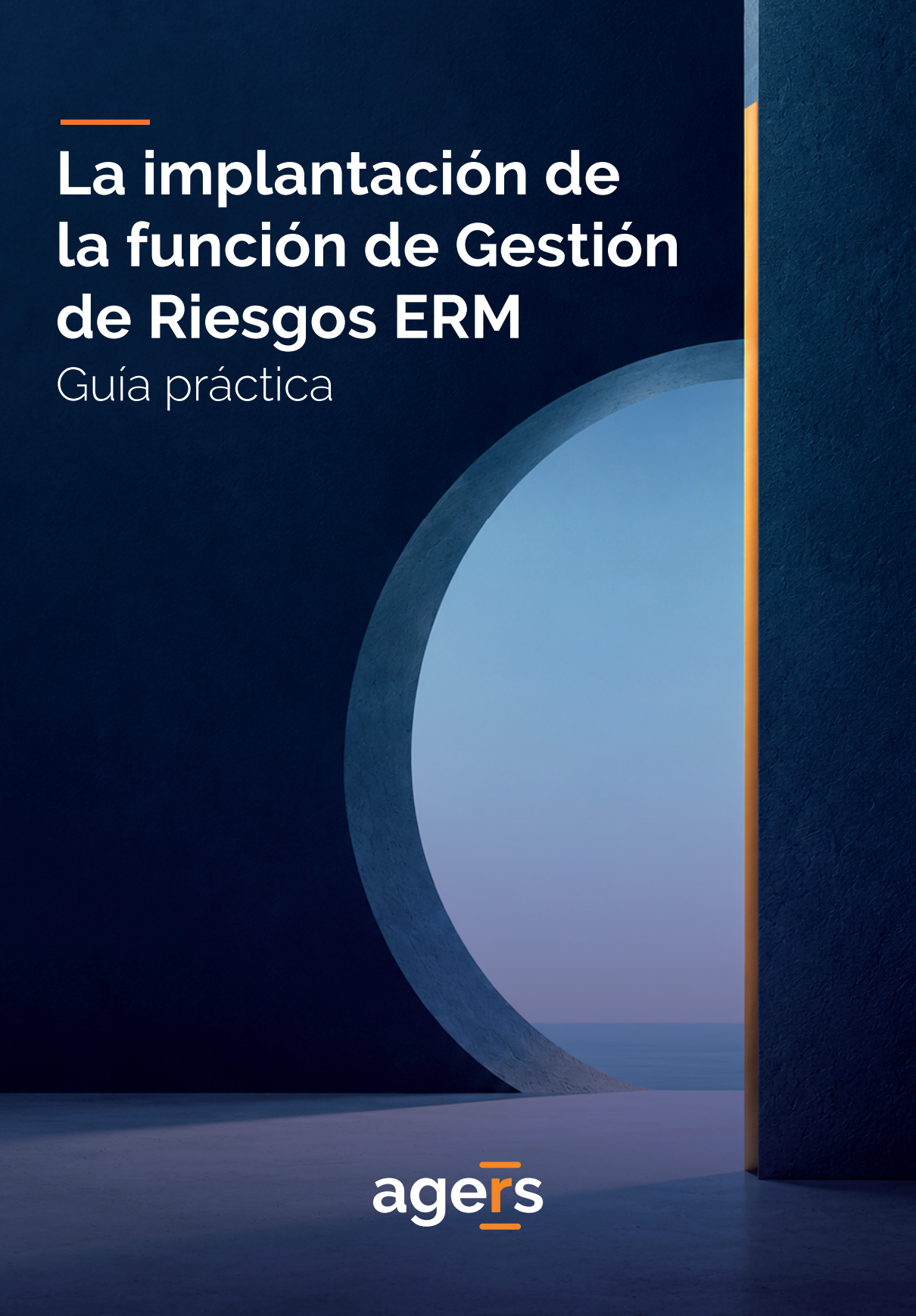
La implantación de la función de Gestión de Riesgos ERM

Guía práctica



agers

ISBN: 978-84-09-95557-2
Copyright: DEP639313061391962973
Nota Legal - Copyright

© 2026 AGERS España, las conclusiones de este texto son emitidas por la comisión.
Los contenidos de este trabajo (texto, imágenes, gráficos, elementos de diseño, etc.) están protegidos por los derechos de autor y por las leyes de protección de la propiedad intelectual. La reproducción o divulgación de sus contenidos precisa la aprobación previa por escrito de AGERS y solo puede afectarse citando la fuente y la fecha correspondiente.

ÍNDICE

AGRADECIMIENTOS 6

PRÓLOGO 8

PARTE I. FUNDAMENTOS DEL ENTERPRISE RISK MANAGEMENT 11

1. Introducción al ERM 13

1.1. Qué es el Enterprise Risk Management 13

1.2. Diferencia entre gestión tradicional de riesgos y ERM 14

1.3. ERM como parte de la gobernanza corporativa 16

1.4. Marcos de referencia para la gestión del riesgo 20

1.5. Principios fundamentales del Enterprise Risk Management 25

2. Contexto organizacional 28

2.1. Qué es "contexto" en ERM y por qué importa 28

2.2. Entorno externo (PESTEL práctico) 29

2.3. Entorno interno y capacidades/gobernanza existentes 31

2.4. Tone at the top 33

2.5. Relación con otras áreas 35

2.6. Cultura de riesgo 36

2.7. Comunicación y sensibilización 37

2.8. Expectativas de los grupos de interés 39

PARTE II. IMPLEMENTACIÓN DEL ERM 41

3. Fase inicial: Definición del marco ERM 43

3.1. Diagnóstico Inicial de la Organización 43

3.2 Análisis DAFO aplicado al ERM 45

3.3. Política de Gestión del Riesgo 46

3.4. Apetito al riesgo 48

3.5. Estructura Organizativa del ERM 50

4. Identificación de riesgos 52

4.1. Designación de los Propietarios del riesgo (Risk Owners) 53

4.2. Técnicas para la Identificación de Riesgos 57
4.3. Taxonomía e Inventario 60
4.4. Interdependencias y correlaciones entre riesgos 68

5. Análisis y evaluación de riesgos 73
5.1. Objetivo y alcance 73
5.2. Riesgo inherente y riesgo residual 74
5.3. Variables para la evaluación del riesgo 76
5.3.1. Probabilidad 77
5.3.2. Impacto 77
5.3.3. Escalas de probabilidad e impacto 78
5.3.4. Otras variables complementarias 80
5.4. Métodos de evaluación 81
5.4.1. Métodos cualitativos y semicuantitativos 82
5.4.2. Métodos cuantitativos y modelos analíticos 84
5.4.3. Enfoque combinado 87
5.5. Criticidad y priorización de riesgos 87
5.6. Resultado de la evaluación y conexión con tratamiento y monitorización 90

6. Tratamiento del riesgo 92
6.1. Las respuestas al riesgo 92
6.2. Acciones, controles y planes de acción 95
6.3. El papel del seguro en la gestión de riesgos 96

7. Monitorización, *reporting* y mejora continua 97
7.1. Seguimiento de planes de acción 98
7.2. Periodicidad del reporte a Alta Dirección y Consejo 99
7.3. Definición y monitorización de KRIs 101
7.4. Reporting a grupos de interés: IAGC (Informe Anual de Gobierno Corporativo) e Informe de Sostenibilidad 102
7.5. Evaluación periódica del desempeño del ERM a través de KPIs 103
7.6. Evaluación independiente del modelo ERM 104
7.7. Formación en gestión de riesgos 104

PARTE III. EVOLUCIÓN DEL ERM **107**

8. Riesgos emergentes y oportunidades **109**
8.1. Identificación y evaluación de riesgos emergentes **109**
8.2 Marcos de referencia para la identificación de riesgos emergentes **110**
8.3. Evaluación de riesgos emergentes **114**
8.4. Tratamiento de los riesgos emergentes **115**
8.5. Comunicación y *reporting* de riesgos emergentes **116**

9. Integración en la organización **117**
9.1. Planificación estratégica **118**
9.2. Gestión de Proyectos **120**
9.3. *Business Impact Analysis* (BIA) **121**
9.4. Gestión de crisis y protocolos **123**
9.5. Resiliencia operativa y digital (DORA, NIS2, etc.) **124**

10. Conclusiones **127**
10.1. Factores críticos de éxito **127**
10.2. ERM como ventaja competitiva **128**
10.3. *Evolución futura de la gestión de riesgos: Strategic Foresight* **130**

11. Bibliografía **132**

ANEXO I. Glosario de términos **134**
ANEXO II. Relación con ISO 31000 y COSO ERM **143**
ANEXO III. Principales técnicas de evaluación de riesgos **144**

AGRADECIMIENTOS

Queremos agradecer su trabajo, dedicación y apoyo a los profesionales que en colaboración con AGERS han hecho posible la edición de esta guía:

Ángela Nuñez González

Fernando de Santiago Cardama

Irene Lobejón González

Carlos Madrona Guillén

Eva López Fernández

moeve	Eva López de Sebastián Miró
noatum	Ana Ruíz Fernández
redeia	Eva Rodicio
redeia	Mercedes Mota
repsol	Miguel Martín Martín

Prólogo

En un entorno empresarial cada vez más complejo, interconectado y cambiante, la gestión de riesgos se ha consolidado como un elemento esencial para el adecuado gobierno de las organizaciones y para la toma de decisiones. Las organizaciones, independientemente de su tamaño o sector, operan en un contexto marcado por la incertidumbre, la volatilidad y la aparición constante de nuevos riesgos de diversas tipologías que pueden afectar a la consecución de sus objetivos.

La presente guía tiene como finalidad servir de apoyo en la comprensión de los elementos esenciales del Enterprise Risk Management (ERM, por sus siglas en inglés), o gestión integral de riesgos empresariales, así como orientar en el diseño de un modelo adaptado a las características, necesidades y nivel de madurez de cada organización. La Guía adopta un enfoque práctico, orientado a facilitar la integración de la gestión de riesgos en la estrategia, la toma de decisiones y la operativa diaria, contribuyendo a una gestión más estructurada, coherente y alineada con los objetivos.

La guía está dirigida a aquellas organizaciones y profesionales que deseen implantar, desarrollar o fortalecer sus sistemas de gestión de riesgos bajo un enfoque de Enterprise Risk Management. En particular, podrá resultar de interés para miembros de órganos de gobierno, Alta Dirección, responsables de riesgos y funciones de control, así como para aquellos perfiles involucrados en la toma de decisiones estratégicas y operativas. Asimismo, puede ser de utilidad para organizaciones que, aun no disponiendo de una función formal de gestión de riesgos, deseen avanzar hacia modelos más estructurados y alineados con las mejores prácticas, así como para aquellas que buscan evolucionar o consolidar sistemas de gestión y control de riesgos ya existentes.

El desarrollo de la gestión de riesgos se enmarca en un contexto en el que los requerimientos regulatorios, de buen gobierno y de transparencia adquieren una creciente relevancia. Normativas, estándares internacionales y recomendaciones en materia de

gobierno corporativo han reforzado la necesidad de disponer de sistemas estructurados para la identificación, evaluación y gestión de los riesgos. En este sentido, marcos como COSO — Enterprise Risk Management: Integrating with Strategy and Performance (2017) o ISO 31000:2018 — Risk management, junto con regulaciones sectoriales específicas —como Solvencia II o los acuerdos de Basilea—, contribuyen a consolidar la gestión de riesgos como un elemento clave en la supervisión y dirección de las organizaciones.

Más allá del cumplimiento normativo, el contexto actual exige a las organizaciones una mayor capacidad para anticipar y gestionar la incertidumbre, así como para responder a las expectativas de sus distintos grupos de interés. En este sentido, la gestión de riesgos se configura como una herramienta fundamental para reforzar la transparencia, la resiliencia y la sostenibilidad de las organizaciones en el medio y largo plazo.

La implantación de un sistema de Enterprise Risk Management aporta valor al permitir una gestión más estructurada de la incertidumbre y mejorar la calidad de la toma de decisiones mediante una visión global del riesgo. Del mismo modo, facilita la identificación y priorización de los riesgos más relevantes, optimiza la asignación de recursos y refuerza los mecanismos de control y supervisión. A su vez, contribuye a anticipar cambios del entorno, mejorar la capacidad de respuesta ante situaciones adversas y favorecer una asunción de riesgos más informada.

La guía se ha estructurado de forma progresiva, combinando fundamentos conceptuales con orientaciones prácticas para facilitar su aplicación. Puede utilizarse tanto como referencia para la implantación del ERM desde sus fases iniciales como herramienta de consulta para revisar elementos concretos del sistema.

Su aplicación debe entenderse de forma flexible, adaptando los contenidos a las características y nivel de madurez de cada organización. En este sentido, la implantación del ERM debe contemplarse desde una doble perspectiva temporal: por un lado,

un horizonte de corto plazo, generalmente asociado a ciclos anuales, que permite la identificación, evaluación y seguimiento periódico de los riesgos; y por otro, un horizonte de medio y largo plazo, alineado con el plan estratégico, que facilita la incorporación del riesgo en la definición de objetivos y en la toma de decisiones estratégicas.

La adecuada articulación de ambos horizontes permite integrar la gestión del riesgo en la actividad de la organización de forma continua y coherente, reforzando su capacidad para anticipar, adaptarse y responder a un entorno cambiante.

Parte I

Fundamentos del Enterprise Risk Management

La implantación de un sistema de Enterprise Risk Management requiere partir de una comprensión común de sus fundamentos, alcance y finalidad. Esta primera parte establece la base conceptual de la guía, definiendo qué se entiende por ERM, cómo se diferencia de enfoques tradicionales de gestión de riesgos y de qué manera se integra en la gobernanza, la estrategia y la toma de decisiones.

Asimismo, se abordan los principales marcos de referencia, los principios fundamentales del ERM y la importancia del contexto organizacional, la cultura, el liderazgo y las expectativas de los grupos de interés. Su objetivo es proporcionar un lenguaje común que facilite el desarrollo posterior del modelo de gestión de riesgos.

Capítulo 1.
Introducción al ERM

1.1. Qué es el *Enterprise Risk Management*

El *Enterprise Risk Management (ERM)*, o gestión integral de riesgos empresariales, es un enfoque estructurado, continuo e integrado para identificar, analizar, evaluar, gestionar, monitorizar y comunicar los riesgos que pueden afectar a la consecución de los objetivos de una organización.

El ERM proporciona un marco común que permite a la organización entender su exposición al riesgo de manera agregada, priorizar sus principales exposiciones e incertidumbres y tomar decisiones informadas en un entorno dinámico.

Desde una perspectiva práctica, el ERM parte de la premisa de que toda organización, sin importar su naturaleza, persigue unos objetivos de creación de valor a sus partes interesadas. Por ello, toda organización está expuesta a incertidumbres que pueden dificultar, desviar o impedir su cumplimiento. Gestionar riesgos significa, por tanto, conocer y gestionar el efecto de esa incertidumbre sobre los objetivos.

En consecuencia, el ERM es un sistema que, adecuadamente diseñado e implementado, permite a la organización tomar mejores decisiones, asignar mejor sus recursos, priorizar adecuadamente

sus esfuerzos de control, anticiparse a cambios del entorno y reaccionar con mayor rapidez ante eventos adversos. Del mismo modo, permite identificar oportunidades que, de otro modo, podrían pasar inadvertidas.

En ocasiones, la gestión de riesgos se percibe internamente como una función defensiva, burocrática o centrada en limitar iniciativas. Sin embargo, una aproximación madura al ERM no busca paralizar la actividad ni evitar toda exposición al riesgo, algo además imposible en cualquier organización que aspire a crecer, invertir, innovar o competir. Su propósito es ayudar a asumir riesgos de manera consciente, informada y alineada con la estrategia, dentro de parámetros aceptables para la organización. En otras palabras, el ERM no consiste en eliminar el riesgo, sino en comprenderlo, priorizarlo y gestionarlo de manera que la organización pueda avanzar con mayor seguridad y criterio.

En definitiva, el ERM puede definirse como el sistema mediante el cual la organización gestiona de forma integrada la incertidumbre asociada al logro de sus objetivos. Su valor reside en que ofrece un lenguaje común, una metodología compartida y una base para la toma de decisiones que permite a la empresa actuar con mayor coherencia, disciplina y anticipación.

1.2. Diferencia entre gestión tradicional de riesgos y ERM

La gestión de riesgos en las organizaciones ha evolucionado de forma significativa en las últimas décadas. Tradicionalmente, los riesgos se gestionaban de manera fragmentada, abordándose de forma aislada en función de su naturaleza o del área responsable. Este enfoque, conocido como gestión tradicional de riesgos, puede caracterizarse como un modelo reactivo y no integrado. En este modelo, cada área identifica y gestiona sus propios riesgos utilizando criterios, metodologías y horizontes temporales distintos, lo que dificulta la obtención de una visión agregada y coherente. Como

consecuencia, pueden pasar desapercibidas correlaciones entre riesgos, concentraciones de exposición o efectos cruzados que, en conjunto, pueden tener un impacto significativo sobre la organización.

El ERM surge como respuesta a estas limitaciones, proponiendo un enfoque integrado y transversal que permite gestionar el riesgo de manera coordinada en toda la organización. Frente a la visión parcial del enfoque tradicional, el ERM proporciona una perspectiva global que facilita la comprensión del perfil de riesgo en su conjunto y su alineación con los objetivos estratégicos.

A diferencia de la gestión tradicional, el ERM promueve un enfoque proactivo, incorporando el análisis del riesgo en la planificación estratégica, la evaluación de alternativas y la definición de objetivos. De este modo, el riesgo deja de ser un elemento externo a la decisión para convertirse en un factor integrado en la misma.

Asimismo, el ERM implica un cambio en la responsabilidad sobre la gestión del riesgo. En el modelo tradicional, esta responsabilidad suele concentrarse en funciones específicas, mientras que en el ERM se distribuye a lo largo de toda la organización. Las áreas de negocio asumen la gestión de sus riesgos, apoyadas por una función especializada que proporciona metodología, coordinación y una visión agregada.

Otra diferencia relevante es la consideración del riesgo en términos de oportunidad. Mientras que el enfoque tradicional se centra fundamentalmente en la mitigación de pérdidas, el ERM reconoce que la asunción controlada de riesgos es inherente a la actividad empresarial y puede ser fuente de valor. Este enfoque permite a las organizaciones no solo protegerse frente a amenazas, sino también identificar y aprovechar oportunidades de crecimiento o mejora.

En definitiva, el paso de la gestión tradicional de riesgos al ERM supone una evolución desde un modelo fragmentado, reactivo y centrado en el control hacia un sistema integrado, proactivo y alineado con la estrategia. Este cambio de enfoque permite a las organizaciones

gestionar de forma más eficaz la incertidumbre y mejorar la calidad de sus decisiones en un entorno cada vez más complejo.

1.3.ERM como parte de la gobernanza corporativa

El Enterprise Risk Management constituye un elemento esencial del sistema de gobernanza corporativa, al proporcionar un marco estructurado para gestionar la incertidumbre asociada al cumplimiento de los objetivos empresariales. Su integración en la organización permite reforzar la calidad de las decisiones, mejorar la transparencia y facilitar una adecuada supervisión de los riesgos por parte de los órganos de gobierno.

La gobernanza corporativa se basa en el establecimiento de estructuras, procesos y responsabilidades que aseguren una dirección y control adecuados de la organización. En este contexto, la gestión de riesgos no puede considerarse una actividad independiente o secundaria, sino un componente intrínseco al propio modelo de gobierno.

El ERM facilita que el Consejo de Administración y la Alta Dirección dispongan de información estructurada y relevante para el ejercicio de sus funciones. En particular, contribuye a mejorar la evaluación de las decisiones estratégicas al incorporar el análisis de riesgos, y a reforzar los mecanismos de supervisión mediante una comprensión global del perfil de riesgo de la organización.

Entre las responsabilidades del Consejo de Administración se encuentran la aprobación de la política de gestión de riesgos, el establecimiento de directrices generales y la supervisión de la eficacia del sistema implantado. Asimismo, debe asegurarse de que el nivel de riesgo asumido es coherente con la estrategia y con el apetito al riesgo definido.

Las Comisiones de Auditoría apoyan al Consejo de Administración en la supervisión del sistema de control interno y gestión de riesgos. Su función es revisar, con una visión técnica e independiente, la eficacia de estos sistemas, la actividad de auditoría interna y la

calidad de la información sobre riesgos que se eleva a los órganos de gobierno, reforzando así la capacidad del Consejo para ejercer una supervisión efectiva. Organizaciones con una exposición al riesgo elevada o compleja, o cuando el sector/regulación exige una supervisión más especializada, cuentan con Comisiones específicas de riesgos.

Habitualmente, la Alta Dirección propone un apetito al riesgo y el Consejo lo aprueba o supervisa, según el modelo de gobierno aplicable. Este apetito puede establecerse por categorías de riesgo, mediante límites asociados a KRIs que permitan identificar desviaciones respecto a los niveles de tolerancia definidos. Por ejemplo, declarar un apetito bajo en seguridad de la información implica que ningún proyecto crítico pueda salir a producción sin revisión previa de ciberseguridad. Si la empresa mantiene un apetito moderado por la innovación, la política puede permitir pilotos y prototipos siempre que existan mecanismos claros de seguimiento y puntos definidos de parada o escalado.

Por su parte, la Alta Dirección es responsable de implantar y desarrollar el sistema de gestión de riesgos, integrándolo en la operativa de la organización y asegurando su correcta aplicación en los distintos niveles. Esto implica no solo definir procesos y metodologías, sino también promover una cultura que favorezca la identificación, comunicación y gestión de los riesgos.

En este marco, resulta especialmente relevante el modelo de las Tres Líneas del IIA[1], que proporciona una referencia clara para la asignación de responsabilidades en materia de gestión y supervisión del riesgo dentro de la organización. En su actualización de 2026, recogida en el documento *Three Lines Model: Assurance and Advice in Support of Effective Governance*, el IIA mantiene la estructura básica del modelo, pero refuerza su enfoque como marco de aseguramiento y asesoramiento coordinado al servicio de una gobernanza eficaz.

1. Aunque el modelo de referencia se estructura en torno a tres líneas, algunas organizaciones utilizan de forma informal el concepto de “cuarta línea” para referirse a fuentes externas de aseguramiento, como auditores externos, reguladores, certificadores o revisores independientes. No obstante, esta denominación no forma parte del Modelo de las Tres Líneas del IIA.

La distribución de responsabilidades entre los órganos de gobierno, la Alta Dirección y las distintas líneas puede representarse mediante el Modelo de las Tres Líneas, que facilita la asignación de roles de gestión, supervisión y aseguramiento independiente, como se muestra en la Figura 1.

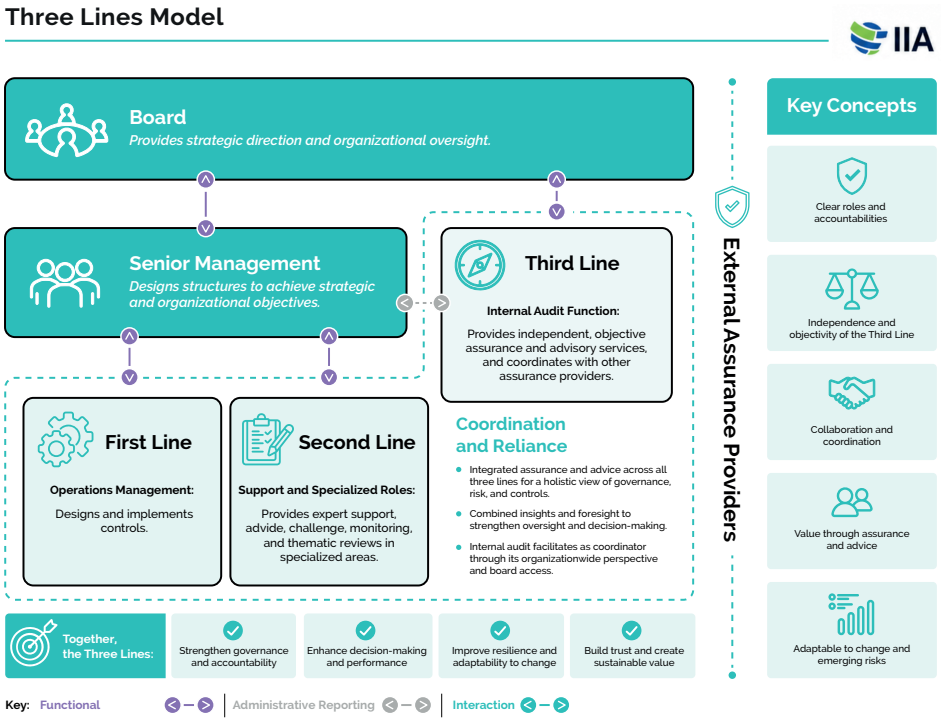


Figura 1 **Modelo de las Tres Líneas: aseguramiento y asesoramiento coordinado.**

Fuente: The Institute of Internal Auditors (IIA) — Three Lines Model: Assurance and Advice in Support of Effective Governance.

El modelo distingue tres tipos de roles complementarios:

- **Primera línea:** formada por las áreas de negocio, operativas y de soporte que gestionan los riesgos en el día a día. Son responsables de diseñar y operar procesos y controles, gestionar los riesgos derivados de su actividad, tomar decisiones dentro del apetito y las tolerancias definidos, y escalar las desviaciones relevantes.

- **Segunda línea:** integrada por funciones especializadas —como riesgos, cumplimiento, control interno, seguridad, calidad, sostenibilidad, continuidad de negocio u otras funciones de supervisión— que proporcionan metodología, asesoramiento experto, monitorización, revisión temática y desafío a la primera línea. Su función no es sustituir la responsabilidad del negocio, sino reforzar la calidad, consistencia y trazabilidad de la gestión del riesgo.

- **Tercera línea:** representada por auditoría interna, que proporciona aseguramiento independiente y objetivo sobre la eficacia del gobierno, la gestión de riesgos, el cumplimiento y los controles. Auditoría interna puede también aportar asesoramiento, perspectivas y recomendaciones para mejorar el modelo, siempre que no asuma responsabilidades de gestión ni comprometa su independencia u objetividad.

La actualización de 2026 refuerza que las tres líneas no deben operar como compartimentos estancos. La independencia de auditoría interna es esencial, pero no implica aislamiento. Un modelo eficaz requiere coordinación, intercambio de información, claridad de responsabilidades y, cuando proceda, mecanismos de aseguramiento integrado que permitan evitar duplicidades, identificar lagunas de cobertura y proporcionar al Consejo y a la Alta Dirección una visión coherente y fiable sobre gobierno, riesgos, cumplimiento y controles.

No obstante, la colaboración entre líneas debe apoyarse en límites claros. Auditoría interna puede asesorar, facilitar discusiones, revisar metodologías, desafiar supuestos o aportar buenas prácticas sobre el modelo ERM, pero no debe asumir decisiones de gestión, definir respuestas al riesgo, operar controles ni sustituir la responsabilidad de la primera o segunda línea. Cuando existan solapamientos por razones de tamaño, madurez, recursos o diseño organizativo, deberán documentarse las responsabilidades, aprobarse por los órganos de gobierno correspondientes y establecerse salvaguardas para preservar la independencia y objetividad del aseguramiento.

Asimismo, la integración del ERM en la gobernanza corporativa facilita la coordinación entre distintas funciones clave, optimizando el uso de recursos y mejorando la eficacia global del sistema.

En un entorno en el que los requerimientos regulatorios y de buen gobierno son cada vez más exigentes, el ERM se convierte en una herramienta fundamental para asegurar el cumplimiento de dichas exigencias, especialmente en materia de transparencia y reporting.

Por último, cabe destacar la importancia del denominado *"tone at the top"*, entendido como el compromiso y ejemplo de la Alta Dirección en materia de gestión de riesgos. Una organización en la que el riesgo forma parte de la toma de decisiones estará mejor preparada para afrontar la incertidumbre y adaptarse a un entorno cambiante. Este concepto será desarrollado con mayor detalle en apartados posteriores de la guía.

En definitiva, el ERM forma parte esencial del sistema de gobernanza corporativa, al permitir una gestión más estructurada y alineada con los objetivos de la organización.

1.4.Marcos de referencia para la gestión del riesgo

Para la implantación de un sistema ERM en una organización no es necesario partir de cero. Existen diferentes marcos que proporcionan principios, directrices y buenas prácticas para el diseño, implantación y mejora de la gestión de riesgos en las organizaciones.

Estos marcos no deben interpretarse como modelos rígidos ni como soluciones estandarizadas de aplicación directa, sino como referencias que permiten estructurar el enfoque, asegurar la consistencia metodológica y alinear la gestión del riesgo con las mejores prácticas internacionales. Cada organización debe adaptar dichos marcos a su contexto, teniendo en cuenta su tamaño, sector, complejidad y nivel de madurez.

Entre los principales marcos de referencia destacan los siguientes:

- **COSO ERM**

El marco COSO ERM *(Enterprise Risk Management – Integrating Strategy and Performance)* es uno de los referentes internacionales más relevantes en la gestión de riesgos empresariales. Fue desarrollado por el *Committee of Sponsoring Organizations of the Treadway Commission*, organización creada en Estados Unidos en 1985 con el objetivo de mejorar la calidad de la información financiera, el control interno y la gobernanza corporativa.

