly & Moeller, 2020).

4.4.2.1 Apetito de riesgo

Una declaración de apetito de riesgo define cuánto riesgo está dispuesta a aceptar una organización al perseguir sus objetivos. Definir el apetito de riesgo significa evaluar todos los posibles riesgos que enfrenta una organización, establecer los límites para incidentes aceptables e inaceptables y crear los controles necesarios que estos límites exigen (Chapelle, 2019). Tener determinado cuánto riesgo está la empresa dispuesta a asumir para realizar sus operaciones será crítico para la toma de decisiones. El apaetito de riesgo que la dirección determine afectará a la hora de decidir. Este tema se desarrollará en mayor detalle en el Capítulo 6, sin embargo, en este punto se introducirá el concepto.

Este concepto puede ilustrarse a través de una inversión financiera: es posible optar por una alternativa arriesgada, con potencial de generar grandes beneficios o pérdidas significativas; o bien por una segura, que ofrezca un rendimiento menor, pero con escaso o nulo riesgo de pérdida. La elección entre una o la otra depende del apetito de riesgo de quien toma la decisión. Las declaraciones de apetito de riesgo son aún más útiles cuando se combinan con las tolerancias al riesgo, que definen umbrales y límites para asumir riesgos. Esto permite a las organizaciones monitorear mejor los riesgos y recibir alertas cuando alguna actividad o evento se acerque o supere esos límites (Wesioly & Moeller, 2020).

4.4.2.2 Política de riesgos

Una política de gestión de riesgos proporcionará orientación para desarrollar e implementar prácticas de gestión de riesgos en toda la organización. La política y su estructura variarán de una organización a otra, dependiendo de la naturaleza del negocio y de sus activos. Los siguientes componentes básicos deben estar incluidos (Wesioly & Moeller, 2020):

- propósito u objetivos de la política
- definiciones de riesgo y de gestión de riesgos
- tipos generales de riesgos o categorías de riesgo que afectan a la organización
- visión general de las prácticas de gestión de riesgos y los componentes del marco
- roles y responsabilidades en la gestión de riesgos (incluyendo consejo y comités, si los hay)
- referencias a otras políticas y/o normas relacionadas

La política de gestión de riesgos debe actuar como la política marco general bajo la cual se alinean las demás políticas y normas relacionadas con riesgos de la organización (por ejemplo, gestión de continuidad del negocio, seguridad de la información). Además, para que la política de gestión de riesgos sea efectiva, debe ser revisada periódicamente y adaptarse a los cambios en el entorno operativo, normativo o estratégico de la organización.

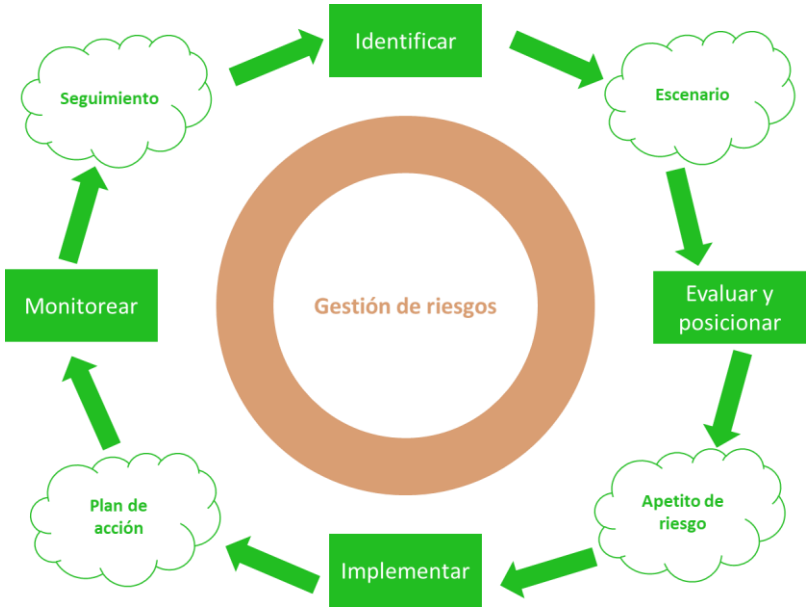

Figura 4.4: Pasos para implementar la gestión de riesgos. Fuente: *Instituto Brasileiro de Governança Corporativa* (2017)

4.4.2.3 Responsabilidades de riesgo

Definir claramente las responsabilidades en la gestión de riesgos ayuda a garantizar que todos los ejecutivos y el personal comprendan sus funciones. Deberían establecerse responsabilidades para:

- El consejo de administración: por su rol de supervisión de la gestión de riesgos. Tanto la norma ISO más reciente como el estándar COSO ERM destacan la creciente presión para que los consejos reconozcan y ejerzan adecuadamente esta función de supervisión.
- Comités de riesgos: por su rol de supervisión, en caso de que exista un comité de este tipo.
- Alta dirección: por sus funciones en la definición de la estrategia y en la gestión de riesgos.
- Gerentes de línea y personal: por su responsabilidad en la ejecución de las prácticas aprobadas de gestión de riesgos y en la implementación de respuestas al riesgo (por ejemplo, controles internos), así como en la provisión de aportes prácticos durante los procesos de revisión.

Es posible que las organizaciones más pequeñas no cuenten con esta configuración detallada, pero debería existir una distinción entre las funciones de supervisión y gestión (Wesioly & Moeller, 2020).

4.4.3. Evaluación de riesgos

La evaluación de riesgos en el contexto del modelo de implementación de gestión de riesgos corporativos consiste en un proceso estructurado y sistemático que permite identificar, analizar y priorizar los riesgos que puedan afectar los objetivos estratégicos de una organización. Esta evaluación se enmarca dentro de una metodología holística que integra factores tanto internos como externos, y se apoya en la comprensión del entorno organizativo, la determinación del apetito de riesgo y el establecimiento de criterios claros para valorar la probabilidad y el impacto de los eventos de riesgo. A través de herramientas como matrices de riesgo, análisis de escenarios y consultas a expertos, el

modelo proporciona una base sólida para la toma de decisiones informadas y la asignación eficiente de recursos en función de los riesgos identificados (*Instituto Brasileiro de Governança Corporativa*, 2017). Los pasos propuestos son: identificar, evaluar, implementar y monitorear (Figura 4.4).

4.4.3.1 Identificar y clasificar

El primer paso consiste en identificar y clasificar los riesgos a los que está expuesta la organización. Este proceso debe ser continuo y estructurado, y tiene como objetivo anticiparse a eventos que puedan afectar el cumplimiento de los objetivos estratégicos. Para identificar los riesgos, se pueden emplear diversos métodos como entrevistas, talleres, análisis de procesos y revisión documental. Una vez identificados, los riesgos deben clasificarse de acuerdo con criterios como su naturaleza (financieros, operativos, sistemáticos, etc.), su origen (interno o externo), o su impacto en la estrategia corporativa. Esta clasificación permite una comprensión más profunda de los riesgos y facilita su evaluación posterior. El uso de matrices de riesgo u otras herramientas visuales es recomendado para organizar y priorizar los riesgos de forma eficiente.

4.4.3.2 Evaluar

El segundo paso consiste en evaluar los riesgos previamente identificados y clasificados. Esta evaluación tiene como objetivo determinar el grado de exposición de la organización ante cada riesgo, lo cual se logra analizando dos variables principales: la probabilidad de ocurrencia y el impacto potencial en caso de que el evento se materialice. Este método, ampliamente utilizado y descrito en la bibliografía es compatible con una representación gráfica que se conoce como matriz de probabilidad-impacto (Figura 4.5). En ella, se añaden valores para la probabilidad y el impacto que se multiplican entre sí, obteniendo un número que puede usarse para priorizar los riesgos más importantes. Cada empresa debe decidir qué valores obtenidos considera que representan un riesgo menor, importante o crítico.

La evaluación puede realizarse mediante enfoques cualitativos, cuantitativos o mixtos, dependiendo del nivel de madurez de la organización y de la disponibilidad de datos. La matriz de la Figura 4.5 se consideraría mixta, puesto que se valoran aspectos cualitativos y se cuantifica con números. Esta información permite priorizar aquellos que requieren mayor atención o intervención. Un ejemplo de enfoque cualitativo sería esta misma matriz sin valores y un enfoque puramente cuantitativo sería la simulación de Monte Carlo. Además, se destaca la importancia de considerar tanto el riesgo inherente (sin controles) como el riesgo residual (después de aplicar controles existentes), así como de establecer criterios de tolerancia al riesgo para guiar la toma de decisiones estratégicas.

4.4.3.3 Implementar

En el tercer paso se aborda la implementación efectiva de la función de gestión de riesgos junto con una estructura adecuada de controles internos. Esta etapa tiene como finalidad asegurar que los riesgos priorizados durante la evaluación sean tratados de forma sistemática y que se establezcan los mecanismos de control necesarios para mitigar su impacto y probabilidad.

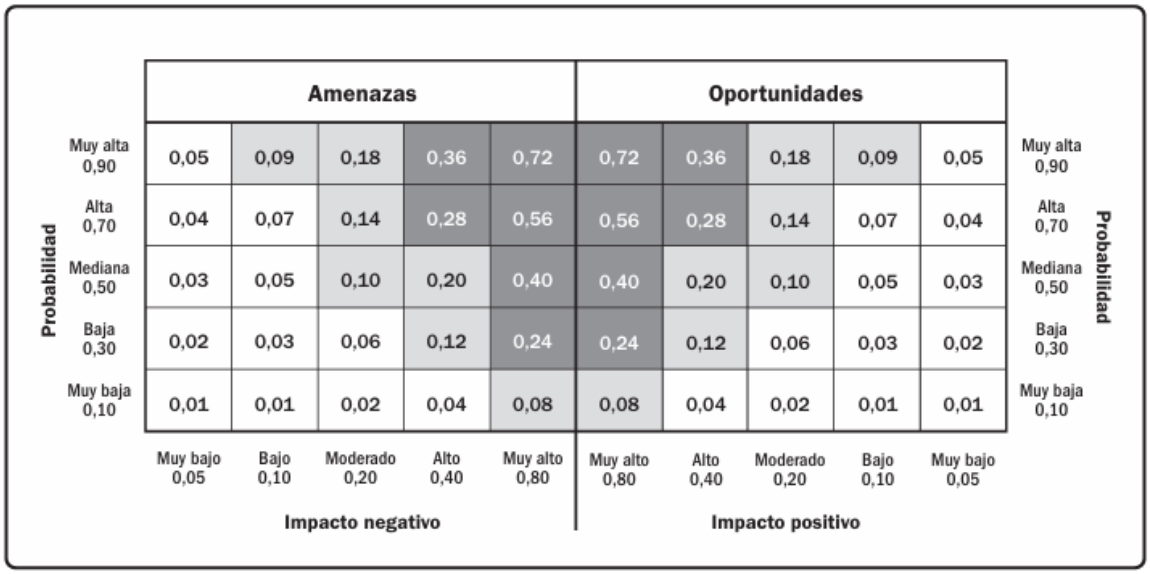

Figura 4.5: Matriz probabilidad-impacto. Fuente: *Project Management Institute* (2017)

Se subraya la importancia de definir claramente responsabilidades, procesos, herramientas y reportes relacionados con la gestión de riesgos. Se recomienda establecer una estructura organizacional específica, como comités y unidades dedicadas, y promover la integración de la gestión de riesgos en la cultura corporativa. Además, se enfatiza que la función de gestión de riesgos debe estar alineada con otras funciones clave como auditoría interna, cumplimiento, finanzas y operaciones, fomentando una visión integral del riesgo. También se debe contar con políticas y procedimientos documentados, así como con un sistema de seguimiento continuo y reporte periódico, para garantizar la eficacia del sistema de control.

4.4.3.4 Monitorear

El cuarto paso es el monitoreo continuo del proceso de gestión de riesgos y de los controles internos implementados. Este monitoreo tiene como objetivo verificar la eficacia de las acciones adoptadas, garantizar la actualización constante del perfil de riesgos y facilitar la toma de decisiones basada en información confiable y oportuna.

Hay tres componentes clave del monitoreo:

- Definir indicadores de desempeño: se deben establecer métricas para medir la efectividad de los controles y la evolución de los riesgos. Estos indicadores permiten identificar desviaciones y oportunidades de mejora.
- Elaborar informes periódicos: se recomienda preparar y comunicar informes de riesgos y controles de forma regular, dirigidos a los distintos niveles de la organización, especialmente a la alta dirección y al consejo de administración.
- Registrar y cuantificar pérdidas: es fundamental documentar los eventos de riesgo que se materialicen, cuantificando sus consecuencias financieras y no financieras. Esta información retroalimenta el sistema y fortalece la capacidad de aprendizaje organizacional.

El monitoreo no es un proceso aislado, sino un mecanismo permanente y transversal que asegura la mejora continua del sistema de gestión de riesgos.

4.4.4. **Involucrar al personal**

Tras haber formado a la junta y al equipo de directivos en todo a lo que la gestión de riesgos respecta, el siguiente paso es involucrar al resto de la organización. El objetivo es crear conciencia sobre las prácticas de gestión de riesgos, recopilar perspectivas únicas y facilitar que se sumen a este nuevo método de trabajo.

