GESTIÓN POR RIESGOS

concepto, retos e implicaciones

Governance Actually somos un Think Tank y un observatorio sobre temas de Gobierno Corporativo, Riesgos, Control Interno y Auditoría.

Position Paper

Abril 2026

ÍNDICE

La gestión por riesgos, entendida como la integración del riesgo en la toma de decisiones de la organización y no únicamente como una disciplina de control, se ha consolidado en los últimos años como una de las exigencias supervisoras y de buen gobierno más relevantes para las grandes corporaciones. Su despliegue efectivo, sin embargo, dista todavía de ser homogéneo.

Este documento sitúa el concepto en su marco de referencia (COSO ERM, Principios de Gobierno Corporativo del G20/OCDE y el Código de Buen Gobierno de las sociedades cotizadas de la Comisión Nacional del Mercado de Valores), explicita el papel del consejo de administración en todo el proceso y la, cada día, mayor necesidad de este tipo de gestión en las compañías; e identifica los principales retos para su implantación y discute sus implicaciones para los órganos de administración y la alta dirección.

1. Introducción y propósito

El término “gestión por riesgos” ha ganado tracción en el discurso de gobierno corporativo durante los últimos diez años. Su uso, sin embargo, no es unívoco. En ocasiones, se utiliza como sinónimo de “gestión de riesgos” (risk management) o incluso de “control interno”. En otras se reserva para describir un estadio más maduro: aquel en el que **el riesgo se incorpora explícitamente como variable a la formulación de la estrategia, a la asignación de capital, a la fijación de objetivos y a la evaluación del desempeño**.

Este documento adopta esta segunda lectura, más exigente y acorde a los tiempos actuales y madurez de las organizaciones. Su propósito es reflexivo: sintetizar los referentes conceptuales y regulatorios disponibles, exponer los retos que plantea su despliegue y exponer, con la mayor neutralidad posible, sus implicaciones para los órganos responsables del gobierno y la dirección de las organizaciones.

2. Concepto: gestión “de” riesgos frente a gestión “por” riesgos

Distingamos inicialmente tres planos que la práctica requiere aclarar.

En primer lugar, el **control interno** persigue asegurar la fiabilidad de la información, el cumplimiento normativo y la eficacia operativa. Su marco de referencia más extendido es el COSO Internal Control Integrated Framework.

En segundo lugar, la **gestión de riesgos o Enterprise Risk Management (ERM),** por sus siglas en inglés, que amplía el perímetro al universo de eventos que pueden afectar a la consecución de los objetivos e introduce la noción de apetito de riesgo, tolerancias y respuestas. El estándar de referencia es el COSO ERM Integrating with Strategy and Performance.

En tercer lugar, la **gestión por riesgos** es un estadio en el que el riesgo no se aborda como una función paralela a la gestión, sino como una **dimensión del propio proceso de decisión**. Sus rasgos distintivos son tres: (1) el apetito y las tolerancias se definen ex ante y se trasladan a métricas (cuantitativas y cualitativas) operativas vinculantes; (2) la información de riesgos integra la información de gestión y se reporta junto con ella, no de forma aislada; y (3) las decisiones materiales —inversiones, fusiones y adquisiciones, lanzamientos, expansión geográfica— se acompañan de una valoración explícita del riesgo, con responsable identificado, antes de su aprobación.

Esta lectura es coherente con la formulación de COSO ERM 2017, que define la gestión de riesgos empresariales como “la cultura, las capacidades y las prácticas, integradas con el establecimiento de la estrategia y su ejecución, en las que las organizaciones confían para gestionar el riesgo en la creación, preservación y realización de valor”. También es coherente con la definición de la norma internacional ISO 31000:2018, que entiende el riesgo como “el efecto de la incertidumbre sobre los objetivos” y exige integrar su gestión en todas las actividades de la organización, no en una función separada.

3. Marco conceptual de referencia

Varios documentos articulan el lenguaje común de la gestión por riesgos.

COSO ERM: su aportación principal no reside tanto en una taxonomía de riesgos, sino en cinco componentes que vinculan riesgo y estrategia: gobierno y cultura; estrategia y fijación de objetivos; desempeño; revisión y mejora; e información, comunicación y reporte. El marco insiste en que el riesgo debe considerarse antes y durante la formulación de la estrategia, no únicamente en su ejecución posterior. Es un texto de referencia tanto para empresas cotizadas como para grandes grupos no cotizados.