La evolución del modelo ha estado marcada por dos hitos principales: la publicación inicial del marco en 2004 (Enterprise Risk Management – Integrated Framework) y su actualización en 2017, que refuerza la integración del riesgo en la estrategia y el desempeño organizativo.

La principal aportación de COSO ERM consiste en situar la gestión del riesgo como un elemento central en la toma de decisiones y en la creación, preservación y materialización de valor. Su enfoque conecta de forma directa la gestión del riesgo con la definición de la estrategia, la ejecución del negocio y los mecanismos de gobierno corporativo.

El modelo se estructura en cinco componentes interrelacionados:

- Gobierno y cultura
- Estrategia y establecimiento de objetivos
- Desempeño
- Revisión y monitorización
- Información, comunicación y reporte

Cada uno de estos componentes se desarrolla a través de un conjunto de principios que orientan su implantación, proporcionando una guía práctica para diseñar, implementar y evaluar la eficacia del sistema de gestión de riesgos.

En conjunto, COSO ERM ofrece un marco estructurado que facilita la integración del riesgo en la estrategia, el desempeño y el gobierno corporativo.

- **ISO 31000**

La norma ISO 31000 constituye uno de los principales marcos de referencia internacionales en materia de gestión de riesgos, por su carácter transversal y su aplicabilidad a cualquier tipo de organización, independientemente de su tamaño, sector o complejidad. Fue desarrollada por la Organización Internacional de Normalización, entidad independiente creada en 1947 que elabora estándares internacionales con el objetivo de facilitar buenas prácticas y armonizar criterios a nivel global.

La primera versión de la norma ISO 31000 se publicó en 2009 y fue revisada en 2018, incorporando un enfoque más claro hacia la integración del riesgo en la gestión global de la organización y reforzando su conexión con la toma de decisiones. ISO 31000 adopta un enfoque flexible orientado a facilitar la integración del riesgo en cualquier tipo de organización.

El modelo se articula en torno a tres elementos clave:

- Principios, que establecen las bases para una gestión eficaz del riesgo.
- Marco de referencia, que define cómo integrar la gestión del riesgo en la gobernanza, la estrategia y los procesos organizativos.
- Proceso de gestión del riesgo, que describe las etapas para identificar, analizar, evaluar, tratar, monitorizar y comunicar los riesgos.

En conjunto, ISO 31000 proporciona un marco adaptable y escalable que facilita la integración del riesgo en la gestión, adaptándolo al contexto específico de cada organización.

Además de ISO 31000 como marco general de referencia, existen otros estándares ISO que complementan la gestión integral de riesgos desde perspectivas específicas. Entre ellos destacan IEC 31010:2019 — Risk management — Risk assessment techniques, centrado en técnicas de evaluación del riesgo; ISO/TS 31050:2023

— Risk management — Guidelines for managing emerging risks to enhance resilience, orientado a la identificación y gestión de riesgos emergentes; ISO 31022:2020 — Risk management — Guidelines for the management of legal risk, relativa a la gestión del riesgo legal; e ISO 31073:2022 — Risk management — Vocabulary, que proporciona vocabulario común en materia de gestión de riesgos. Estos estándares no sustituyen a ISO 31000, sino que la complementan y permiten profundizar en ámbitos concretos del sistema ERM, en función del contexto, sector, nivel de madurez y necesidades de cada organización.

- **FERMA**

La *Federation of European Risk Management Associations* constituye uno de los principales marcos de referencia en la disciplina de la gestión de riesgos a nivel europeo. A través de su estándar de gestión de riesgos, FERMA proporciona un enfoque estructurado y homogéneo que facilita a las organizaciones la identificación, evaluación y tratamiento de los riesgos asociados a sus actividades.

A diferencia de otros marcos normativos, FERMA no tiene carácter regulatorio ni certificable, sino que se configura como una guía de buenas prácticas ampliamente aceptada en el ámbito profesional. Su valor radica en ofrecer un lenguaje común y un conjunto de principios que permiten integrar la gestión de riesgos dentro de la estrategia y la toma de decisiones empresariales.

En el contexto de ERM, el marco FERMA se posiciona como un complemento a otros estándares internacionales, aportando una visión práctica y orientada al negocio. Su utilización permite a las organizaciones avanzar hacia modelos de gestión más maduros, basados en la integración de los riesgos en todos los niveles de la organización y en la generación de valor sostenible.

- **Marcos regulatorios sectoriales (Basilea y Solvencia II)**

En determinados sectores, especialmente en el ámbito financiero y asegurador, existen marcos regulatorios específicos que establecen requisitos en materia de gestión de riesgos, entre los que destacan los acuerdos de Basilea y el régimen de Solvencia II.

Ambos marcos han sido desarrollados con el objetivo de reforzar la estabilidad financiera de las entidades, promoviendo una gestión del riesgo más rigurosa e integrada en la toma de decisiones.

En el caso del sector bancario, los acuerdos de Basilea, impulsados por el Comité de Supervisión Bancaria de Basilea, han introducido un enfoque basado en el riesgo que vincula los requerimientos de capital con la exposición asumida por las entidades. Por su parte, Solvencia II, aplicable al sector asegurador y desarrollado en el ámbito europeo bajo la supervisión de la Autoridad Europea de Seguros y Pensiones de Jubilación, establece un modelo similar basado en tres pilares: requerimientos cuantitativos, gobernanza y gestión de riesgos, y transparencia.

En otras palabras, estos marcos constituyen una referencia relevante para organizaciones que operan en entornos regulados o que requieren un mayor nivel de sofisticación en la gestión del riesgo. No obstante, en el contexto de una guía general de implantación del ERM, su aplicación debe entenderse como complementaria a marcos más transversales como COSO ERM o ISO 31000.

Existen, además, otros marcos de referencia, estándares sectoriales y guías de buenas prácticas que pueden complementar los enfoques descritos, especialmente en contextos regulatorios específicos o en ámbitos especializados de la gestión de riesgos. En la práctica, las organizaciones suelen combinar elementos de distintos modelos en función de sus necesidades, construyendo un sistema propio, coherente y alineado con sus objetivos. En este sentido, el valor del ERM no reside en la adopción formal de un marco concreto, sino en su adecuada adaptación a la realidad de la organización y en su capacidad para integrarse en la gestión de forma efectiva.

1.5. Principios fundamentales del Enterprise Risk Management

La implantación de un sistema de Enterprise Risk Management debe sustentarse en una serie de principios que orienten su diseño, aplicación y evolución en la organización. Los principales marcos de referencia en materia de gestión de riesgos, como COSO ERM e ISO 31000, establecen sus propios conjuntos de principios que guían la implantación de sistemas eficaces. Estos principios constituyen una base sólida y ampliamente reconocida, que cada organización puede adaptar a su contexto, teniendo en cuenta su tamaño, sector, complejidad y nivel de madurez.

En este sentido, y con el objetivo de facilitar su comprensión y utilización práctica, se propone a continuación una síntesis de los elementos esenciales que deben sustentar un sistema de ERM, organizada en cuatro dimensiones clave que recogen, de forma estructurada, los principios fundamentales de la gestión de riesgos. Esta propuesta no pretende sustituir los marcos de referencia existentes, sino ofrecer una visión integrada y operativa que facilite su adaptación e implantación en las organizaciones.

i) Gobernanza y cultura

El ERM debe apoyarse en un modelo de gobernanza claro, en el que se definan adecuadamente las responsabilidades en materia de gestión del riesgo y se garantice la supervisión por parte de los órganos de gobierno. Este principio implica que el Consejo de Administración (o máximo órgano de gobierno en la organización) y la Alta Dirección asuman un papel activo en la definición de las directrices de gestión de riesgos, en la aprobación del apetito al riesgo y en la supervisión del sistema. Asimismo, requiere la existencia de estructuras organizativas adecuadas y una clara asignación de responsabilidades entre las distintas funciones. La eficacia del ERM depende en gran medida de la cultura organizativa. Es necesario promover un entorno en el que la gestión del riesgo forme parte de la actividad habitual, fomentando la transparencia, la comunicación y

la adecuada consideración de la incertidumbre en todos los niveles de la organización.

ii) Estrategia y toma de decisiones

La gestión del riesgo debe integrarse en la definición de la estrategia y en la toma de decisiones clave de la organización. El ERM aporta valor cuando permite analizar las implicaciones de riesgo de las distintas alternativas estratégicas y asegurar su coherencia con el nivel de riesgo que la organización está dispuesta a asumir. Este principio incluye el análisis del contexto interno y externo, la definición del apetito al riesgo y su consideración en el establecimiento de objetivos. Asimismo, implica que el riesgo sea un elemento relevante en la evaluación de inversiones, proyectos y decisiones operativas significativas. La incorporación del riesgo en la toma de decisiones permite mejorar la calidad de las mismas y alinear la actuación de la organización con sus objetivos estratégicos.

iii) Evaluación y gestión del riesgo

El ERM debe basarse en un enfoque estructurado que permita identificar, analizar, evaluar y tratar los riesgos de forma sistemática y consistente en toda la organización. Este principio implica la utilización de metodologías homogéneas que faciliten la comparabilidad entre riesgos, la priorización de los mismos y la definición de respuestas adecuadas. De esta forma, incluye la consideración del riesgo desde una perspectiva agregada, permitiendo entender su impacto conjunto sobre la organización. La gestión del riesgo no se limita a la mitigación de amenazas, sino que también debe contemplar la identificación de oportunidades y la adopción de decisiones informadas sobre la asunción de riesgos.

iv) Seguimiento, información y mejora

El sistema de gestión de riesgos debe incorporar mecanismos que permitan su monitorización continua, la evaluación de su eficacia y su mejora a lo largo del tiempo. Este principio incluye el seguimiento de los riesgos y de las acciones definidas, la elaboración de información relevante para los distintos niveles de la organización y la revisión

periódica del sistema. Del mismo modo, implica la capacidad de adaptación ante cambios en el entorno, en la estrategia o en el perfil de riesgo. La mejora continua del ERM permite a la organización evolucionar hacia modelos más maduros, reforzando su capacidad para anticipar riesgos, adaptarse a nuevas situaciones y gestionar la incertidumbre de forma eficaz.

En conjunto, estas cuatro dimensiones permiten estructurar de forma clara y coherente los elementos esenciales de un sistema de *Enterprise Risk Management*, facilitando su comprensión y aplicación práctica en la organización. Lejos de constituir un modelo rígido, este enfoque debe entenderse como una referencia que orienta el diseño del sistema de gestión de riesgos, permitiendo a cada organización adaptarlo a su contexto, prioridades y nivel de madurez.

Su aplicación integrada favorece que la gestión del riesgo se incorpore de manera natural en la actividad de la organización, contribuyendo a una mayor coherencia en la toma de decisiones, una mejor utilización de los recursos y una mayor capacidad de adaptación ante un entorno incierto y cambiante.

Este marco conceptual constituye, por tanto, una base sobre la que desarrollar e implantar el sistema de gestión de riesgos, cuyos aspectos prácticos se abordan en los siguientes apartados de esta guía.

Capítulo 2.
Contexto organizacional

2.1. Qué es "contexto" en ERM y por qué importa

Definir el contexto organizacional no es opcional: es el paso previo que permite concentrar el ERM en los riesgos realmente materiales para el negocio y evitar esfuerzos dispersos. Los marcos reconocidos coinciden en tres ideas clave: el ERM debe integrarse en la estrategia y en la ejecución, personalizarse al entorno interno y externo de la organización, y contar con liderazgo y compromiso explícitos desde la Alta Dirección.

En esta guía se propone trabajar con un doble horizonte, por un lado, de 12 meses, que permita realizar un seguimiento y reporte cíclico anual alineado con los ciclos de planificación y seguimiento directivo, y un segundo horizonte alineado con el plan estratégico de la organización y con los objetivos de negocio más habituales en empresas medianas y grandes: internacionalización, diversificación, digitalización y mantenimiento de la calidad y del servicio. El resultado buscado es un Resumen de Contexto conciso que permita priorizar decisiones y recursos en los próximos comités, en coherencia con la estrategia.

Dentro del contexto de la compañía deberá analizarse:

- Objetivos y prioridades a 12 meses, con criterios de éxito y dependencias entre áreas.

- Proyectos estratégicos en curso o planificados (p. ej., transformación digital, ERP (Enterprise Resource Planning), expansión, internacionalización, diversificación…) y su vinculación explícita con la estrategia y con la toma de decisiones de riesgo.
- Entorno externo (PESTEL "ligero" [2]): priorizar situación geopolítica, estabilidad regulatoria, competencia, ciberseguridad y sostenibilidad.
- Entorno interno y funciones de aseguramiento existentes: auditoría interna y otras funciones de aseguramiento, seguridad y salud laboral, cumplimiento normativo, calidad, ciberseguridad; control interno de información financiera y de sostenibilidad, entre otras; clarificar desde el inicio la separación práctica entre gestión, funciones de control y auditoría interna de acuerdo con el modelo de las tres líneas (ver modelo de las tres líneas descrito en el punto 1.3 de la Introducción).
- Lecciones aprendidas: presiones del regulador, accionistas y clientes para reforzar control de riesgos, resiliencia y continuidad de negocio; incidentes o "casi incidentes" que se hayan producido en la organización.

2.2. Entorno externo (PESTEL práctico)

PESTEL es una herramienta para analizar el entorno externo de la organización agrupando los factores en seis categorías: Políticos, Económicos, Sociales, Tecnológicos, Legales y Ambientales. Sirve para detectar tendencias y condicionantes que pueden incidir en los objetivos y decisiones de la empresa, y es ampliamente utilizada en dirección y gestión como apoyo a la planificación y a la gestión del riesgo.

Es recomendable definir, al inicio del análisis, los siguientes puntos:

- Ámbito y horizonte: confirmar alcance temporal del análisis y

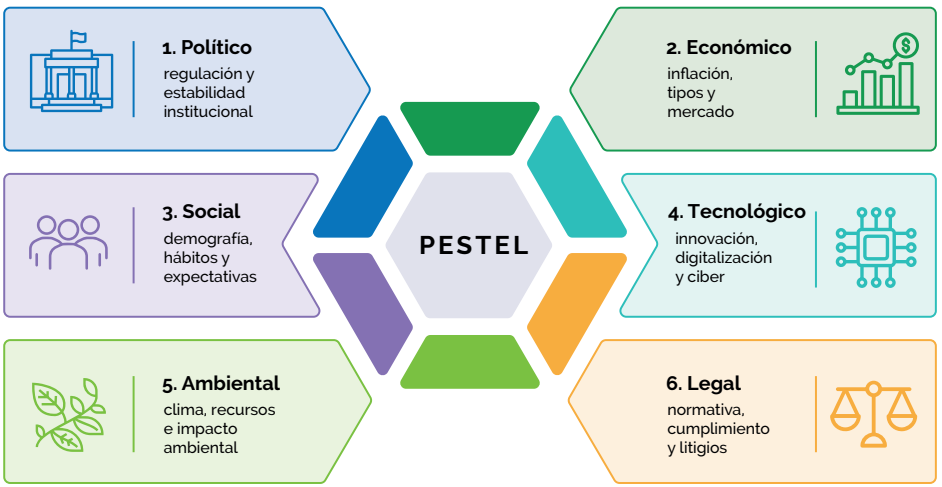
2. Versión simplificada de la herramienta de planificación estratégica Análisis PESTEL. Se utiliza para evaluar rápidamente cómo el macroentorno afecta a un proyecto o negocio, enfocándose sólo en las variables más críticas en lugar de hacer un estudio exhaustivo de las seis dimensiones originales (Político, Económico, Sociocultural, Tecnológico, Ambiental y Legal).

centrarlo en factores con potencial efecto material sobre objetivos (crecimiento, rentabilidad, servicio, digitalización, resiliencia).

- Periodicidad de revisión: Establecer una periodicidad para revisar el sistema, trimestral en entornos muy cambiantes o semestral si hay mayor estabilidad.

Análisis del entorno PESTEL

Herramienta para analizar el contexto externo de la organización



El análisis PESTEL facilita la identificación de riesgos y oportunidades del entorno externo.

Figura 2: **Análisis del entorno PESTEL.** Fuente: elaboración propia.

Para realizar el análisis PESTEL, se pueden analizar las siguientes categorías:

- Político: políticas públicas, estabilidad institucional, relaciones comerciales, incentivos o restricciones sectoriales, entorno geopolítico.
- Económico: actividad y crecimiento, inflación y tipos de interés, tipo de cambio, empleo, acceso a crédito, costes de insumos y energía.
- Social: demografía y talento, hábitos y sensibilidad de clientes (precio/calidad/servicio), expectativas de transparencia y

seguridad.

- Tecnológico: automatización e inteligencia artificial, dependencia de proveedores tecnológicos, ciberamenazas, estándares y gestión de datos.
- Legal/Regulatorio: cambios normativos relevantes (competencia, protección de datos, seguridad, producto/servicio, comercio), exigencias de reporte.
- Ambiental: clima y eventos extremos, políticas ambientales, eficiencia de recursos, expectativas de sostenibilidad en la cadena de suministro.

2.3. Entorno interno y capacidades/gobernanza existentes

Desde la Alta Dirección, se debe determinar cómo se decide y con qué capacidades cuenta la organización para gestionar riesgos hoy (estructura, responsabilidades, procesos y controles, personas, información y sistemas, y cultura). El alcance debe permitir cubrir todo aquello considerado crítico por impacto potencial alto o probabilidad alta de materialización; la concreción de criterios y umbrales se definirá en Fase inicial: definición del marco ERM. La toma de decisiones debe armonizarse con la estructura directiva, evitando el exceso de comités y garantizando capacidad real de decisión de quienes integren el comité de riesgos.

Internamente, deben analizarse la estructura organizativa, los comités existentes y otros elementos de organización y toma de decisiones: organigrama, foros y relación práctica entre las tres líneas (ver modelo de las tres líneas descrito en el punto 1.3 de la Introducción).

Además, es necesario realizar un análisis integral que tenga en cuenta los procesos y controles existentes, identificando aquellos procesos críticos, los controles ya implantados y posibles puntos únicos de fallo. Este análisis debe completarse con una revisión de las personas y competencias disponibles, considerando los recursos existentes, los perfiles críticos, las coberturas necesarias y el nivel

de formación. Asimismo, resulta clave evaluar la información y los sistemas que soportan la actividad, incluyendo las aplicaciones, los datos maestros y las dependencias técnicas más relevantes.

Todo ello debe enmarcarse en el contexto de las políticas y procedimientos vigentes, como los relacionados con calidad, seguridad de la información, cumplimiento normativo o continuidad de negocio, verificando su adecuación y grado de implantación. De igual modo, conviene tener en cuenta las funciones ya existentes dentro de la organización, como auditoría interna y externa, prevención de riesgos laborales, cumplimiento, calidad, seguridad de la información, protección de datos, seguridad física y continuidad de negocio. Finalmente, el análisis debe incorporar las lecciones aprendidas en los últimos 12 a 24 meses, de manera que la experiencia reciente sirva como base para reforzar y mejorar el enfoque global.

Aspectos a revisar en el diagnóstico

Como parte del análisis del entorno interno, la organización deberá identificar aquellos aspectos que puedan limitar la implantación efectiva del modelo ERM o reducir la calidad de la información utilizada para la toma de decisiones. Esta revisión no debe plantearse como un ejercicio de cumplimiento formal, sino como una herramienta para detectar brechas reales de gobernanza, metodología, cultura, información y capacidades.

- Madurez cultural en gestión del riesgo en desarrollo: reforzar reporte temprano, trazabilidad y mejora continua; diferenciar riesgo corporativo de incidencias operativas puntuales.
- Alineación dirección–equipos y decisiones informadas por datos: establecer un sistema de información de riesgos corporativos que conecte riesgos–objetivos–decisiones con datos objetivos y método homogéneo.
- Transversalidad e intercambio de información: acordar un catálogo mínimo de datos y reglas de intercambio entre áreas; clarificar roles entre las tres líneas (ver modelo de las tres líneas).

- Percepción del riesgo y comunicación interna: explicitar que el reporte temprano es esperado y positivo; pautas no sancionadoras.
- Claridad funcional y complementariedad con continuidad de negocio: diferenciar anticipación/priorización (riesgos) de respuesta/recuperación (continuidad) y coordinar con funciones afines.
- Criterios y escalas de evaluación heterogéneos.
- Comunicaciones y consulta fragmentada.
- Documentación y trazabilidad de decisiones insuficientes.
- Recursos y competencias limitados en gestión del riesgo.
- Integración incompleta del riesgo en planificación, presupuesto y proyectos.
- Vigilancia de riesgos emergentes poco sistemática.

El resultado de esta revisión deberá permitir priorizar las principales brechas a corregir, evitando generar planes excesivamente amplios que no puedan ser implantados o supervisados con los recursos disponibles.

2.4. Tone at the top

El *"Tone at the Top"* hace referencia al compromiso efectivo de la Alta Dirección con la Gestión de Riesgos y constituye un pilar esencial del enfoque ERM. Un *"Tone at the Top"* adecuado se manifiesta cuando la Alta Dirección actúa de forma coherente con los principios de la gestión de riesgos, los integra en la toma de decisiones estratégicas y comunica de manera clara y constante su relevancia para el conjunto de la organización. De este modo, la gestión de riesgos deja de percibirse como un mero ejercicio de cumplimiento formal y se consolida como un valor corporativo y estratégico, reforzando la rendición de cuentas y la responsabilidad individual en todos los niveles.

Para ello, resulta clave que la Alta Dirección incorpore la gestión de riesgos de forma sistemática en la definición de objetivos, la planificación, la asignación de recursos y los mecanismos de

seguimiento, así como que fomente una cultura en la que el reporte temprano de riesgos sea esperado y valorado positivamente como un elemento de anticipación y mejora continua. Asimismo, debe exigir información periódica y estructurada sobre los riesgos más relevantes para asegurar una visión actualizada y coherente del perfil de riesgo, y velar por una correcta delimitación de funciones entre la gestión de riesgos, propia de la segunda línea, y la auditoría interna, correspondiente a la tercera, garantizando en todo momento la independencia de esta última.

El compromiso de la Alta Dirección debe traducirse en comportamientos visibles, decisiones coherentes y mecanismos de seguimiento que refuercen la cultura de riesgo en todos los niveles, como se muestra en la Figura 3.

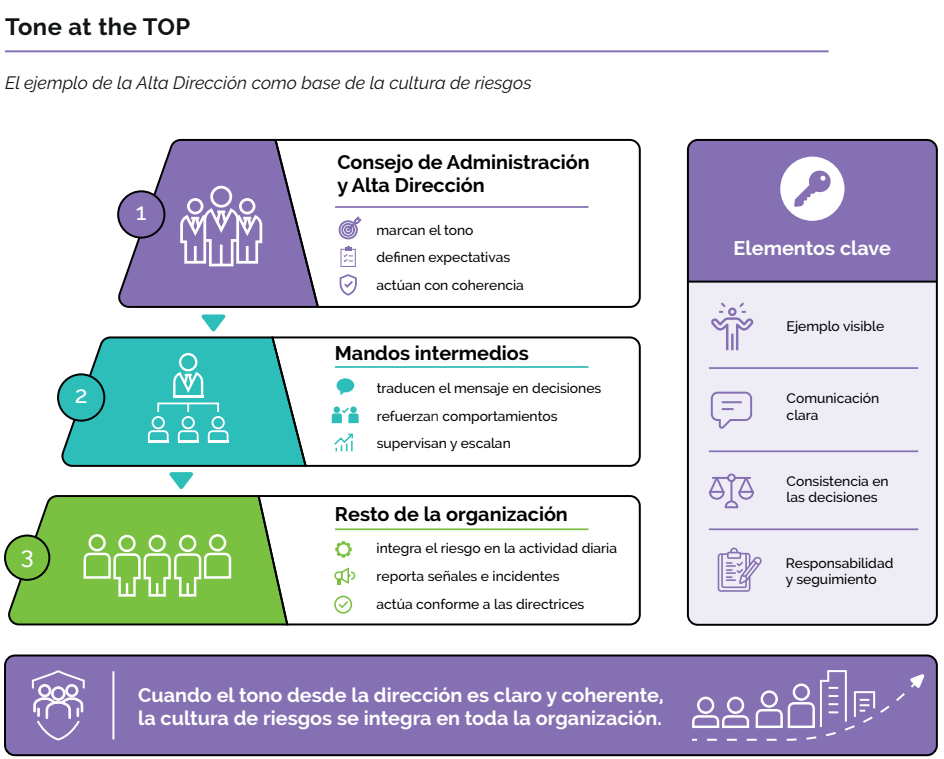


Figura 3: **Tone at the top y cultura de riesgo.** Fuente: elaboración propia.

Aplicación práctica a corto plazo

- Mensajes directivos programados (inicio y recordatorios trimestrales).
- Integración en rutinas de gestión: punto de riesgos en reuniones de dirección y de unidad.
- Seguimiento periódico: calendario de revisión con responsables.
- Escalado ordenado: criterios de escalado (definición operativa en Fase inicial).
- Coordinación entre líneas manteniendo la independencia de auditoría interna.

2.5 Relación con otras áreas

Desde la Alta Dirección, es clave establecer interfaces claras entre las distintas áreas, definiendo con precisión qué decisiones corresponden a cada una, qué información debe compartirse y con qué frecuencia, de modo que se eviten solapamientos y vacíos de responsabilidad. En este marco, resulta especialmente importante preservar la independencia de la auditoría interna, cuya misión es proporcionar aseguramiento objetivo e independiente sobre la eficacia del sistema de gestión y control del riesgo.

En este contexto, puede resultar útil avanzar hacia un enfoque de aseguramiento combinado, entendido como la coordinación estructurada de las actividades de aseguramiento desarrolladas por las distintas funciones de segunda línea de la organización, como riesgos, junto con auditoría interna. Este enfoque permite obtener una visión más integrada de la cobertura de riesgos, identificar posibles solapamientos o lagunas de control y optimizar los esfuerzos de supervisión. No obstante, el aseguramiento combinado no modifica las responsabilidades propias del Modelo de las Tres Líneas ni debe comprometer la independencia de auditoría interna.

Asimismo, conviene evitar la proliferación innecesaria de comités, priorizando en su lugar rutinas de gestión eficaces y bien integradas, con un punto de referencia estable para el seguimiento de los riesgos.

Este enfoque contribuye a una gobernanza más ágil, coherente y orientada a la toma de decisiones.

Aplicación práctica a corto plazo: Matriz de interfaces

De forma práctica se propone realizar la matriz de interfaces, como mínimo producto viable, considerando los siguientes departamentos:

- Finanzas y Control de gestión, Estrategia/Planificación, Operaciones/Producción/Logística.
- Tecnologías de la información y seguridad de la información; Datos y Delegado de Protección de Datos (DPO).
- Cumplimiento y Asuntos legales; Continuidad de negocio; PRL y seguridad física; Calidad y Sostenibilidad/ESG; Compras y Terceros.
- Auditoría interna: receptor de la consolidación para su plan de aseguramiento (independiente).

2.6 Cultura de riesgo

La cultura de riesgo se refiere al conjunto de valores, comportamientos, expectativas y rutinas mediante los cuales la organización identifica, comunica, escala y gestiona los riesgos en su actividad diaria. Una cultura de riesgo adecuada busca que la gestión de riesgos sea un comportamiento organizativo integrado en la toma de decisiones, y no una tarea aislada de una función concreta.

Esta cultura se apoya en factores humanos y organizativos, en línea con ISO 31000, y en la dimensión de gobierno y cultura recogida en COSO ERM. En la práctica, se manifiesta en comportamientos observables: reporte temprano de riesgos e incidentes, transparencia sobre supuestos e incertidumbres, aprendizaje a partir de errores, claridad de responsabilidades y decisiones coherentes con el apetito y las tolerancias definidos.

Para la Alta Dirección, resulta esencial definir y comunicar de forma explícita las expectativas de conducta en materia de

riesgo, fomentando el reporte temprano, la transparencia sobre supuestos e incertidumbres y el aprendizaje documentado a partir de la experiencia. Esta coherencia debe reflejarse también en la alineación entre las decisiones adoptadas, los objetivos estratégicos de la organización y el apetito al riesgo definido.

La cultura de riesgo debe integrarse de manera natural en las revisiones periódicas de la Alta Dirección y de las distintas unidades, de modo que forme parte habitual del diálogo directivo y no se perciba como un elemento aislado. En este contexto, es igualmente importante reconocer y reforzar las conductas deseadas, creando un entorno en el que el reporte de riesgos no sea objeto de sanción, sino entendido como una contribución positiva a la gestión y a la mejora continua de la organización.

Para aplicar de forma práctica la cultura de riesgo, pueden impulsarse medidas sencillas con apoyo de los mandos intermedios, tales como:

- **Dominios culturales:** fomentar la transparencia y el reporte temprano de alertas y riesgos; el aprendizaje y la mejora continua; la responsabilidad asignada y el escalado; la coordinación entre líneas conforme al Modelo de las Tres Líneas; y la toma de decisiones basada en información.
- **Pulso cultural periódico:** realizar una autoevaluación breve, con carácter semestral o anual, que permita valorar avances en transparencia, escalado, aprendizaje, coordinación y responsabilidad sobre los riesgos.
- **Acciones iniciales de corto plazo:** lanzar mensajes iniciales, pautas básicas o materiales prácticos que permitan a los equipos comprender los conceptos esenciales de gestión de riesgos, conocer los canales de escalado y generar evidencias ligeras de aplicación.