Conseguir esto brinda muchas oportunidades a la hora de identificar riesgos y para crear registros adicionales. La identificación realizada a bajo nivel jerárquico por parte del personal puede aportar riesgos no identificados por la junta o el equipo directivo, lo que tiene sentido debido a que la cúpula de la compañía debe estar más preocupada del ámbito estratégico y no tanto del operativo. Es posible que algunas compañías piensen que no es necesario hacer este tipo de trabajo con los empleados de bajo nivel, pero se pueden perder riesgos importantes y crear otros, como generar descontento entre los empleados por su exclusión en un proceso tan importante. Es indispensable ganarse la confianza de los miembros de la corporación. Entender el impacto humano en este proceso es esencial, tanto como apoyarse en prácticas de gestión del cambio (Deszca, 2020).

El éxito del cambio está ligado también a la formación continua de los empleados. Ofrecer educación en la gestión de riesgos “a pie de campo” puede ser una parte importante de esta formación. Ligar los conceptos abstractos que se ha explicado a la junta con ejemplos o aplicaciones prácticas para el día a día del personal aumenta las posibilidades de que realicen la gestión de riesgos que se espera de ellos. A parte de formación básica, se pueden dar sesiones sobre temas concretos que hayan sido identificados como necesarios, como códigos de conducta, privacidad, seguridad, fraude… Este alcance formativo mayor puede promover el diálogo, las soluciones y la capacidad de resolución de problemas; además de compartir experiencias.

4.4.5. **Aumentar el valor**

Una vez consolidadas las prácticas fundamentales, la gestión de riesgos debe orientarse hacia su perfeccionamiento continuo, a fin de garantizar su adecuación a las necesidades cambiantes de la organización. Esta etapa implica la revisión periódica del marco de gestión y la incorporación de herramientas que refuercen tanto el análisis como el monitoreo y la comunicación de riesgos.

En primer lugar, resulta útil emplear metodologías que permitan vincular visualmente los eventos de riesgo con sus causas y consecuencias. Una estructura eficaz para este fin es el modelo de "riesgo *bow tie*" (Figura 4.6), que facilita la identificación de causas raíz y la formulación de controles preventivos y correctivos, con el objetivo de mantener los riesgos dentro del apetito definido por la organización. En la Figura 4.6 se observa la identificación del evento crítico, que constituye el eje central del análisis. Posteriormente, se realiza una evaluación de las causas raíz, situadas en el lado izquierdo del diagrama. En el caso de la rotación de personal altamente cualificado, estas causas pueden incluir factores como la falta de desafíos laborales o una gestión ineficaz. La implementación de controles preventivos, como evaluaciones de desempeño de 360 grados o programas de formación para mandos intermedios, puede contribuir a reducir la probabilidad de ocurrencia. En el lado derecho del diagrama se analizan las consecuencias del evento, que en este caso podrían implicar la pérdida significativa de conocimiento organizacional. Para mitigar estos efectos, resultan adecuados los controles correctivos tales como programas de formación cruzada continua y la sistematización documental de procesos y procedimientos clave. Esta aproximación no solo facilita la comprensión del riesgo, sino que permite definir de forma más precisa las medidas de prevención y respuesta necesarias para mantenerlo dentro del umbral de tolerancia aceptable.

Por otra parte, el seguimiento de los riesgos debe fortalecerse mediante la definición de indicadores clave de riesgo (KRIs). Estos indicadores permiten evaluar en tiempo real el desempeño de las medidas de control implementadas y anticipar desviaciones que puedan comprometer los objetivos estratégicos u operativos. La integración de KRIs predictivos y retrospectivos contribuye a una vigilancia más precisa y oportuna.

Finalmente, es fundamental contar con informes de riesgo estructurados que articulen, de manera clara y periódica, los principales riesgos, los indicadores asociados, el estado de las medidas de mitigación y la evolución de la exposición global de la organización. Este ejercicio de reporte facilita la toma de decisiones informadas y refuerza la rendición de cuentas ante los órganos de gobierno (Wesioly & Moeller, 2020).

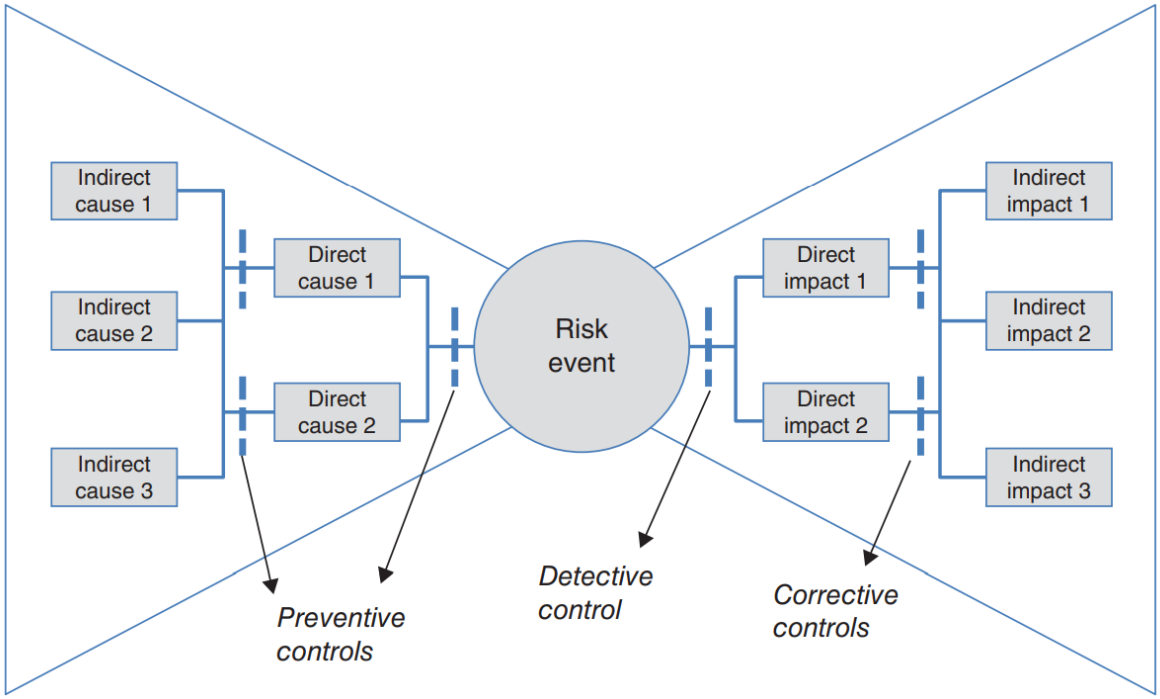

Figura 4.6: Ejemplo de riesgo bow tie. Fuente: Chapelle, (2019)

4.4.6. **Integrar las prácticas de gestión de riesgos**

La etapa final del proceso consiste en consolidar la gestión de riesgos como una parte integral de la cultura organizacional y de los procesos de toma de decisiones estratégicas y operativas. Esta integración se manifiesta cuando las consideraciones sobre riesgos son incorporadas de manera sistemática en la planificación, la evaluación de nuevos proyectos y la mejora continua de productos y servicios.

La alineación entre gestión de riesgos y planificación estratégica resulta esencial. Dado que los riesgos representan incertidumbres que pueden afectar el logro de los objetivos institucionales, es necesario que los procesos de planificación contemplen explícitamente su identificación, análisis y tratamiento. Cuestiones como la viabilidad de las estrategias, la capacidad operativa o los riesgos reputacionales deben ser objeto de análisis desde una perspectiva anticipatoria.

Asimismo, la preparación ante eventos extremos o de baja probabilidad, pero alto impacto, conocidos como "*worst case scenarios*", requiere de ejercicios sistemáticos de simulación y análisis. Estos permiten evaluar la resiliencia organizacional y determinar la eficacia de los controles existentes, así como la necesidad de implementar mecanismos adicionales de continuidad operativa, gestión de crisis y recuperación ante desastres.

Finalmente, la evaluación del sistema de gestión de riesgos debe realizarse de manera periódica. Esta evaluación abarca tanto aspectos cualitativos, como el nivel de compromiso de los órganos de gobierno o la calidad de las decisiones estratégicas como aspectos cuantitativos, tales como la reducción de eventos inesperados o la mejora en la previsibilidad de los resultados. La revisión continua y la comparación con prácticas de referencia en el sector permiten identificar oportunidades de mejora y asegurar la evolución del sistema hacia mayores niveles de madurez y eficacia (Wesioly & Moeller, 2020).

4.5 Conclusiones del capítulo

Este capítulo presenta el paso decisivo desde la conceptualización del riesgo hacia su gestión práctica dentro de la empresa. A través del análisis del modelo de gestión integral del riesgo, *Enterprise Risk Management* (ERM), se establece una metodología estructurada que permite a las organizaciones identificar, evaluar, responder y monitorear los riesgos que afectan a su capacidad para crear y preservar valor. Lejos de entender el riesgo como un fenómeno aislado, el enfoque ERM propone integrarlo de forma transversal en los procesos estratégicos y operativos de la compañía.

Se dedica una atención especial al marco COSO, ampliamente adoptado tanto en el entorno académico como profesional. Este marco se estructura en cinco componentes principales que incluyen el gobierno y la cultura corporativa, la formulación estratégica, la evaluación del desempeño, la revisión continua y los procesos de comunicación y reporte. Cada uno de estos elementos no solo define responsabilidades y funciones, sino que también establece principios orientadores que garantizan la coherencia y eficacia del sistema de gestión del riesgo. El marco COSO no se limita a identificar amenazas, sino que también promueve una cultura de riesgo alineada con los objetivos generales de la organización.

El capítulo también aborda con detalle el proceso de implementación de un sistema ERM. Se destacan etapas clave como el compromiso de la dirección, el establecimiento de la gobernanza de riesgos, la identificación y clasificación de amenazas, y la necesidad de integrar a todo el personal en una lógica común de prevención y respuesta. Este enfoque integral busca evitar que la gestión del riesgo se convierta en una función aislada o simbólica, y en su lugar se integre como una herramienta útil para la toma de decisiones y la mejora del desempeño empresarial.

Otro punto destacado es la relación entre la gestión del riesgo y la creación de valor. Lejos de representar únicamente un mecanismo defensivo, el ERM se presenta como un recurso estratégico que permite anticipar oportunidades, mejorar la resiliencia de la empresa y reforzar la confianza de los grupos de interés. La gestión del riesgo se vincula así a la eficiencia operativa, la asignación óptima de recursos y la sostenibilidad de la estrategia empresarial a largo plazo.

En conjunto, el capítulo ofrece una visión clara y estructurada de cómo debe diseñarse, organizarse e interiorizarse la gestión del riesgo en la empresa moderna. Más allá de las herramientas concretas o las métricas específicas, lo que se plantea es un cambio de enfoque, en el que el riesgo deje de ser una amenaza periférica para convertirse en un eje fundamental de la planificación y el gobierno corporativo.

Capítulo 5 Riesgos clave para la empresa: ESG, fraude, corrupción.

En el entorno actual, cada vez más exigente desde el punto de vista regulatorio, social y reputacional, las organizaciones deben adoptar una visión estratégica de los riesgos que enfrentan. La gestión del riesgo ha dejado de centrarse exclusivamente en variables financieras para integrar nuevas dimensiones que afectan de manera directa a la sostenibilidad del negocio. Este capítulo aborda tres tipologías de riesgo que, por su impacto potencial y transversalidad, deben ser consideradas prioritarias por la alta dirección: los riesgos relacionados con factores ESG (ambientales, sociales y de gobernanza), el fraude y la corrupción.

Los riesgos ESG han ganado protagonismo en los últimos años, impulsados por una mayor presión de los inversores, los consumidores y los reguladores. Factores como el cambio climático, las condiciones laborales en la cadena de suministro o la composición de los órganos de gobierno corporativo ya no pueden ser gestionados como elementos externos o secundarios. Su integración en los procesos de toma de decisiones empresariales es clave para anticiparse a crisis reputacionales, evitar sanciones regulatorias y fortalecer la confianza de los grupos de interés.

Por su parte, el fraude representa un riesgo estructural que afecta a la calidad de la información financiera, la transparencia organizativa y la confianza en la empresa. La existencia de incentivos mal diseñados, culturas organizativas permisivas o sistemas de control poco efectivos pueden favorecer comportamientos oportunistas que, si no se detectan a tiempo, derivan en daños económicos y legales considerables. Comprender las motivaciones individuales y los factores organizativos que propician este tipo de conductas es esencial para desarrollar una prevención eficaz.

Finalmente, se analizará el riesgo de corrupción, tanto en su dimensión interna como en relación con terceros. Este tipo de riesgo es especialmente relevante en organizaciones con operaciones internacionales o en sectores con alta interacción con administraciones públicas. Se presentarán los principales estándares internacionales en materia de cumplimiento anticorrupción y se abordarán los elementos clave de los programas de integridad corporativa. A través de esta revisión, se propone dotar a la empresa de herramientas para reducir su exposición, responder con eficacia y consolidar una cultura ética sólida como ventaja competitiva.