Principios de Gobierno Corporativo del G20/OCDE: refuerzan la responsabilidad del consejo en la definición del apetito de riesgo, la supervisión del sistema de gestión y la integración de los riesgos no financieros —sostenibilidad, ciberseguridad, transformación digital— en el marco general. Son la base sobre la que se construyen los códigos nacionales.

A nivel español, el Código de Buen Gobierno de las sociedades cotizadas de la Comisión Nacional del Mercado de Valores (CNMV): las recomendaciones referidas a la política de control y gestión de riesgos atribuyen al consejo de administración su aprobación, incluido el riesgo fiscal, así como la supervisión periódica de los sistemas internos de información y control. Las recomendaciones sobre la comisión de auditoría perfilan el seguimiento del sistema de control interno y de la gestión de riesgos.

4. El papel del consejo: estrategia, supervisión y marco de apetito al riesgo

Antes de adentrarse en los retos prácticos de la gestión por riesgos, conviene explicitar el papel que el consejo de administración ocupa en esta arquitectura de gestión.

Aunque las funciones concretas dependen del marco jurídico de cada jurisdicción y de los estatutos sociales, el consenso internacional en torno a tres responsabilidades nucleares es fuerte y unánime; y se refleja claramente en los marcos de referencia ya citados.

La primera responsabilidad es la **aprobación de la estrategia**. El consejo no es ejecutor de la estrategia, pero sí es el órgano competente para aprobarla y para revisarla con la cadencia que el negocio requiera. Los Principios de Gobierno Corporativo del G20/OCDE atribuyen al consejo, entre sus funciones esenciales, la revisión y orientación de la estrategia corporativa, los principales planes de actuación, la política de riesgos, los presupuestos anuales y los planes de negocio; así como, la fijación de objetivos de desempeño y el seguimiento de su consecución. La Ley de Sociedades de Capital española, en su artículo 529 ter, recoge, entre las facultades indelegables del consejo de las sociedades cotizadas, la aprobación del plan estratégico o de negocio, los objetivos de gestión y el presupuesto anual, así como la política de control y gestión de riesgos y la supervisión de los sistemas internos de información y control.

La segunda responsabilidad es la **supervisión efectiva de los riesgos**. Esta función es, lógicamente, posterior a la aprobación de la estrategia, pero la sustenta: una estrategia aprobada sin un sistema de supervisión que verifique su ejecución dentro del perímetro de riesgo deseado convierte al consejo en un órgano deliberativo sin instrumentos de control. Los Principios del G20/OCDE atribuyen al consejo velar por la integridad de los sistemas contables y de información financiera de la sociedad, incluidos los procesos independientes de auditoría y por la existencia de adecuados sistemas de control; en particular, sistemas de gestión del riesgo, control financiero y operativo y respeto de la ley y de las normas pertinentes. El Código de Buen Gobierno de las sociedades cotizadas de la CNMV atribuye la aprobación de la política de control y gestión de riesgos al consejo y reserva su seguimiento a la comisión de auditoría o, en su caso, a una comisión específica de riesgos, ambas integradas mayoritariamente por consejeros no ejecutivos y presididas por consejeros independientes.

La tercera responsabilidad, instrumental respecto a las dos anteriores, es la **aprobación y revisión periódica del marco de apetito al riesgo**. El apetito al riesgo es el nivel agregado y los tipos de riesgo que la organización está dispuesta a asumir para alcanzar sus objetivos estratégicos y operativos. Su formulación trasciende la mera declaración de principios: requiere una articulación coherente que conecte estrategia, capital, liquidez y resultados con métricas y umbrales operativos.

El marco de apetito al riesgo (Risk Appetite Framework, RAF) es un enfoque global que incluye las políticas, los procesos, los controles y los sistemas; a través del cual, se establece,

comunica y supervisa los límites de aceptación de riesgo que el consejo fija a los gestores en el desarrollo de los objetivos estratégicos.

El RAF se compone, en general, elementos como la declaración de apetito al riesgo, los límites de riesgo, el papel y las responsabilidades de los órganos y funciones que lo aprueban, supervisan y aplican, y los procesos de revisión y reporte. La declaración debe ser comprensible, accionable y consistente con el plan estratégico de la entidad.