2.7 Comunicación y sensibilización

La comunicación y la sensibilización son elementos esenciales para que el ERM se integre en la cultura y en las rutinas de trabajo. Sin

ellas, el modelo puede convertirse en un conjunto de documentos sin impacto real en la toma de decisiones ni en la gestión diaria.

La comunicación tiene como objetivo asegurar que las personas conocen el modelo de gestión de riesgos, sus objetivos, roles asignados, criterios de escalado, canales disponibles y la información que debe ser reportada. Esta comunicación debe ser clara, práctica y adaptada a los distintos niveles de la organización, evitando mensajes excesivamente técnicos o alejados de la realidad operativa.

La sensibilización busca que las personas comprendan por qué la gestión de riesgos es relevante para su actividad, qué se espera de ellas y cómo pueden contribuir al modelo. No se limita a informar sobre procedimientos, sino que pretende generar conciencia sobre la importancia de identificar riesgos a tiempo, escalar situaciones relevantes, documentar decisiones y aprender de incidentes o errores.

Para la Alta Dirección, el "tone at the top" se demuestra con acciones visibles. Incluir la revisión de riesgos en las reuniones de Dirección, aprobar mensajes periódicos e impulsar materiales prácticos consolida la cultura de riesgo desde el inicio y refuerza la percepción de que el ERM es una herramienta de gestión, no una carga administrativa.

Para los mandos intermedios, la sensibilización debe traducirse en acciones concretas: incorporar un punto de riesgos en las reuniones de equipo, revisar incidentes con enfoque de aprendizaje, recordar criterios de escalado y utilizar guías breves o materiales sencillos para asegurar que todos comprenden qué se espera de ellos.

La comunicación también debe funcionar de abajo arriba y de forma transversal, permitiendo que las áreas reporten riesgos, señales tempranas, incidentes, cambios relevantes, debilidades de control o necesidades de escalado. Esta comunicación ascendente es clave para que la función de riesgos y la Alta Dirección dispongan de una visión actualizada y realista del perfil de riesgo.

Cuando la comunicación, la sensibilización, el liderazgo y la práctica diaria están alineados, el ERM deja de percibirse como una carga y pasa a formar parte natural del funcionamiento de la organización.

2.8 Expectativas de los grupos de interés

Para la Alta Dirección, es fundamental identificar, reconocer y priorizar los grupos de interés que resultarán críticos en los próximos 12 meses, asegurando que sus expectativas y posibles impactos estén claramente entendidos. A partir de este análisis, deben establecerse principios claros que guíen la relación con estos grupos, basados en la transparencia, el reporte temprano de riesgos, la trazabilidad de las respuestas y la capacidad de aprendizaje a lo largo del proceso.

Asimismo, los resultados de esta interacción con los grupos de interés deben incorporarse de manera sistemática en las revisiones directivas y reflejarse en los documentos de decisión, de forma que contribuyan a una toma de decisiones más informada, coherente y alineada con las prioridades estratégicas de la organización.

Aplicación práctica a corto plazo

1. Identificación: listar grupos, por qué son relevantes y quién se relaciona con ellos.
2. Priorización: matriz influencia/interés y selección del Top-5.
3. Captura de expectativas: qué esperan, obligaciones, información de riesgos que esperan recibir y decisiones afectadas.
4. Plan de relación y seguimiento: interlocutor, frecuencia y señales tempranas.

Parte II

Implementación del ERM

Una vez establecidos los fundamentos del ERM, esta segunda parte aborda su implantación práctica en la organización. Para ello, se desarrollan las principales fases del proceso: definición del marco inicial, identificación, análisis y evaluación, tratamiento, monitorización, reporting y mejora continua.

El enfoque propuesto debe entenderse de forma flexible y proporcional, adaptando las herramientas y niveles de profundidad al tamaño, sector, complejidad y grado de madurez de cada organización. La finalidad es facilitar una implantación progresiva, útil y alineada con los objetivos empresariales.

Capítulo 3.
Fase inicial: Definición del marco ERM

3.1. Diagnóstico inicial de la Organización

El diagnóstico inicial es el punto de partida imprescindible para construir un modelo ERM creíble, proporcionado y adaptado a la realidad de la organización. Su propósito no es generar documentación extensa, sino ofrecer a la Alta Dirección un diagnóstico claro y realista de cómo se toman decisiones hoy, qué capacidades existen realmente, y qué brechas podrían comprometer la implantación del modelo en los próximos doce meses.

A lo largo de este apartado se distinguen las necesidades y actuaciones de la Alta Dirección y de los mandos intermedios, al desempeñar roles complementarios en la implantación del ERM: la primera define el marco, las prioridades y los mensajes clave que orientan la gestión, mientras que los segundos son esenciales para trasladar esas directrices a la operativa diaria, facilitar su aplicación práctica y asegurar su seguimiento efectivo.

Para la **Alta Dirección**, hay varios elementos que deben considerarse como mínimos. El primero consiste en aprobar un alcance que cubra los elementos que realmente condicionan la gestión del riesgo: la estructura y responsabilidades actuales, los procesos esenciales, los controles existentes, las capacidades del equipo, los sistemas de información y la cultura organizativa. Por ejemplo, si la gestión de pedidos o la facturación depende de un proceso

manual gestionado por una única persona, el diagnóstico debe reflejar esta vulnerabilidad, aunque no conste formalmente en ningún procedimiento. Lo mismo ocurre si la organización sufrió recientemente un incidente crítico —como la caída de un sistema que interrumpió operaciones durante horas—: el diagnóstico debe analizar no solo la causa técnica, sino también cómo funcionaron el escalado, la coordinación entre áreas y la comunicación interna.

El análisis debe alinearse con un **horizonte de doce meses**, para que sus conclusiones sean útiles en el ciclo real de planificación y seguimiento directivo. Si la empresa planea implantar un nuevo ERP (*Enterprise Resource Planning*, es un sistema de software que centraliza y automatiza los procesos clave de una empresa—como finanzas, ventas, inventario y recursos humanos—en una única plataforma, eliminando los programas aislados), el diagnóstico debe evaluar si la estructura actual tiene capacidad para absorber el cambio. Es habitual encontrar departamentos de TI saturados por tareas operativas y áreas usuarias con poca formación en procesos de transformación, lo que puede generar retrasos y aumentar la exposición al riesgo.

La Alta Dirección deberá asegurar que exista un responsable claro del diagnóstico, habitualmente la función de riesgos o quien asuma dicha responsabilidad, con acceso completo a áreas clave como auditoría interna, cumplimiento, seguridad de la información, calidad o continuidad de negocio. También debe exigir visibilidad explícita sobre elementos críticos como dependencias excesivas de proveedores, puntos únicos de fallo o presiones recientes de reguladores y clientes. Muchas organizaciones descubren, en esta fase, que dependen del conocimiento tácito de una única persona o de procesos no documentados que podrían paralizar la operación en caso de ausencia o error.

Más allá de estos mínimos, las organizaciones con mayor madurez pueden solicitar un diagnóstico ampliado que analice la coherencia entre comités, la calidad de los datos, la integración del riesgo en la planificación y la trazabilidad de decisiones. También es útil incorporar un análisis comparado de madurez o un resumen ejecutivo que

identifique con claridad qué capacidades deben reforzarse y qué decisiones serán necesarias durante el año.

Para los **mandos intermedios**, el diagnóstico se convierte en un ejercicio práctico y aplicable. Se inicia con la recopilación de información sobre procesos críticos, roles reales, dependencias técnicas y lecciones aprendidas. Este trabajo revela frecuentemente dinámicas que no aparecen en los organigramas: por ejemplo, procesos importantes gestionados mediante acuerdos informales entre dos áreas, o sistemas esenciales mantenidos por un único técnico experto.

Los talleres operativos ayudan a identificar capacidades reales, puntos de fallo y brechas tanto culturales como procedimentales. En muchas organizaciones aparecen patrones recurrentes: criterios de evaluación de riesgos distintos según el área, dificultades para consolidar datos o ausencia de canales de escalado claros. Los equipos consolidan toda esta información en seis ámbitos —organización, procesos, personas, sistemas, políticas y cultura— y priorizan solo las brechas más críticas.

En empresas que están empezando, este diagnóstico ofrece una visión clara de los elementos que deben reforzarse antes de avanzar. En organizaciones más maduras, ayuda a detectar inconsistencias estructurales que dificultan la evolución del ERM. El resultado final debe ser un resumen conciso que informe a la Alta Dirección sobre la situación real de partida y las decisiones clave para los próximos doce meses.

3.2. Análisis DAFO aplicado al ERM

El análisis DAFO es una herramienta ágil que permite conectar la realidad de la organización con sus objetivos estratégicos. Su valor no reside en completar una matriz, sino en identificar cómo las fortalezas, debilidades, oportunidades y amenazas afectan a la implantación del ERM y a la toma de decisiones.

El análisis DAFO permite conectar capacidades internas y factores externos con las prioridades de implantación del ERM, como se muestra en la Figura 4.



Figura 4: **Análisis DAFO aplicado al diagnóstico del ERM.** Fuente: elaboración propia.

Para la **Alta Dirección**, el DAFO ofrece una visión sintética de los factores internos y externos que pueden acelerar o frenar el despliegue del modelo ERM. Una fortaleza típica puede ser la existencia de equipos con experiencia operativa y conocimiento profundo del negocio; una debilidad frecuente puede ser la falta de trazabilidad de decisiones, la dispersión de datos o la dependencia de procesos manuales, sistemas críticos o controles insuficientemente implantados.

Las amenazas externas deben analizarse siempre a la luz de las capacidades y vulnerabilidades internas de la organización. Por

ejemplo, un incremento de la exposición a amenazas tecnológicas, regulatorias o de continuidad no tendrá el mismo impacto en una organización con controles maduros, sistemas redundantes y criterios claros de escalado que en otra con dependencias críticas, información fragmentada o responsabilidades poco definidas.

El DAFO solo resulta útil cuando se vincula directamente con los objetivos estratégicos y con decisiones concretas de refuerzo, priorización o tratamiento. Si la organización quiere mejorar su eficiencia operativa, crecer en nuevos mercados o reforzar su resiliencia, el análisis deberá ayudar a identificar qué debilidades internas deben abordarse y qué amenazas externas deben considerarse en la planificación.

Para los **mandos intermedios**, el DAFO es un ejercicio práctico que ayuda a comprender cómo condicionan los procesos, datos y dinámicas reales la implantación del ERM. Por ejemplo, un área puede tener una fortaleza en la coordinación interna, pero una debilidad importante en la disponibilidad de datos fiables. Estos elementos permiten priorizar acciones, preparar mejor los flujos de reporte y anticipar riesgos.

Las oportunidades procedentes del entorno externo también deben interpretarse en clave operativa. En organizaciones que se encuentran en pleno proceso de digitalización, la automatización puede mejorar el control y la calidad del dato, siempre que la segunda línea acompañe el proceso y supervise los riesgos tecnológicos.

3.3. Política de Gestión del Riesgo

La política de gestión del riesgo es el documento que establece cómo se gestionan los riesgos en la organización, qué roles intervienen, bajo qué principios se toman las decisiones y cuáles son los límites aceptables de exposición. No es un documento formal para cumplir expediente: es el marco que garantiza coherencia y consistencia en todas las áreas.

Para la **Alta Dirección**, lo primero es definir un alcance que abarque todas las categorías relevantes: riesgos estratégicos, operacionales, financieros, de cumplimiento, incluyendo, cuando proceda, impactos reputacionales y factores ESG. Debe establecer el objetivo de gestión de riesgos para la organización, así como los principios básicos de actuación, organización y gobernanza, y una frecuencia mínima de reporte y actualización. Es recomendable que se apoye en el Modelo de las Tres Líneas, dejando claro que la primera línea es responsable de gestionar los riesgos, la segunda línea los supervisa y define metodología, y la tercera línea —auditoría interna— garantiza la independencia y el aseguramiento.

Para los **mandos intermedios**, la política debe ser aplicable desde el primer día. Su trabajo consiste en elaborar un borrador inicial basado en prácticas reales, coordinarse con Legal, Cumplimiento, Seguridad de la Información y otras funciones, y asegurar que los flujos de reporte, escalado y supervisión son comprensibles. Cuando coexisten funciones como calidad o PRL, o riesgos y resiliencia, la política debe evitar duplicidades: si calidad revisa trimestralmente un proceso, esa revisión puede integrarse en el modelo ERM sin añadir trámites adicionales.

3.4. Apetito al riesgo

Según COSO ERM, el apetito al riesgo representa el grado de riesgo que una entidad acepta en su búsqueda de valor. El apetito al riesgo permite orientar la toma de decisiones, estableciendo qué nivel y tipo de riesgo está dispuesta a asumir la organización para alcanzar sus objetivos estratégicos. Por ejemplo, una pequeña empresa familiar que no quiera tener deuda y prefiera financiarse únicamente con capital propio tendrá un apetito muy bajo o nulo al endeudamiento financiero. En cambio, una empresa muy especializada en aportar valor técnico en un determinado sector podrá tener un mayor apetito al riesgo técnico, al contar con conocimiento, experiencia y capacidades suficientes para gestionar ese tipo de exposición.

El apetito al riesgo de una compañía será distinto en función de la categoría de riesgo de que se trate. Estas categorías dependerán de la taxonomía definida y de su adaptación al contexto, modelo de negocio y perfil de riesgo de cada organización (ver apartado 4.3, Taxonomía e Inventario).

Conviene diferenciar el apetito al riesgo de otros conceptos relacionados. La capacidad de riesgo representa el nivel máximo de riesgo que la organización podría asumir sin comprometer su viabilidad, solvencia, continuidad o cumplimiento de objetivos esenciales. El apetito al riesgo refleja el nivel de riesgo que la organización está dispuesta a asumir dentro de esa capacidad. Las tolerancias concretan el apetito en rangos aceptables de variación o exposición, mientras que los límites y umbrales permiten monitorizar desviaciones y activar actuaciones, decisiones o escalados cuando se superan determinados niveles.

La relación entre capacidad, apetito, tolerancias, límites y umbrales permite traducir la estrategia de riesgo en criterios observables de decisión, seguimiento y escalado, como se muestra en la Figura 5.

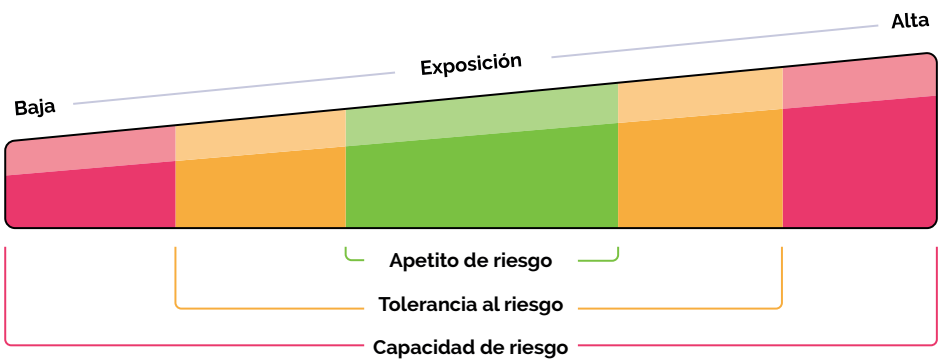


Figura 5: **Relación entre capacidad, apetito, tolerancias, límites y umbrales.**

Fuente: La Fábrica del Pensamiento. Instituto de Auditores Internos de España.

El apetito al riesgo será, por tanto, una de las bases sobre las que se tomarán decisiones y se gestionará el riesgo en la organización. Para que resulte útil, debe estar alineado con la estrategia corporativa,

vinculado a la taxonomía de riesgos y traducido en tolerancias, límites, indicadores y criterios de escalado aplicables en la gestión diaria.

Para ampliar información sobre el apetito al riesgo, se recomienda la lectura de la guía de AGERS, "La gestión del apetito al riesgo".

3.5. Estructura Organizativa del ERM

La estructura organizativa define cómo fluye la información, quién decide y cómo se coordinan las funciones relacionadas con el riesgo. Una buena estructura no añade burocracia, sino claridad y eficiencia. A continuación, se indica una propuesta de principales funciones que se deben incluir en los distintos niveles de la estructura organizativa, y que cada empresa podrá adaptar en función de su estructura, cultura, misión, visión, y características.

Para la **Alta Dirección**, el principio fundamental es mantener una separación funcional clara entre primera, segunda y tercera línea. Esta separación no implica crear nuevos departamentos, sino asignar roles correctamente. También es necesario decidir qué órgano supervisará los riesgos: en organizaciones pequeñas o que están empezando, puede ser el propio Comité de Dirección; en organizaciones más complejas, puede ser conveniente la creación de un Comité de Riesgos.

El Consejo aprobará la política de gestión de riesgos, referencia principal a más alto nivel de la gestión de riesgos dentro de la compañía (ver apartado 3.3, Política de Gestión del Riesgo), el apetito al riesgo y el documento marco, manual o procedimiento de gestión de riesgos (documento que permitiría trasladar y adaptar para la empresa el contenido de la presente guía). Asimismo, será informado de los principales hitos y novedades en materia de gestión de riesgos en la compañía (mapa de calor, riesgos fuera de tolerancia, planes de mitigación implantados, etc.).

La estructura organizativa debe contemplar, asimismo, la existencia de una función de gestión de riesgos o responsable corporativo

de ERM, encargado de diseñar y mantener la metodología común, coordinar el ciclo de identificación, evaluación, seguimiento y reporte de riesgos, consolidar la visión global del perfil de riesgo y facilitar el escalado de información a la Alta Dirección y, en su caso, a los órganos de gobierno. Además, tendrá un papel relevante en la coordinación e impulso de las acciones de cultura, comunicación, sensibilización y formación en gestión de riesgos, sin sustituir la responsabilidad de la Alta Dirección ni de las áreas de negocio en la integración efectiva del modelo. Esta función no sustituye la responsabilidad de los Risk Owners, que permanecen como propietarios de los riesgos en sus respectivos ámbitos, sino que actúa como segunda línea, asegurando coherencia, homogeneidad y visión transversal del modelo ERM. Para liderar la gestión y control de riesgos, se puede contar con un departamento específico, o por el contrario, disponer de esas funciones en equipos de trabajo ya consolidados, que asuman esas nuevas funciones.

Además, los riesgos deberán tener un responsable que monitorice el desarrollo del riesgo, haciendo seguimiento del mismo, controlando los principales indicadores de riesgo y si se encuentran dentro de los umbrales de tolerancia definidos, así como impulsar los planes de acción o mitigación que correspondan para devolver al riesgo a niveles aceptables.

Capítulo 4.
Identificación de riesgos

El proceso de **identificación de riesgos** constituye la primera etapa fundamental en cualquier sistema sólido de Enterprise Risk Management (ERM). Identificar los riesgos implica comprender aquellos eventos, internos o externos, que podrían afectar la consecución de los objetivos estratégicos, operativos, financieros o de cumplimiento de una organización.

Dentro del ciclo completo de gestión de riesgos, la identificación desempeña un rol de anclaje: establece el inventario inicial de riesgos sobre el que se construyen las fases posteriores de evaluación, gestión, monitorización y reporte. La importancia de este proceso radica en que **toda decisión de valoración, priorización y respuesta depende de la calidad de la identificación previa**. Un riesgo no identificado es un riesgo no gestionado; y un riesgo mal definido puede conducir a respuestas ineficaces, asignaciones inadecuadas de recursos o una falsa sensación de control. Por ello, la identificación de riesgos debe ser sistemática, transversal y apoyarse en múltiples fuentes de información, integrando la perspectiva de diferentes áreas, niveles jerárquicos y expertos internos y externos.

En el marco COSO ERM, esta actividad se encuentra directamente vinculada **al componente de estrategia y establecimiento de objetivos**, ya que los riesgos deben identificarse en relación con los objetivos que la organización busca alcanzar.

La identificación, además, **es un proceso dinámico y continuo**, que debe revisarse periódicamente **para capturar cambios en el entorno**

operativo, regulatorio, tecnológico y económico. La aparición de riesgos emergentes y las correlaciones crecientes entre riesgos exigen que este proceso no se aborde como un ejercicio puntual, sino como una práctica viva, integrada en la gestión diaria y en la toma de decisiones estratégicas.

Finalmente, la identificación de riesgos es también un componente crítico para fortalecer la cultura de riesgo de la organización. Cuando las áreas participan activamente en este proceso, se fomenta una mayor conciencia sobre las amenazas y oportunidades, se mejora la anticipación y se impulsa un comportamiento más proactivo. En este sentido, la calidad de la identificación no solo determina la robustez del ERM, sino que refleja el grado de madurez, alineamiento y compromiso de la organización con su propia resiliencia.

Para que la identificación de riesgos sea realmente útil, no basta con elaborar un listado de eventos potenciales: es necesario vincular cada riesgo con las personas o áreas que mejor conocen su origen, evolución e impacto potencial. Por ello, antes de profundizar en las técnicas de identificación, resulta conveniente clarificar quiénes serán los responsables de aportar información, validar la descripción del riesgo y asumir su seguimiento posterior. Esta asignación de responsabilidades se articula a través de la designación de los Risk Owners.

4.1. Designación de los Propietarios del riesgo *(Risk Owners)*

La Gestión de Riesgos demanda un conjunto de responsabilidades que deben estar claras para todos los integrantes de la organización, de modo que estos puedan contribuir eficazmente en la toma de decisiones y proteger correctamente la sostenibilidad de la organización.

La designación de los Propietarios de los riesgos o *Risk Owners* es un proceso fundamental en la Gestión de Riesgos corporativos. **La correcta asignación de Propietarios de riesgos asegura que los riesgos no sean gestionados de forma genérica**, sino con medidas específicas y eficientes, mejorando el control integral del gobierno corporativo.

Además, la correcta designación de *Propietarios de riesgos* es un elemento clave dentro del proceso de identificación de riesgos, ya que garantiza que cada riesgo tenga un responsable claro que disponga del conocimiento, la autoridad y la visión operativa necesaria para identificarlo con precisión.

En la fase de identificación de riesgos, la participación activa de los *Propietarios de los riesgos* permite capturar información de primera mano sobre las actividades, procesos y decisiones que pueden originar riesgos, asegurando que la identificación sea completa, realista y alineada con la realidad de la organización.

- **¿Qué es un Propietario del riesgo o Risk Owner?**

Los Propietarios de los riesgos, también llamados a veces responsables de los riesgos, son las **personas áreas o unidades organizativas** dentro de la organización a las que **se delega la autoridad sobre la gestión de uno o varios riesgos**.

Se designa como Propietario del riesgo a directores, gerentes o empleados de la organización con responsabilidad operacional sobre un área, departamento, unidad de negocio o entidad legal, es decir, empleados que tienen el control sobre los procesos, activos o la toma de decisiones que generan dicho riesgo.

Dentro del modelo de las tres líneas, los Propietarios de los riesgos son responsables de gestionar el riesgo en su ámbito y de asegurar su seguimiento operativo, impulsar las medidas de tratamiento y escalar desviaciones cuando corresponda (ver modelo de las tres líneas descrito en el punto 1.3 de la Introducción). Entre sus **responsabilidades**, destacan:

i. **Identificar y evaluar** los riesgos de su respectiva área de responsabilidad, aportando información para el esclarecimiento del contexto del riesgo.
ii. **Gestionar operativamente los riesgos** bajo su área de responsabilidad, **incluyendo la ejecución de respuestas al riesgo**: actividades de control, planes de acción o de contingencia.

iii. Realizar un seguimiento periódico de la evolución y estado de sus riesgos mediante indicadores establecidos.
iv. **Reportar o informar sobre los riesgos** bajo su área de responsabilidad, y hacer las actualizaciones necesarias para asegurar la correcta gestión del riesgo.
v. Proponer la **inclusión de nuevos riesgos y/o amenazas** detectadas, así como proponer las estrategias necesarias ante el mismo.
vi. Habilitar y fomentar la identificación de riesgos por parte del resto de sus empleados bajo su área de responsabilidad.

- **Pasos para una correcta designación de Propietarios de los riesgos**

1. **Identificación**: identificar claramente el riesgo y delimitar el proceso, área, unidad o entidad más afectada. Para ello, se deben analizar procesos, revisar incidentes históricos y mantener entrevistas para determinar cuál es la función organizativa que posee mayor conocimiento operativo y visibilidad sobre el origen del riesgo. Esta fase es esencial para garantizar que la futura designación recaiga en la persona más cercana al riesgo, con entendimiento directo de su dinámica y de los factores que pueden agravarlo o mitigarlo.

2. **Asignación**: una vez identificado el riesgo y el área impactada, se debe contactar con **la persona que tiene la autoridad última para tomar decisiones** relacionadas con dicho riesgo. Esto incluye la capacidad de asignar recursos, definir acciones, modificar procesos o priorizar iniciativas que permitan gestionarlo adecuadamente. Este paso asegura que el Propietario del riesgo pueda influir directamente en la gestión del riesgo.

3. **Capacitación**: una vez asignado el rol, es fundamental asegurar que el Propietario del riesgo comprende plenamente sus responsabilidades y dispone del conocimiento y las competencias necesarias para desempeñarlas de forma efectiva. Este paso es crítico para garantizar la calidad del modelo de Gestión de Riesgos. El Propietario del riesgo debe entender que la Gestión de Riesgos es un proceso dinámico, continuo y cíclico, en el

que los riesgos evolucionan y pueden interactuar entre sí. Para ello, la organización debe proporcionar formación específica en Gestión de Riesgos y reforzar la importancia de mantener una vigilancia activa sobre cualquier cambio en el riesgo, incluyendo señales de alerta temprana (*Key Risk Indicators*, o KRIs), riesgos emergentes o posibles correlaciones con otros riesgos. El objetivo es evitar que la designación sea meramente formal y asegurar un desempeño real, proactivo y orientado a la mejora continua del riesgo bajo su responsabilidad.

4. **Formalización**: finalmente, la designación del Propietario del riesgo debe quedar **formalizada y documentada en las herramientas de gestión de riesgos de la organización** (matrices, repositorios, plataforma ERM). La formalización no solo garantiza trazabilidad y transparencia, sino que permite una revisión periódica del rol, asegurando que cada riesgo mantiene un responsable adecuado en función de los cambios organizativos, operativos o estratégicos.

Uno de los principales retos en la designación de Propietarios del riesgo es que, en muchas organizaciones, las responsabilidades asociadas al rol no forman parte explícita de sus tareas habituales. Cuando estas responsabilidades no están debidamente integradas en la gestión del desempeño, pueden percibirse como actividades accesorias u opcionales, sujetas a la disponibilidad de tiempo o al interés individual, lo que limita la efectividad del modelo de gestión de riesgos.

En ciertas organizaciones, para reforzar la rendición de cuentas (*accountability* en inglés), las responsabilidades del Propietario del riesgo pueden ser formalmente incorporadas en los objetivos y criterios de evaluación del desempeño de su puesto de trabajo. Integrar esta función en el proceso estándar de evaluación del rendimiento asegura que la gestión del riesgo forme parte de las expectativas profesionales del rol y no un compromiso voluntario. De este modo, se favorece un comportamiento consistente, se incrementa la trazabilidad de las responsabilidades y se establece un marco claro en el que el incumplimiento tenga consecuencias definidas, contribuyendo así a fortalecer la cultura de riesgo y la gobernanza corporativa.

4.2 Técnicas para la Identificación de Riesgos

Existen diversas técnicas para identificar los riesgos. Si bien **en una organización pueden identificarse riesgos de forma natural a través de actividades ya integradas** o internas—como la presupuestación, la planificación estratégica, las revisiones de calidad, el análisis de datos internos sobre incidentes y pérdidas, o los procesos de auditoría interna— **estas actividades deben complementarse con otras técnicas de identificación**, diseñadas para captar riesgos nuevos, emergentes o transversales que no afloran de manera espontánea en los procesos habituales. Solo mediante una **combinación equilibrada de procesos integrados y metodologías formale**s es posible favorecer una identificación suficientemente completa, consistente y alineada con el contexto estratégico y operativo de la organización.

A continuación, se describen las principales técnicas de identificación de riesgos utilizadas en los modelos de Gestión de Riesgos corporativos, las cuales pueden complementarse entre sí:

Técnicas clásicas:

- **Entrevistas individuales**: permiten obtener información detallada directamente de personas con conocimiento profundo sobre un proceso, área o actividad concreta. Esta técnica es especialmente útil para identificar riesgos técnicos, específicos o emergentes que pueden no surgir en un entorno grupal. Además, facilita que el entrevistado pueda expresar libremente sus percepciones, hipótesis y señales de alerta, proporcionando una comprensión más granular de causas, factores desencadenantes y posibles escenarios de materialización del riesgo.

- **Talleres internos**: reúnen a profesionales de diferentes funciones y niveles para aprovechar el conocimiento colectivo de la organización. Permiten identificar tanto riesgos transversales como correlaciones entre áreas, algo que difícilmente emerge desde perspectivas individuales. Además, fomentan el debate, la reflexión conjunta y la alineación sobre los riesgos más

relevantes, lo que contribuye a fortalecer la cultura de riesgo. Esta técnica también facilita la detección de correlaciones y efectos en cadena, y genera un entendimiento compartido del riesgo, impulsando la colaboración y la responsabilidad conjunta en su gestión.