5.1 Riesgos ESG: definición y relevancia

Los riesgos ESG, por sus siglas en inglés (*Environmental, Social and Governance*), son aquellos vinculados al entorno natural, a las condiciones sociales y laborales, y a la gobernanza corporativa. Estos riesgos tienen la capacidad de afectar de forma directa o indirecta a los resultados económicos, la reputación, la operativa y, en última instancia, a la supervivencia de las organizaciones. A diferencia de los riesgos tradicionales, los ESG poseen una naturaleza más compleja, interconectada y en muchos casos más difícil de cuantificar, lo que ha contribuido históricamente a que se infravaloren en los procesos de toma de decisiones estratégicas (WBCSD, 2018).

La dimensión ambiental comprende amenazas relacionadas con el cambio climático, la escasez de recursos naturales, la contaminación, la gestión de residuos o la pérdida de biodiversidad. Estos riesgos, aunque puedan parecer lejanos o abstractos, ya están afectando directamente a sectores clave como la agricultura, la energía o la logística, a través de fenómenos como sequías extremas, tormentas más violentas o la interrupción de cadenas de suministro. La creciente presión normativa y social por reducir las emisiones contaminantes y por adoptar prácticas sostenibles está haciendo que las empresas que no se adapten sufran no solo penalizaciones legales, sino también un deterioro de su imagen y una pérdida de competitividad.

La dimensión social abarca aspectos que van desde las condiciones laborales, la igualdad de oportunidades y los derechos humanos hasta la relación con las comunidades locales o la salud y seguridad de empleados y consumidores. A medida que las sociedades se vuelven más conscientes y exigentes con las prácticas de las empresas, los riesgos sociales se han convertido en un factor determinante para conservar la llamada licencia social para operar. La falta de control sobre la cadena de suministro, los escándalos por explotación laboral o las prácticas discriminatorias pueden desembocar en boicots, litigios o pérdida de clientes, generando impactos difíciles de revertir.

Por último, la dimensión de gobernanza hace referencia al marco normativo y ético bajo el que opera una organización. Aquí se incluyen temas como la transparencia, la composición y funcionamiento del consejo de administración, la gestión de conflictos de interés, las prácticas fiscales o la prevención de corrupción. Aunque los riesgos de gobernanza han sido tradicionalmente más reconocidos en la gestión empresarial, su relación directa con los riesgos ambientales y sociales ha ganado relevancia en los últimos años. Una gobernanza débil no solo favorece el fraude o la mala conducta, sino que además impide una gestión efectiva y coherente del resto de los riesgos ESG.

En definitiva, lo que hace relevantes a los riesgos ESG no es únicamente su contenido, sino su capacidad de generar consecuencias sistémicas. Son riesgos que no se limitan a un único departamento ni a un periodo corto de tiempo. Pueden desencadenar crisis reputacionales, legales y operativas que se amplifican entre sí y erosionan el valor de la empresa de forma profunda y duradera. Por esta razón, su comprensión y gestión ya no es una opción ni una cuestión de imagen, sino una necesidad estratégica (WBCSD, 2018).

5.2 Identificación y priorización de riesgos ESG

Identificar y priorizar adecuadamente los riesgos ESG es un paso fundamental para que una organización pueda anticiparse a los impactos potenciales y tomar decisiones estratégicas bien fundamentadas. Sin embargo, este proceso presenta particularidades que lo distinguen de la gestión de riesgos convencionales. Por un lado, muchos de estos riesgos tienen un carácter emergente o poco tangible, lo que dificulta su detección con las herramientas habituales. Por otro lado, su naturaleza transversal y a menudo prolongada en el tiempo complica su evaluación inmediata en términos económicos.

Una de las primeras tareas necesarias es construir un inventario de riesgos que integre adecuadamente los factores ESG en todas las áreas de la empresa. Para ello, se pueden emplear distintos enfoques complementarios. Entre los más útiles se encuentra el análisis de megatendencias, que permite detectar grandes fuerzas de cambio en el entorno como el calentamiento global, la automatización del trabajo o la transformación demográfica. También es útil realizar un mapeo de impactos y dependencias, donde se analice en qué medida la actividad de la empresa afecta o depende de determinados recursos naturales o condiciones sociales. Otra herramienta habitual es el análisis DAFO, que ayuda a relacionar debilidades internas con amenazas del entorno, muchas de las cuales pueden estar vinculadas a factores ESG (WBCSD, 2018).

Un aspecto clave de este proceso es el conocimiento interno. A menudo, los riesgos ESG no se identifican adecuadamente porque el personal encargado de la gestión de riesgos no dispone del nivel de especialización suficiente en materias como derechos humanos, biodiversidad o impacto social. Por este motivo, es recomendable fomentar la colaboración activa entre los equipos de sostenibilidad y los responsables de riesgos, de forma que los primeros puedan aportar una visión especializada y ayudar a traducir estos desafíos en riesgos que afecten a los objetivos estratégicos de la empresa.

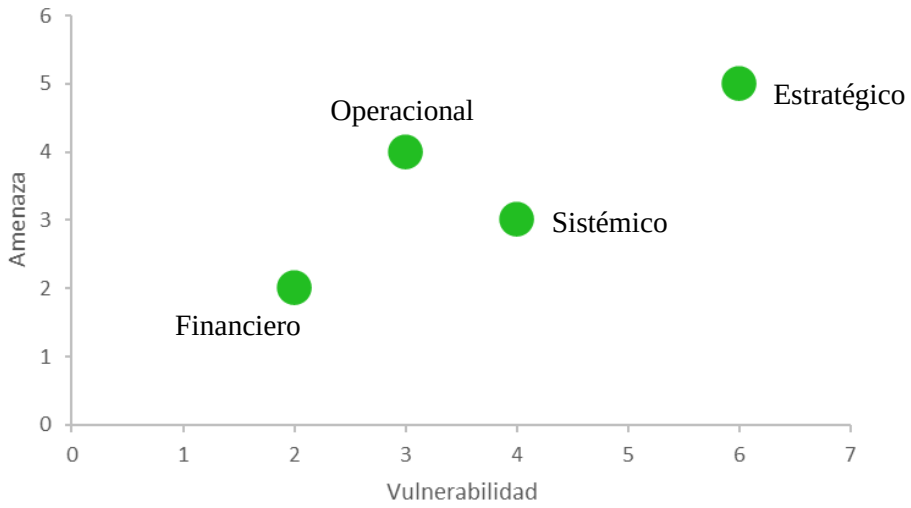

Figura 5.1: Ejemplo de matriz de amenaza y vulnerabilidad. Fuente: Traducido de WBSCD (2018)

Una vez identificados, es necesario priorizar los riesgos ESG en función de su severidad y probabilidad, una forma recomendada es usando "*heat-maps*" o la matriz de probabilidad-impacto (Figura 4.5). Además de este método, WBCSD (2018) proponen usar matrices de amenaza y vulnerabilidad (Figura 5.1), en las que se represente de forma gráfica el impacto y velocidad de riesgos individuales para la empresa (amenaza) y la capacidad de adaptación y recuperación de la empresa (vulnerabilidad). En este punto, muchas organizaciones se enfrentan a un reto importante: la falta de datos cuantitativos y la dificultad de proyectar impactos en el largo plazo lleva a infravalorar o descartar riesgos que en realidad pueden ser críticos. Por ejemplo, un riesgo climático como la escasez de agua puede parecer irrelevante en el corto plazo, pero tener un efecto devastador sobre la operativa de una compañía en cinco o diez años. Para evitar esta incertidumbre, es fundamental incorporar métricas cualitativas, conocimiento experto y escenarios prospectivos en la evaluación.

La priorización también debe estar alineada con el apetito de riesgo de la empresa y con su estrategia corporativa. No todos los riesgos requieren la misma atención ni los mismos recursos. Por tanto, es esencial establecer criterios claros y coherentes que permitan decidir cuáles deben abordarse de forma urgente y cuáles pueden ser monitorizados a medio plazo. En cualquier caso, lo que no puede permitirse una organización es ignorar riesgos solo porque no sean fácilmente medibles. La experiencia ha demostrado que muchos de los grandes escándalos empresariales recientes no se debieron a riesgos imprevistos, sino a riesgos conocidos que fueron mal evaluados o relegados por considerarse secundarios (WBSCD, 2018).

5.3 Estrategias de respuesta ante riesgos ESG

Una vez que los riesgos ESG han sido correctamente identificados y priorizados, el siguiente paso es determinar cómo responder a ellos de manera eficaz. La forma en que una empresa actúe ante estos riesgos no solo define su capacidad de resistencia, sino también su potencial para diferenciarse en el mercado. A diferencia de los riesgos tradicionales, las respuestas ante riesgos ESG suelen requerir un enfoque más amplio, que combine medidas preventivas, acciones correctoras, adaptaciones estructurales y, en muchos casos, transformaciones culturales profundas.

La prevención es la primera línea de defensa. Implica modificar procesos, políticas y comportamientos para evitar que los riesgos lleguen a materializarse. Por ejemplo, una empresa con una cadena de suministro expuesta a prácticas laborales deficientes puede revisar sus criterios de selección de proveedores, exigir auditorías independientes y establecer cláusulas contractuales que garanticen el cumplimiento de estándares éticos. En el ámbito ambiental, prevenir puede suponer invertir en tecnologías limpias, optimizar el uso de recursos o rediseñar productos para reducir su huella ecológica.

Cuando la prevención no es suficiente, la organización debe ser capaz de mitigar los impactos negativos. Esto incluye reducir la severidad de los efectos una vez que el riesgo se ha manifestado. Un ejemplo sería un plan de respuesta ante desastres naturales que minimice el tiempo de inactividad o los daños a los empleados y las infraestructuras. También puede implicar campañas de comunicación transparentes y rápidas para proteger la reputación y recuperar la confianza de los grupos de interés.

En algunos casos, el riesgo no puede evitarse completamente. Es entonces cuando la empresa debe adaptarse. Adaptarse significa modificar la estrategia o el modelo de negocio para operar de forma viable en un nuevo contexto. Por ejemplo, las compañías del sector energético están incorporando cada vez más fuentes renovables no solo por presión regulatoria, sino también como respuesta a los cambios en la demanda social y la evolución tecnológica. En el ámbito social, adaptarse puede suponer adoptar modelos laborales más inclusivos o crear productos que respondan a nuevas sensibilidades éticas y culturales.

No todas las respuestas deben concebirse como defensivas. Algunos riesgos ESG ofrecen oportunidades estratégicas si se abordan de forma proactiva. Identificar tendencias emergentes en sostenibilidad o cambios en la regulación ambiental puede permitir a una empresa posicionarse como líder en su sector y acceder a nuevos mercados, atraer capital responsable o mejorar su marca empleadora. En este sentido, la gestión de riesgos se convierte en un motor de innovación y creación de valor.

Para que estas estrategias sean eficaces, es necesario que estén respaldadas por una evaluación rigurosa del coste y beneficio de cada alternativa. Tomar decisiones informadas implica considerar no solo los impactos financieros inmediatos, sino también los efectos a largo plazo sobre la reputación, la resiliencia operativa y la licencia para operar. Las respuestas deben ser proporcionales al riesgo, coherentes con la estrategia empresarial y ejecutables con los recursos disponibles. Asimismo, deben ser evaluadas y revisadas periódicamente para adaptarse a la evolución del entorno.

Responder adecuadamente a los riesgos ESG no es únicamente una cuestión técnica. Requiere voluntad, liderazgo y una visión clara del papel que la empresa quiere desempeñar en la sociedad. Aquellas organizaciones que integren este enfoque en sus procesos de decisión estarán mejor preparadas para afrontar los desafíos del presente y aprovechar las oportunidades del futuro.

5.4 El fraude corporativo: causas y facilitadores

El fraude corporativo, especialmente aquel vinculado a la manipulación intencionada de la información financiera, representa una de las amenazas más graves a la integridad y sostenibilidad de las organizaciones. No solo pone en riesgo los resultados económicos de una empresa, sino que también compromete la confianza de los inversores, la estabilidad del mercado y la legitimidad institucional. El impacto del fraude trasciende lo contable; puede desatar consecuencias legales, dañar de forma profunda la reputación corporativa y desestabilizar la cultura organizacional.

Una de las aproximaciones más extendidas para entender por qué se produce el fraude es el llamado triángulo del fraude (Figura 5.2), propuesto originalmente por Cressey (1950), adaptado por Dorminey y colaboradores (2012) y ampliamente adoptado por la profesión auditora. Este modelo identifica tres condiciones necesarias para que se produzca un acto fraudulento: la presión o incentivo que impulsa a la persona a actuar, la oportunidad que le permite llevar a cabo la acción sin ser descubierto, y la actitud o racionalización que justifica moralmente el comportamiento ante sí mismo. En el contexto empresarial, estas condiciones se manifiestan con frecuencia: la presión puede venir de la exigencia de resultados financieros; la oportunidad, de deficiencias en los controles internos; y la racionalización, de un clima organizativo permisivo o de convicciones éticas laxas.