COSO ERM, en su componente de “estrategia y fijación de objetivos”, incorpora explícitamente la articulación del apetito al riesgo en el proceso de planificación estratégica e insiste en que el consejo es el órgano que aprueba el apetito y supervisa que la organización opere dentro de él.

En el ámbito bancario europeo, las directrices de la Autoridad Bancaria Europea sobre gobernanza interna y los principios de gobierno corporativo del Comité de Supervisión Bancaria de Basilea elevan el RAF de una buena práctica a obligación explícita: el consejo aprueba el RAF, lo revisa al menos con periodicidad anual, supervisa su cumplimiento mediante un reporte periódico de la función de riesgos y vela por que los límites se respeten en la actividad ordinaria.

La articulación práctica de estas tres responsabilidades: aprobación de la estrategia, supervisión de los riesgos y aprobación del marco de apetito; se traduce, en organizaciones complejas, en una secuencia anual recurrente. El consejo revisa o aprueba la estrategia y, en el mismo ciclo, revisa o aprueba el marco de apetito al riesgo que la acompaña; durante el ejercicio, recibe a través de su comisión de auditoría información periódica sobre el grado de uso de los límites, los principales movimientos y los incidentes materiales; y, al cierre del periodo, evalúa la suficiencia del sistema y, en su caso, lo recalibra.

5. Retos para una implantación efectiva

La distancia entre la formulación teórica y la práctica observada suele ser significativa. Sin pretender exhaustividad, pueden destacarse seis retos transversales que aparecen con regularidad en organizaciones de tamaño medio y grande.

El primero es de **calidad y trazabilidad del dato**. Una gestión por riesgos efectiva requiere un universo de datos único, en el que cada riesgo se vincule a sus procesos, controles, responsables y valoraciones, tanto inherente como residual. La fragmentación documental, la duplicidad de catálogos y la convivencia de versiones paralelas; son problemas habituales que erosionan la fiabilidad del sistema y, en última instancia, la confianza del órgano de administración en la información que recibe. La depuración del dato es un trabajo previo a cualquier sofisticación analítica posterior.

El segundo es la **conexión entre la visión Top-Down** —el apetito y la mirada estratégica del consejo y de la alta dirección— y la visión Bottom-Up —la operativa de procesos, controles e incidentes. Sin un mecanismo periódico de contraste entre ambas, los riesgos materiales identificados desde abajo no se reflejan a nivel global y, a la inversa, las prioridades

estratégicas no se traducen en gestiones operativas. La frecuencia y el formato de ese contraste son una decisión estructural; los marcos no la prescriben, pero su ausencia es un indicador fiable de falta de madurez del sistema e imposibilita, en la práctica, una adecuada gestión por riesgos.

El tercero es la cultura de propiedad del riesgo. La asignación formal de risk owners y control owners es una práctica extendida sobre el papel, pero su efectividad depende de que esos responsables dispongan autoridad, recursos y métricas vinculadas a su evaluación de desempeño. Igualmente, que sus riesgos estén efectivamente vinculados a los objetivos estratégicos asignados. Cuando la propiedad es nominal, el sistema deviene un repositorio de declaraciones sin consecuencias verificables ni capacidades de gestión.

El cuarto es la vinculación con la estrategia. COSO ERM 2017 sitúa el riesgo en el corazón del proceso estratégico, pero la práctica común es la elaboración paralela de un plan estratégico y de un mapa de riesgos sin un mecanismo formal de integración. Los riesgos emergentes —tecnológicos, geopolíticos, climáticos— quedan con frecuencia fuera del horizonte estratégico hasta que se materializan, momento en el que la respuesta es necesariamente más costosa.

El quinto es la suficiencia de los sistemas de información. La existencia de un cuadro de mando de riesgos auditable, con datos primarios trazables y con histórico, es excepción más que norma. La proliferación de hojas de cálculo paralelas —en ocasiones denominadas “shadow IT”— es un riesgo operativo en sí misma y un obstáculo para la rendición de cuentas: si la cifra que se reporta al consejo no se puede reconstruir desde el dato primario, la confianza del supervisor en el sistema se resiente.

El sexto, por último, es la integración de los riesgos financieros y no financieros. La regulación europea ha avanzado en este terreno, pero su translación a los sistemas internos de gestión es todavía un proceso en curso.

6. Implicaciones para los órganos de gobierno y la alta dirección

El despliegue de una gestión por riesgos en sentido pleno tiene implicaciones que trascienden lo metodológico y que afectan a la propia arquitectura y cultura de gobierno de la organización.