- **Cuestionarios**: permiten recopilar información de forma estandarizada y llegar a un número amplio de empleados o unidades de negocio. Están diseñados con preguntas claras y homogéneas, lo que facilita la comparación entre áreas y la detección de patrones recurrentes (riesgos recurrentes o transversales). Esta técnica es especialmente eficaz cuando se necesita cubrir distintas líneas o unidades de negocio, o cuando la disponibilidad de los participantes es limitada. Asegura una participación más amplia y reduce los sesgos generados por dinámicas grupales.

- **Listas de comprobación**: proporcionan una estructura clara para garantizar que la identificación de riesgos sea completa y coherente. Funcionan como una guía que recuerda a los participantes las categorías de riesgo más relevantes (estratégicos, financieros, operacionales, cumplimiento, etc.). Su principal ventaja es que minimizan la posibilidad de omisiones importantes y aseguran que todas las áreas evalúen los riesgos bajo un marco de referencia común. Son especialmente útiles en las fases iniciales de implantación de un sistema de Gestión de Riesgos o en organizaciones grandes y con procesos muy diversos, donde la homogeneidad es clave para construir un mapa de riesgos consistente.

Técnicas analíticas:

- **Análisis de datos o incidentes históricos**: revisión sistemática de incidentes, pérdidas operacionales, reclamaciones, desviaciones de auditoría y fallos de control ocurridos en el pasado. A través de este análisis se identifican riesgos que ya se han materializado, sus causas raíz y las circunstancias que permitieron o favorecieron su aparición. Pueden analizarse

tanto datos o incidentes internos de la propia organización como externos (sector, región, país, etc.). Es una herramienta basada en evidencia objetiva que ayuda a reconocer patrones repetitivos y vulnerabilidades estructurales, evitando que los mismos incidentes vuelvan a ocurrir.

- **Análisis de procesos**: revisión detallada de las actividades clave de un área o unidad de negocio para identificar riesgos inherentes en cada etapa. Implica desarrollar diagramas de procesos para comprender mejor las interrelaciones de sus entradas, tareas, resultados y responsabilidades. Se identifican puntos críticos, dependencias, fallos potenciales y actividades susceptibles de error. Esta técnica es particularmente eficaz para identificar riesgos operacionales, tecnológicos y de continuidad del negocio. Permite también evaluar la robustez de los controles existentes y detectar lagunas o redundancias que pueden generar riesgos no evidentes desde una perspectiva estratégica.

- **Análisis del entorno**: análisis de factores externos que pueden generar riesgos estratégicos, emergentes o sistémicos: cambios regulatorios, innovación tecnológica, situación económica, tendencias sectoriales, expectativas de grupos de interés, riesgos geopolíticos o ambientales. Incluye herramientas como análisis PESTEL, análisis comparativo sectorial, informes de asociaciones industriales o estudios prospectivos. Su objetivo es anticipar riesgos que no provienen de procesos internos, pero que pueden impactar significativamente en el modelo de negocio o en la estrategia.

Otras técnicas:

- **Grupos de trabajo sectoriales**: reúnen a profesionales de distintas organizaciones pertenecientes al mismo sector, generalmente responsables de riesgos o expertos en áreas de control. Su principal valor reside en que permiten identificar riesgos comunes del sector, tendencias emergentes y vulnerabilidades compartidas que pueden no ser evidentes analizando únicamente el entorno interno. Además, facilitan el intercambio de buenas prácticas, enfoques metodológicos y lecciones aprendidas, enriqueciendo

la perspectiva de la organización y fortaleciendo la alineación con estándares sectoriales. Esta técnica es especialmente útil en sectores regulados o con riesgos altamente especializados, donde la colaboración interinstitucional contribuye a anticipar amenazas sistémicas y elevar la madurez global del modelo de gestión de riesgos.

- **Análisis de escenarios y pruebas de estrés**: permiten explorar situaciones futuras plausibles o severas para analizar qué riesgos podrían surgir o intensificarse ante cambios relevantes. Aunque puedan ser más propias de la fase de análisis y evaluación del riesgo, en ocasiones se utilizan de forma complementaria en la identificación para detectar vulnerabilidades, interdependencias, efectos en cascada o riesgos emergentes que no fueron identificados mediante técnicas tradicionales.

Independientemente de las técnicas aplicadas para la identificación de riesgos, la organización debe reconocer que cualquier cambio en las hipótesis que sustentan su estrategia y sus objetivos puede dar lugar a riesgos nuevos o emergentes, por lo que es esencial mantener una vigilancia continua y un enfoque dinámico en la identificación.

4.3 Taxonomía e Inventario

Taxonomía de riesgos

La taxonomía de riesgos proporciona una estructura común, homogénea y comprensible para clasificar y agrupar los riesgos de una organización. Contar con una taxonomía clara y consistente permite mejorar la calidad de la identificación, facilitar el análisis comparativo entre áreas y fortalecer la comunicación. Una taxonomía bien definida actúa como punto de referencia para todas las fases del ciclo de gestión de riesgos: identificación, análisis y evaluación, tratamiento, seguimiento y reporte.

Una adecuada taxonomía debe reflejar tanto el modelo de negocio como el entorno regulatorio y sectorial, y debe ser lo suficientemente

flexible como para adaptarse a la evolución de los riesgos, especialmente en contextos de alta incertidumbre o cambios tecnológicos, regulatorios o estratégicos. Por ello, la taxonomía debe revisarse de forma periódica para incorporar riesgos emergentes y nuevas categorías relevantes, garantizando que la organización mantiene una visión actualizada y coherente de sus exposiciones.

De forma habitual, y tomando como referencia las categorías de objetivos utilizadas en marcos como COSO, muchas organizaciones agrupan sus riesgos en grandes categorías como riesgos estratégicos, operacionales, financieros, de información y reporte, y de cumplimiento. Esta clasificación proporciona una base metodológica ampliamente utilizada para ordenar el universo de riesgos y facilitar una visión integrada de las exposiciones que pueden afectar a la consecución de los objetivos de la organización.

No obstante, la taxonomía de riesgos no debe entenderse como una estructura rígida, cerrada o universal. Debe adaptarse al contexto interno y externo de cada organización, a su modelo de negocio, a sus objetivos estratégicos, a su estructura operativa, a su marco regulatorio y a su perfil de riesgo.

Por ello, en esta guía se propone una taxonomía de referencia diseñada para reflejar de forma más precisa el perfil de riesgo de la organización y permitir una clasificación más granular, comparable y útil para la toma de decisiones.

Las categorías y subcategorías incluidas a continuación son orientativas y deberán adaptarse al sector, modelo de negocio, estructura organizativa, marco regulatorio y perfil de riesgo de cada organización. Asimismo, cuando un riesgo pueda vincularse a varias categorías, se recomienda asignar una categoría principal y, en su caso, categorías secundarias o etiquetas adicionales, evitando duplicidades y facilitando su consolidación.

Riesgos Estratégicos

Afectan a las decisiones de alto nivel y a la capacidad de la organización para alcanzar objetivos estratégicos. Permiten que la

Alta Dirección analice si la estrategia está alineada con el entorno y si existen amenazas u oportunidades críticas. Ejemplos de posibles subcategorías:

i. Cambios en el mercado
ii. Cambios en la competencia
iii. Innovación y disrupción tecnológica
iv. Decisiones de crecimiento (fusiones, adquisiciones) o desinversiones

Riesgos Financieros
Afectan a la situación/estabilidad financiera general de la empresa. Proporcionan una visión clara de la exposición financiera y garantizan la alineación con el apetito de riesgo. Ejemplos de posibles subcategorías:

i. Capital y solvencia
ii. Deuda y liquidez
iii. Tipos de cambio
iv. Tipos de interés

Riesgos Operacionales
Derivados de fallos en procesos internos, personas, sistemas o factores externos que pueden afectar a la operativa diaria de la organización. Suelen ser numerosos y su materialización puede ser más frecuente. Ejemplos de posibles subcategorías:

i. Disponibilidad de bienes y servicios
ii. Interrupciones operativas
iii. Costes de bienes, servicios y suministros
iv. Composición de la cartera de proveedores

Riesgos Macroeconómicos
Derivados del entorno macroeconómico o de factores externos económicos que afectan a la demanda, el coste de capital o la estabilidad del negocio. Por lo tanto, son riesgos que no provienen de la organización, son factores externos. Ejemplos de posibles subcategorías:

i. Inflación o deflación
ii. Cambios macroeconómicos globales
iii. Riesgos geopolíticos con impacto económico
iv. Variaciones en políticas económicas

Riesgos de Cumplimiento
Derivados del incumplimiento de leyes, regulaciones, normativas internas o estándares éticos. Suelen afectar directamente a la reputación y suelen implicar multas y sanciones o una pérdida de licencia, por lo que requieren una supervisión importante. Ejemplos de posibles subcategorías:

i. Fraude y Apropiación indebida de activos
ii. Soborno y Corrupción
iii. Blanqueo de capitales y Financiación del terrorismo
iv. Manipulación del mercado y defensa de la competencia

Riesgos Legales
Derivados de litigios, reclamaciones judiciales o disputas legales. Se diferencian de los riesgos de cumplimiento en que los riesgos legales son riesgos derivados de procesos legales o judiciales, no de la regulación/normativa general. Ejemplos de posibles subcategorías:

i. Demandas de clientes o proveedores
ii. Reclamaciones laborales
iii. Conflictos contractuales
iv. Responsabilidad civil

Riesgos Medioambientales
Derivados tanto del impacto del entorno natural sobre la organización como los efectos de la propia organización sobre el medio ambiente. Ejemplos de posibles subcategorías:

i. Fenómenos climáticos (desastres naturales)
ii. Escasez de recursos naturales
iii. Contaminación y emisiones
iv. Cambios regulatorios ambientales

Riesgos Tecnológicos
Relacionados con la infraestructura tecnológica, los sistemas de información, la ciberseguridad y la protección o gestión de los datos. Tienen como origen directo fallos o vulnerabilidades tecnológicas. Ejemplos de posibles subcategorías:

i. Ciberseguridad y amenazas digitales
ii. Fallo de sistemas e infraestructuras tecnológicas
iii. Fallos en la integridad y la protección de datos
iv. Uso o gobernanza indebida de la Inteligencia Artificial

Riesgos de Seguridad
Asociados a la protección de las personas, los activos y las instalaciones de la organización. Incluyen amenazas que pueden comprometer la integridad física de empleados, contratistas o visitantes, así como la seguridad de bienes materiales y espacios críticos. Se trata de riesgos de naturaleza física o de protección, no relacionados con tecnología ni con fallos operativos de procesos. Ejemplos de posibles categorías:

i. Accesos no autorizados a instalaciones
ii. Incendios, robos o vandalismo
iii. Accidentes o incidentes de seguridad laboral
iv. Seguridad en viajes o entornos críticos

Riesgos de Personas
Derivados de la gestión, disponibilidad, capacitación, conducta, bienestar, seguridad y compromiso de las personas que forman parte de la organización. Estos riesgos pueden afectar a la continuidad operativa, al cumplimiento de objetivos, a la cultura corporativa, a la productividad y a la capacidad de la organización para ejecutar su estrategia. Ejemplos de posibles subcategorías:

i. Atracción, retención y sucesión de talento crítico
ii. Dependencia de personas clave o conocimiento no documentado
iii. Rotación, absentismo o falta de capacidades críticas

iv. Clima laboral, cultura, conducta y relaciones laborales
v. Seguridad, salud y bienestar de empleados y contratistas

Riesgos de Terceros
Derivados de la dependencia de proveedores, contratistas, socios, distribuidores, clientes relevantes u otros terceros que intervienen en la cadena de valor o prestan servicios críticos para la organización. Incluyen riesgos asociados a incumplimientos contractuales, interrupciones de servicio, concentración de proveedores, dependencia operativa, fallos de calidad, riesgos financieros, regulatorios, reputacionales o de conducta de dichos terceros. Ejemplos de posibles subcategorías:

i. Dependencia o concentración en proveedores críticos
ii. Incumplimiento contractual, regulatorio o de estándares exigidos
iii. Interrupción del servicio, fallos de calidad o problemas de suministro
iv. Riesgos financieros, éticos, reputacionales o de conducta de terceros
v. Riesgos derivados de subcontratación, externalización o cadena de suministro

La reputación puede tratarse como una categoría específica de riesgo o como una dimensión de impacto transversal, en función de la metodología de cada organización. En muchos modelos ERM resulta más útil considerarla como una dimensión de impacto, ya que la pérdida reputacional suele ser consecuencia de la materialización de riesgos estratégicos, operacionales, legales, de cumplimiento, tecnológicos, medioambientales o de terceros.

Inventario de riesgos

El inventario o registro de riesgos es el catálogo que recoge los riesgos específicos identificados en la organización, incluyendo su descripción, causas, consecuencias, responsable, controles asociados, valoración, planes de tratamiento y estado de seguimiento.

A diferencia de la taxonomía de riesgos, que actúa como una estructura jerárquica y común para clasificar los riesgos por categorías y subcategorías, el inventario constituye el registro vivo y operativo de los riesgos concretos que pueden afectar a la consecución de los objetivos de la organización.

Por tanto, mientras la taxonomía ordena el universo de riesgos, el inventario documenta y actualiza los riesgos efectivamente identificados, facilitando su evaluación, priorización, tratamiento, monitorización y reporte.

Definición de los riesgos

Una taxonomía de riesgos sólida no solo depende de categorías bien estructuradas, sino también de la **definición precisa y homogénea de cada riesgo**. La forma en la que se titula y describe un riesgo influye directamente en la eficacia de su identificación, evaluación, priorización y seguimiento. Cuando los riesgos están mal definidos (por ser demasiado amplios, ambiguos o confundir causas con consecuencias), se dificulta la toma de decisiones. Un riesgo correctamente definido debe permitir comprender, de manera inmediata, qué puede suceder, por qué y con qué consecuencia.

Cómo definir correctamente un riesgo:

Para asegurar consistencia, cada riesgo deberá definirse siguiendo una estructura común que distinga entre **causa, evento y consecuencia**, identificando los factores que pueden originar o favorecer el riesgo (causa), el hecho incierto que podría materializarse (evento) y los efectos que tendría sobre los objetivos, operaciones, resultados, personas, cumplimiento o reputación de la organización (consecuencia), como se muestra, de forma ilustrativa, en la Figura 6.

Estructura para la definición del riesgo

Una forma práctica de redactar un riesgo es partir de tres elementos: **causa, evento y consecuencia.**



Figura 6: **Estructura recomendada para la definición del riesgo.**

Fuente: elaboración propia.

- **Evento (qué puede pasar)**: El hecho incierto que, de materializarse, afectaría a la organización. Ejemplo: *Fallo en un proveedor crítico…*
- **Causa (por qué podría ocurrir)**: Factores internos o externos que desencadenan el evento. Ejemplo: *…debido a interrupciones logísticas internacionales…*
- **Consecuencia (qué efecto tiene sobre el negocio)**: Efectos sobre operaciones, finanzas, reputación, personas, clientes, etc., si se llegase a materializar el riesgo. Ejemplo: *…generando retrasos en la producción y aumento de costes.*

Ejemplo de definición completa: "Interrupción del proveedor crítico (evento) debido a tensiones logísticas internacionales (causa), provocando retrasos en la producción y sobrecostes (consecuencia)."

Entre los errores comunes al definir riesgos se puede encontrar:

- titular el riesgo como impacto, no como evento; por ejemplo, "pérdida de ingresos";

- describir únicamente la causa, pero no el riesgo; por ejemplo, "falta de personal";
- utilizar descripciones demasiado genéricas; por ejemplo, "problemas operativos";
- definir riesgos excesivamente detallados o atomizados que dificultan su gestión agregada;
- mezclar múltiples riesgos en un único enunciado;
- no vincular la redacción a una consecuencia concreta;
- confundir riesgos con controles, incidencias, acciones o planes de tratamiento;
- utilizar nombres diferentes para riesgos equivalentes en distintas áreas.

4.4. Interdependencias y correlaciones entre riesgos

El análisis de interdependencias y correlaciones entre riesgos es un elemento clave dentro del proceso de Identificación de Riesgos, ya que permite comprender cómo diferentes riesgos o eventos de riesgo pueden interactuar entre sí, modificando su probabilidad, impacto, velocidad de propagación o capacidad de respuesta. En vez de ver los riesgos de forma aislada, se busca identificar correlaciones o interdependencias para mejorar la toma de decisiones estratégicas. Por tanto, forman parte del entendimiento integral del riesgo, al reconocer que los riesgos no operan de manera aislada, sino como parte de una cartera interconectada. Esta visión integrada es fundamental para anticiparse a escenarios complejos, evaluar impactos agregados y tomar decisiones estratégicas más informadas.

A estos efectos, conviene diferenciar ambos conceptos. La correlación hace referencia a la tendencia de dos o más riesgos a comportarse de forma conjunta o simultánea, especialmente cuando existe evidencia o datos que permiten observar esa relación. La interdependencia, en cambio, se refiere a una relación causal, funcional u operativa entre riesgos, aunque no exista una correlación estadística demostrada. En la práctica, ambos términos se utilizan

con frecuencia de forma amplia para describir relaciones relevantes entre riesgos, si bien no siempre responden al mismo tipo de vínculo.

La identificación de relaciones entre riesgos requiere diferenciar entre causalidad, interdependencia y correlación, evitando tratar todas las conexiones como si tuvieran la misma naturaleza, como se muestra en la Figura 7.

Interdependencia y causalidad de riesgos

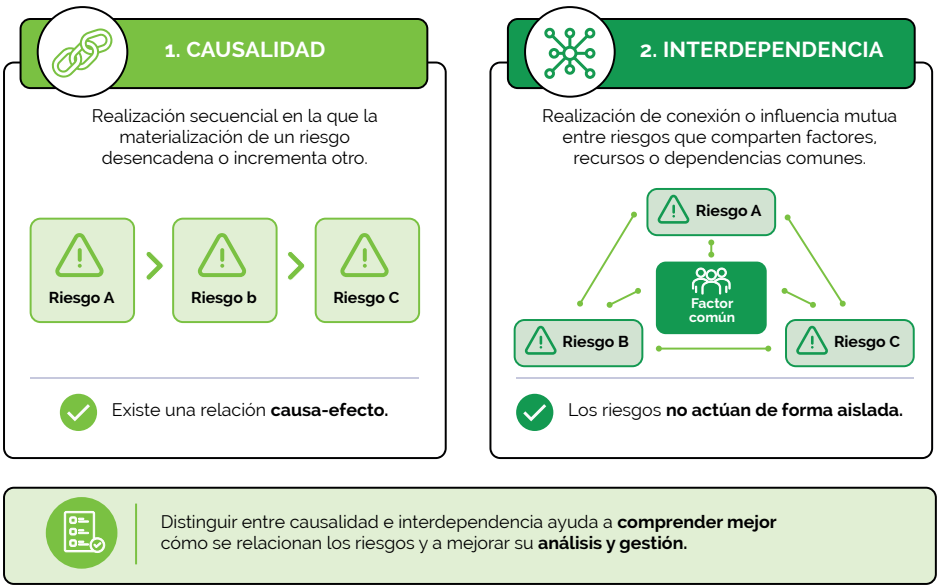


Figura 7: **Diferencia entre causalidad e interdependencia de riesgos.**

Fuente: elaboración propia.

La interdependencia de riesgos ayuda a responder preguntas fundamentales como:

- ¿Qué riesgos tienden a ocurrir simultáneamente?
- ¿Qué riesgos actúan como desencadenantes de otros?
- ¿Qué riesgos, aun siendo moderados individualmente, pueden generar un impacto elevado cuando se combinan?
- ¿Qué relaciones entre riesgos pueden generar efectos en cascada?

Comprender estas relaciones permite a la organización identificar vulnerabilidades sistémicas, anticipar posibles escenarios adversos y priorizar mejor los riesgos que requieren un tratamiento conjunto o medidas de mitigación más robustas.

A continuación, se detallan los principales tipos de relación entre riesgos:

- **Causa común**: dos o más riesgos comparten el mismo origen o factor desencadenante. Por ejemplo, un cambio regulatorio puede impactar simultáneamente a riesgos de cumplimiento y operacionales o estratégicos.
- **Efecto en cascada**: la materialización de un riesgo aumenta la probabilidad o el impacto de otro riesgo. Por ejemplo, una interrupción operativa (riesgo operacional) puede derivar en incumplimientos contractuales (riesgo legal).
- **Dependencia común (operacional, recursos, controles, etc.)**: riesgos que están vinculados a procesos, controles o recursos comunes. Por ejemplo, fallos en un proveedor crítico afectan a riesgos de suministro y de calidad.
- **Acumulación de impactos**: varios riesgos, que de forma individual pueden parecer asumibles, generan un impacto agregado relevante cuando coinciden en un mismo periodo, escenario o área de la organización.

La identificación de interdependencias debe integrarse como parte habitual del proceso, y puede realizarse mediante:

- **Talleres de identificación** con enfoque transversal (varias áreas a la vez).
- **Mapas de interdependencias** que representen conjuntos de riesgos y sus interdependencias.
- **Lecciones aprendidas** de incidentes pasados donde la materialización de un riesgo desencadenó otros.
- **Análisis de procesos** para detectar riesgos que comparten recursos, actividades o proveedores.
- **Revisión** de KRIs comunes o indicadores que puedan anticipar el deterioro simultáneo de varios riesgos;

- Análisis de escenarios multirriesgo, especialmente para riesgos estratégicos, operacionales, tecnológicos, climáticos, geopolíticos o de continuidad de negocio.

En organizaciones con riesgos transversales, puede ser útil representar las conexiones entre categorías de riesgo para identificar dependencias, efectos en cascada y posibles concentraciones de exposición, como se muestra en la Figura 8.

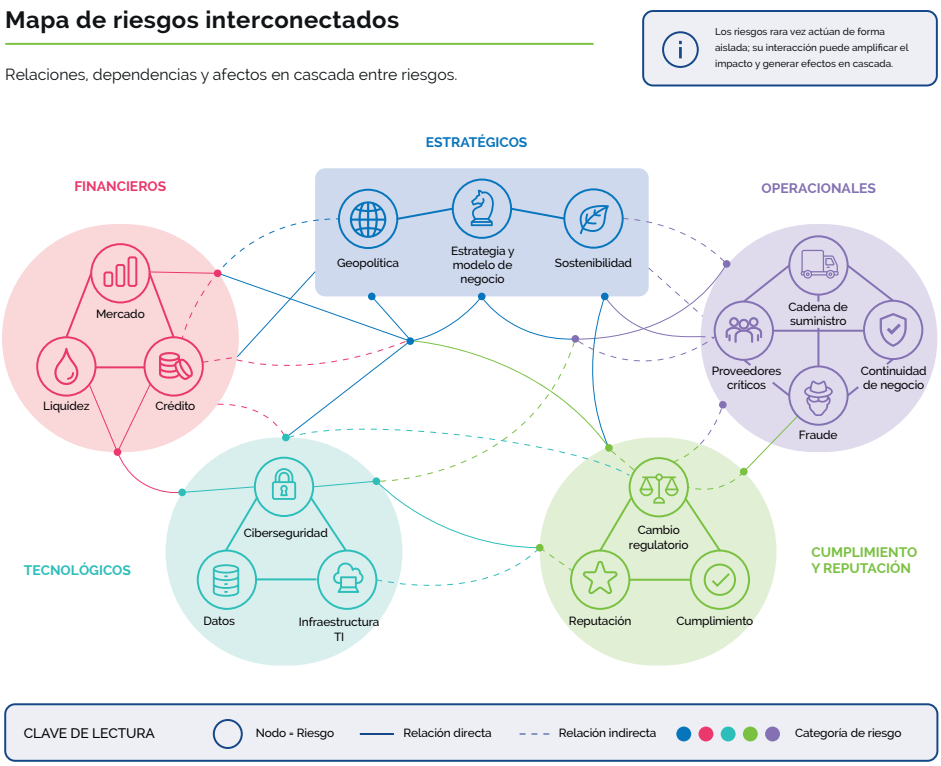


Figura 8: **Mapa de riesgos interconectados.** Fuente: elaboración propia.

En organizaciones con mayor madurez, se emplean metodologías avanzadas, como análisis de escenarios multirriesgo o modelos cuantitativos de correlación (más frecuentes en sectores regulados).

Incorporar el análisis de relaciones entre riesgos como parte de la identificación de riesgos permite a la organización pasar de

una visión fragmentada a un entendimiento integrado del riesgo. Reconocer cómo interactúan los riesgos es esencial para anticiparse a escenarios complejos, fortalecer la resiliencia y asegurar que el modelo ERM refleje la realidad operativa y estratégica en toda su dimensión.

Capítulo 5.
Análisis y evaluación de riesgos

5.1. Objetivo y alcance

El análisis y evaluación de riesgos constituye una de las fases centrales del modelo de Enterprise Risk Management (ERM), ya que permite a la organización comprender la naturaleza de los riesgos identificados, estimar su relevancia y priorizar las decisiones de tratamiento, seguimiento y supervisión. Esta fase tiene como finalidad transformar la identificación inicial de riesgos en información útil para la toma de decisiones, proporcionando una visión estructurada de la exposición al riesgo de la organización y de su posible impacto sobre la estrategia, los objetivos corporativos, la sostenibilidad financiera, la continuidad operativa y la generación de valor.

El análisis y evaluación de riesgos debe permitir a la organización:

- comprender las causas y factores que originan los riesgos;
- valorar la probabilidad de ocurrencia y el impacto potencial;
- identificar riesgos prioritarios;
- analizar la efectividad de los controles existentes;
- determinar el nivel de exposición residual;
- facilitar la asignación eficiente de recursos;
- apoyar la toma de decisiones por parte de la Alta Dirección y del Consejo;
- mejorar la resiliencia organizativa y la capacidad de anticipación.

La evaluación deberá realizarse utilizando metodologías homogéneas, documentadas y consistentes en toda la organización, permitiendo la comparabilidad entre riesgos, unidades de negocio y periodos temporales.

Asimismo, el modelo de evaluación deberá ser suficientemente flexible para adaptarse a la naturaleza de cada riesgo, al contexto sectorial y al nivel de madurez de la organización.

El análisis permite comprender la naturaleza del riesgo, sus causas, consecuencias, controles existentes e incertidumbres asociadas. La evaluación, por su parte, permite valorar su relevancia y compararla con los criterios definidos por la organización, incluyendo el apetito, las tolerancias, los límites o los umbrales aplicables. De esta forma, la organización puede priorizar riesgos, identificar exposiciones fuera de tolerancia y orientar las decisiones posteriores de tratamiento, seguimiento o escalado.

5.2. Riesgo inherente y riesgo residual

La evaluación de un riesgo puede realizarse desde dos perspectivas complementarias: el riesgo inherente y el riesgo residual. El riesgo inherente permite comprender la exposición bruta asociada a una actividad, proceso, proyecto, decisión o factor externo, sin considerar el efecto de controles o medidas de mitigación. El riesgo residual permite valorar la exposición que permanece una vez considerados dichos controles y medidas. La utilización de una u otra perspectiva dependerá del objetivo del análisis, del nivel de madurez del modelo y de la información disponible.

Riesgo inherente

El riesgo inherente representa la exposición natural existente antes de aplicar controles o medidas de mitigación.

Refleja el riesgo bruto asociado a:

- actividades;
- procesos;
- proyectos;
- decisiones;
- entornos externos.

Riesgo residual

El riesgo residual representa el nivel de exposición que permanece después de aplicar controles y medidas de mitigación.

Evaluación de controles

Para determinar el riesgo residual será necesario evaluar:

- diseño de controles;
- grado de implantación;
- efectividad operativa;
- grado de automatización;
- frecuencia de ejecución;
- responsable del control;
- evidencia disponible;
- naturaleza preventiva, detectiva o correctiva;
- efecto esperado sobre la probabilidad y/o impacto.

Importancia del análisis inherente vs residual

La comparación entre ambos conceptos permite:

- evaluar eficacia del control interno;
- identificar debilidades;
- justificar inversiones;
- priorizar tratamientos;
- facilitar reporting al Consejo.

La valoración inherente y residual no debe entenderse como un ejercicio puramente mecánico. Su utilidad reside en permitir a la

organización comprender qué parte de la exposición procede de la propia naturaleza del riesgo y qué parte permanece después de considerar la efectividad los controles y medidas existentes.

5.3. Variables para la evaluación del riesgo

La evaluación del riesgo deberá considerar múltiples variables para obtener una visión integral de la exposición de la organización. Habitualmente se usan las variables probabilidad e impacto, si bien existen otras adicionales que se detallan a continuación.

La evaluación básica del riesgo suele apoyarse en la combinación de probabilidad e impacto, complementada, cuando proceda, con otras variables como velocidad, proximidad, tendencia, detectabilidad, recuperación o adaptabilidad, como se muestra en la Figura 9.