Dorminey et *al*. (2012) amplían, además, este modelo clásico incorporando tres elementos adicionales: el acto delictivo, la ocultación y la conversión del beneficio (Figura 5.2). Según esta visión, el fraude no es un suceso aislado, sino un proceso compuesto de acciones concretas para ejecutar la falsificación, mecanismos deliberados para ocultarla y estrategias para obtener un beneficio, ya sea económico, reputacional o profesional. Esta ampliación permite entender mejor los esquemas más complejos de fraude contable, donde intervienen múltiples actores y se requiere una planificación coordinada.
A nivel individual, se han identificado numerosos factores que predisponen a una persona a participar en un fraude. Entre ellos destacan la presión económica, la ambición desmedida, la percepción de impunidad o la existencia de rasgos de personalidad como el narcisismo o la impulsividad. Desde la psicología social, teorías como la disonancia cognitiva o las técnicas de neutralización explican cómo los individuos pueden justificar internamente actos ilícitos, minimizando el conflicto moral. Algunos estudios incluso señalan que ciertos directivos presentan una menor tolerancia al fracaso y una mayor propensión a tomar decisiones de alto riesgo para proteger su estatus o sus beneficios personales (Trompeter *et al*., 2013).

Pero el fraude no es solo responsabilidad de individuos concretos. El entorno organizacional desempeña un papel fundamental en su génesis. Estructuras de gobierno corporativo débiles, culturas orientadas únicamente al logro de objetivos financieros, sistemas de incentivos mal diseñados y ausencia de mecanismos efectivos de supervisión son condiciones que favorecen tanto la aparición como la perpetuación del fraude. En muchos casos, no se trata de una única persona actuando en solitario, sino de redes de colusión entre miembros de la alta dirección y personal clave, que aprovechan su posición para manipular los registros contables, anular controles o desinformar deliberadamente a los auditores (Palmer, 2009).

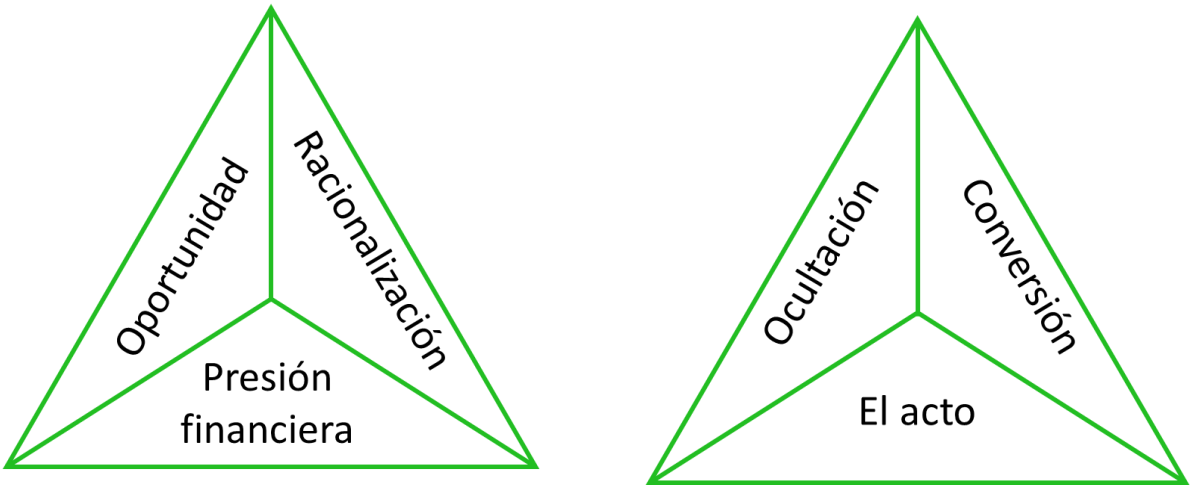

Figura 5.2. Izquierda: Triángulo del fraude. Derecha: Triángulo de la acción fraudulenta. Fuente: Traducido de Dorminey *et al*. (2012)

Comprender estas causas y factores facilitadores no solo permite identificar mejor los riesgos de fraude, sino que también es un primer paso para construir entornos organizativos más íntegros y resilientes. Las empresas deben asumir que el fraude no es un fenómeno excepcional, sino un riesgo latente que puede materializarse cuando convergen ciertas condiciones personales, estructurales y culturales.

5.5 Medidas antifraude y percepción del riesgo

El control del fraude dentro de una organización no depende únicamente de la existencia de normas o procedimientos formales, sino también de cómo estos son percibidos, aplicados y reforzados en la práctica. Una de las ideas centrales recogidas en la literatura es que los controles internos, por sólidos que sean en su diseño, solo resultan efectivos si son percibidos como tales por los posibles infractores. En este sentido, la percepción del riesgo de ser detectado se convierte en un elemento disuasorio tan importante como la existencia objetiva de medidas antifraude.

Según el modelo ampliado propuesto por Trompeter *et al*. (2013), los controles internos y los mecanismos de gobernanza deben evaluarse no solo por su arquitectura técnica, sino por su capacidad real de reducir las oportunidades de que se cometa y oculte un fraude. Este enfoque incluye elementos como la independencia del consejo de administración, la calidad de la auditoría interna, la existencia de canales de denuncia efectivos, y el llamado "tono en la cima" o compromiso ético del liderazgo. Un entorno organizativo que tolera irregularidades menores incentiva prácticas agresivas o resta importancia a los controles puede terminar por erosionar el sistema en su conjunto, abriendo la puerta a comportamientos más graves.

Un aspecto clave es que los defraudadores no actúan únicamente sobre la base de controles objetivos, sino sobre su interpretación de la efectividad de esos controles. Así, una empresa puede contar con mecanismos sofisticados de supervisión, pero si estos no se comunican adecuadamente o no se aplican con rigor, el riesgo persiste. Este desfase entre el diseño y la implementación real de las medidas antifraude es especialmente peligroso en contextos donde la alta dirección tiene capacidad para ejercer presión o anular los controles existentes mediante prácticas como la colusión o el *override* (Van de Bunt, 2010).

Además de los sistemas internos, existen factores externos que pueden reforzar las defensas de una organización frente al fraude. Entre ellos se encuentran la regulación pública, la presión ejercida por los inversores institucionales, el escrutinio de los medios de comunicación y la acción de organismos supervisores. En conjunto, estos elementos conforman un ecosistema que puede incrementar la transparencia, fortalecer la rendición de cuentas y reducir la impunidad. Sin embargo, su efectividad también está condicionada por el contexto cultural y jurídico en el que opera la empresa. En entornos donde la corrupción está normalizada o la justicia es ineficiente, incluso los controles más avanzados pueden resultar insuficientes.

La auditoría externa desempeña un papel clave en este entramado. Su doble función, como mecanismo de detección y como instrumento disuasorio, ha sido ampliamente estudiada. La presencia de una auditoría rigurosa puede modificar el cálculo de riesgos del potencial defraudador, elevando su percepción del peligro de ser descubierto. No obstante, Trompeter *et al*. advierten que este efecto depende en gran medida de la calidad del trabajo de auditoría, del grado de escepticismo profesional aplicado, y del uso de herramientas adecuadas para la evaluación del riesgo de fraude. Sesiones de *brainstorming* (o lluvia de ideas), análisis de indicadores no financieros y contraste de explicaciones ofrecidas por la dirección son algunas de las técnicas que han demostrado ser útiles para identificar señales de alerta.

La integración efectiva de controles, cultura y percepción del riesgo requiere, por tanto, un enfoque multidimensional. No basta con diseñar normas o aplicar procedimientos. Las organizaciones deben fomentar un entorno en el que el fraude no solo sea difícil de ejecutar, sino también inconcebible desde un punto de vista ético y cultural. Solo así se podrá reducir de forma significativa la probabilidad de que estas conductas se materialicen.

5.6 Respuesta empresarial al riesgo de fraude

El fraude corporativo no debe entenderse únicamente como una desviación ética o un problema de cumplimiento, sino como un riesgo estratégico de primer orden. Su materialización puede comprometer la sostenibilidad de la empresa, afectar de manera irreversible su reputación, destruir valor económico y desencadenar responsabilidades legales para los directivos y el órgano de gobierno. En un entorno empresarial cada vez más expuesto al escrutinio público y regulatorio, minimizar el riesgo de fraude se convierte en una condición necesaria para preservar la legitimidad y la viabilidad de las organizaciones.

Trompeter *et al*. (2013) insisten en que una parte del riesgo asociado al fraude reside precisamente en la falsa percepción de que se trata de un fenómeno improbable o excepcional. Esta creencia puede llevar a muchas empresas a relegar la prevención del fraude a un plano secundario, confiando en que su cultura interna o sus buenos resultados económicos bastan para protegerlas. Sin embargo, la evidencia empírica sugiere que las condiciones que facilitan el fraude como presión, oportunidad y racionalización pueden aparecer en prácticamente cualquier organización si no se detectan y abordan a tiempo.

Adoptar una visión estratégica implica reconocer que los riesgos de fraude no son estáticos, sino que evolucionan junto con el entorno competitivo, los modelos de negocio, las dinámicas de poder interno y las condiciones del mercado. Por ello, las respuestas deben ir más allá de la simple implementación de controles o la realización de auditorías periódicas. La prevención efectiva del fraude requiere alinear los sistemas de control con la estrategia empresarial, identificar vulnerabilidades estructurales y reforzar los mecanismos de supervisión en los puntos críticos del proceso de toma de decisiones.

Una respuesta empresarial madura también debe incluir una reflexión sobre el diseño de los incentivos, tanto a nivel individual como colectivo. Sistemas de retribución que premian únicamente los resultados económicos, sin considerar el "cómo" se consiguen, pueden generar presiones indebidas que aumenten la probabilidad de conductas fraudulentas. Del mismo modo, la falta de consecuencias visibles ante comportamientos poco éticos puede enviar señales equivocadas al conjunto de la organización. En este sentido, el compromiso visible de la alta dirección con la integridad y la rendición de cuentas resulta clave para consolidar una cultura corporativa adversa al fraude (Armstrong *et al*., 2010).

Finalmente, aquellas empresas que incorporan la prevención del fraude como parte de su gestión estratégica del riesgo no solo se protegen mejor ante contingencias graves, sino que también ganan en confianza frente a sus grupos de interés. Inversores, clientes, empleados y reguladores valoran cada vez más a aquellas organizaciones que demuestran una gobernanza sólida, transparencia informativa y coherencia entre sus valores declarados y sus prácticas reales. La lucha contra el fraude, lejos de ser una carga, puede convertirse en una ventaja competitiva sostenida, especialmente en entornos donde la credibilidad es un recurso escaso.

5.7 La corrupción en la empresa

La corrupción empresarial representa uno de los riesgos más severos y persistentes que enfrentan las organizaciones, especialmente aquellas que operan en contextos globales complejos o en sectores regulados. Lejos de tratarse de un fenómeno marginal o aislado, la corrupción puede penetrar profundamente en la estructura de una empresa y deteriorar sus cimientos éticos, legales y operativos. Su impacto se manifiesta tanto en el corto como en el largo plazo, afectando la competitividad, la reputación institucional, la relación con las autoridades y la confianza de clientes, inversores y empleados.

Desde una perspectiva organizacional, la corrupción adopta múltiples formas, entre las que se incluyen el soborno directo, los pagos de facilitación, la manipulación de licitaciones públicas, el uso indebido de información privilegiada y el desvío de recursos públicos o empresariales para fines personales o ilegítimos (Ivanov, 2020). Estas conductas, cuando son toleradas o sistemáticamente ignoradas, no solo suponen un incumplimiento legal, sino que introducen un sesgo destructivo en los procesos de toma de decisiones. La corrupción distorsiona la competencia, socava la rendición de cuentas y mina la legitimidad institucional de las empresas involucradas.

En las últimas décadas, se ha producido un avance significativo en la consolidación de un marco internacional de responsabilidad empresarial frente a la corrupción. Instrumentos como la Convención de las Naciones Unidas contra la Corrupción, la Convención Antisoborno de la OCDE, las directrices del Banco Mundial o los Principios del Pacto Mundial de la ONU, han establecido estándares que obligan a las empresas a adoptar medidas proactivas para prevenir y detectar conductas corruptas dentro de su organización. Más allá del cumplimiento formal, estos estándares promueven una lógica de debida diligencia, que exige identificar riesgos, implementar controles razonables y fomentar una cultura de integridad.

Uno de los aspectos más relevantes es que el riesgo de corrupción no puede entenderse como un mero asunto legal o de cumplimiento normativo. Se trata de un riesgo estratégico que debe abordarse desde la alta dirección y gestionarse con la misma seriedad que otros riesgos empresariales críticos. En particular, las empresas que operan en mercados emergentes, con estructuras de gobernanza débiles o con alta dependencia del sector público, enfrentan una exposición mayor que exige evaluaciones constantes y respuestas diferenciadas (UNODC, 2013). La corrupción, en estos casos, puede no solo dar lugar a sanciones penales o administrativas, sino también provocar la pérdida de contratos, la exclusión de licitaciones internacionales y un deterioro profundo de la reputación corporativa.