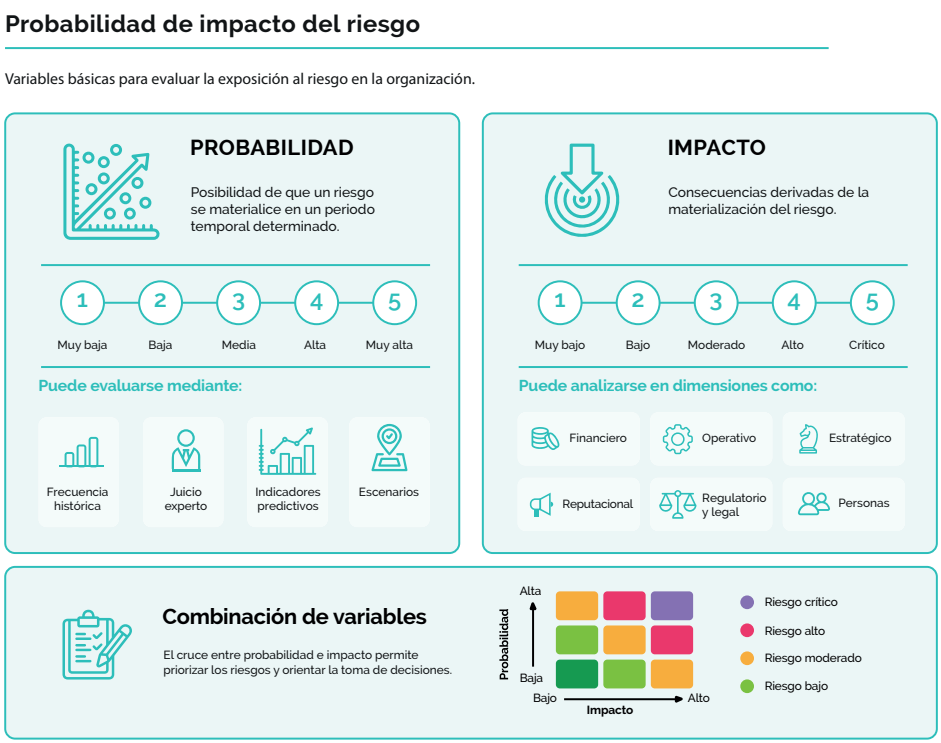


Figura 9: **Probabilidad e impacto del riesgo.** Fuente: elaboración propia.

5.3.1. Probabilidad

La probabilidad representa la posibilidad de que un riesgo se materialice en un periodo temporal determinado. La organización deberá definir expresamente el horizonte temporal de referencia utilizado en la evaluación, por ejemplo anual, plurianual o vinculado al plan estratégico.

Puede evaluarse mediante:

- frecuencia histórica;
- juicio experto;
- indicadores predictivos;
- análisis estadístico;
- escenarios.

La organización deberá definir escalas homogéneas para asegurar consistencia.

5.3.2 Impacto

El impacto refleja las consecuencias derivadas de la materialización del riesgo. El análisis deberá contemplar diferentes dimensiones:

- Impacto financiero (pérdida económica; incremento de costes; reducción de ingresos; deterioro de activos).
- Impacto operativo (interrupción de actividades; pérdida de productividad; fallos tecnológicos; problemas logísticos).
- Impacto estratégico (afectación a objetivos corporativos; pérdida de ventaja competitiva; retraso en proyectos estratégicos).
- Impacto reputacional (deterioro de imagen; pérdida de confianza; impacto mediático).
- Impacto regulatorio y legal (sanciones; litigios; incumplimientos normativos).
- Impacto sobre personas (seguridad; salud; clima laboral; talento).

Cuando un riesgo pueda generar impactos en varias dimensiones, la metodología deberá definir cómo se determina el impacto final: por impacto máximo, por ponderación, por criterio dominante o

mediante otra regla definida. Esta decisión es importante para evitar valoraciones inconsistentes entre áreas o una agregación artificial de impactos no comparables.

Asimismo, se pueden evaluar distintos escenarios: peor escenario, escenario esperado, escenario agregado, etc.

5.3.3. Escalas de probabilidad e impacto

Para aplicar de forma homogénea las variables de probabilidad e impacto, cada organización deberá definir escalas de valoración adaptadas a su contexto, tamaño, complejidad, apetito al riesgo y madurez del modelo. No existe un número único de niveles válido para todas las organizaciones.

Una escala con mayor número de niveles puede aportar mayor granularidad y facilitar la diferenciación entre riesgos con exposiciones similares, pero también puede incrementar la subjetividad, la carga administrativa y la dificultad de aplicación homogénea. Por el contrario, una escala con menos niveles puede facilitar la comunicación y aplicación práctica, aunque puede limitar la capacidad de priorización y diferenciación.

A modo ilustrativo, muchas organizaciones utilizan escalas de cinco niveles, que permiten equilibrar simplicidad, comparabilidad y capacidad de diferenciación. Los siguientes ejemplos deben entenderse como una referencia inicial que deberá adaptarse a la realidad de cada organización y completarse con descriptores, umbrales y criterios específicos.

Escala ilustrativa de probabilidad

Nivel	Probabilidad	Descripción orientativa
1	Muy baja	Evento excepcional o muy improbable.
2	Baja	Evento poco probable, aunque posible.
3	Media	Evento que podría ocurrir en determinadas circunstancias.
4	Alta	Evento probable, con una posibilidad relevante de ocurrencia.
5	Muy alta	Evento esperado o con exposición continuada que hace probable su materialización.

Escala ilustrativa de impacto

Nivel	Impacto	Descripción orientativa
1	Muy bajo	Evento no material, absorbible dentro de la gestión ordinaria de la organización.
2	Bajo	Impacto limitado sobre resultados, procesos, cumplimiento o actividad, gestionable por el área afectada.
3	Moderado	Impacto relevante que requiere medidas de gestión, seguimiento o refuerzo de controles.
4	Alto	Impacto significativo sobre objetivos, operaciones, resultados, cumplimiento o reputación. Requiere seguimiento reforzado.
5	Crítico	Impacto severo que puede comprometer objetivos críticos, continuidad, cumplimiento, reputación o viabilidad de una actividad.

Las escalas anteriores tienen carácter meramente ilustrativo. Cada organización deberá definir los niveles, descriptores y umbrales que mejor se adapten a su realidad, asegurando que permitan una aplicación homogénea entre áreas, unidades de negocio y periodos de evaluación.

En la definición del impacto deberán considerarse las distintas dimensiones relevantes para la organización, como impacto financiero, operativo, reputacional, regulatorio, legal, sobre personas o sobre continuidad de negocio. Cuando un riesgo pueda afectar a varias dimensiones, la metodología deberá establecer una regla clara para determinar el impacto final, que deberá ser coherente con el apetito al riesgo, las tolerancias y los criterios de escalado definidos.

En el caso del impacto financiero, la organización podrá traducir los niveles de impacto a rangos económicos, de EBITDA, presupuesto, margen u otra magnitud relevante, calibrados en función de su tamaño, capacidad financiera y materialidad interna.

Cuando existan diferentes dimensiones de impacto, la organización deberá definir cómo se consolida la valoración global del riesgo, por ejemplo mediante el impacto máximo, una ponderación entre dimensiones o criterios específicos por categoría de riesgo.

5.3.4. Otras variables complementarias

Las variables complementarias no tienen por qué incorporarse siempre al cálculo de criticidad. Su utilización deberá ser proporcional a la naturaleza del riesgo, al objetivo de la evaluación y al nivel de madurez del modelo. En muchos casos bastará con utilizarlas como información cualitativa adicional para orientar el tratamiento, la monitorización o el escalado.

Velocidad

La velocidad mide la rapidez con la que el riesgo produce efectos una vez desencadenado.

Esta variable resulta especialmente importante en:

- ciberataques;
- crisis reputacionales;
- fallos tecnológicos;
- incidentes operativos críticos.

Los riesgos de alta velocidad requieren mecanismos reforzados de monitorización y respuesta.

Proximidad

La proximidad analiza el horizonte temporal estimado de ocurrencia del riesgo.

Permite clasificar riesgos en:

- corto plazo;
- medio plazo;
- largo plazo.

Esta variable facilita la planificación preventiva.

Tendencia

Mide si la exposición al riesgo está aumentando, disminuyendo o permanece estable. Esta variable resulta útil para priorizar riesgos cuyo nivel actual puede no ser crítico, pero muestra señales claras de deterioro.

Persistencia o duración

Evalúa cuánto tiempo pueden mantenerse los efectos del riesgo tras su materialización.

Detectabilidad

Mide la capacidad de la organización para identificar señales tempranas antes de la materialización del riesgo. Una baja detectabilidad puede incrementar la criticidad del riesgo, al reducir la capacidad de anticipación y respuesta.

Recuperación

Mide la capacidad de la organización para volver a un nivel aceptable de funcionamiento tras la materialización del riesgo, considerando recursos, planes de continuidad, alternativas operativas, redundancias y tiempos de recuperación.

Adaptabilidad

Mide la capacidad de la organización para ajustar su estrategia, procesos, recursos o modelo operativo ante cambios relevantes en el entorno o en el perfil de riesgo.

5.4. Métodos de evaluación

La evaluación de riesgos puede realizarse mediante métodos cualitativos, semicuantitativos o cuantitativos. La elección del método dependerá de la naturaleza del riesgo, la disponibilidad y

calidad de los datos, el nivel de incertidumbre, la madurez analítica de la organización, la criticidad del riesgo y el uso que vaya a darse al resultado de la evaluación.

Estos métodos no deben entenderse como excluyentes. En la práctica, muchos modelos ERM combinan juicio experto, escalas homogéneas, datos históricos, escenarios y análisis cuantitativos cuando existe información suficiente. El objetivo no es alcanzar una precisión aparente, sino obtener una valoración razonable, trazable y útil para la toma de decisiones.

5.4.1. Métodos cualitativos y semicuantitativos

Los métodos cualitativos se basan principalmente en el juicio experto, el conocimiento del negocio, la experiencia profesional y la percepción estructurada de los responsables implicados en la gestión del riesgo. Son especialmente útiles cuando no existe información histórica suficiente, cuando el riesgo presenta elevada incertidumbre o cuando su impacto no puede expresarse fácilmente en términos financieros.

En un modelo ERM, estos métodos permiten analizar riesgos estratégicos, reputacionales, regulatorios, geopolíticos, emergentes, tecnológicos, ESG o asociados al comportamiento humano y organizativo. Su valor reside en facilitar una valoración estructurada de riesgos complejos, incorporando la visión de diferentes áreas y niveles de la organización.

En la práctica, muchas organizaciones utilizan métodos semicuantitativos, en los que el juicio experto se traduce en escalas homogéneas de probabilidad e impacto. Estas escalas permiten comparar riesgos, construir mapas de calor, asignar niveles de criticidad y priorizar respuestas. Aunque utilicen puntuaciones numéricas, estas escalas no deben interpretarse como mediciones exactas, sino como una forma estructurada de ordenar y comparar exposiciones.

Entre las técnicas cualitativas y semicuantitativas más habituales destacan:

- **Entrevistas individuales:** permiten obtener información detallada de responsables clave, especialmente cuando el riesgo requiere conocimiento técnico, operativo o estratégico específico. Son útiles para profundizar en causas, consecuencias, controles existentes, señales tempranas y posibles escenarios de materialización.
- **Talleres de riesgos:** permiten contrastar visiones de distintas áreas, construir consenso sobre la valoración del riesgo e identificar interdependencias, efectos en cadena o discrepancias relevantes entre funciones. Son especialmente útiles para riesgos transversales o con impacto en varias unidades.
- **Cuestionarios y autoevaluaciones:** facilitan la recopilación sistemática de información cuando participan múltiples áreas, geografías o unidades de negocio. Deben diseñarse con preguntas claras y escalas homogéneas para evitar respuestas poco comparables.
- **Juicio experto estructurado:** permite incorporar conocimiento especializado interno o externo, especialmente en riesgos con poca información histórica. Para evitar sesgos, debe apoyarse en criterios comunes, evidencia disponible, contraste entre expertos y documentación de los principales supuestos utilizados.
- **Análisis de escenarios:** permite evaluar situaciones futuras plausibles, severas o inciertas, analizando sus posibles efectos sobre objetivos, operaciones, finanzas, cumplimiento, reputación o personas. Puede utilizarse de forma cualitativa, semicuantitativa o cuantitativa, en función del grado de desarrollo del escenario y de los datos disponibles.
- **Matrices de probabilidad e impacto:** Las matrices de probabilidad e impacto permiten valorar y priorizar riesgos mediante escalas homogéneas que combinan la probabilidad de ocurrencia y la magnitud de sus consecuencias. Son una herramienta ampliamente utilizada en modelos ERM para facilitar la comparación y comunicación del perfil de riesgo.
- **Bow Tie:** El análisis Bow Tie permite representar visualmente la relación entre las causas del riesgo, el evento, las consecuencias, los controles preventivos y las medidas de recuperación o mitigación. Es especialmente útil para riesgos críticos o de baja frecuencia y alto impacto, ya que facilita la identificación de barreras de control y posibles puntos de fallo.

Los métodos cualitativos y semicuantitativos presentan ventajas relevantes: son ágiles, flexibles, de bajo coste, facilitan la participación del negocio y permiten valorar riesgos difíciles de cuantificar. No obstante, también presentan limitaciones: pueden incorporar sesgos, depender excesivamente de la experiencia de los participantes, generar diferencias de criterio entre áreas y transmitir una falsa sensación de precisión cuando se utilizan puntuaciones numéricas sin descriptores claros.

Por ello, cuando el riesgo sea material, exista información suficiente o la decisión lo requiera, estas valoraciones podrán complementarse con análisis cuantitativos, manteniendo siempre el juicio profesional y evitando una falsa precisión numérica.

5.4.2. Métodos cuantitativos y modelos analíticos

Las técnicas cuantitativas de evaluación de riesgos permiten estimar la exposición al riesgo mediante datos, modelos matemáticos y herramientas estadísticas que facilitan una aproximación más trazable y comparable de los riesgos organizativos.

Estas metodologías son especialmente útiles en organizaciones con suficiente madurez analítica y disponibilidad de información histórica, y permiten complementar el juicio experto derivado de metodologías cualitativas.

La elección de una u otra técnica dependerá de diversos factores, entre ellos:

- naturaleza del riesgo;
- disponibilidad y calidad de los datos;
- complejidad del análisis requerido;
- horizonte temporal;
- criticidad del riesgo;
- capacidad analítica de la organización.

Cuando se aplican adecuadamente, los métodos cuantitativos pueden reforzar la evaluación al aportar una base analítica más sólida para contrastar hipótesis, estimar rangos de impacto, analizar la sensibilidad de los resultados ante cambios en variables clave y evaluar escenarios complejos. También pueden resultar útiles para apoyar la definición de tolerancias, límites o umbrales, así como para priorizar recursos destinados a controles, medidas de mitigación o planes de acción.

No obstante, una mayor cuantificación no implica necesariamente una mejor evaluación. La fiabilidad de estos métodos depende de la calidad, suficiencia y representatividad de los datos utilizados, así como de la solidez de las hipótesis, distribuciones y supuestos aplicados. Por ello, pueden resultar menos adecuados para riesgos emergentes, estratégicos, reputacionales o de elevada incertidumbre, en los que no existe histórico suficiente o el comportamiento futuro del riesgo es difícil de modelizar.

Asimismo, la aplicación de técnicas cuantitativas puede requerir capacidades técnicas específicas para construir, interpretar, revisar y mantener los modelos utilizados. Si estas capacidades no existen o los resultados no son comprensibles para quienes deben tomar decisiones, el análisis puede generar una falsa sensación de precisión o convertirse en un ejercicio técnico con limitada utilidad práctica.

Por tanto, los resultados cuantitativos no deberán interpretarse como predicciones exactas ni utilizarse de forma mecánica. Deben considerarse un apoyo complementario al juicio profesional, al conocimiento del negocio y a la toma de decisiones, manteniendo siempre la responsabilidad de gestión en los responsables del riesgo y en los órganos que correspondan.

A modo orientativo, y sin carácter obligatorio, las principales técnicas cuantitativas o con componente cuantitativo utilizadas en la evaluación de riesgos incluyen:

- **Análisis estadístico:** permite analizar datos históricos para identificar patrones, tendencias, frecuencias o distribuciones asociadas al comportamiento del riesgo.

- **Modelización de escenarios:** permite valorar posibles situaciones futuras mediante la combinación de eventos, condiciones o hipótesis alternativas incorporando estimaciones cuantitativas.
- **Simulación Monte Carlo:** permite modelizar incertidumbre mediante múltiples simulaciones probabilísticas para estimar rangos de resultados y posibles desviaciones.
- **Análisis de sensibilidad:** permite evaluar cómo varían los resultados ante cambios en variables clave o supuestos relevantes.
- **Árboles de decisión:** permiten comparar alternativas considerando eventos inciertos, probabilidades y resultados esperados.
- **Pruebas de estrés:** permiten analizar la capacidad de resistencia de la organización ante escenarios extremos, severos pero plausibles.
- **Pruebas de estrés inversas:** parten de un resultado no deseado para identificar qué combinación de eventos, vulnerabilidades o fallos podría conducir a dicha situación.
- **Value at Risk (VaR):** permite estimar pérdidas potenciales dentro de un nivel de confianza y horizonte temporal determinados, principalmente en riesgos financieros.
- **Modelos predictivos:** utilizan datos históricos y técnicas estadísticas o analíticas avanzadas para anticipar comportamientos, eventos o patrones futuros.

La selección de una técnica u otra deberá realizarse de forma proporcional, considerando la naturaleza del riesgo, la disponibilidad y calidad de los datos, la criticidad de la decisión, el horizonte temporal del análisis y la capacidad de la organización para interpretar y mantener el modelo utilizado.

En todos los casos, deberán documentarse los principales supuestos utilizados, fuentes de información, limitaciones, responsable del análisis, fecha de actualización y finalidad prevista de los resultados. El detalle ampliado de estas técnicas se recoge en el **Anexo III — Principales técnicas de evaluación de riesgos.**

5.4.3. Enfoque combinado

En la práctica, la evaluación de riesgos suele requerir un enfoque combinado. Los métodos cualitativos aportan conocimiento experto, contexto y comprensión del riesgo; los métodos semicuantitativos facilitan la comparación y priorización; y los métodos cuantitativos permiten profundizar cuando existen datos suficientes o cuando la decisión requiere una estimación más analítica.

La elección del método deberá ser proporcional al riesgo y al uso previsto del resultado. No todos los riesgos requieren modelización cuantitativa, ni todos los análisis cualitativos son insuficientes. Un modelo ERM eficaz debe evitar tanto la valoración puramente intuitiva como la cuantificación excesiva sin datos fiables.

Como criterio práctico:

- los riesgos estratégicos, emergentes o reputacionales suelen requerir análisis cualitativo, escenarios y juicio experto;
- los riesgos operacionales recurrentes pueden evaluarse mediante escalas semicuantitativas y datos históricos;
- los riesgos financieros, asegurables, de continuidad, proyectos relevantes o exposiciones con suficiente información pueden beneficiarse de análisis cuantitativos;
- los riesgos críticos o fuera de tolerancia pueden requerir una combinación de métodos para justificar decisiones de tratamiento, aceptación, transferencia o escalado.

El resultado de la evaluación deberá ser comprensible para los responsables del riesgo, útil para la Alta Dirección y suficientemente trazable para soportar decisiones, seguimiento y reporting.

5.5. Criticidad y priorización de riesgos

La criticidad no debe entenderse como una variable aislada de evaluación, sino como el resultado de combinar distintas variables y criterios para determinar la prioridad relativa de un riesgo dentro del modelo ERM. Su finalidad es orientar la toma de decisiones, la

asignación de recursos, el nivel de seguimiento, la necesidad de tratamiento y los criterios de escalado.

La criticidad suele determinarse a partir de la combinación entre probabilidad e impacto, pudiendo complementarse, cuando la metodología lo prevea, con otros factores como velocidad, proximidad, persistencia, detectabilidad, capacidad de recuperación, tendencia del riesgo, interdependencias y comparación con el apetito y las tolerancias definidos.

La organización podrá establecer metodologías de puntuación o priorización adaptadas a sus necesidades, siempre que los criterios utilizados estén documentados y se apliquen de forma homogénea entre riesgos, unidades de negocio y periodos de evaluación.

La metodología utilizada deberá evitar la doble contabilización de factores. Por ejemplo, si la eficacia de los controles ya ha sido considerada para calcular el riesgo residual, no debería volver a ponderarse automáticamente en el cálculo de criticidad, salvo que la metodología lo justifique expresamente.

La criticidad suele estructurarse en categorías que facilitan la priorización y el escalado:

Nivel	Descripción
Baja	Riesgo asumible y monitorizable.
Moderada	Riesgo que requiere seguimiento periódico.
Alta	Riesgo que requiere acciones específicas o seguimiento reforzado.
Crítica	Riesgo que requiere intervención prioritaria y escalado a los órganos correspondientes.

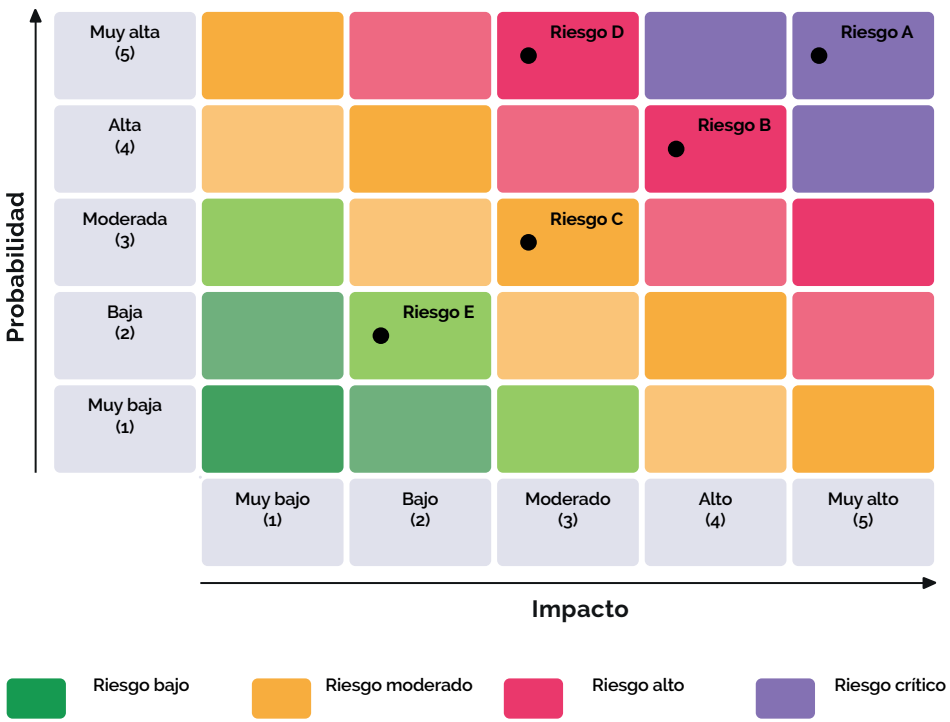
Representación de la criticidad mediante mapas de calor

Una de las formas más habituales de representar los resultados de la evaluación es el mapa de calor o matriz de riesgos, que permite visualizar la posición relativa de los riesgos en función de las variables utilizadas en su valoración, habitualmente probabilidad e impacto.

Los mapas de calor facilitan la comparación y priorización de riesgos y constituyen una herramienta útil para comunicar el perfil de riesgo de la organización. Las categorías y colores utilizados deberán ser coherentes con los criterios de criticidad establecidos en la metodología.

Esta representación debe interpretarse como una herramienta de apoyo a la priorización y comunicación, y no como un sustituto del análisis del riesgo. Riesgos con una posición similar en el mapa pueden requerir respuestas diferentes en función de su naturaleza, interdependencias, evolución o situación respecto al apetito y las tolerancias definidas.

A continuación se muestra un ejemplo orientativo de mapa de calor para la representación de riesgos.



Nota: La escala, categorías y colores utilizados en este ejemplo son orientativos y podrán adaptarse a la metodología de cada organización.

Figura 10: **Ejemplo de mapa de calor.** Fuente: elaboración propia.

La categoría de criticidad asignada deberá tener consecuencias prácticas dentro del modelo ERM. No debe limitarse a clasificar visualmente los riesgos, sino orientar la frecuencia de seguimiento, el nivel de escalado, la necesidad de planes de acción, la intensidad de monitorización mediante KRIs y el nivel de aprobación requerido para aceptar o tratar el riesgo.

A modo orientativo:

- Los riesgos de criticidad baja podrán mantenerse bajo seguimiento ordinario, salvo que presenten una tendencia de deterioro o se produzcan cambios relevantes en el contexto.

- Los riesgos de criticidad moderada requerirán seguimiento periódico y revisión de controles, especialmente cuando existan señales tempranas de deterioro o proximidad a los umbrales definidos.

- Los riesgos de criticidad alta deberán contar con seguimiento reforzado, responsable asignado, análisis de controles y, cuando proceda, planes de acción específicos con plazos y evidencias de avance.

- Los riesgos de criticidad crítica deberán ser objeto de escalado prioritario a los órganos correspondientes, seguimiento frecuente y decisiones explícitas de tratamiento, aceptación, transferencia o evitación, de acuerdo con el apetito y las tolerancias aprobadas.

La metodología deberá definir de forma clara qué implicaciones tiene cada nivel de criticidad para evitar que la priorización quede como un ejercicio meramente descriptivo.

5.6. Resultado de la evaluación y conexión con tratamiento y monitorización

El resultado del análisis y evaluación de riesgos deberá traducirse en información útil para la toma de decisiones. Entre los principales

resultados esperados se encuentran el mapa de riesgos actualizado, la priorización de riesgos por criticidad, la identificación de riesgos fuera de apetito o tolerancia, la valoración del nivel inherente y residual de exposición, la identificación de brechas entre riesgo residual y riesgo objetivo, la detección de debilidades de control y la definición de necesidades de tratamiento, seguimiento o escalado.

Como resultado práctico, cada riesgo evaluado debería contar, al menos, con una valoración inherente y residual, responsable del riesgo, controles principales, nivel de criticidad, situación frente al apetito o tolerancias, necesidad de tratamiento adicional, responsable de las acciones y frecuencia de seguimiento.

La evaluación no debe entenderse como un ejercicio aislado, sino como el punto de conexión entre la identificación de riesgos, las decisiones de tratamiento, la definición de controles, la monitorización mediante indicadores y el reporting a la Alta Dirección y a los órganos de gobierno.

Capítulo 6.
Tratamiento del Riesgo

El tratamiento del riesgo constituye una de las fases esenciales del modelo de Gestión Integral de Riesgos (ERM). Es en este punto donde la organización transforma el análisis y evaluación de los riesgos en decisiones concretas, orientadas a proteger los objetivos estratégicos, garantizar la continuidad del negocio y favorecer una gestión responsable y sostenible.

Gestionar riesgos no implica eliminarlos por completo —algo ni deseable ni posible—, sino comprenderlos, priorizarlos y decidir conscientemente cómo abordarlos, de acuerdo con el apetito al riesgo definido por la organización y con sus capacidades operativas, financieras y organizativas.

El tratamiento del riesgo debe entenderse como un proceso dinámico, sujeto a revisión continua y estrechamente vinculado a la evolución del entorno, del negocio, de la estrategia y del nivel residual de exposición. Las decisiones de tratamiento deberán basarse en la criticidad del riesgo, su situación frente al apetito y las tolerancias, la eficacia de los controles existentes, el coste-beneficio de las medidas disponibles y las obligaciones legales, regulatorias o contractuales aplicables.

6.1. Las respuestas al riesgo

Una vez identificado y evaluado un riesgo, la organización debe decidir cuál es la respuesta más adecuada. En el marco del ERM se reconocen cuatro grandes enfoques, que no son excluyentes

entre sí y que, en la práctica, pueden combinarse: aceptar, mitigar o reducir, compartir o transferir, y evitar.

La selección de la respuesta no debe realizarse de forma automática únicamente en función de la probabilidad e impacto. Debe considerar también el apetito y tolerancias definidos, la capacidad de la organización, el nivel de exposición residual, la existencia de controles eficaces, el coste de las medidas, la urgencia de actuación, las interdependencias con otros riesgos y el nivel de aprobación requerido.

La selección de la respuesta al riesgo puede apoyarse en una matriz orientativa basada en probabilidad e impacto, sin perjuicio de que la decisión final deba considerar también el apetito, las tolerancias, la eficacia de los controles, el coste-beneficio y la capacidad real de implantación, como se muestra en la Figura 11.

Matriz orientativa de respuestas al riesgo

Referencia inicial para orientar la selección de la respuesta al riesgo en función de si probabilidad e impacto.



Figura 11: **Matriz orientativa de respuestas al riesgo.** Fuente: elaboración propia.

- **Aceptar el riesgo:**

Aceptar un riesgo significa asumirlo conscientemente, sin adoptar medidas adicionales más allá de las ya existentes. Esta decisión no es pasiva ni automática; por el contrario, requiere un análisis previo y una validación explícita.

La aceptación resulta apropiada cuando el riesgo se sitúa dentro de los niveles de tolerancia de la organización, cuando su impacto potencial es limitado o cuando las medidas de mitigación disponibles resultarían desproporcionadas frente al beneficio esperado. En estos casos, el foco se sitúa en la monitorización del riesgo, manteniéndolo bajo observación y revisándolo periódicamente para detectar posibles cambios en su perfil.

Aceptar un riesgo no implica ignorarlo, sino reconocerlo y gestionarlo desde la vigilancia y la preparación.

- **Mitigar/Reducir el riesgo:**

Mitigar un riesgo supone actuar sobre él para reducir su probabilidad de ocurrencia, su impacto o ambos factores a la vez. Se trata, probablemente, de la respuesta más habitual en la gestión de riesgos operativos, financieros, legales y de cumplimiento.

La mitigación se materializa a través de acciones concretas: mejoras en los procesos, implementación de controles internos, formación del personal, inversiones en sistemas o ajustes organizativos. Estas medidas pueden adoptarse antes de que el riesgo se materialice, para prevenirlo, o bien orientarse a detectarlo tempranamente y minimizar sus consecuencias.

Una mitigación eficaz no busca eliminar por completo el riesgo, sino reducirlo hasta un nivel residual aceptable, equilibrando protección y eficiencia.

- **Compartir/Transferir el riesgo**

Transferir el riesgo implica desplazar total o parcialmente las consecuencias económicas de un evento a un tercero. Es importante

destacar que lo que se transfiere no es el riesgo en sí mismo, sino su impacto financiero.

La transferencia puede realizarse de distintas formas: mediante la contratación de seguros, a través de cláusulas contractuales que repartan responsabilidades, mediante la subcontratación de actividades a especialistas o mediante acuerdos de reparto de riesgos con socios o terceros.

Esta estrategia resulta especialmente útil para riesgos de baja frecuencia pero alto impacto. Sin embargo, la transferencia nunca es absoluta: la organización mantiene la responsabilidad última sobre su actividad y debe complementar esta respuesta con controles adecuados y una correcta gestión operativa del riesgo.

- **Evitar/Rechazar el riesgo**

Evitar un riesgo supone renunciar a la actividad que lo genera, eliminando así su exposición. Se trata de una decisión de alto impacto, habitualmente vinculada a riesgos que exceden claramente el apetito al riesgo de la organización o que presentan consecuencias potencialmente críticas y no mitigables de forma razonable.

La evitación puede implicar abandonar determinados mercados, no prestar ciertos servicios o descartar iniciativas estratégicas. Por su naturaleza, este tipo de decisiones debe adoptarse de forma informada, documentada y alineada con la visión a largo plazo de la organización.

6.2. Acciones, controles y planes de acción

La respuesta al riesgo se concreta mediante acciones y controles que permiten llevar la decisión al terreno operativo.

Las acciones son las iniciativas específicas que se ponen en marcha para implementar la respuesta elegida: revisar un procedimiento, reforzar un control, modificar un contrato o implantar una nueva herramienta. Cada acción debe contar con un responsable claro, un plazo definido y recursos asignados.

Los controles, por su parte, constituyen los mecanismos recurrentes que ayudan a prevenir la materialización del riesgo, a detectarlo a tiempo o a corregir desviaciones. Un sistema de controles eficaz es proporcional al riesgo, está bien documentado y se revisa periódicamente para asegurar su adecuación.

Cuando un riesgo presenta una especial relevancia, las acciones y controles se articulan en planes de acción, que permiten coordinar esfuerzos, hacer seguimiento de los avances y asegurar la reducción progresiva del riesgo hasta niveles aceptables.

6.3. El papel del seguro en la gestión de riesgos

Dentro del conjunto de herramientas disponibles para el tratamiento del riesgo, el seguro desempeña un papel destacado como mecanismo de transferencia del impacto económico de determinados eventos adversos, y como mecanismo para delimitar la parte del impacto económico que la organización retiene, por ejemplo mediante franquicias, exclusiones o sublímites.

El seguro permite a la organización proteger su estabilidad financiera frente a riesgos tales como daños materiales, responsabilidades frente a terceros, pérdidas en el transporte, accidentes laborales o determinados riesgos profesionales. No obstante, su función debe entenderse siempre como complementaria a otras medidas de mitigación y control.

El seguro no elimina el riesgo ni sustituye la gestión responsable del mismo. Además, presenta limitaciones inherentes: exclusiones, franquicias, sublímites o riesgos no asegurables. Por ello, su contratación debe evaluarse en términos de coste-beneficio, coherencia con el perfil de riesgo de la organización y adecuación a los objetivos estratégicos.

Integrado adecuadamente en el marco ERM, el seguro contribuye a una gestión equilibrada del riesgo y a la protección de la continuidad del negocio.

Capítulo 7.
Monitorización, reporting y mejora continua

La monitorización, el reporting y la mejora continua constituyen una fase esencial del modelo de Enterprise Risk Management (ERM), cuyo objetivo es garantizar que la gestión de riesgos permanezca actualizada, eficaz, dinámica y alineada con el contexto interno y externo de la organización.

La exposición al riesgo de una entidad no es estática. Los cambios en el entorno económico, regulatorio, tecnológico, geopolítico, social o competitivo pueden modificar de manera significativa el perfil de riesgos de la organización en períodos relativamente cortos de tiempo. En consecuencia, el sistema ERM debe incorporar mecanismos formales de seguimiento, supervisión y adaptación continua.

La monitorización del riesgo tiene como finalidad:

- supervisar la evolución del perfil de riesgos;
- verificar el grado de implantación de medidas mitigadoras;
- detectar desviaciones respecto al apetito al riesgo;
- identificar riesgos emergentes;
- anticipar deterioros potenciales;
- facilitar la toma de decisiones basada en información actualizada;
- fortalecer la resiliencia organizativa;
- evaluar la eficacia del propio modelo ERM.

Un sistema de monitorización maduro debe combinar información retrospectiva (qué ha ocurrido), información presente (qué está ocurriendo) e información prospectiva (qué podría ocurrir).

La función ERM deberá asegurar que la monitorización se realiza de forma continua y proporcional a la criticidad de los riesgos.

7.1. Seguimiento de planes de acción

El seguimiento de planes de acción constituye uno de los elementos fundamentales para garantizar que la gestión de riesgos genere un impacto real sobre la reducción de exposición de la organización.

La identificación y evaluación de riesgos carece de utilidad si no se traduce en acciones concretas destinadas a:

- reducir la probabilidad de ocurrencia;
- disminuir el impacto potencial;
- fortalecer controles;
- incrementar capacidad de detección;
- mejorar resiliencia;
- reducir vulnerabilidades.

Los planes de acción deberán diseñarse especialmente para aquellos riesgos:

- críticos;
- por encima del apetito al riesgo;
- con insuficiente entorno de control;
- emergentes;
- con tendencia de deterioro.

Contenido mínimo de un plan de acción

Cada plan de acción deberá documentarse formalmente e incluir, al menos:

- Descripción de la acción: Detalle específico de la medida propuesta. Ejemplo: "Implementación de autenticación multifactor para sistemas críticos".
- Riesgo asociado: Riesgo o conjunto de riesgos mitigados.
- Responsable del plan de acción: Persona responsable de implantación.
- Fecha objetivo: Calendario comprometido.
- Estado de ejecución (no iniciado; en progreso; parcialmente implantado; completado; retrasado).
- Impacto esperado: Estimación de reducción del riesgo.
- Dependencias: Recursos, proyectos o aprobaciones necesarias.

Seguimiento y escalado

La función ERM deberá realizar seguimiento periódico de los planes de acción mediante:

- revisiones periódicas;
- reuniones con *risk owners*;
- validación de evidencias;
- actualización de estados;
- identificación de retrasos.

Los retrasos significativos o incumplimientos deberán escalarse a la Alta Dirección y, cuando proceda, al Consejo o Comisión de Auditoría/Riesgos.

La monitorización deberá centrarse no solo en la ejecución, sino también en la efectividad real de las medidas implantadas.

7.2. Periodicidad del reporte a Alta Dirección y Consejo

Un modelo ERM eficaz requiere un sistema de reporting periódico, estructurado y orientado a la toma de decisiones.

La periodicidad deberá adaptarse:

- a la criticidad de los riesgos;
- al dinamismo del entorno;
- a los requerimientos regulatorios;
- a las necesidades de gobierno corporativo.

El reporting deberá evitar convertirse en un ejercicio meramente descriptivo, priorizando información accionable.

Reporting a Alta Dirección

Como referencia, muchas organizaciones establecen una periodicidad trimestral o semestral para el reporting ordinario a la Alta Dirección, complementada con reportes extraordinarios cuando se produzcan eventos relevantes, deterioros significativos o superaciones de umbrales.

El informe deberá incluir:

- **Perfil global de riesgos:** Visión consolidada de exposición.
- **Evolución del mapa de riesgos:** Cambios respecto al período anterior.
- **Riesgos críticos:** Especial foco en riesgos fuera de apetito.
- **KRIs relevantes:** Indicadores deteriorados o próximos a umbral.
- **Estado de planes de acción:** Avance y retrasos.
- **Riesgos emergentes:** Nuevas amenazas.
- **Incidentes significativos:** Eventos ocurridos y lecciones aprendidas.

Reporting al Consejo/Comisión de Auditoría o Riesgos

Se recomienda una frecuencia **trimestral o semestral**, dependiendo del perfil de riesgo de la organización. El reporting al Consejo deberá ser:

- estratégico;
- ejecutivo;
- orientado a decisiones;
- centrado en excepciones.

El Consejo debe recibir especial información sobre:

- riesgos críticos;
- evolución del apetito al riesgo;
- resiliencia organizativa;
- principales vulnerabilidades;
- tendencias emergentes.

Asimismo, cualquier evento severo deberá comunicarse de forma inmediata mediante reporting extraordinario.

7.3. Definición y monitorización de KRIs

Los **Key Risk Indicators (KRIs)** son métricas utilizadas para monitorizar la evolución de los riesgos y detectar señales tempranas de deterioro.

Su objetivo es proporcionar alertas preventivas antes de que el riesgo se materialice o antes de que sus efectos se agraven. Los KRIs constituyen un mecanismo clave de anticipación y permiten pasar de una gestión reactiva a una gestión proactiva del riesgo.

Un KRI eficaz debe ser:

- relevante;
- medible;
- objetivo;
- sensible;
- accionable;
- actualizado periódicamente.

Asimismo, debe estar claramente vinculado a un riesgo concreto. La organización deberá:

- **Identificar factores de riesgo:** Factores que anticipan deterioro.
- **Definir métricas:** Indicadores cuantificables.
- **Establecer umbrales:**
  verde: dentro de los parámetros definidos;
  amarillo: alerta temprana;
  rojo: fuera de los parámetros definidos.

- **Asignar responsables:** Monitorización y reporting.
- **Definir frecuencia:** Mensual, trimestral, etc.

Los KRIs deberán visualizarse mediante:
- Cuadros de mando;
- semáforos;
- tendencias temporales;
- análisis comparativo.

La función ERM deberá supervisar desviaciones y activar escalados cuando se superen umbrales.

Conviene aclarar que los KRIs no deben confundirse con KPIs ni KCIs. Aunque pueden estar relacionados, su finalidad principal es anticipar cambios en la exposición al riesgo.

KRI: mide exposición o deterioro del riesgo.
KPI: mide desempeño del negocio o del proceso.
KCI: mide funcionamiento de controles.

7.4. Reporting a grupos de interés: IAGC (Informe Anual de Gobierno Corporativo) e Informe de Sostenibilidad

La gestión de riesgos constituye un elemento esencial de transparencia y buen gobierno corporativo.

La organización deberá asegurar un reporting claro, consistente y verificable hacia grupos de interés internos y externos, cuando aplique.

Informe Anual de Gobierno Corporativo (IAGC)

El IAGC deberá incluir información suficiente sobre:

- sistema de gestión de riesgos;
- principales riesgos;

- mecanismos de control;
- supervisión del Consejo;
- riesgos financieros y no financieros;
- eficacia del sistema de control interno.

La divulgación deberá reflejar adecuadamente el nivel de madurez del modelo ERM.

Informe de Sostenibilidad

La creciente relevancia de factores ESG requiere integrar el riesgo dentro del reporting de sostenibilidad. Deberá incluirse información sobre:

- Riesgos climáticos: (físicos; transición).
- Riesgos sociales: (talento; derechos humanos; cadena de suministro).
- Riesgos de gobernanza: (ética; compliance; corrupción).

Asimismo, deberá explicarse:

- metodología de evaluación;
- integración en estrategia;
- gestión de riesgos ESG;
- resiliencia organizativa.

El reporting deberá alinearse con marcos regulatorios y estándares aplicables.

7.5. Evaluación periódica del desempeño del ERM a través de KPIs

La función ERM deberá medir periódicamente su propio desempeño para garantizar su eficacia y madurez. El objetivo no es únicamente gestionar riesgos, sino verificar si el propio sistema funciona adecuadamente.

Ejemplo de KPIs a incluir:

- **Cobertura del mapa de riesgos:** % de procesos evaluados.
- **Calidad de evaluaciones:** % riesgos revisados en plazo.
- **Ejecución de planes:** % acciones completadas.
- **Riesgos fuera de apetito:** nº y evolución.
- **Tiempo de respuesta:** ante incidentes relevantes.
- **Participación organizativa:** % áreas involucradas.
- **Formación:** % empleados formados.

Se recomienda revisión **anual**, complementada con seguimiento trimestral.

7.6. Evaluación independiente del modelo ERM

La evaluación proporciona una visión independiente sobre la madurez, diseño y efectividad del sistema ERM. Puede realizarse de forma interna (normalmente auditoría interna) o de forma externa.

Permite identificar oportunidades de mejora, brechas metodológicas, benchmarking y alineación regulatoria. El alcance de la evaluación puede incluir:

- gobierno;
- metodología;
- reporting;
- cultura de riesgo;
- KPIs;
- apetito al riesgo;
- integración estratégica.

Se recomienda realizar una revisión independiente cada **3–5 años**, o ante transformaciones relevantes.

7.7. Formación en gestión de riesgos

La formación en gestión de riesgos es un elemento clave para asegurar que el modelo ERM se comprende y se aplica de forma homogénea en la organización. Complementa la cultura de riesgo y las acciones

de comunicación y sensibilización, pero tiene un enfoque más práctico y orientado a dotar a cada colectivo de los conocimientos necesarios para desempeñar su rol dentro del modelo.

La formación debe garantizar que empleados, mandos intermedios, responsables del riesgo, funciones de control, Alta Dirección y órganos de gobierno comprenden, en función de su nivel de responsabilidad:

- qué es un riesgo y cómo se diferencia de una causa, una consecuencia, un incidente o un control;
- cuál es su papel dentro del modelo de gestión de riesgos;
- cómo se identifican, evalúan, tratan y monitorizan los riesgos;
- cuáles son los criterios de escalado y reporte;
- cómo se utilizan el apetito al riesgo, las tolerancias, los límites, los KRIs y los planes de acción.

El modelo formativo deberá adaptarse al perfil de cada colectivo, evitando una formación única y genérica para toda la organización. Como referencia, puede estructurarse en los siguientes niveles:

- **Formación general:** dirigida al conjunto de la organización, centrada en conceptos básicos de riesgo, cultura de reporte temprano, canales de comunicación y criterios generales de escalado.
- **Formación específica:** dirigida a responsables del riesgo y mandos intermedios, centrada en la metodología de identificación, evaluación, tratamiento, seguimiento, documentación de evidencias, actualización de riesgos y gestión de planes de acción.
- **Formación ejecutiva:** dirigida a la Alta Dirección y al Consejo, centrada en el perfil global de riesgos, apetito y tolerancias, riesgos críticos, riesgos emergentes, escenarios, decisiones bajo incertidumbre y criterios de supervisión.
- **Formación especializada:** dirigida a funciones como ERM, cumplimiento, auditoría interna, ESG, ciberseguridad, continuidad de negocio u otras áreas técnicas, centrada en metodologías específicas, normativa aplicable, controles, indicadores, reporting y aseguramiento.

Los contenidos mínimos de la formación podrán incluir el marco ERM, la taxonomía de riesgos, la metodología de evaluación, el apetito al riesgo, las tolerancias, los KRIs, los controles, los incidentes, los planes de acción, el reporting, los criterios de escalado y la gestión de riesgos emergentes.

Para medir su efectividad, la organización deberá evaluar no solo la participación o satisfacción de los asistentes, sino también la aplicación práctica de los conocimientos adquiridos. Para ello, podrán utilizarse indicadores como:

- porcentaje de colectivos formados;
- resultados de pruebas o autoevaluaciones de conocimiento;
- calidad de la información reportada por las áreas;
- cumplimiento de plazos de actualización de riesgos y planes de acción;
- mejora en la identificación temprana y escalado de riesgos;
- reducción de errores metodológicos recurrentes;
- evolución de indicadores de madurez cultural.

La formación deberá considerarse un proceso continuo y no una actividad puntual. Deberá actualizarse cuando se produzcan cambios relevantes en la metodología ERM, en la taxonomía, en el apetito al riesgo, en las herramientas de reporte, en la regulación aplicable o en el perfil de riesgo de la organización.

Parte III

Evolución del ERM

La gestión de riesgos no termina con la implantación de una metodología, un mapa de riesgos o un sistema de reporting. Para que el ERM aporte valor de forma sostenida, debe evolucionar junto con la organización, su estrategia y el entorno en el que opera.

Esta parte aborda cómo avanzar hacia una gestión de riesgos más integrada, anticipativa y conectada con la realidad del negocio. Para ello, se tratan aspectos como los riesgos emergentes, la identificación de oportunidades, la planificación estratégica, la gestión de proyectos, la continuidad de negocio, la gestión de crisis y la resiliencia operativa.

Capítulo 8.
Riesgos emergentes y oportunidades

8.1. Identificación y evaluación de riesgos emergentes

La definición de riesgos emergentes suele descansar en un conjunto de atributos comunes que se pueden agrupar en dos aspectos fundamentales: la naturaleza del riesgo y el horizonte de materialización.

En relación con la **naturaleza del factor emergente**, de forma general los riesgos emergentes abarcan materias que:

- Pueden generar impactos materiales, significativos
- Son fenómenos novedosos
- Son fenómenos que, sin ser novedosos, están cambiando o creciendo
- Son sistémicos, es decir, afectan a múltiples compañías y sectores (vinculados a tendencias macro o globales)
- Son fenómenos en los que falta conocimiento por lo que su estimación/ cuantificación es difícil.

En relación con el **horizonte**, no existe una práctica común de referencia.

- Los horizontes de posible materialización varían en función de la fuente consultada. Tradicionalmente se tendía a asimilar

estos riesgos con un horizonte a largo plazo, superior a 5 años. Sin embargo, la velocidad de cambio del entorno actual ha acortado el horizonte de análisis de estos riesgos.

- En los informes de referencia suelen convivir diferentes horizontes a corto, medio y largo, aunque no todos están presentes en todos los informes, ni utilizan los mismos tramos temporales.

Se puede afirmar que, como factor común, los riesgos emergentes se caracterizan por tener un importante **componente exógeno** y una **elevada incertidumbre** en cuanto al momento y al impacto en la organización resultado de su evolución y/o materialización.

En este sentido y aplicando un enfoque anticipativo, se debe considerar la monitorización y análisis de riesgos emergentes como un aspecto clave en la gestión de riesgos de las organizaciones.

8.2. Marcos de referencia para la identificación de riesgos emergentes

En el **ámbito regulatorio** español y europeo no existe a la fecha, una definición legal explícita de "riesgo emergente". Sin embargo, hay que considerar que la regulación vigente requiere la identificación, análisis y divulgación de aquellos riesgos que puedan tener un impacto relevante en los objetivos o las perspectivas futuras de la compañía.

Cabe destacar que la Ley de Sociedades de Capital exige que el Informe de Gestión incluya los principales riesgos e incertidumbres que afectan a la sociedad y que puedan condicionar su evolución futura. Así, el concepto de "riesgos e incertidumbres relevantes", actúa como paraguas bajo el cual se pueden encuadrar una amplia variedad de riesgos considerados como emergentes, aun cuando estos no se encuentren todavía plenamente materializados.

Adicionalmente, los supervisores han puesto especial foco en riesgos geopolíticos, macroeconómicos, regulatorios y climáticos.

Sirva de ejemplo la directiva europea de reporte de información de sostenibilidad (CSRD) que a través de los estándares de reporte (ESRS) ha introducido el enfoque de doble materialidad, reforzando la obligación de analizar riesgos que puedan surgir en el medio y largo plazo, aunque su impacto aún no sea inmediato.

En este contexto, los estándares y marcos técnicos internacionales adquieren relevancia, proporcionando un lenguaje común, principios y procesos estructurados que permiten a las organizaciones abordar de forma consistente la incertidumbre asociada a factores emergentes.

Entre ellos destacan:

- **ISO 31000**, como marco general de gestión de riesgos, ampliamente aceptado a nivel global
- **ISO/TS 31050:2023**, primer estándar específico dedicado a los riesgos emergentes, que los define como riesgos nuevos, crecientes o insuficientemente comprendidos y establece directrices para su identificación temprana, caracterización y gestión desde una perspectiva de resiliencia.
- **COSO ERM (2017),** que integra la gestión de riesgos en la estrategia y el desempeño, enfatizando el papel del órgano de gobierno y la necesidad de considerar los cambios del entorno como parte del proceso estratégico.

El estándar técnico ISO/TS 31050:2023, proporciona una guía metodológica para la gestión de riesgos emergentes que, alineada con el marco de gestión de riesgos ISO 31000, permite mejorar la resiliencia de las organizaciones.

En consecuencia, ISO/TS 31050 se apoya en el proceso ISO 31000 (comunicación y consulta; alcance, contexto y criterios; evaluación del riesgo; tratamiento; seguimiento y revisión; registro y reporte), **enfatizando la necesidad de detección temprana**, construcción progresiva de conocimiento y conexión explícita con la capacidad de resiliencia de la organización (anticipación, recuperación y adaptación).

Metodología de identificación y evaluación según ISO/TS 31050

La gestión de riesgos emergentes debe partir de la asunción de que este tipo de riesgos presentan características diferenciadoras — incertidumbre elevada, falta de datos históricos y velocidad en su evolución — que limitan la eficacia de los enfoques tradicionales basados en probabilidades y pérdidas esperadas.

La guía que plantea el estándar técnico es aplicable a organizaciones de cualquier sector y tamaño, permitiendo su adaptación al contexto regulatorio, estratégico y operativo de las empresas cotizadas, donde la anticipación y la rendición de cuentas ante órganos de gobierno adquieren especial relevancia.

La **identificación de riesgos emergentes** debe basarse en el análisis continuo del contexto interno y externo de la organización. ISO/TS 31050 enfatiza la necesidad de ir más allá del contexto actual, incorporando la **observación de tendencias, señales** débiles **y cambios incipientes** que puedan derivar en riesgos materiales.

Este proceso requiere el uso combinado de fuentes internas (estrategia, nuevos modelos de negocio, proyectos de transformación, resultados de auditoría y KRI) y externas (informes de organismos internacionales, reguladores, asociaciones sectoriales, consultoras y foros de expertos).

Asimismo, se debe adoptar un enfoque inclusivo, involucrando a diversas funciones y niveles de la organización, así como a grupos de interés externos clave, con el objetivo de reducir sesgos cognitivos y enriquecer la identificación mediante perspectivas complementarias.

Un posible enfoque consiste en el **desarrollo de una taxonomía específica de riesgos emergentes** que sirva de lenguaje común a los diferentes grupos que participarán en el proceso de identificación y posterior valoración. Esta taxonomía puede inspirarse en la utilizada por los organismos e instituciones que elaboran publicaciones y estudios sobre riesgos emergentes de manera periódica. Cabe destacar:

- El World Economic Forum, que publica anualmente, en enero, un informe de riesgos de ámbito global que refleja el resultado de una encuesta sobre una muestra de cientos de expertos del mundo académico, empresarial, gubernamental y organizaciones de la sociedad civil, y que entre sus resultados incorpora una visión de la severidad relativa de un conjunto de riesgos globales en un horizonte de 1, 2 a 10 años.

- Publicaciones específicas de riesgos emergentes de entidades no sectoriales, tales como el Emerging Risk Report que elabora Gartner trimestralmente.

- Publicaciones de organizaciones sectoriales, principalmente del ámbito asegurador y de auditoría.

- Publicaciones temáticas sobre riesgos, tales como riesgos de ciberseguridad, que tienen en cuenta el entorno geoeconómico y analizan las tendencias de nuevos riesgos en el sector, considerando la evolución de la tecnología.

En general, estas fuentes de información proporcionan clasificaciones de factores emergentes que pueden servir de base a las organizaciones para la elaboración de una taxonomía propia. En este sentido, las categorías de riesgos emergentes más habituales son:

- Económicos
- Ambientales
- Geopolíticos
- Sociales, de personas y/o talento
- Tecnológicos

Cada categoría se desarrolla en un listado de factores emergentes, cuya evolución se analiza desde la perspectiva de indicadores que anticipan cambios significativos que pueden resultar en una aceleración e incremento de la exposición global, local, sectorial u organizacional en diversos horizontes temporales así como del impacto sistémico esperado.

8.3. Evaluación de riesgos emergentes

La **evaluación de riesgos emergentes** se puede estructurar conforme al proceso definido en la norma ISO 31000, adaptándose a un entorno de alta incertidumbre. Tras la identificación inicial, el análisis se orientará a comprender la naturaleza del riesgo, sus posibles escenarios de desarrollo así como los efectos potenciales que puede llegar a tener su materialización sobre los objetivos estratégicos, bien de forma directa, bien porque el riesgo emergente, en caso de materializarse, actúe como potenciador de otros riesgos a los que la compañía se ve expuesta.

Dado que la información disponible suele ser limitada, es recomendable que el planteamiento inicial sea el de llevar a cabo un **análisis cualitativo** apoyándose en el uso de escenarios prospectivos, en los cuales se **consideren tanto impactos adversos como oportunidades**. La probabilidad se trata de forma implícita o cualitativa, prestando especial atención a la velocidad de cambio y a los impactos en la organización en función del momento de la materialización del riesgo.

A continuación, la valoración obtenida se puede comparar con criterios definidos internamente, permitiendo decidir si el riesgo debe ser tratado de forma activa o mantenerse bajo vigilancia, en función de la vulnerabilidad percibida de la organización a la evolución de los factores emergentes analizados.

Los mencionados criterios de valoración definidos por la organización pueden estar basados en la selección de un conjunto de reglas que permitan determinar la importancia de cada factor y su posterior comparabilidad, tales como:

- probabilidad percibida de que ocurra la situación,
- velocidad del cambio del contexto,
- escala temporal en la que pueden ocurrir consecuencias,
- factibilidad de controles, y
- opinión de grupos de interés.

8.4. Tratamiento de los riesgos emergentes

El **tratamiento de los riesgos emergentes** debe ser progresivo y adaptable a la evolución percibida de la exposición de la organización. En fases tempranas, la respuesta más adecuada puede ser la monitorización estructurada (estrategia Vigilar/ Watch), orientada a mejorar el conocimiento y a preparar respuestas futuras.

A medida que el riesgo gana probabilidad o concreción, se justifica la adopción de medidas de mitigación específicas (estrategia Actuar/ Do), que pueden incluir cambios estratégicos, inversiones, refuerzos de control o planes de contingencia.

La monitorización continua del contexto, de las señales de cambio y de la eficacia de las medidas adoptadas es un elemento crítico. La revisión periódica permite reclasificar riesgos, ajustar escenarios y, en su caso, transferir la contribución de factores emergentes a la valoración de los riesgos del mapa de compañía cuando su materialización resulta más probable.

Además de la monitorización del contexto externo, es importante mantener un seguimiento interno sobre cambios operativos y estratégicos, de gobernanza interna, cultura y actividad (p. ej., nuevos negocios, relaciones societarias, productos o servicios), con el objeto de anticipar cambios que puedan resultar en alteraciones significativas de la exposición de la organización a factores emergentes.

Asimismo, la monitorización continua y simultánea de ambos entornos (interno y externo) y la valoración de la evolución y severidad de los factores emergentes permitirá identificar no sólo riesgos sino también oportunidades estratégicas y por tanto la estrategia Watch and Do actuará en dos sentidos: el de mitigación de potenciales amenazas y el aprovechamiento temprano de oportunidades que puedan generar ventajas competitivas.

8.5. Comunicación y reporting de riesgos emergentes

La comunicación eficaz entre los diferentes grupos afectados, el **registro y el reporte a los órganos de gobierno** es un pilar esencial en la gestión de riesgos emergentes. La información debe fluir de manera oportuna y estructurada hacia la Alta Dirección y los órganos de gobierno, facilitando la toma de decisiones informadas en contextos de incertidumbre.

Es recomendable mantener registros actualizados que documenten la evolución de los riesgos emergentes, las fuentes de información utilizadas, los escenarios considerados y las decisiones adoptadas. Estos registros sustentan la trazabilidad y la mejora continua.

En el caso de empresas cotizadas, los riesgos emergentes relevantes deben integrarse en los sistemas de reporting corporativo, incluyendo el reporte periódico a la Comisión de Auditoría, reforzando así la supervisión, la transparencia y la resiliencia organizativa.

Capítulo 9.
Integración en la organización

La gestión de riesgos corporativos (ERM) ha evolucionado desde enfoques fragmentados o "de silos", en los que se analizan los riesgos por función (por ejemplo, seguridad, finanzas, sistemas de información, cumplimiento, etc.), con una metodología independiente en cada caso impidiendo la comparabilidad o la priorización, hacia un modelo integrado que conecta riesgo–estrategia–desempeño–resiliencia.