Por tanto, comprender la naturaleza de la corrupción y sus implicaciones va más allá de identificar comportamientos ilícitos. Implica reconocer que, en determinados contextos, los incentivos estructurales, las presiones comerciales y la falta de controles efectivos pueden crear un entorno propicio para su aparición. Una empresa que no evalúe adecuadamente su exposición a la corrupción está asumiendo un riesgo latente que puede materializarse en cualquier momento, comprometiendo su sostenibilidad y la confianza de sus grupos de interés.

5.8 Elementos de un programa anticorrupción

Ante la complejidad y los riesgos que entraña la corrupción, las empresas están cada vez más llamadas a implementar programas de cumplimiento anticorrupción sólidos, eficaces y adaptados a su contexto operativo. Estos programas no deben limitarse a enunciados éticos generales o códigos formales, sino que deben estructurarse como sistemas vivos, integrados en la estrategia organizacional y gestionados con recursos adecuados (Ivanov, 2020). La literatura internacional en materia de cumplimiento ha

avanzado hacia un consenso sobre los elementos que toda organización debería contemplar para prevenir, detectar y responder de forma adecuada ante conductas corruptas (Figura 5.3).

El primer componente esencial de un programa eficaz es la evaluación de riesgos, entendida como un proceso sistemático para identificar, analizar y priorizar los riesgos de corrupción específicos que enfrenta la organización. Esta evaluación debe considerar el tipo de actividad empresarial, los países en los que opera, su relación con entidades públicas, y la naturaleza de sus vínculos con terceros. El objetivo es detectar aquellas áreas donde el riesgo de corrupción es mayor, y así poder diseñar medidas preventivas más ajustadas y eficaces.

En segundo lugar, el programa debe incluir un código de conducta y políticas anticorrupción claras, accesibles y actualizadas. Estas políticas deben establecer de forma inequívoca la prohibición del soborno y otras formas de corrupción, y proporcionar directrices concretas sobre temas como regalos, hospitalidad, contribuciones políticas o patrocinio. Asimismo, deben aplicarse de forma coherente a todos los niveles jerárquicos de la empresa, sin excepciones ni privilegios, y acompañarse de sanciones proporcionales ante su incumplimiento.

La formación y concienciación interna constituye otro pilar fundamental del sistema. No basta con difundir políticas escritas: es necesario asegurarse de que los empleados comprenden los riesgos asociados a la corrupción, reconocen situaciones de riesgo y saben cómo actuar. La formación debe adaptarse a las funciones específicas de cada colectivo y repetirse de forma periódica, especialmente en áreas expuestas como ventas, compras, relaciones institucionales o expansión internacional.

El programa también debe contemplar procedimientos eficaces de diligencia debida respecto a terceros. En muchas ocasiones, las prácticas corruptas no se materializan directamente a través de empleados, sino mediante agentes, consultores, intermediarios o socios locales. La selección, contratación y supervisión de estos actores debe realizarse mediante protocolos que evalúen su historial, reputación y relación con entidades públicas. Esto incluye cláusulas contractuales específicas, controles continuos y mecanismos de rendición de cuentas.

Figura 5.3. Elementos de un programa anticorrupción. Fuente: Elaboración propia.

Además, es imprescindible contar con canales de denuncia confidenciales, accesibles y confiables, que permitan a empleados y terceros reportar sospechas o incidentes sin temor a represalias. Estos mecanismos deben gestionarse con independencia y asegurar la protección del denunciante. La existencia de canales efectivos no solo contribuye a la detección temprana de irregularidades, sino que refuerza el mensaje organizacional de que la corrupción no será tolerada.

Todo este sistema debe estar respaldado por un liderazgo comprometido. El llamado tono desde la cima (o "*tone from the top*" en inglés), la actitud visible y activa de la alta dirección frente a la corrupción, es un factor determinante para que el programa tenga credibilidad interna (UNODC, 2013). Sin un liderazgo ejemplar, incluso las mejores políticas corren el riesgo de ser percibidas como cosméticas o inoperantes. Del mismo modo, la asignación de recursos humanos, técnicos y financieros suficientes es clave para garantizar la efectividad real del programa, así como la presencia de un responsable claro, como un oficial de cumplimiento, con autonomía y autoridad dentro de la estructura empresarial.

En conjunto, estos elementos conforman la arquitectura de un programa de cumplimiento anticorrupción robusto, capaz de reducir la exposición al riesgo, fortalecer la cultura ética y proteger los intereses estratégicos de la empresa.

5.9 Seguimiento y evaluación del programa anticorrupción

Para que un programa de cumplimiento anticorrupción sea verdaderamente eficaz, no basta con diseñarlo correctamente e implementarlo una vez. Es imprescindible que se someta a un proceso continuo de seguimiento, evaluación y mejora, que garantice su adecuación a los cambios del entorno, a las lecciones aprendidas de su propia experiencia y a las expectativas crecientes de los grupos de interés. Esta visión dinámica del cumplimiento no solo responde a exigencias normativas, sino que refleja una concepción más madura y estratégica del gobierno corporativo.

Según los estándares internacionales revisados por Ivanov (2020), un sistema de cumplimiento robusto debe contar con mecanismos regulares de monitoreo, orientados tanto a verificar el cumplimiento de las políticas como a identificar posibles debilidades o áreas de riesgo no cubiertas. Esta tarea puede incluir controles internos específicos, auditorías periódicas, revisiones de transacciones sensibles y seguimiento de los informes recibidos a través de los canales de denuncia. La detección de deficiencias no debe percibirse como un fracaso, sino como una oportunidad de mejora que refuerza la integridad del sistema.

Además del monitoreo operativo, es recomendable llevar a cabo evaluaciones globales del programa con una periodicidad determinada. Estas evaluaciones deben analizar no solo los resultados formales (por ejemplo, número de formaciones realizadas o denuncias tramitadas), sino también la efectividad real del programa en términos de cultura organizativa, percepción del riesgo y compromiso de la alta dirección. La participación de evaluadores internos con independencia, o incluso de auditores externos, puede aportar objetividad y nuevas perspectivas.

Una herramienta complementaria de gran utilidad es el benchmarking, entendido como la comparación sistemática del programa propio con los de otras organizaciones del mismo sector o con las mejores prácticas internacionales. Este ejercicio permite identificar innovaciones útiles, detectar brechas relevantes y posicionarse mejor frente a expectativas externas, como las de inversores institucionales, agencias de calificación o autoridades regulatorias. En muchos casos, el benchmarking ha servido para elevar los estándares de cumplimiento incluso más allá de lo exigido legalmente, como muestra el creciente número de empresas que adoptan voluntariamente marcos como ISO 37001.

La mejora del sistema requiere también una comunicación efectiva de los resultados del seguimiento, tanto hacia dentro como hacia fuera de la organización. Compartir aprendizajes, actualizar procedimientos, reconocer públicamente los esfuerzos realizados y sancionar las malas prácticas cuando se detectan, refuerza el mensaje de que la lucha contra la corrupción no es retórica, sino una política activa y sostenida. Esta transparencia interna y externa contribuye a generar confianza, legitimar el programa y fomentar una cultura organizativa más alineada con los valores de integridad y responsabilidad.

En definitiva, un sistema de cumplimiento anticorrupción no debe considerarse un producto acabado, sino un proceso evolutivo, que requiere atención constante, apertura al cambio y compromiso institucional. Solo las organizaciones que asumen esta lógica de mejora continua estarán preparadas para afrontar los desafíos éticos y regulatorios que plantea un entorno cada vez más exigente en materia de integridad corporativa.

5.10 Conclusiones del capítulo

Este capítulo aborda un conjunto de riesgos cuya relevancia ha crecido significativamente en los últimos años y que representan una dimensión crítica dentro del panorama de la gestión empresarial actual. A diferencia de los riesgos tradicionales, los riesgos asociados a criterios ESG, al fraude y a la corrupción no solo impactan en los resultados financieros, sino que también afectan de forma directa a la legitimidad social, la sostenibilidad y la reputación de las organizaciones. En este sentido, el capítulo ofrece una visión actualizada y necesaria de las amenazas que enfrentan las empresas en un entorno donde los factores éticos, sociales y regulatorios tienen un peso cada vez mayor.

El análisis de los riesgos ESG permite comprender cómo cuestiones medioambientales, sociales y de gobernanza han pasado de ser consideraciones secundarias para convertirse en fuentes potenciales de vulnerabilidad o ventaja competitiva. La identificación, priorización y gestión de estos riesgos no es únicamente un imperativo moral, sino también una necesidad estratégica. Las empresas que no abordan estos aspectos de forma proactiva se exponen a sanciones regulatorias, pérdida de inversores, fuga de talento y deterioro de imagen frente a una sociedad cada vez más exigente en materia de sostenibilidad y transparencia.

Del mismo modo, el tratamiento del fraude y la corrupción permite dimensionar cómo estos riesgos afectan a la integridad de las operaciones empresariales y a la confianza de los distintos grupos de interés. El capítulo explora tanto las causas internas del fraude, como los factores culturales o los incentivos perversos, como las respuestas que pueden adoptar las organizaciones, incluyendo programas antifraude, medidas de control interno y sistemas de supervisión. En el caso de la corrupción, se enfatiza la necesidad de implementar políticas preventivas y mecanismos de seguimiento eficaces, más allá del cumplimiento formal de las normativas.

El punto común entre estos riesgos es su carácter transversal y su dificultad para ser cuantificados con precisión. No se trata de amenazas técnicas o financieras aisladas, sino de fenómenos complejos que exigen una respuesta integral, tanto desde la cultura corporativa como desde los sistemas de gobernanza. Su impacto se produce tanto en la dimensión tangible del negocio como en aspectos intangibles, como la confianza, la legitimidad o el posicionamiento competitivo.

En conjunto, este capítulo refuerza la idea de que la gestión del riesgo no puede limitarse a lo previsible o cuantificable. Para ser realmente eficaz, debe incorporar dimensiones éticas, sociales y estructurales que, aunque más difíciles de modelar, resultan igual de decisivas para la sostenibilidad y el valor a largo plazo de la empresa.

Capítulo 6 Risk decision making

La toma de decisiones es una función esencial en la gestión empresarial, especialmente en entornos marcados por la incertidumbre. Este capítulo explora cómo el riesgo influye en los procesos decisionales, combinando enfoques desde la neurociencia, la teoría de sistemas y la psicología del comportamiento.

Se analiza la dualidad entre mente consciente y subconsciente, la estructura de los sistemas de decisión y factores como el contexto, la narrativa y la percepción del riesgo residual. Asimismo, se abordan los sesgos cognitivos que afectan el juicio y se introduce el concepto de "apetito de riesgo" como herramienta clave para alinear decisiones estratégicas con los objetivos y límites de la organización.

Este capítulo actúa como puente entre la teoría del riesgo y su aplicación práctica, proporcionando un marco integral para una toma de decisiones más coherente y sostenible.

6.1 La ciencia tras la toma de decisiones

El campo de la toma de decisiones ha sido abordado desde distintas disciplinas bajo nombres como ciencia de la decisión o teoría de la decisión en entornos académicos, y simplemente toma de decisiones en contextos organizacionales. Se trata de un ámbito transversal que afecta tanto a lo personal como a lo colectivo, incluyendo sectores como la salud, las finanzas o la política.

Originalmente, se asumía que los humanos tomaban decisiones de forma racional y lógica, una idea que dominó hasta los años 50. Esta noción fue cuestionada por Herbert Simon, quien propuso el concepto de racionalidad limitada, aludiendo a las restricciones cognitivas y de información con las que las personas toman decisiones.

A partir de los años 70, Daniel Kahneman y Amos Tversky identificaron sesgos cognitivos sistemáticos que desvían nuestras elecciones de la racionalidad, introduciendo el concepto de los dos sistemas de pensamiento: uno intuitivo y otro deliberativo. Su trabajo marcó el inicio de la ciencia moderna de la decisión, al demostrar que los errores en el juicio humano no son aleatorios, sino predecibles.

La ciencia de la decisión ha crecido con aportes de la psicología, las matemáticas y la economía, estudiando cómo las personas hacen juicios y eligen entre alternativas. Aunque modelos clásicos como el "bayesiano conservador" asumían una lógica optimizadora, los experimentos de Kahneman y Tversky revelaron que las decisiones humanas están fuertemente influidas por heurísticas y errores no conscientes (Redinger, 2024).