Esta evolución se refleja en marcos de referencia ampliamente utilizados como ISO 31000, que enfatiza la integración del riesgo en la gobernanza, la estrategia, la cultura y los procesos de decisión, y en el enfoque COSO ERM, que refuerza explícitamente la integración de ERM con estrategia y desempeño.

De forma simplificada, pueden distinguirse tres olas de madurez en un sistema ERM:

- ERM "de cumplimiento" (compliance-driven): foco en requerimientos regulatorios (por ejemplo, control interno, auditoría), con un modelo de reporte principalmente reactivo.
- ERM "integrado" (enterprise-wide): universo/diccionario común de riesgos, apetito y tolerancias, procesos homogéneos de evaluación y seguimiento, y escalado consistente.
- ERM "estratégico y resiliente" (strategy & resilience): ERM como mecanismo integrador de la gestión de la organización: conecta

planificación estratégica, cartera de proyectos, continuidad, ciber-resiliencia y terceros; con reporte integrado y aprendizaje continuo.

En el contexto actual (digitalización, cadenas de suministro complejas, riesgos climáticos, tensiones geopolíticas y exigencias de continuidad), la frontera entre gestión de riesgos y resiliencia operativa se ha estrechado: la organización no solo debe "gestionar" riesgos, sino absorber impactos, adaptarse y recuperar. Esta visión está alineada con la lógica de resiliencia organizacional recogida en ISO 22316:2017 — Security and resilience — Organizational resilience — Principles and attributes.

Para que ERM esté realmente integrado (y no sea un ejercicio anual de inventario), el diseño debe asegurar:

- Gobernanza clara: roles, decisiones, escalado y responsabilidad asignada de riesgos (propietario del riesgo).
- Apetito y tolerancias como "reglas de juego" para decidir (qué riesgos se aceptan y en qué umbrales).
- Integración del ERM en procesos clave: planificación estratégica, presupuestación, inversiones, proyectos, compras/terceros, continuidad y crisis.
- Cultura, comunicación y formación: aplicar en los procesos clave de gestión los principios de cultura de riesgo, comunicación, sensibilización y formación desarrollados en los apartados correspondientes de esta guía.
- Ciclo de mejora continua: revisión, lecciones aprendidas, prueba y actualización dinámica (no como una revisión estática).

En la práctica, esto se traduce en un ciclo ERM: contexto >> identificación >> evaluación >> respuesta/mitigación >> monitorización y reporting >> revisión y mejora, aplicado de forma consistente y proporcional a la realidad de cada organización.

9.1. Planificación estratégica

De cara a integrar el ERM en el proceso de Planificación Estratégica de la compañía, se deben tener en cuenta los siguientes aspectos:

- Vincular riesgos a objetivos estratégicos y métricas de desempeño (no solo a procesos): cada objetivo clave debe tener sus principales riesgos, oportunidades y supuestos críticos. Esta es una idea central de COSO ERM (integración con estrategia y desempeño). Definir apetito al riesgo y tolerancias al riesgo conectándolos con las métricas y aserciones estratégicas, límites operativos y criterios de inversión.

- Escenarios y "stress tests" estratégicos: la evaluación de riesgos integrada en el proceso de planificación estratégica permite evaluar robustez de la estrategia frente a disrupciones plausibles (p. ej., restricciones regulatorias, interrupciones de suministro, incidentes ciber, eventos climáticos).

- Integrar la gestión del riesgo en la toma de decisiones y planificación. Gestión del portafolio: Una vez analizados los riesgos del Plan estratégico se debe revisar la estrategia teniéndolos en cuenta. Por ejemplo, alinear la cartera de iniciativas con el apetito, la capacidad de ejecución y la resiliencia (evitando concentración de riesgos).

- Entregables y aspectos prácticos:

  - Mapa de riesgos del Plan Estratégico, indicando cómo se han tenido en cuenta en el proceso.
  - Declaración de apetito al riesgo y tolerancias (a nivel Consejo/ Comité de Dirección).
  - Integración con presupuestos y capital: para grandes decisiones.

Indicadores de integración (ejemplos):

- Porcentaje objetivos estratégicos con riesgos críticos asociados y con respuestas a dichos riesgos definidas.
- Porcentaje iniciativas estratégicas con análisis de escenarios / sensibilidad.
- Número de decisiones escaladas por exceder tolerancias (evidencia de uso real del apetito).

En definitiva, la clave de la integración del ERM en el proceso de Planificación Estratégica es que el riesgo sea un criterio explícito para su planteamiento. Esto es: definir objetivos, asignar capital y priorizar iniciativas, no presentar los riesgos como un "anexo" posterior.

9.2. Gestión de Proyectos

El éxito del desarrollo de proyectos, en particular de aquellos de gran complejidad, coste elevado o relevancia estratégica, reside en gran parte en la capacidad de anticipar los riesgos y de implementar respuestas adecuadas a los más relevantes o críticos. Para conseguirlo, se deben tener en cuenta los siguientes aspectos:

- Implantar un proceso estándar de gestión de riesgos de proyecto: planificación, identificación, análisis (cualitativo/ cuantitativo), respuestas, implementación y monitorización. Esta secuencia está alineada con prácticas de gestión de riesgos de proyecto difundidas en la comunidad de Gestión de Proyectos.

- Mantener un registro de riesgos de proyecto vivo (no documental), con responsables del riesgo, acciones, fechas y señales de alerta.

- Conectar hitos del proyecto con ERM mediante:

  - Revisiones por fase (riesgo como criterio formal para pasar de fase). Previo a la decisión de inversión u otras fases del proyecto.
  - Escalado cuando se superan tolerancias (coste, plazo, seguridad, cumplimiento, ciber).
  - Taxonomía común de riesgos (para consolidar a nivel empresa). Una vez se da comienzo al proyecto, sus riesgos se pueden incorporar directamente al ciclo de riesgos, si se considera que la gestión del proyecto es una actividad más de la compañía, alineada con el despliegue del plan estratégico.

  - Seguimiento de proyectos que mitigan riesgos. Integración en este caso del criterio de riesgo en la toma de decisión de inversión.

- Buenas prácticas operativas:

  - Definir métricas de medición de riesgos alineadas con las de seguimiento de los proyectos, para facilitar el entendimiento de sus impactos en el proyecto: métricas de rentabilidad, coste o plazo de los proyectos.
  - Análisis de riesgos de terceros (contratistas, proveedores críticos, tecnología) desde el diseño del proyecto. (Conexión directa con resiliencia operativa y cadena de suministro).
  - Integrar oportunidades (riesgos positivos) en la gestión del proyecto para mejorar probabilidad de éxito.

Indicadores de éxito:

- Porcentaje de proyectos críticos en el registro de riesgos y revisiones mensuales.
- Variación coste/plazo explicado por riesgos materializados vs. no identificados.
- Variación de rentabilidad explicada por los riesgos.

El objetivo de este proceso es incorporar la disciplina ERM en el "día a día" de ejecución (proyectos, programas y cartera), donde se materializa gran parte del riesgo (coste, plazo, calidad, seguridad, compliance, ciber, terceros), sin perder de vista el impacto en los objetivos estratégicos, de acuerdo con la naturaleza y dimensión de cada proyecto.

9.3. Business Impact Analysis (BIA)

El estándar ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements establece requisitos para un sistema de gestión de continuidad de negocio y contempla la necesidad de planificación para responder y recuperar ante disrupciones.

En muchas organizaciones, este proceso no se encuentra relacionado con el ERM, si bien ambos procesos tienen sinergias relevantes tanto en su metodología de análisis como en la de gestión.

El Análisis de Impacto en Negocio, Business Impact Analysis (BIA), tiene por objeto identificar actividades críticas, dependencias y objetivos de recuperación para priorizar recursos y diseñar continuidad y resiliencia, ante una disrupción.

Contenidos típicos de un BIA "bien integrado":

- Procesos/servicios críticos y su contribución a objetivos (operativos, legales, clientes, seguridad).
- Impactos por horizonte temporal (financiero, reputación, regulatorio, seguridad, servicio) para justificar prioridades, en línea con los criterios de evaluación de riesgos.
- Dependencias: personas/roles, ubicaciones, TI/OT, datos, proveedores, suministros, logística.
- objetivos de recuperación, incluyendo el MTPD/MAO —periodo máximo tolerable de interrupción—, el RTO —tiempo objetivo de recuperación—, el RPO —pérdida máxima tolerable de datos medida en tiempo— y los niveles mínimos aceptables de servicio o actividad (MBCO).
- Protocolos y guías de actuación ante una tipología de disrupción (ciber, suministro, etc.).
- Pruebas prácticas, simulacros o ejercicios de validación para ajustar la documentación y reforzar la preparación de los equipos.

Integración del BIA con ERM:

- El BIA alimenta el mapa de riesgos operacionales y prioriza planes de tratamiento (mitigaciones) para riesgos de interrupción.
- Permite justificar inversiones en resiliencia (redundancias, recuperación ante desastres, proveedores alternativos) con lógica de impacto y tolerancias.
- Las evaluaciones de impacto son coherentes en cuanto a escalas utilizadas para evaluación de riesgos.

Indicadores (ejemplos):

- Porcentaje de procesos críticos con BIA actualizado (12–24 meses).
- Cobertura de dependencias de terceros críticos identificadas y tratadas.

9.4. Gestión de crisis y protocolos

El objetivo de la gestión de crisis es coordinar respuesta estratégica, ejecutiva y operativa ante incidentes de alto impacto, reduciendo confusión, tiempos de decisión y daños colaterales (personas, activos, reputación, cumplimiento).

ISO 22320:2018 — Security and resilience — Emergency management — Guidelines for incident Management proporciona directrices para la gestión de incidentes, incluyendo principios, componentes (procesos/estructura), roles, gestión de recursos y cooperación.

En muchas organizaciones, este proceso no se encuentra relacionado con el ERM, si bien la participación de ERM es muy relevante para la detección temprana de riesgos que pueden desencadenar una crisis o, una vez desencadenada, para la identificación y análisis de riesgos relacionados con la misma.

Elementos clave de un sistema integrado de crisis:

- Estructura de mando y control: definición de los órganos, roles, responsabilidades, niveles de autoridad y suplencias que se activan ante una crisis, asegurando una toma de decisiones rápida, coordinada y trazable.
- Criterios de escalado: establecimiento de condiciones o umbrales que permitan determinar cuándo un incidente debe escalarse a nivel de crisis, considerando impactos sobre personas, operaciones, continuidad, seguridad, medioambiente, cumplimiento, reputación, clientes o terceros críticos.
- Protocolos y guías de actuación por tipología: desarrollo de pautas específicas para distintos escenarios de crisis —ciber, tecnología operacional, suministro, HSSE, reputación, fraude

u otros eventos críticos—, incluyendo responsables, primeras actuaciones, canales de comunicación, decisiones clave y coordinación con áreas afectadas.

- Comunicación de crisis: definición de flujos de comunicación interna y externa, portavoces, mensajes clave, circuitos de validación y coordinación con áreas como comunicación corporativa, legal, cumplimiento, recursos humanos, relación con autoridades, clientes, proveedores y otros grupos de interés.
- Ejercicios, simulacros y aprendizaje: realización periódica de pruebas prácticas que permitan validar los protocolos, entrenar a los equipos, identificar brechas de coordinación y reforzar la capacidad de respuesta ante situaciones de alta presión.
- Integración con ERM: conexión de los escenarios de crisis con el mapa de riesgos, los indicadores clave de riesgo, los planes de tratamiento, la continuidad de negocio y los criterios de escalado, asegurando que la gestión de crisis no opere de forma aislada respecto al modelo corporativo de riesgos.

Los incidentes reales y simulacros alimentan el ciclo de revisión y mejora del ERM: actualización de escenarios, indicadores y planes.

9.5. Resiliencia operativa y digital (DORA, NIS2, etc.)

La implantación de un modelo de Enterprise Risk Management (ERM) deberá integrarse de forma coherente con las nuevas exigencias regulatorias derivadas de los marcos europeos de resiliencia operativa y ciberseguridad en los casos en los que aplique. En particular el Reglamento Digital Operational Resilience Act (DORA) y la Directiva Network and Information Systems Directive 2 (NIS2).

Ambos marcos regulatorios refuerzan la necesidad de adoptar un enfoque integral, transversal y basado en riesgos, exigiendo a las organizaciones fortalecer sus capacidades de identificación, evaluación, monitorización y respuesta ante riesgos tecnológicos, operacionales y de ciberseguridad.

En este contexto, el ERM no deberá concebirse como una función independiente o paralela a los marcos de resiliencia digital, sino como el mecanismo integrador que permita incorporar dichos riesgos dentro del modelo global de gobierno corporativo y toma de decisiones. La organización deberá asegurar que los riesgos derivados de tecnologías de la información y comunicaciones (TIC) (ICT), ciberseguridad, dependencia de terceros críticos, continuidad operativa y resiliencia digital queden plenamente integrados dentro del mapa corporativo de riesgos, utilizando metodologías homogéneas de evaluación, priorización y seguimiento.

En particular, DORA exige a las entidades sujetas un marco robusto de gestión del riesgo TIC (ICT Risk Management Framework), incluyendo identificación continua de vulnerabilidades, clasificación de activos críticos, pruebas de resiliencia operativa, gestión de incidentes y supervisión reforzada de terceros tecnológicos. El modelo ERM deberá facilitar la integración de estos elementos dentro del universo de riesgos corporativos, evitando silos organizativos y asegurando una visión consolidada de la exposición al riesgo digital.

Por su parte, NIS2 amplía significativamente las obligaciones de gobernanza y supervisión sobre ciberseguridad, estableciendo responsabilidades explícitas para los órganos de dirección respecto a la adopción de medidas de gestión del riesgo, supervisión de controles y formación específica. En consecuencia, el ERM deberá contemplar mecanismos de reporting periódico a la Alta Dirección y al Consejo sobre el estado de exposición a riesgos cibernéticos, indicadores clave (KRIs), incidentes relevantes, vulnerabilidades críticas y grado de cumplimiento regulatorio.

Asimismo, la integración del ERM con DORA y NIS2 deberá reflejarse en aspectos tales como:

- Incorporación de riesgos TIC y de ciberseguridad en el apetito al riesgo corporativo;
- Definición de KRIs específicos de resiliencia digital y ciberseguridad;

- Integración de escenarios de ciber crisis y disrupción tecnológica en ejercicios de pruebas de estrés;
- Coordinación entre las funciones de ERM, Seguridad de la Información, Continuidad de Negocio, Compliance y Auditoría Interna;
- Supervisión de proveedores tecnológicos críticos y riesgos de concentración;
- Fortalecimiento de la cultura de riesgo digital mediante formación y sensibilización;
- Evaluación periódica de la resiliencia operativa y capacidad de recuperación.

La integración efectiva de DORA y NIS2 dentro del marco ERM permitirá evolucionar desde una visión fragmentada del riesgo tecnológico hacia un enfoque integrado de resiliencia organizativa, favoreciendo no solo el cumplimiento regulatorio, sino también una mayor capacidad de anticipación, adaptación y respuesta ante amenazas digitales crecientemente complejas y dinámicas.

En definitiva, la integración de la resiliencia operativa y digital dentro del ERM debe entenderse de forma dinámica. No debe limitarse a DORA o NIS2, sino extenderse a cualquier normativa actual o futura que resulte aplicable en materia de ciberseguridad, continuidad, tecnología, datos, terceros críticos o resiliencia operativa, asegurando que sus obligaciones se incorporan al mapa de riesgos, controles, indicadores, reporting y criterios de escalado de la organización.

Capítulo 10. Conclusiones

10.1. Factores críticos de éxito

La implantación de un Enterprise Risk Management (ERM) alcanza un mayor grado de madurez cuando deja de ser un ejercicio periódico de identificación y reporte de riesgos y pasa a integrarse en el sistema de gobierno y toma de decisiones de la organización, conectando estrategia, desempeño, ejecución, cultura y resiliencia.

Para lograrlo, se requieren los siguientes factores:

- Patrocinio real y visible ("tone at the top" + uso en decisiones): El Consejo de Administración y la Alta Dirección deben respaldar el ERM y, sobre todo, usarlo: que el riesgo sea un criterio explícito en decisiones estratégicas, inversión y priorización. La señal inequívoca de éxito es que el ERM cambia decisiones (aceptación, mitigación, transferencia, renuncia) y no se limita a describir riesgos.
- Gobernanza clara y responsabilidad asignada del negocio (no de la función de riesgos): ERM funciona cuando cada riesgo tiene propietario en el negocio y una cadena de escalado clara; la función de riesgos facilita, desafía y consolida, pero no sustituye la responsabilidad del negocio. Un modelo de gobernanza sólido se apoya en roles, responsabilidades, comités y ritmos de revisión, alineado con los componentes de gobernanza y cultura (COSO) y con la integración en gobierno organizativo (ISO) de acuerdo con el Modelo de las Tres Líneas,

que establece una distribución clara de responsabilidades entre gestión, supervisión y aseguramiento independiente.

- Apetito al riesgo y tolerancias operativas "accionables": Definir apetito (nivel y tipo de riesgo que la organización está dispuesta a asumir para alcanzar sus objetivos) y tolerancias (umbrales medibles) es crítico para que ERM guíe decisiones, inversiones y límites operativos. Este paso no consiste en "tener un documento", sino traducirlo a límites, indicadores, umbrales y criterios de escalado aplicables a procesos y unidades.
- Integración en planificación estratégica y desempeño (riesgo/estrategia/resultado): Un ERM maduro conecta riesgos y oportunidades con objetivos estratégicos, supuestos críticos y métricas de desempeño, evitando enfoques aislados por silos organizativos.
- Cultura de riesgo y capacidades (comportamientos, no solo procesos): Importancia de los factores humanos y culturales para sostener una gestión del riesgo eficaz. Elementos clave: formación segmentada por niveles, rutinas de conversación de riesgos, y un entorno que favorezca identificación temprana, transparencia y aprendizaje (sin penalizar la comunicación de problemas).
- Información y reporting de calidad (menos volumen, más utilidad): El reporting de ERM debe habilitar decisiones: un conjunto limitado de indicadores críticos (KRIs), tendencias, exposición vs tolerancias, y narrativa clara del "qué ha cambiado" y "qué se decide".
- Disciplina de revisión y mejora continua (ciclo de aprendizaje): ERM debe ser dinámico: monitorizar, revisar y mejorar continuamente ante cambios internos/externos, coherente con el enfoque iterativo y de mejora continua de ISO 31000. La mejora se acelera incorporando ciclos de retroalimentación: lecciones aprendidas de incidentes, auditorías, cuasi incidentes y revisiones de efectividad de controles/mitigaciones.

10.2. ERM como ventaja competitiva

En el contexto actual, caracterizado por una creciente complejidad del entorno empresarial, la aceleración del cambio tecnológico,

la presión regulatoria y la interdependencia global de los riesgos, disponer de un sistema de gestión integrada de riesgos se ha convertido en un elemento diferencial para las organizaciones. Más allá de su tradicional función de protección, la gestión de riesgos se consolida como una palanca estratégica que contribuye de forma directa a la creación y preservación de valor a largo plazo.

Un sistema ERM maduro permite a las organizaciones disponer de una visión integral de su perfil de riesgos, superando enfoques fragmentados y reactivos. Esta visión integrada mejora sustancialmente la calidad de la información que se traslada a la Alta Dirección y a los órganos de gobierno, fortaleciendo la toma de decisiones estratégicas en un entorno marcado por la incertidumbre y la volatilidad y permitiendo priorizar recursos hacia aquellos riesgos y oportunidades con mayor impacto potencial.

Disponer de un sistema de gestión integrado de riesgos aporta ventajas en la alineación entre estrategia, objetivos y riesgos. Integrar el análisis de riesgos en los procesos estratégicos y de planificación permite evaluar de forma más rigurosa la viabilidad de las decisiones, anticipando desviaciones relevantes y ayudando de este modo a la organización en la consecución de sus metas estratégicas.

Asimismo, abordar la identificación, valoración y tratamiento de los riesgos con un enfoque sistemático refuerza la capacidad de anticipación frente a las incertidumbres derivadas de la rápida evolución y cambios en el entorno en el que opera la organización. La identificación temprana de nuevas amenazas —tecnológicas, regulatorias, geopolíticas, ambientales o reputacionales— y la comprensión de sus interrelaciones permiten mitigar los impactos de potenciales eventos novedosos. Esta anticipación no solo mitiga impactos negativos, sino que facilita la identificación de oportunidades.

Otro factor diferencial del ERM es su contribución a una gobernanza más sólida y transparente. La clara asignación de responsabilidades, la definición de roles y la existencia de procesos estandarizados fortalecen la implantación de una cultura donde el riesgo es una

variable fundamental en la toma de decisiones en todos los niveles y actividades de la organización. Esta robustez en la gestión de riesgos refuerza la confianza de los inversores, reguladores y demás grupos de interés, al demostrar que la compañía dispone de mecanismos eficaces para proteger los intereses a largo plazo y gestionar adecuadamente la incertidumbre.

Desde el punto de vista operativo, un sistema ERM bien implantado mejora la eficiencia en la asignación de recursos. Al priorizar los riesgos verdaderamente relevantes y concentrar los esfuerzos de mitigación donde aportan mayor valor, las organizaciones evitan enfoques dispersos y optimizan el uso de recursos financieros, humanos y operativos.

En resumen, las organizaciones que integran la gestión de riesgos en su estrategia, decisiones y operaciones mediante un lenguaje común, una metodología consistente y responsabilidades claramente definidas estarán mejor preparadas para afrontar entornos inciertos, absorber impactos y aprovechar oportunidades que contribuyan a su resiliencia y sostenibilidad a largo plazo.

10.3. Evolución futura de la gestión de riesgos: Strategic Foresight

La evolución de la gestión de riesgos está avanzando desde un enfoque predominantemente reactivo y centrado en riesgos conocidos hacia modelos más prospectivos, capaces de anticipar cambios estructurales, disrupciones y riesgos emergentes.

En este contexto, el Strategic Foresight se configura como una disciplina complementaria al ERM orientada a explorar futuros plausibles, identificar señales tempranas de cambio, analizar mega tendencias e incorporar incertidumbres estratégicas en la toma de decisiones. Más allá de predecir el futuro, el Strategic Foresight permite a las organizaciones prepararse para distintos escenarios posibles, fortaleciendo su capacidad de anticipación, resiliencia y adaptación.

La integración de capacidades de prospectiva dentro del modelo ERM facilitará una visión más dinámica del riesgo, especialmente ante fenómenos de elevada incertidumbre relacionados con transformación tecnológica, inteligencia artificial, ciberamenazas, cambio climático, geopolítica, cambios regulatorios o evolución de expectativas sociales.

En consecuencia, las organizaciones más maduras tenderán a evolucionar desde modelos de gestión de riesgos centrados exclusivamente en la protección del valor hacia enfoques orientados también a la identificación de oportunidades y creación de valor sostenible a largo plazo.

Capítulo 11. Bibliografía

- ISO 31000:2018 — Risk management — Guidelines (ISO/TC 262).
- IEC 31010:2019 — Risk management — Risk assessment techniques.
- COSO — Enterprise Risk Management (2017): Integrating with Strategy and Performance.
- The Institute of Internal Auditors (IIA) — Three Lines Model: Assurance and Advice in Support of Effective Governance. Statement of Position, issued July 8, 2026.
- The Institute of Internal Auditors (IIA) — The Internal Audit Function's Role in Enterprise Risk Management. Statement of Position, issued July 8, 2026.
- Federation of European Risk Management Associations (FERMA) — A Risk Management Standard.
- Asociación Española de Gerencia de Riesgos y Seguros (AGERS) — La gestión del apetito al riesgo.
- World Economic Forum — The Global Risks Report 2026.
- Gartner — Quarterly Emerging Risk Report / 1Q26 Emerging Risk Report, 2026.ISO/TS 31050:2023 — Risk management — Guidelines for managing emerging risks to enhance resilience
- ISO 31022:2020 — Risk management — Guidelines for the management of legal risk
- ISO 31073:2022 — Risk management — Vocabulary
- ISO 22316:2017 — Security and resilience — Organizational resilience — Principles and attributes

- ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements
- ISO 22320:2018 — Security and resilience — Emergency management — Guidelines for incident management
- Directiva 2009/138/CE — régimen de Solvencia II
- Basel Committee on Banking Supervision — Basel Framework / Basel III

ANEXO I.
Glosario de términos

Aceptar el riesgo
Decisión consciente de asumir un riesgo sin adoptar medidas adicionales de tratamiento, siempre que se encuentre dentro del apetito, tolerancias o límites definidos por la organización y permanezca bajo seguimiento.

Apetito al riesgo
Nivel y tipo de riesgo que la organización está dispuesta a asumir para alcanzar sus objetivos estratégicos y crear valor.

Aseguramiento combinado
Coordinación estructurada de actividades de aseguramiento realizadas por distintas funciones, con el objetivo de evitar duplicidades, identificar brechas de cobertura y proporcionar una visión integrada sobre riesgos y controles.

Auditoría interna
Función independiente y objetiva que proporciona aseguramiento y asesoramiento sobre la adecuación y eficacia del gobierno, la gestión de riesgos y los controles, sin asumir responsabilidades de gestión.

BIA (Business Impact Analysis)
Análisis de impacto en negocio utilizado para identificar actividades críticas, dependencias, impactos potenciales y objetivos de recuperación necesarios para diseñar estrategias de continuidad.

Capacidad de riesgo
Nivel máximo de riesgo que la organización podría asumir sin comprometer su viabilidad, solvencia, continuidad, cumplimiento o consecución de objetivos esenciales.

Causa
Factor interno o externo que puede originar, favorecer o desencadenar un evento de riesgo.

Causa común
Situación en la que dos o más riesgos comparten un mismo origen, factor desencadenante o vulnerabilidad subyacente.

Consecuencia
Efecto derivado de la materialización de un evento de riesgo sobre los objetivos, operaciones, resultados, personas, cumplimiento, reputación o continuidad de la organización.

Continuidad de negocio
Capacidad de la organización para mantener o recuperar actividades críticas ante una disrupción dentro de unos niveles previamente definidos.

Control
Mecanismo, actividad o medida recurrente diseñada para prevenir la materialización de un riesgo, detectarlo a tiempo o corregir desviaciones.

Control correctivo
Control orientado a corregir una desviación, reducir sus consecuencias o restablecer una situación aceptable.

Control detectivo
Control orientado a identificar errores, desviaciones, incidentes o señales tempranas de riesgo.

Control preventivo
Control orientado a reducir la probabilidad de materialización de un riesgo.

Correlación entre riesgos
Relación estadística o de comportamiento conjunto entre dos o más riesgos, que indica que pueden evolucionar de forma relacionada.

DAFO
Herramienta de análisis estratégico que permite identificar fortalezas, debilidades, oportunidades y amenazas relevantes para la organización.

Detectabilidad
Capacidad de la organización para identificar señales tempranas antes de que un riesgo se materialice o antes de que sus consecuencias se incrementen.

Efectividad del control
Grado en que un control está correctamente diseñado, implantado, ejecutado y documentado, y contribuye a reducir la probabilidad o impacto de un riesgo.

Enterprise Risk Management (ERM)
Enfoque estructurado, continuo e integrado para identificar, evaluar, tratar, monitorizar y comunicar los riesgos que pueden afectar a la consecución de los objetivos de una organización.

Escenario
Descripción estructurada de una situación futura plausible utilizada para analizar posibles impactos, vulnerabilidades, decisiones y respuestas.

Evento de riesgo
Hecho incierto que, de materializarse, puede afectar a la consecución de los objetivos de la organización.

Evidencia del control
Documentación, registro o prueba que permite demostrar que un control ha sido ejecutado conforme a lo definido.

Gestión de crisis
Conjunto de estructuras, roles, protocolos y decisiones destinados a coordinar la respuesta ante eventos de alto impacto que pueden afectar gravemente a la organización.

Gestión integral de riesgos
Enfoque coordinado y transversal de gestión de riesgos que integra la identificación, evaluación, tratamiento, seguimiento y comunicación de riesgos en toda la organización.

Gobernanza corporativa
Sistema de estructuras, procesos, responsabilidades y mecanismos mediante los cuales se dirige, supervisa y controla una organización.

Grupos de interés
Personas, colectivos u organizaciones que pueden afectar o verse afectados por las actividades, decisiones, resultados o riesgos de la organización.

Impacto
Consecuencia potencial derivada de la materialización de un riesgo sobre los objetivos de la organización.

Interdependencia entre riesgos
Relación mediante la cual un riesgo puede influir en otro, compartir causas comunes o generar efectos en cadena.

Inventario o registro de riesgos
Catálogo vivo de riesgos identificados por la organización que incluye información relevante como descripción, causas, consecuencias, responsables, controles, valoración y tratamiento.

KCI (Key Control Indicator)
Indicador clave utilizado para monitorizar la existencia, funcionamiento o efectividad de controles relevantes.

KPI (Key Performance Indicator)
Indicador utilizado para medir el desempeño, resultados o eficiencia de un proceso, actividad u objetivo.

KRI (Key Risk Indicator)
Indicador clave utilizado para monitorizar la evolución de un riesgo y detectar señales tempranas de deterioro.