6.1.1. **La mente consciente**

La toma de decisiones es una actividad que tiene que ser emprendida por las personas responsables de la corporación. Incluso dentro de cada individuo, hay una manera diferente de ver la situación sobre la que hay que decidir, y según la literatura, es posible que se reaccione de manera muy diferente. Cada vez es más popular caracterizar el cómo piensan y deciden los humanos aludiendo a dos sistemas en el cerebro, simplificados como Sistema 1 y Sistema 2 (concepto acuñado por Stanovich y West en el año 2000). Kahneman en 2011 los define como:

- Sistema 1 opera automática y rápidamente, sin esfuerzo ni sensación de control voluntario gracias a un subconsciente "entrenado". Sus propiedades son: asociativo, holístico, automático, rápido, instantáneo, adquirido por biología, exposición o experiencia personal.
- Sistema 2 dispone atención a las actividades mentales que demanden esfuerzo, incluyendo las computaciones complejas. Las operaciones del Sistema 2 están asociadas a la experiencia subjetiva de agencia, elección y concentración. Sus propiedades son: estructurado, analítico, controlado, exigente, lento, adquirido por enseñanza cultural y formal

Ambos sistemas funcionan al mismo tiempo. El Sistema 1 opera de manera automática, mientras que el Sistema 2 suele mantenerse en un estado cómodo y de bajo esfuerzo, utilizando solo una parte de su capacidad. El Sistema 1 está generando de forma continua ideas para el Sistema 2: impresiones, intuiciones, intenciones y sentimientos. Cuando el Sistema 2 las acepta, esas impresiones se convierten en creencias y los impulsos se transforman en acciones voluntarias. En la mayoría de los casos, el proceso fluye sin complicaciones, y el Sistema 2 adopta las propuestas del Sistema 1 sin hacer cambios. Por lo general, creemos en nuestras impresiones y actuamos según nuestros deseos, lo cual suele ser adecuado (Kahneman, 2013). Ser consciente de estos sistemas puede ser útil a la hora de tomar decisiones o elegir entre una serie de resultados. Normalmente, el Sistema 1 participará en las decisiones rutinarias, mientras el Sistema 2 participará en las más importantes.

Otro aspecto importante a considerar de la mente humana es el apartado emocional. Las emociones pueden ser esenciales en la toma de decisiones, incluso cuando se aplica un razonamiento frío, ya que muchas veces las emociones positivas son el objetivo final de nuestras elecciones. Tomamos buenas decisiones cuando dirigimos nuestra atención de manera más eficiente hacia aquello que puede hacernos más felices (Dolan, 2014). Sin embargo, despertar emociones sin proporcionar contexto o hechos concretos suele provocar una respuesta visceral que puede ser menos productiva que una conclusión obtenida tras haber reflexionado con detenimiento. Todos los seres humanos se ven impulsados por sus emociones, pero el lugar para una descarga de adrenalina no debería ser el entorno laboral, ya que buscamos que las personas estén sanas y seguras en el trabajo. Reconocer esta paradoja y la tensión existente entre la vida laboral y personal, así como entre emoción y razonamiento, puede ayudar a los profesionales a comunicarse de manera más efectiva (Figura 6.1). Esto facilita la participación de trabajadores, directivos y del público en general en formas innovadoras de pensar sobre la eficacia y solidez de la gestión del riesgo (Redinger, 2024).

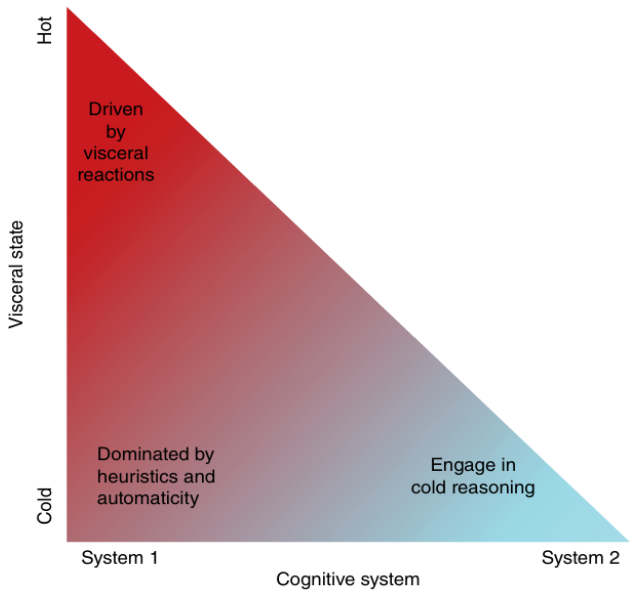

Figura 6.1: Triángulo de decisión *hot-cold*. Fuente: Redinger (2024)

6.1.2. **La mente subconsciente**

Otra parte esencial del cerebro es la parte subconsciente. Esta parte, igualmente importante para la cognición, está formada por el tronco encefálico y el sistema límbico, que procesan información incluso antes de que las áreas cognitivas sean conscientes de que existe un riesgo. Por ejemplo, los reflejos espinales pueden hacer que una persona retire la mano de un objeto caliente antes de que el dolor llegue a la corteza. Sin embargo, esta también influye en cómo se integra la información percibida en una respuesta. Las decisiones subconscientes y el comportamiento frente al riesgo pueden verse influenciados por factores como el hambre, la fatiga, emociones almacenadas (como miedo o recompensa) y emociones del momento (dolor o situaciones de desastre). Estos efectos suelen ser rápidos y eficaces, sin intervención consciente. La información de los tres sistemas decisionales (corteza, sistema límbico, tronco encefálico) se filtra y se interrelaciona constantemente. La confianza entre personas está influida por la oxitocina, una hormona producida por el hipotálamo (parte del sistema límbico), que se libera en interacciones sociales positivas, como los abrazos. En estudios experimentales, la oxitocina ha demostrado aumentar el comportamiento prosocial y disminuir el miedo y la ansiedad (Baumgartner *et al*., 2008).

6.2 Sistema de decisión

En entornos organizacionales complejos y dinámicos, la toma de decisiones no puede entenderse de forma aislada, sino como parte de un sistema interconectado de elementos, relaciones y retroalimentaciones. Adoptar una perspectiva sistémica permite trascender enfoques fragmentados y situar la toma de decisión en la gestión del riesgo, o por sus siglas en inglés, RDM (*Risk Decision-Making*) dentro de un entramado más amplio que incluye tanto marcos normativos como factores organizativos, sociales y humanos. En esta visión, las decisiones relacionadas con el riesgo emergen como el resultado de un proceso que integra juicio, elección y acción, influido por insumos como la observación, la interpretación del contexto y el sentido compartido.

Desde esta óptica, los sistemas no son meros esquemas operativos, sino configuraciones vivas que interactúan con su entorno, procesan información y se adaptan en función del feedback que reciben. Así, la perspectiva sistémica no solo aporta claridad sobre cómo las decisiones de riesgo son concebidas, sino que también proporciona una base metodológica para identificar las dinámicas de entrada (inputs), transformación (procesos) y resultados (outputs, outcomes e impactos). Reconocer esta estructura ayuda a mapear las relaciones causales e influencias cruzadas que determinan la efectividad de sus decisiones y, en última instancia, el valor que estas generan para sus organizaciones y partes interesadas.

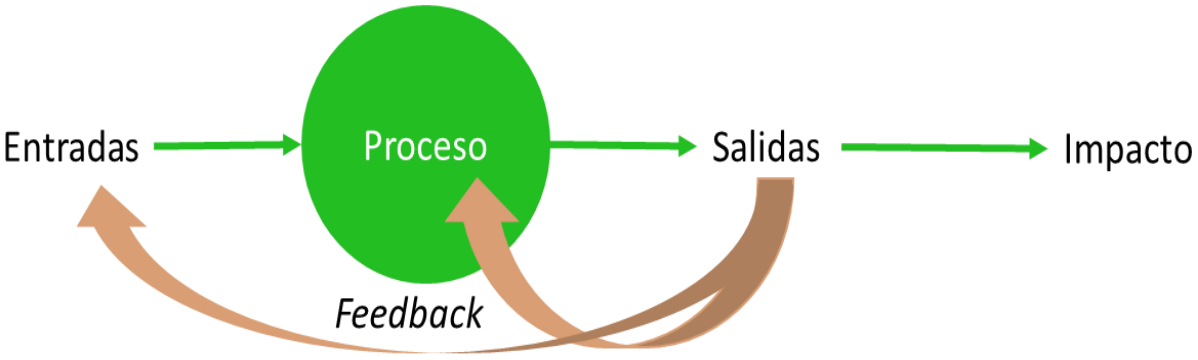

Figura 6.2: Elementos de un sistema. Fuente: Traducido de Redinger (2024)

Para analizar la toma de decisiones desde una perspectiva sistémica, primero hay que exponer el sistema. Uno básico constaría de entradas (que pueden ser internas o externas), un proceso, salidas y el impacto que genera, además se recibe *feedback* que afecta al proceso o que constituirá una entrada (Figura 6.2). A la hora de gestionar riesgos, las entradas o *inputs* pueden ser muchas: riesgos de todo tipo, materiales de ERM, auditorías, comunicados, noticias externas…Todas estas se toman en consideración para su procesado. En el contexto de RDM, ese proceso consta de la toma de una decisión en relación con el riesgo identificado. Para tomarla, se pueden usar los siguientes criterios (Redinger, 2024):

- Marco: proceso, programa, sistema, campo
- Sostenibilidad: ESG, valor, capital
- Personas: Accionistas, trabajadores, *stakeholders*
- ERM: Aseguramiento, *compliance* regulatoria, estándares

Dentro de este proceso, la consideración de los datos y su medición se vuelve crítica, ya que condiciona la calidad y validez de las decisiones que se toman frente al riesgo. Como señala Redinger (2024), es esencial tener en cuenta las características de los datos utilizados como insumos: pueden ser cualitativos o cuantitativos, y medirse en distintos niveles —nominal, ordinal, de intervalo o de razón—, lo que determina las posibilidades de análisis posteriores. Mientras los datos cuantitativos, comunes en análisis técnicos y regulatorios, ofrecen precisión y permiten inferencias estadísticas más robustas, los datos cualitativos —aunque tradicionalmente menos utilizados— permiten capturar aspectos contextuales y narrativos que enriquecen la comprensión del riesgo. La transformación de estos últimos en variables codificadas (por ejemplo, mediante codificación binaria) posibilita su análisis cuantitativo. Esta ampliación en el uso y valoración de distintos tipos de datos refleja una evolución en la toma de decisiones de riesgo, donde ya no basta con indicadores técnicos: también es necesario considerar la narrativa organizacional y social que rodea cada decisión.

Tras la toma de decisión, el sistema genera salidas observables que pueden analizarse en diferentes niveles temporales y de profundidad. En este sentido, es clave distinguir entre salida, resultado e impacto, ya que cada uno refleja una dimensión distinta de los efectos del proceso decisional. El *output* (salida) representa el resultado inmediato de una actividad, como por ejemplo la implementación de un sistema de gestión del riesgo auditado y verificado. El *outcome* (resultado) se refiere al efecto a corto o medio plazo que ese sistema tiene en el contexto operativo, como una reducción en incidentes o un incremento en el valor organizacional. Por último, el impacto alude a los efectos de largo plazo derivados del *outcome*, siendo estos más amplios y transformadores, como la mejora en la salud pública o en la resiliencia organizacional. Comprender esta secuencia es esencial para que los responsables de la toma de decisiones puedan evaluar si sus acciones están generando los cambios esperados. En la práctica, esto implica monitorizar no solo los *outputs*, sino también los *outcomes* y los impactos, con el fin de identificar si el sistema está realmente logrando sus objetivos o si es necesario redefinir entradas y procesos.

Una vez que el sistema produce sus salidas outputs y estas generan consecuencias, entra en juego un elemento esencial para la autorregulación y mejora continua: la retroalimentación (*feedback*). En los sistemas organizacionales, el *feedback* actúa como canal de información que permite monitorear el rendimiento del sistema, detectar desviaciones y realizar ajustes necesarios para mantener el equilibrio. Ejemplos típicos de bucles de retroalimentación en contextos organizacionales incluyen auditorías, investigaciones de incidentes, revisiones de gestión, buzones de sugerencias o foros comunitarios. Estos mecanismos permiten recoger información clave del entorno interno y externo y utilizarla para afinar procesos decisionales y mejorar su efectividad. En la gestión del riesgo, esta retroalimentación no solo valida o invalida decisiones pasadas, sino que alimenta nuevas entradas, cerrando así el ciclo sistémico. En este sentido, el *feedback* se convierte en el motor del aprendizaje organizacional haciendo más robusto el proceso de toma de decisiones.

La utilidad de este modelo en el contexto del RDM reside en su capacidad para visibilizar cómo una decisión, tomada a partir de ciertos inputs y bajo criterios definidos, genera efectos que se encadenan más allá del output inmediato. Permite así identificar impactos indirectos o no previstos, y fortalecer la comprensión sistémica del riesgo como fenómeno transversal que no se limita al cumplimiento técnico, sino que atraviesa dimensiones sociales, humanas y ambientales.

6.3 Otras consideraciones

La toma de decisiones en la organización puede alcanzar un nivel muy alto de complejidad, incluidas las relacionadas con la gestión del riesgo corporativo. En este punto se ofrecen algunas consideraciones clave para la toma de decisiones en materia de gestión de riesgos.

6.3.1. **Contexto, encuadre y narrativa**

El contexto, el encuadre y la narrativa son dinámicas esenciales en la toma de decisiones relacionadas con el riesgo. Abordar estos aspectos puede parecer contraintuitivo para el CRO, ya que históricamente nos hemos orientado principalmente hacia lo analítico y cuantitativo, hacia los números y los niveles de gestión medibles. Esto tiene sentido en muchos casos. El riesgo no es una realidad absoluta, sino que depende del contexto. ¿Para quién o para qué representa algo un riesgo? ¿Es un riesgo para la organización, para el trabajador, para la comunidad o para el medioambiente? Dependiendo del contexto y de a quién o qué se vea afectado, un riesgo puede considerarse aceptable o no. Es fundamental tener en cuenta el contexto, el encuadre y la narrativa en tus procesos de toma de decisiones sobre el riesgo. A medida que se desarrolle una mayor atención hacia estos elementos, las narrativas aparecerán en todas partes. Dentro del campo de riesgo, convergen distintos valores, perspectivas y opiniones.

El contexto, el encuadre y la narrativa son componentes fundamentales en los procesos de toma de decisiones relacionados con el riesgo. Estos elementos están presentes en la forma en que se articulan los distintos puntos de vista, valores y perspectivas dentro de una organización. Su relevancia se acentúa en situaciones donde confluyen intereses diversos, lo que convierte a las narrativas en vehículos clave para interpretar y abordar el riesgo de manera significativa y estratégica. Factores como el estado interno, los modelos mentales y la orientación cognitiva influyen de manera sustancial en cómo se configura una decisión. Las dimensiones regulatorias, técnicas, organizacionales y sociales también moldean el entorno en el que las decisiones se enmarcan y ejecutan. Reconocer estas dinámicas permite no solo una comprensión más profunda del proceso decisional, sino también una mejora en la calidad de sus resultados y efectos, tanto a nivel interno como externo (Redinger, 2024).

6.3.2. **Riesgo residual y aceptable**

El riesgo residual se refiere al nivel de riesgo que permanece tras aplicar controles, y representa un componente constante en los procesos de toma de decisiones relacionados con el riesgo. Aunque a menudo se busca eliminarlo completamente, alcanzar un riesgo cero es imposible; lo máximo que puede lograrse es un nivel aceptable, definido como seguro según las consecuencias esperadas más que por su probabilidad.

La evaluación de este tipo de riesgos implica tensiones entre distintos enfoques del campo del riesgo, especialmente entre decisiones basadas en evidencia y aquellas guiadas por la intuición. En el ámbito

de las políticas públicas, se equilibra el coste de reducir riesgos con la voluntad social de asumir ese gasto, a menudo utilizando indicadores como el valor estadístico de la vida. Sin embargo, la definición de lo que constituye un riesgo aceptable varía según el contexto, lo que hace que herramientas como la matriz de riesgo sean fundamentales para facilitar decisiones informadas.

6.4 Sesgos

A la hora de tomar decisiones, a pesar de seguir un sistema establecido y de conocer el proceso psicológico, las personas estamos sujetas a sesgos a la hora de interpretar la información obtenida, lo que puede provocar que no se decida lo mejor o más conveniente. Para tomar decisiones libres de sesgos es importante tomarse un tiempo, analizar, usar la lógica, y de nuevo, pensar lentamente. Reaccionar deprisa, hace que sea más probable cometer errores (Kahneman, 2011). Dentro de RMD, los sesgos más habituales son: prominencia, disponibilidad, anclaje, confirmación, optimismo y costo hundido.

- Sesgo de prominencia: A la hora de tomar decisiones sobre resultados inciertos, es habitual darles más peso a los eventos prominentes. Por ejemplo, si ocurre una riada en una zona, es más probable que la gente en una zona colindante perciba un riesgo mayor de riada por el evento prominente que ha sido la anterior riada. Esta gente puede incluso que contrate algún seguro que cubra los daños por inundación, durante un tiempo. Una vez que el evento haya perdido la prominencia, dejarán de contratar el seguro. Por lo tanto, la evaluación de riesgo de inundación que cada vecino haga volverá a los valores previos a la riada.
- Sesgo de disponibilidad: La información disponible a la hora de tomar la decisión puede condicionar el resultado, debido a que la gente suele valorar mucho lo que sabe en el momento. Por ejemplo, si una persona habla de la mala experiencia que tuvo en un restaurante, es posible que el receptor no vaya nunca y no compruebe la opinión de otros clientes. De esa forma, toma la información que tiene disponible y no trata de buscar más fuentes.
- Sesgo de anclaje: Este sesgo consiste en la influencia que un dato numérico hace a la hora de percibir cantidades abstractas. Cuando se presenta el valor de algo que no está en el consumo habitual de una persona y, por lo tanto, normalmente no sabe cuánto vale, esta persona lo usará como punto de referencia para evaluar otros valores numéricos. A la hora de gestionar riesgos es muy probable anclarse en el valor más reciente de pérdidas y tomarlo como referencia, condicionando toda la toma de decisiones.
- Sesgo de confirmación: Cuando se examinan pruebas o indicios sobre un tema que se esté investigando, la gente tiene mayor tendencia a dar más peso a los que confirman sus sospechas. Por ejemplo, a la hora de decidir si arrancar o no un nuevo proyecto, si el director cree que es una buena inversión es más probable que ignore las amenazas que le afectan, aunque sean claras.
- Sesgo de optimismo: Ser demasiado optimista y subestimar la probabilidad o magnitud de un riesgo es un sesgo típico del pensamiento humano. Además, este se encuentra especialmente acusado en las personas que han tenido éxito previamente, y el haber tenido éxito en el pasado no lo asegura en el futuro.
- Falacia del costo hundido: Consiste en continuar invirtiendo en una actividad cuyos costes ya han sobrepasado la previsión porque se ha invertido en el pasado y el abandono de financiación se consideraría una pérdida. El ejemplo más conocido es el caso del *Concorde*, proyecto que no se rentabilizó nunca y que costó mucho más de lo planeado. A la larga, haber abandonado el proyecto a tiempo habría supuesto una pérdida menor que haberlo terminado.

Comprender y mitigar los sesgos cognitivos más comunes no solo mejora la calidad de las decisiones, sino que constituye un paso esencial hacia una gestión del riesgo más racional, crítica y alineada con los objetivos estratégicos de la organización.

6.5 Risk apetite en RDM (*Risk Decision Making*)

Como se adelantó en el Capítulo 4, el apetito de riesgo que la dirección determine afectará en la toma de decisiones. En un ERM (*Enterprise Risk Management*), la organización debe definirlo, entendido como la cantidad de riesgo que la compañía está dispuesta a aceptar. Esto se puede interpretar como que hay una cantidad absoluta de riesgo definida por alguna métrica, a partir del que la empresa no está dispuesta a ir. Esto se puede conceptualizar como un punto en una escala de riesgo que la organización no cruzará nunca. El problema con esta interpretación es que sugiere que el apetito de riesgo es fijo y es independiente del retorno potencial de la actividad considerada. Por ejemplo, si una actividad supusiese un riesgo mayor al que se está dispuesto a aceptar, pero su retorno potencial fuese enorme, quedaría rechazado inmediatamente según la interpretación dada. Esto se puede representar en una gráfica en la que vemos el riesgo como eje horizontal y el retorno como eje vertical (Figura 6.3).

Este modelo es rígido, y puede no ser el ideal para RDM. Niehaus (2017) sugiere que el apetito de riesgo esté condicionado a la compensación entre el riesgo asumido y el retorno esperado. Si se grafica esto, se obtiene una curva que establece el mínimo retorno esperado para un riesgo concreto (Figura 6.4). De esta manera, cualquier valor que quede a la izquierda de la curva sería aceptable y, por lo tanto, se podría decidir continuar con la actividad involucrada mientras que el que quede a la derecha sería rechazado. La empresa es la responsable de diseñar su propia curva, que previsiblemente, no sería lineal. Al final, el apetito de riesgo no debería ser un límite absoluto y cada caso que se encuentre cerca de la línea de compensación debería ser estudiado por la dirección. Esta gráfica sería una herramienta más a la hora de tomar decisiones en la organización.

Finalmente, según cómo se funcione en cada compañía es importante mencionar que puede haber un sesgo estructural para asumir más riesgo del que se debería. Si hay compensación económica para los gerentes y directores por liderar proyectos exitosos mientras que no hay penalización por el fracaso, es posible que haya un mayor apetito por el riesgo del que debería. En un ERM y a la hora de tomar decisiones orientadas al riesgo se debe tener muy en cuenta.

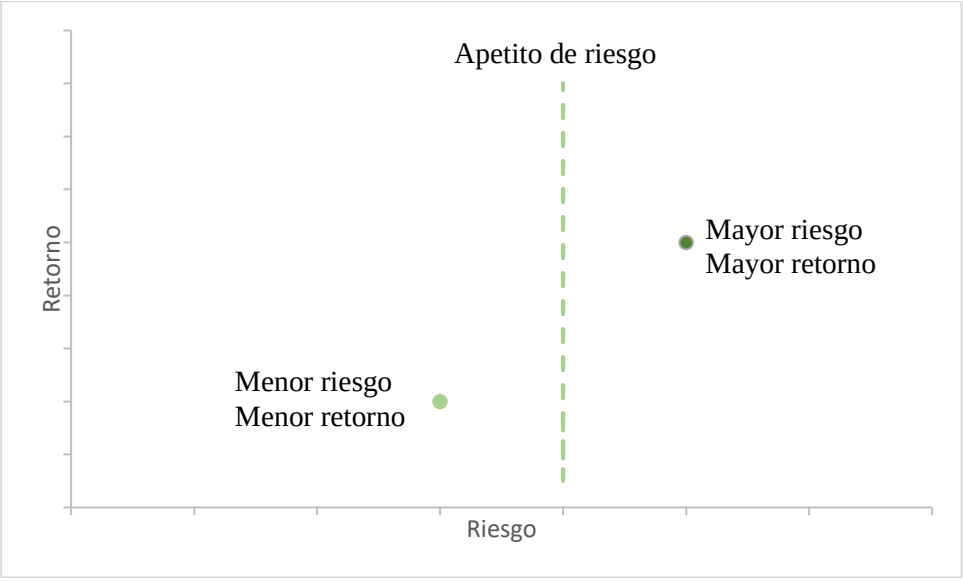

Figura 6.3: Gráfica que representa el *risk appetite*. Fuente: Traducido de Niehaus (2017)

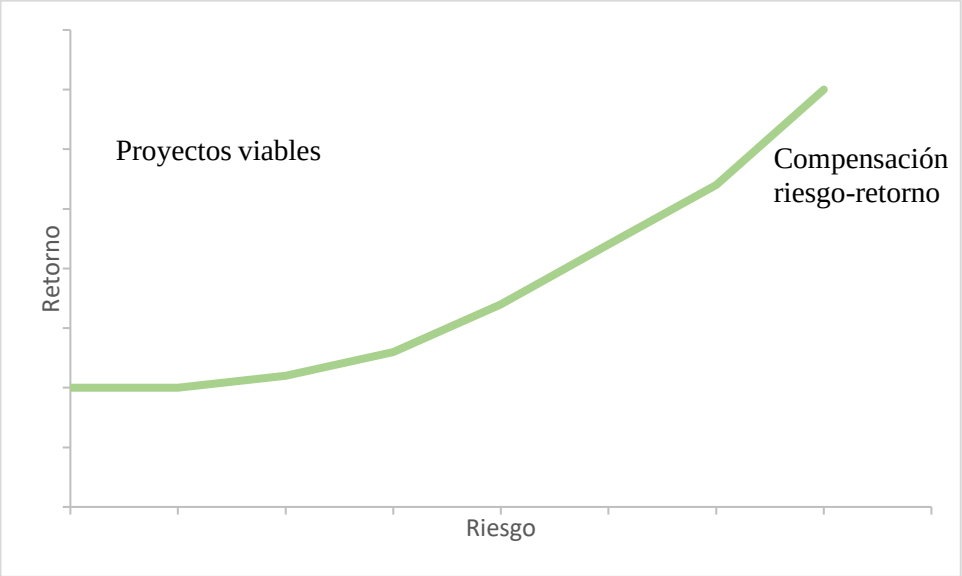

Figura 6.4: Compensación entre riesgo y retorno. Fuente: Traducido de Niehaus (2017)

6.6 Conclusiones del capítulo

El capítulo final del trabajo aborda una de las dimensiones más complejas y menos previsibles de la gestión del riesgo: la toma de decisiones en condiciones de incertidumbre. A diferencia de los enfoques técnicos o estructurales desarrollados en capítulos anteriores, aquí se pone el foco en los mecanismos cognitivos, emocionales y organizativos que intervienen cuando los individuos y equipos directivos se enfrentan a situaciones de riesgo. Esta perspectiva resulta esencial, ya que incluso los marcos de gestión mejor diseñados pueden verse neutralizados si las decisiones que los sustentan no responden a una lógica racional o estratégica.

El análisis parte de la diferenciación entre la mente consciente y la subconsciente, y cómo ambas influyen en los procesos de decisión. Se exponen los sesgos cognitivos más comunes, como la aversión a la pérdida, el exceso de confianza o el sesgo de disponibilidad, y se muestra cómo estos pueden distorsionar la percepción del riesgo y llevar a decisiones subóptimas. Estos patrones de comportamiento no se eliminan mediante información adicional ni por el simple hecho de contar con un sistema formal de gestión del riesgo, lo que subraya la importancia de comprender su origen y anticipar sus efectos.