Límite de riesgo
Valor máximo o mínimo definido para controlar una exposición concreta cuya superación puede requerir acciones correctoras, escalado o revisión de decisiones.

Mapa de calor
Representación gráfica de riesgos basada normalmente en la combinación de probabilidad e impacto para facilitar su comparación y priorización.

Mapa de riesgos
Representación estructurada del perfil de riesgos de una organización, normalmente ordenada por criticidad, categoría, responsable y estado de tratamiento.

MBCO (Minimum Business Continuity Objective)
Nivel mínimo de servicio, actividad o capacidad operativa que debe mantenerse o recuperarse tras una disrupción.

Medida de mitigación
Acción destinada a reducir la probabilidad, impacto o exposición asociada a un riesgo.

Modelo de las Tres Líneas
Modelo de gobierno que distingue entre primera línea, responsable de gestionar riesgos; segunda línea, responsable de supervisión, metodología y apoyo; y tercera línea, auditoría interna, responsable de proporcionar aseguramiento independiente.

Oportunidad
Situación, capacidad o circunstancia que puede generar un efecto positivo para la organización, mejorar su posicionamiento, reforzar sus capacidades o favorecer la consecución de sus objetivos.

Objetivo de recuperación de datos (RPO — Recovery Point Objective)
Pérdida máxima de datos aceptable medida en tiempo tras una interrupción, utilizada para definir requisitos de recuperación de información.

Objetivo de recuperación temporal (RTO — Recovery Time Objective)
Tiempo máximo objetivo para recuperar una actividad, proceso o sistema tras una interrupción.

PESTEL
Herramienta de análisis del entorno externo que considera factores políticos, económicos, sociales, tecnológicos, ambientales y legales que pueden afectar a la organización.

Plan de acción
Conjunto de medidas concretas destinadas a tratar un riesgo o corregir una brecha identificada, incluyendo responsable, plazo, recursos, estado y seguimiento.

Primera línea
Áreas de negocio, operativas o de soporte responsables de gestionar los riesgos asociados a sus actividades diarias y de ejecutar los controles y medidas de tratamiento correspondientes.

Principio de proporcionalidad
Criterio según el cual la profundidad del análisis, documentación, controles y seguimiento debe adaptarse a la criticidad del riesgo, tamaño, complejidad y capacidades de la organización.

Probabilidad
Posibilidad de que un riesgo se materialice en un periodo determinado. Puede evaluarse mediante información histórica, juicio experto, indicadores predictivos, análisis estadístico o escenarios.

Propietario del riesgo (Risk Owner)
Persona, área o unidad organizativa responsable de gestionar un riesgo, realizar su seguimiento, impulsar medidas de tratamiento y escalar desviaciones cuando corresponda.

Proximidad
Horizonte temporal estimado en el que un riesgo podría materializarse.

Prueba de estrés
Evaluación de la capacidad de resistencia de una organización frente a escenarios severos pero plausibles.

Prueba de estrés inversa
Técnica que parte de un resultado inaceptable para analizar qué combinación de eventos, vulnerabilidades o fallos podría provocarlo.

Recuperación
Capacidad de la organización para restablecer sus actividades, servicios, procesos o capacidades tras la materialización de una interrupción o evento adverso.

Resiliencia operativa
Capacidad de la organización para anticipar, absorber, responder, recuperarse y adaptarse ante eventos adversos o disrupciones.

Responsable del control
Persona o área encargada de ejecutar, supervisar, mantener o revisar un control asociado a un riesgo.

Riesgo
Efecto de la incertidumbre sobre los objetivos de una organización. Puede afectar positiva o negativamente a la consecución de objetivos estratégicos, operativos, financieros, regulatorios o de sostenibilidad.

Riesgo emergente
Riesgo nuevo, creciente o insuficientemente comprendido, caracterizado por elevada incertidumbre, falta de información histórica, evolución dinámica o posible impacto futuro relevante.

Riesgo inherente
Nivel de exposición al riesgo existente antes de considerar el efecto de controles, medidas de mitigación o respuestas implantadas.

Riesgo objetivo
Nivel de exposición al riesgo que la organización pretende alcanzar después de aplicar las medidas de tratamiento previstas.

Riesgo residual
Nivel de exposición al riesgo que permanece después de considerar los controles y medidas de tratamiento existentes.

Riesgo tolerable
Nivel de riesgo que la organización puede aceptar de acuerdo con sus criterios de apetito, tolerancias, capacidad y objetivos definidos.

Segunda línea
Funciones especializadas que proporcionan metodología, asesoramiento, supervisión, monitorización y desafío a la primera línea, sin asumir la gestión directa de los riesgos.

Señal temprana
Información, indicador, evento o tendencia que puede anticipar un deterioro del perfil de riesgo o la aparición de un riesgo emergente.

Sensibilización en riesgos
Acciones destinadas a que las personas comprendan la importancia de la gestión de riesgos, sus responsabilidades y cómo pueden contribuir al modelo ERM.

Taxonomía de riesgos
Estructura común utilizada para clasificar y agrupar los riesgos de una organización por categorías y subcategorías, facilitando su identificación, análisis, consolidación y comunicación.

Tendencia del riesgo
Evolución observada o esperada de un riesgo, indicando si su exposición aumenta, disminuye o permanece estable.

Tercera línea
Auditoría interna, que proporciona aseguramiento independiente y objetivo sobre la adecuación y eficacia del gobierno, la gestión de riesgos y los controles.

Tolerancia al riesgo
Nivel máximo de variación aceptable respecto al apetito al riesgo definido por la organización.

Tone at the top
Compromiso visible y coherente de la Alta Dirección y los órganos de gobierno con la gestión de riesgos, reflejado en decisiones, prioridades, recursos y comportamientos.

Tratamiento del riesgo
Proceso mediante el cual la organización decide cómo abordar un riesgo, seleccionando respuestas como aceptar, reducir, transferir o evitar.

Umbral de alerta
Nivel definido que permite identificar una desviación o deterioro antes de superar un límite o tolerancia establecido.

Valor en riesgo (VaR — Value at Risk)
Medida cuantitativa utilizada para estimar la pérdida máxima esperada de una cartera, exposición o actividad durante un periodo determinado y bajo un nivel de confianza definido.

Velocidad del riesgo
Rapidez con la que un riesgo puede producir consecuencias una vez materializado, así como el tiempo disponible para responder antes de que el impacto se incremente.

ANEXO II.
Relación con ISO 31000 y COSO ERM

Dimensión del ERM	Principios ISO 31000 (2018)	Principios COSO ERM (2017)
1. Gobernanza y cultura	Integrado Estructurado y exhaustivo Adaptado Inclusivo Factores humanos y culturales	1. Ejerce la supervisión de riesgo a través del Consejo 2. Establece estructuras operativas 3. Define la cultura deseada 4. Demuestra compromiso con los valores fundamentales 5. Atrae, desarrolla y retiene a profesionales capacitados 20. Informa sobre riesgo, cultura y desempeño
2. Estrategia y toma de decisiones	Integrado Adaptado Dinámico	6. Analiza el contexto empresarial 7. Define el apetito al riesgo 8. Evalúa estrategias alternativas 9. Formula objetivos de negocio
3. Gestión y evaluación del riesgo	Mejor información disponible Estructurado y exhaustivo Dinámico	10. Identifica el riesgo 11. Evalúa la severidad del riesgo 12. Prioriza riesgos 13. Implementa respuestas al riesgo 14. Desarrolla una visión de cartera 15. Evalúa cambios sustanciales
4. Seguimiento, información y mejora	Mejora continua Inclusivo Mejor información disponible Dinámico	16. Evalúa el desempeño del ERM 17. Revisa el riesgo y el desempeño 18. Aprovecha la información y la tecnología 19. Comunica la información sobre riesgos 20. Informa sobre riesgo, cultura y desempeño

Las dimensiones propuestas agrupan los principios recogidos en los principales marcos de referencia, permitiendo estructurar su aplicación de forma coherente y adaptada a la realidad de cada organización.

ANEXO III.
Principales técnicas de evaluación de riesgos

1. Introducción

Este anexo recoge una descripción práctica de las principales técnicas que pueden utilizarse para analizar y evaluar riesgos dentro de un modelo de Enterprise Risk Management. Su objetivo es servir como referencia de apoyo para seleccionar el enfoque de evaluación más adecuado en función de la naturaleza del riesgo, la información disponible, la criticidad de la decisión y el nivel de madurez de la organización.

Las técnicas incluidas no deben entenderse como obligatorias, excluyentes ni aplicables de forma automática. En la práctica, la evaluación de riesgos suele combinar juicio experto, conocimiento del negocio, datos históricos, escalas homogéneas, análisis de escenarios y, cuando existe información suficiente, herramientas cuantitativas. El criterio fundamental debe ser la utilidad del análisis para la toma de decisiones, evitando tanto la excesiva simplificación como una falsa precisión basada en datos o hipótesis insuficientemente contrastados.

2. Criterios para seleccionar la técnica de evaluación

La selección de la técnica de evaluación deberá realizarse considerando la naturaleza del riesgo, la disponibilidad y calidad de los datos, el nivel de incertidumbre, la criticidad del riesgo, el horizonte temporal del análisis y el uso previsto del resultado. No requiere el mismo enfoque un riesgo financiero con histórico suficiente que un riesgo reputacional, emergente o estratégico con información limitada y elevada incertidumbre.

También deberá tenerse en cuenta la madurez analítica de la organización y su capacidad real para aplicar, mantener e interpretar

la técnica seleccionada. Una técnica sencilla, bien aplicada y documentada puede aportar más valor que un modelo complejo basado en datos incompletos, supuestos débiles o resultados difíciles de explicar. Por tanto, la selección de la técnica debe responder al principio de proporcionalidad: cuanto mayor sea la criticidad del riesgo o la relevancia de la decisión, mayor deberá ser la exigencia de análisis, trazabilidad y revisión.

A efectos meramente ilustrativos, y sin carácter obligatorio, puede utilizarse la siguiente orientación práctica:

Tipo de riesgo o situación	Enfoque de evaluación orientativo
Riesgos estratégicos	Juicio experto, análisis de escenarios, sensibilidad y pruebas de estrés
Riesgos emergentes	Escenarios, vigilancia de señales tempranas, juicio experto y revisión periódica
Riesgos operacionales recurrentes	Escalas semicuantitativas, histórico de incidentes, frecuencia e impacto
Riesgos financieros	Análisis estadístico, sensibilidad, VaR, escenarios y pruebas de estrés
Riesgos de continuidad	BIA, escenarios, pruebas de estrés y pruebas de estrés inversas
Riesgos de proyectos	Matriz de riesgos, sensibilidad, escenarios, árboles de decisión y Monte Carlo cuando proceda
Riesgos de terceros	Cuestionarios, scoring, indicadores, análisis financiero, escenarios y concentración
Riesgos de ciberseguridad	Escenarios, KRIs, análisis de incidentes, pruebas de estrés y modelos predictivos cuando existan datos suficientes
Riesgos reputacionales	Juicio experto, escenarios, indicadores tempranos y análisis de impacto cualitativo
Riesgos de cumplimiento	Autoevaluaciones, análisis histórico, indicadores, pruebas de control y escenarios

Esta tabla no sustituye el criterio metodológico ni la adaptación al contexto de cada organización. Su finalidad es orientar la selección inicial de técnicas, que deberá ajustarse en función de la información disponible, la criticidad del riesgo, el apetito definido, las capacidades internas y el uso previsto del resultado.

3. Métodos cualitativos y semicuantitativos

Las técnicas cualitativas se apoyan principalmente en el juicio experto, el conocimiento del negocio, la experiencia profesional y la percepción estructurada de las áreas implicadas. Son especialmente útiles cuando no existe información histórica suficiente o cuando el riesgo presenta un alto grado de incertidumbre, complejidad o subjetividad.

Las técnicas semicuantitativas transforman ese juicio experto en escalas homogéneas, normalmente mediante puntuaciones de probabilidad e impacto. Aunque utilizan valores numéricos, no deben interpretarse como mediciones exactas, sino como una forma estructurada de comparar, priorizar y comunicar riesgos.

Descripción de los principales métodos cualitativos y semicuantitativos

Entrevistas individuales

Las entrevistas individuales permiten profundizar en riesgos específicos mediante conversaciones estructuradas con responsables, expertos o propietarios del riesgo. Son especialmente útiles para identificar causas, consecuencias, controles existentes, vulnerabilidades, señales tempranas y posibles medidas de tratamiento.

Su principal limitación es que pueden depender excesivamente de la visión, experiencia o información disponible del entrevistado. Por ello, es recomendable contrastar la información obtenida con otras fuentes, evidencias disponibles y la visión de otras áreas implicadas.

Talleres de riesgos

Los talleres de riesgos permiten reunir diferentes perspectivas para identificar riesgos, analizar causas y consecuencias, evaluar interdependencias y construir una visión compartida entre áreas.

Son especialmente útiles para riesgos transversales, estratégicos, emergentes o aquellos que requieren la participación de múltiples funciones. No obstante, pueden verse afectados por sesgos de grupo, participación desigual, influencia jerárquica o falta de preparación previa.

Cuestionarios y autoevaluaciones
Los cuestionarios y autoevaluaciones permiten recopilar información homogénea de distintas áreas, unidades de negocio o geografías, facilitando la identificación y valoración inicial de riesgos.

Su utilidad depende en gran medida de la calidad del diseño del cuestionario, la claridad de las preguntas y el nivel de conocimiento de los participantes. Si no se gestionan adecuadamente, pueden generar respuestas superficiales o poco comparables.

Juicio experto estructurado
El juicio experto estructurado consiste en utilizar el conocimiento y experiencia de especialistas para evaluar riesgos cuando existe poca información histórica, elevada incertidumbre o una alta complejidad técnica.

Puede ser especialmente relevante para riesgos estratégicos, tecnológicos, reputacionales, regulatorios o emergentes. Para reducir la subjetividad, debe apoyarse en criterios definidos, documentación de los razonamientos utilizados y, cuando sea posible, contraste entre diferentes expertos.

Análisis de escenarios
El análisis de escenarios permite evaluar situaciones futuras plausibles mediante la combinación de eventos, condiciones o supuestos diferentes. Puede aplicarse tanto de forma cualitativa como semicuantitativa o cuantitativa.

Es especialmente útil para riesgos con elevada incertidumbre, como riesgos estratégicos, geopolíticos, regulatorios, climáticos, tecnológicos, de continuidad o de cadena de suministro. Su principal limitación es la dependencia de la calidad de los supuestos y de

la capacidad para definir escenarios relevantes y conectados con decisiones reales.

Matrices de probabilidad e impacto
Las matrices de probabilidad e impacto permiten valorar riesgos mediante escalas homogéneas, combinando la probabilidad de ocurrencia y la magnitud de sus consecuencias para facilitar la comparación y priorización.

Son una herramienta sencilla y ampliamente utilizada en modelos ERM. No obstante, deben diseñarse cuidadosamente para evitar una falsa precisión, asegurando que los niveles estén claramente definidos y que exista consistencia entre las distintas áreas de la organización.

Bow Tie
El análisis Bow Tie representa gráficamente la relación entre causas, evento de riesgo, controles preventivos, consecuencias y medidas de mitigación o recuperación.

Es especialmente útil para riesgos críticos o de baja frecuencia y alto impacto, ya que permite visualizar barreras de control y posibles puntos de fallo. Su principal limitación es que puede simplificar excesivamente riesgos complejos si no se actualiza periódicamente con información real sobre controles, incidentes y cambios en el entorno.

4. Métodos cuantitativos y modelos analíticos

Las técnicas cuantitativas permiten aportar mayor trazabilidad, comparabilidad y soporte analítico a la evaluación de riesgos mediante el uso de datos, modelos matemáticos, análisis estadístico o simulaciones. Son especialmente útiles cuando existen datos históricos suficientes, cuando el riesgo tiene una dimensión financiera relevante o cuando la decisión requiere estimar rangos de impacto, sensibilidad, probabilidad o escenarios.

No obstante, la cuantificación no debe considerarse siempre la aproximación más precisa o adecuada. En determinados casos, una valoración cualitativa basada en el conocimiento experto del

negocio puede proporcionar una estimación más fiable que un modelo matemático construido sobre datos incompletos, de baja calidad o cuya integridad no haya sido validada.

Además, determinados riesgos presentan por su propia naturaleza dificultades para ser expresados económicamente, como ocurre con algunos riesgos reputacionales, estratégicos o emergentes. En estos casos, puede resultar más adecuado utilizar aproximaciones cualitativas o semicuantitativas, por ejemplo definiendo rangos económicos asociados a niveles de impacto (como impactos bajos, moderados o altos vinculados a determinados intervalos de EBITDA).

La selección de la técnica deberá realizarse aplicando siempre el principio de proporcionalidad, considerando el tamaño y complejidad de la organización, la criticidad del riesgo, la disponibilidad de datos, la capacidad analítica existente y el valor real que el análisis aporta a la toma de decisiones.

Los resultados cuantitativos no deben interpretarse como predicciones exactas. Su fiabilidad depende de la calidad de los datos, los supuestos utilizados, las hipótesis consideradas, el horizonte temporal y la estabilidad del entorno analizado.

Descripción de los principales métodos cuantitativos

Análisis estadístico

El análisis estadístico es una metodología cuantitativa basada en la utilización de datos históricos para identificar patrones, relaciones, tendencias y probabilidades asociadas a determinados eventos de riesgo.

Su finalidad es transformar datos históricos en conocimiento útil para estimar comportamientos futuros y facilitar una toma de decisiones más informada.

Esta técnica parte del supuesto de que ciertos patrones observados en el pasado pueden ofrecer información relevante sobre el comportamiento futuro del riesgo, aunque sin asumir que la historia se repetirá exactamente.

El análisis estadístico busca identificar frecuencias de ocurrencia, analizar tendencias, estimar distribuciones de pérdidas, detectar anomalías, calcular probabilidades y anticipar desviaciones.

Principales técnicas estadísticas utilizadas:

I. Análisis descriptivo

Permite resumir datos históricos mediante indicadores como:

-media;
-mediana;
-desviación estándar;
-dispersión;
-máximos y mínimos;
-percentiles.

Por ejemplo, una organización puede analizar el coste medio de incidentes operativos sufridos durante los últimos cinco años.

II. Análisis de frecuencia

Mide cuántas veces ocurre un determinado evento.

Ejemplo: Número de incidentes de ciberseguridad anuales, reclamaciones de clientes, incumplimientos regulatorios.

III. Análisis de tendencia

Permite observar si el riesgo está aumentando, disminuyendo o manteniéndose estable.

Ejemplo: Incremento sostenido de ataques de phishing en los últimos tres años.

IV. Distribuciones probabilísticas

Permiten modelizar comportamientos del riesgo utilizando distribuciones estadísticas (normal, log normal, Poisson, binomial, etc.).

Resumiendo, el análisis estadístico resulta especialmente útil en lo relativo a riesgo operacional, fraude, siniestralidad, ciberseguridad, compliance, seguridad laboral, continuidad de negocio.

Ventajas: objetividad; facilidad de comparación; utilización de datos reales; identificación de patrones.

Limitaciones: fuerte dependencia del histórico; menor utilidad para riesgos emergentes; posibilidad de ignorar cambios estructurales.

Ejemplo práctico: Una compañía analiza 10 años de interrupciones tecnológicas para calcular: frecuencia anual; coste medio; tiempo medio de recuperación; tendencia de crecimiento. Con esta información puede estimar pérdidas futuras esperadas.

Modelización de escenarios

Lamodelización de escenarios es una técnica utilizada para evaluar cómo diferentes situaciones futuras plausibles pueden afectar a los objetivos de la organización. Permite analizar posibles evoluciones del entorno, combinando hipótesis sobre variables internas y externas, especialmente cuando no existe suficiente información histórica.

Su finalidad es identificar vulnerabilidades, comprender posibles impactos y evaluar la capacidad de respuesta de la organización ante situaciones inciertas.

La metodología consiste generalmente en:

- **Definir escenarios plausibles:** identificar diferentes situaciones futuras, desde un escenario base hasta escenarios adversos o extremos.

- **Analizar impactos potenciales:** evaluar las consecuencias sobre objetivos, operaciones, resultados económicos u otros ámbitos relevantes.
- **Valorar respuestas necesarias:** identificar medidas preventivas, de mitigación o de recuperación.

Es especialmente útil para riesgos estratégicos, emergentes, continuidad de negocio, ciberseguridad, riesgos climáticos, cadena de suministro o proyectos relevantes.

Sus principales ventajas son:
- permite analizar situaciones sin depender exclusivamente de datos históricos; facilita la preparación ante eventos inciertos;
- ayuda a identificar interdependencias y vulnerabilidades.

Sus principales limitaciones son:
- dependencia de la calidad de los supuestos utilizados;
- posible subjetividad en la definición de escenarios;
- dificultad para asignar probabilidades precisas a determinados eventos.

Ejemplo práctico: Una organización analiza el impacto de una interrupción prolongada de un proveedor crítico considerando distintos escenarios de duración, disponibilidad de alternativas y capacidad de recuperación. El análisis permite identificar medidas necesarias para reforzar la resiliencia.

Simulación Monte Carlo

La simulación Monte Carlo es una técnica cuantitativa avanzada utilizada para modelizar incertidumbre mediante la generación de miles de escenarios probabilísticos posibles.

En lugar de asumir un único resultado, esta metodología analiza múltiples combinaciones de variables para estimar el rango completo de resultados potenciales.

La técnica recibe su nombre del casino de Monte Carlo debido a su naturaleza probabilística y aleatoria.

Su finalidad es comprender escenarios extremos, dispersión de resultados, incertidumbre, riesgos agregados y probabilidad de pérdidas severas.

La metodología consiste en:

- Identificación de variables clave, por ejemplo inflación; tipos de interés; precio de materias primas; demanda; tipos de cambio; ciberataques.
- Asignación de distribuciones probabilísticas. A cada variable se le asigna un comportamiento estadístico esperado.

Ejemplo: Precio energético →distribución triangular.

- Simulación masiva: El modelo ejecuta miles de iteraciones aleatorias. Ejemplo: 10.000 escenarios posibles.
- Obtención de resultados. Se calcula la pérdida esperada; peor escenario razonable; percentiles de impacto; probabilidad de incumplir objetivos.

Muy útil para planificación financiera, riesgos estratégicos, liquidez, inversiones, continuidad de negocio, riesgos agregados. Sus principales ventajas son incorporar incertidumbre, permitir múltiples escenarios, facilitar una visión probabilística y ser útil en riesgos complejos.

En cuanto a las limitaciones, se requiere alta capacidad técnica, depende de supuestos y la complejidad de interpretación.

Como ejemplo práctico, una empresa modeliza el impacto combinado de inflación; caída de ventas; interrupción logística; incremento energético. La simulación muestra un 15% de probabilidad de incumplir EBITDA.

Análisis de sensibilidad

El análisis de sensibilidad evalúa cómo cambios en una o varias variables afectan al resultado de un modelo de riesgo. Permite identificar qué variables tienen mayor capacidad de alterar los resultados y, por tanto, representan mayores focos de incertidumbre.

Busca responder preguntas como: ¿Qué ocurre si aumentan los costes energéticos? ¿Cómo afecta una caída del 15% en ventas? ¿Qué variable genera mayor exposición?

Consiste en modificar individualmente determinadas variables manteniendo constantes el resto.

Ejemplo: Variación del margen EBITDA según: ±10% ventas; ±15% inflación; ±20% tipo de cambio.

Especialmente útil en planificación estratégica; escenarios financieros; cadena de suministro; riesgos macroeconómicos. Además es sencillo, intuitivo, fácil comunicación al Consejo; identifica variables críticas. Las principales limitaciones son que simplifica relaciones complejas y no siempre refleja correlaciones.

Ejemplo práctico: Una empresa descubre que un aumento del 25% en energía reduce EBITDA un 18%, siendo el principal factor de riesgo.

Árboles de decisión

Los árboles de decisión son modelos visuales y cuantitativos que permiten analizar decisiones alternativas y sus consecuencias probables. Representan decisiones secuenciales mediante nodos y ramas.

Su objetivo es ayudar a comparar alternativas, medir impactos, valorar probabilidades y optimizar decisiones.

Incluyen:

- Nodo de decisión: Representa alternativas posibles. Ejemplo: internalizar servicio; externalizar.
- Nodo probabilístico: Representa eventos inciertos. Ejemplo: éxito; fallo; retraso.
- Resultado esperado: Se calcula el valor esperado ponderado.

Esta técnica es especialmente útil en inversiones, expansión internacional, externalización, litigios y operaciones de fusiones y adquisiciones (M&A). Sus principales ventajas son la claridad visual, facilitar la toma de decisiones e incorporar incertidumbre. Sus limitaciones son la simplificación excesiva; crecimiento exponencial de complejidad.

Ejemplo: Empresa evalúa abrir una filial. Éxito: +20 M€ Fracaso: –8 M€ El árbol permite valorar el riesgo-retorno esperado.

Pruebas de estrés

Las pruebas de estrés consisten en evaluar la capacidad de resistencia de una organización frente a escenarios extremos, severos pero plausibles. No pretende estimar probabilidad, sino entender vulnerabilidades.

Busca responder cuestiones como:

- ¿Qué ocurriría si…?
- ¿Cuánto puede resistir la organización?

Los principales tipos de pruebas de estrés son:

- Estrés macroeconómico: Recesión, inflación.
- Estrés operativo: Fallo tecnológico.
- Estrés reputacional. Crisis mediática.
- Estrés financiero. Falta de liquidez.

Pruebas de estrés inversas

Las pruebas de estrés inversas parten de un resultado inaceptable —por ejemplo, incumplimiento de objetivos críticos, interrupción

prolongada de una actividad esencial, pérdida severa de liquidez o deterioro significativo de la reputación— y analizan qué combinación de eventos, vulnerabilidades o fallos de control podría provocar esa situación.

Su principal aplicación se encuentra en resiliencia, continuidad de negocio, capital, solvencia y planificación estratégica.

Value at Risk (VaR)

El VaR es una medida estadística utilizada para estimar el nivel de pérdida que no se espera superar, bajo un determinado nivel de confianza y horizonte temporal.

Ejemplo: "Existe un 95% de probabilidad de no perder más de X millones."

$$VaR_{(95\%)}=X$$

Las variables clave son el horizonte temporal, el nivel de confianza, la volatilidad y las correlaciones.

Existen distintos métodos de cálculo:

- Histórico: Basado en datos reales.
- Paramétrico: Distribución normal.
- Monte Carlo: Simulación avanzada.

Se aplica sobre todo en tesorería, divisas, commodities y liquidez. En cuanto a sus limitaciones, no mide eventos extremos fuera del percentil, y existe una fuerte dependencia de las hipótesis.

Ejemplo práctico:

VaR diario de 3 M€ al 99%.
Solo 1 de cada 100 días se espera perder más.

Modelos predictivos

Los modelos predictivos utilizan técnicas estadísticas avanzadas, aprendizaje automático (*machine learning*) e inteligencia artificial para anticipar comportamientos futuros. Se basan en relaciones identificadas entre variables históricas.

Su objetivo es anticipar fraude, impagos, rotación, fallos operativos, incidentes, etc. Las técnicas más habituales son regresión, clasificación, redes neuronales, random forests, NLP, machine learning supervisado.

Se aplican principalmente en el análisis de riesgo de fraude, compliance, ciberseguridad, riesgos laborales y cadena de suministro.

Sus ventajas son la capacidad predictiva, la detección temprana y la automatización.

Sus limitaciones principales son la dependencia de calidad de datos, el riesgo de sesgos algorítmicos y la explicabilidad limitada.

Ejemplo práctico: Modelo predictivo detecta patrones que anticipan fraude con un 85% de precisión antes de producirse.

5. Documentación mínima y cautelas de aplicación

La aplicación de técnicas de evaluación de riesgos deberá quedar suficientemente documentada para asegurar la trazabilidad del análisis y facilitar su revisión posterior. Como mínimo, deberá identificarse el riesgo evaluado, el objetivo del análisis, la técnica utilizada, las fuentes de datos, las hipótesis principales, las limitaciones existentes, el horizonte temporal, el responsable del análisis, la fecha de actualización y el uso previsto del resultado.

La profundidad de esta documentación deberá ser proporcional a la criticidad del riesgo y a la relevancia de la decisión que se pretende soportar. No requerirá el mismo nivel de detalle una evaluación cualitativa preliminar que un análisis cuantitativo utilizado para

justificar una inversión relevante, aceptar un riesgo fuera de tolerancia, definir coberturas, establecer provisiones o elevar una decisión a la Alta Dirección o al Consejo.

En todos los casos, la organización deberá evitar que las técnicas de evaluación se conviertan en un ejercicio meramente formal o excesivamente técnico. Su valor dependerá de que los resultados sean comprensibles, trazables y útiles para adoptar decisiones reales de tratamiento, aceptación, transferencia, escalado, reporting o seguimiento.

Asimismo, deberá evitarse la falsa precisión derivada de puntuaciones, modelos o simulaciones que no estén suficientemente respaldados por datos fiables, hipótesis razonables y revisión crítica. La técnica utilizada debe apoyar el juicio profesional y el conocimiento del negocio, no sustituir la responsabilidad de gestión de los responsables del riesgo ni de los órganos correspondientes.


agers