El capítulo también introduce el concepto de sistema de decisión, que permite estructurar el proceso desde una perspectiva organizativa. Se reconocen factores como el encuadre narrativo de los riesgos, la percepción del riesgo residual y aceptable, y el apetito de riesgo como elementos que moldean las elecciones estratégicas. Esto implica que la forma en la que se presenta un riesgo puede llegar a ser tan influyente como el riesgo mismo, lo que resalta la dimensión comunicativa y cultural de la toma de decisiones.

Además, se establece una conexión clara entre la gestión del riesgo y la gobernanza estratégica. No se trata únicamente de identificar amenazas, sino de generar un entorno donde las decisiones se tomen con información suficiente, criterios compartidos y conciencia de los límites inherentes a la

racionalidad humana. Esta visión requiere no solo herramientas y modelos, sino también formación, cultura y liderazgo.

En definitiva, el capítulo pone de relieve que gestionar el riesgo no es solo cuestión de estructuras, políticas o métricas, sino también de personas y procesos de decisión. Cerrar el trabajo con esta reflexión refuerza la idea de que el riesgo no es un fenómeno externo a la organización, sino una realidad que se construye y se enfrenta en el interior mismo de la empresa, en sus hábitos, sus decisiones y su forma de interpretar el entorno.

CONCLUSIONES

La gestión del riesgo empresarial se configura como un componente esencial para la sostenibilidad y la creación de valor en las organizaciones. A lo largo de este trabajo se ha llevado a cabo un recorrido teórico riguroso que permite comprender la complejidad del riesgo en el contexto corporativo, desde su conceptualización hasta su vinculación con los procesos estratégicos y de toma de decisiones.

Uno de los primeros hallazgos fundamentales es la necesidad de entender la compañía como una entidad jurídica compleja, cuya estructura de gobierno y toma de decisiones condiciona directamente el modo en que se gestionan los riesgos. La distinción entre los individuos que componen la organización y la entidad legal que esta representa es clave para ubicar correctamente las responsabilidades y competencias en la gestión del riesgo, destacando el papel de la dirección y la junta directiva. Este marco organizativo justifica la propuesta de roles específicos como el *Chief Risk Officer* (CRO), cuya implementación todavía enfrenta barreras estructurales, pero representa un paso crucial hacia una gestión más profesionalizada y estratégica del riesgo.

En relación con el concepto de riesgo, se ha evidenciado la utilidad de abordarlo desde una doble perspectiva: como pérdida esperada y como incertidumbre. Esta distinción resulta particularmente relevante para adaptar los modelos de análisis y gestión a las distintas situaciones empresariales. La clasificación de riesgos en operativos, financieros y de mercado ha permitido sistematizar su estudio, identificando elementos clave como los errores de procesos, las vulnerabilidades tecnológicas, el fraude, la volatilidad financiera y los eventos disruptivos.

El análisis del impacto del riesgo en la generación de valor, mediante el modelo DCF, constituye uno de los aportes más significativos del trabajo. Se ha demostrado cómo la correcta gestión del riesgo no solo contribuye a la estabilidad financiera de la empresa, sino que puede tener efectos positivos indirectos sobre los flujos de caja esperados, reduciendo los costes asociados a las dificultades financieras, la ampliación de capital o la volatilidad tributaria. Asimismo, se ha puesto de manifiesto que, si bien la reducción del riesgo específico difícilmente afecta al coste del capital, su influencia en la percepción de solidez y sostenibilidad de la empresa puede ser decisiva.

En este contexto, la gestión integral del riesgo (ERM) se presenta como el enfoque más adecuado para abordar la complejidad del entorno empresarial actual. El modelo COSO, ampliamente tratado en este trabajo, ofrece un marco estructurado que facilita la integración del riesgo en todos los niveles organizativos, desde el gobierno corporativo hasta las operaciones diarias. La identificación de sus componentes como; gobierno, estrategia, desempeño, revisión y comunicación, proporciona una guía clara para su implementación, aunque también revela la necesidad de un compromiso firme por parte de la alta dirección.

Otro aspecto destacado del trabajo ha sido la incorporación de riesgos contemporáneos en la agenda de la gestión empresarial. Los riesgos ESG, el fraude y la corrupción ya no pueden considerarse marginales o secundarios, dado su profundo impacto reputacional, legal y financiero. Su adecuada gestión exige enfoques específicos, programas estructurados y un cambio de cultura organizativa orientado hacia la transparencia, la ética y la sostenibilidad.

Finalmente, el estudio de la toma de decisiones bajo condiciones de incertidumbre ha permitido completar la visión integral del riesgo. La comprensión de los sesgos cognitivos, la estructura de los sistemas de decisión y el papel del apetito de riesgo proporciona herramientas clave para que las empresas puedan actuar de forma más racional, consistente y alineada con sus objetivos estratégicos.

En conjunto, este trabajo permite concluir que la gestión del riesgo empresarial no debe considerarse una función aislada o meramente operativa, sino una capacidad estratégica transversal que incide directamente en el valor, la resiliencia y el futuro de la organización. Solo desde una visión integral, informada y alineada con los objetivos corporativos será posible desarrollar sistemas eficaces de identificación, evaluación y tratamiento de riesgos que conviertan la incertidumbre en una fuente de ventaja competitiva.

BIBLIOGRAFÍA

Acebes, F., Curto, D., De Antón, J., & Villafáñez, F. (2024). Análisis cuantitativo de riesgos utilizando "MCSimulRisk" como herramienta didáctica. Dirección y Organización, 82, 87–99. https://doi.org/https://doi.org/10.37610/dyo.v0i82.662

Acebes, F., González-Varona, J. M., López-Paredes, A., & Pajares, J. (2024). Beyond probability-impact matrices in project risk management: A quantitative methodology for risk prioritisation. Humanities and Social Sciences Communications, 11(1), 670. https://doi.org/10.1057/s41599-024-03180-5

Armstrong, C. S., A. D. Jagolinzer, and D. F. Larcker. 2010. Chief executive officer equity incentives and accounting irregularities. Journal of Accounting Research 48 (2): 225-272.

Basel Committee on Banking Supervision, "Principles for the Sound Management of Operational Risk," June 2011, 3.

Baumgartner, T., Heinrichs, M., Vonlanthen, A., Fischbacher, U., & Fehr, E. (2008). Oxytocin shapes the neural circuitry of trust and trust adaptation in humans. Neuron, 58(4), 639-650.

Chapelle, A. (2019). Operational risk management: Best practices in the financial services industry. John Wiley & Sons.

Committee of Sponsoring Organizations of the Treadway Commission. (2020). Compliance risk management: applying the COSO ERM framework. Committee of Sponsoring Organizations of the Treadway Commission (2020).

COSO (2017). Enterprise Risk Management - Integrating with Strategy and Performance. Executive Summary.

Cressey, D. R. 1950. The Criminal Violation of Financial Trust. American Sociological Review 15 (6): 738-743.

Deszca, G. (2020). Organizational Change Management: the change-path model for ensuring organizational sustainability. Chartered professional accountants of Canada.

Dolan, P. (2014). Happiness by design: Finding pleasure and purpose in everyday life. Penguin UK.

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. Issues in accounting education, 27(2), 555-579.

Fishkin, Charles A. "Controlling the Documentation Vortex," MiddleOffice Spring 2000, 13–17.

Fraser, J. (2010). Enterprise Risk Management by John Fraser and Betty J. Simkins Copyright© 2010 John Wiley & Sons, Inc. Risk (Bernstein), 20(26), 27-28.

GlobalSuite Solutions. (s.f.). (2023). ¿Qué es el modelo COSO? Recuperado de https://www.globalsuitesolutions.com/es/que-es-modelo-coso/

Instituto Brasileiro de Governança Corporativa – IBGC. (2017). Corporate Risk Management: evolution in governance and strategy.; translated by Cintia Isobata Aquino, Fernanda Vitarelli, Gisela Christiano, Mônica Pimentel de Mello Moreira. São Paulo, SP: Instituto Brasileiro de Governança Corporativa – IBGC.

Ivanov, E. (2019). Overview of anti-corruption compliance standards and guidelines. International anti-corruption academy. Режим доступа: https://www. iaca. int/media/attachments/2020/01/09/overview_of_ compliance_standards_and_guidelines. pdf (дата обращения 20.04. 2021).

J. I. Fernández. La empresa donde murieron los cinco trabajadores leoneses había pedido reabrir una mina en León (2025). El Español. https://www.elespanol.com/castilla-y-leon/region/leon/20250403/empresa-murieron-trabajadores-leoneses-pedido-reabrir-mina-leon/1003743697620_0.html

Johnson, G. and Scholes, K. (1999). Exploring Corporate Strategy, 4th Edition. Prentice Hall Europe, Harlow

Kahneman, D. (2011). Thinking, fast and slow. Macmillan.

Kruschwitz, L., & Löffler, A. (2006). Discounted cash flow: a theory of the valuation of firms. John Wiley & Sons.

Lam, J. (2014). Enterprise risk management: from incentives to controls. John Wiley & Sons.
Merna, T. (2012). Risk Management at Corporate Level. In Corporate Risk Management (eds T. Merna and F. AL-Thani). https://doi.org/10.1002/9781119208709.ch7
Ministerio de trabajo y economía social. Gobierno de España. (2024). Estadísticas de accidentes de trabajo de 2023. https://www.mites.gob.es/es/estadisticas/anuarios/2023/index.htm
Monbiot, G. (2000). Captive State: The Corporate Takeover of Britain, Pan, London.
Niehaus, G. (2017). Enterprise risk management and the risk management process. The Palgrave handbook of unconventional risk transfer.
Ojeka, S. A., Adegboye, A., Adegboye, K., Alabi, O., Afolabi, M., & Iyoha, F. (2019). Chief financial officer roles and enterprise risk management: An empirical based study. Heliyon, 5(6).
Pajares, J., Acebes, F., Martín-Cruz, N., Gonzalez-Varona, JM. (2024). Complejidad percibida en la gestión de proyectos. Una visión desde el pensamiento sistémico. 28th International Congress on Project Management and Engineering, 202-215. https://doi.org/10.61547/2401026
Pajares, J., Acebes, F., Poza, D., Martín-Cruz, N., López-Paredes, A. (2022). Managing Project Complexity. Contributions from Systems Thinking. 26th International Congress on Project Management and Engineering, 118-129
Paladugu, B. S., & Grau, D. (2020). Toyota production system-monitoring construction work progress with lean principles. In Encyclopedia of Renewable and Sustainable Materials: Volume 1-5 (pp. 560-565). Elsevier.
Palmer, D. 2009. Business leadership: Three levels of ethical analysis. Journal of Business Ethics 88: 525-536.
Pérez, Y. & Contreras, M. (2021). Aplicando COSO como marco de referencia para la implantación y supervisión del SCIINF, por parte de auditoría interna. KPMG Tendencias.
Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. Journal of information technology, 35(3), 214-231.
Pompella, M. (2017). Reinsurance, insurability and the new paradigms of unconventional risk transfer. The Palgrave Handbook of Unconventional Risk Transfer, 57-107.
Project Management Institute. (2017). Guía de los fundamentos para la dirección de Proyectos (Guía del PMBOK®). Newton Square, Pennsylvania: Project Management Institute, editor.
Real Academia Española. (2014). Diccionario de la lengua española. 23ª ed.
Redinger, C. F. (2024). Organizational Risk Management: An Integrated Framework for Environmental, Health, Safety, and Sustainability Professionals, and their C-Suites. John Wiley & Sons.
Risk Budgeting. (London: Risk Books) 2000.
Safiullah, M., Baghdadi, G. A., & Goergen, M. (2025). Do generalist CEOs reduce corporate default risk?. The British Accounting Review, 101646.
Stanovich, K. E., West, R. F., & Alder, J. E. (2000). Individual differences in reasoning: Implications for the rationality debate?-Open Peer Commentary-Three fallacies. Behavioral and Brain Sciences, 23(5), 665-665.
Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. Journal of Industrial Information Integration, 100604.
Toyota. (s.f.). Toyota production system. https://www.toyota-europe.com/about-us/toyota-vision-and-philosophy/toyota-production-system
Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley, R. A. (2013). A synthesis of fraud-related research. Auditing: A Journal of Practice & Theory, 32(Supplement 1), 287-321.
UNODC, 2013. An Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide. Available at: https://www.unodc.org/documents/corruption/Publications/2013/13-84498_Ebook.pdf
Van De Bunt, H. 2010. Walls of secrecy and silence: The Madoff case and cartels in the construction industry. Criminology & Public Policy 9 (3): 435-453.
Wesioly, B. y Moeller, G. (2020). Enterprise Risk Management: a practical approach to managing risks for small- to medium-size organizations. Chartered professional accountants of Canada.
Woolson, R. F., & Clarke, W. R. (2002). Statistical methods for the analysis of biomedical data. John Wiley & Sons.

Word Bussiness Council for Sustainable Development (WBCSD). (2018). Enterprise Risk Management. Applying enterprise risk management to environmental, social and governance-related risks. Supervised by: Irwin, R., White, P., Bakker, P., Cambers, R. F., Thomson, J. C., Murdock, D. C., Landes, C. E., Prawitt, D. F., Sobel, P. J.

Zhao, Y. (2023). How to Effectively Identify Financial Risks in Financial Management. Advances in Economics, Management and Political Sciences, 18, 344-350.