La primera es la **calidad de la declaración de apetito al riesgo**. No basta con una formulación cualitativa: el apetito debe traducirse a métricas y umbrales operativos, comunicarse de forma comprensible al conjunto de la organización y revisarse con una cadencia explícita. Requiere una cultura de riesgo y una formación en su gestión. Su aprobación corresponde al órgano de administración y su seguimiento suele descansar en la comisión de auditoría. La calidad del apetito se mide por su utilidad como referencia y límites para tomar decisiones.

La segunda es la **calidad de la supervisión**. Una supervisión efectiva exige información comparable a lo largo del tiempo, agregada por país y/o por unidad de negocio, cuando proceda, y acompañada de juicio profesional. La mera presentación de un mapa de calor no

satisface ese estándar; requiere métricas con histórico, narrativa de los principales movimientos y vinculación con las decisiones tomadas en el periodo. La cadencia de reporting, el formato y los destinatarios son decisiones de gobernanza con consecuencias prácticas relevantes.

La tercera es la **integración con el ciclo estratégico y presupuestario**. Las decisiones de inversión, expansión, fusiones y adquisiciones o desinversión deben acompañarse de una valoración explícita del riesgo y de su impacto sobre el apetito; en caso de superación, deben elevarse al órgano competente. Esta práctica, formal y trazable, distingue una organización que se gestiona "por riesgos" de una que se limita a "gestionarlos".

La cuarta es la **rendición de cuentas**. La eficacia del sistema requiere mecanismos de escalado, sanción y aprendizaje. Los incidentes materiales —pérdidas operacionales, fallos de control, sanciones regulatorias, episodios reputacionales— deben analizarse hasta su causa raíz y traducirse en cambios verificables en los procesos, los controles o el propio diseño organizativo. La ausencia de aprendizaje observable es una señal de debilidad del sistema, con independencia de la sofisticación de su documentación.

La quinta, transversal a las anteriores, es la **cultura**. Los marcos coinciden en señalarla como condición necesaria, no como un complemento. Su construcción es lenta, requiere consistencia entre el discurso y la práctica, y se observa en señales prosaicas: cómo se comunican los errores, qué decisiones se documentan, qué consecuencias tienen los incumplimientos, qué se reconoce y qué se sanciona. Una cultura coherente con el sistema formal de gestión de riesgos puede tardar años en consolidarse; una cultura incoherente lo desactiva con rapidez.

7. Las entidades de crédito, un caso específico

La banca constituye un caso particular en el que la gestión por riesgos deja de ser una buena práctica voluntaria para convertirse en un requisito explícito. La regulación europea articula esta exigencia y la traslada a un marco operativo detallado.

Sobre esa base, los principios de gobierno corporativo del Comité de Supervisión Bancaria de Basilea y las directrices de la Autoridad Bancaria Europea sobre gobernanza interna precisan el papel del consejo, del comité de riesgos y de la función independiente de riesgos; así como, el contenido mínimo del marco de apetito al riesgo. La metodología de revisión y evaluación supervisora del Banco Central Europeo y las pruebas de resistencia coordinadas con la EBA traducen esa exigencia a una evaluación periódica con consecuencias vinculantes, incluidos requerimientos de capital adicionales (Pilar 2). El Banco de España aplica estos requisitos en su actividad supervisora y los publica en su Memoria de Supervisión anual.

Otros sectores regulados —seguros con Solvencia II, gestión de activos con MiFID II o infraestructuras críticas con NIS2— han incorporado exigencias análogas. La pauta común es que lo que en una compañía no regulada se considera buena práctica, en una entidad supervisada constituye una obligación con consecuencias administrativas o sancionadoras.

8. Conclusión

La gestión por riesgos no es, en sí misma, una garantía de éxito, pero ofrece un marco coherente para que las decisiones se tomen con consciencia explícita de la incertidumbre y para que las consecuencias de esas decisiones sean trazables y auditables a posteriori.

Su despliegue exige sostener, durante años, una agenda poco vistosa: depurar datos, definir responsables, articular comités, calibrar métricas, escalar incidencias, acumular histórico. No produce hitos espectaculares, pero su ausencia se nota cuando importa: cuando un riesgo material se materializa y la organización descubre que carecía de información, de propietario o de plan de respuesta.

Los marcos disponibles ofrecen un lenguaje común y un nivel de exigencia razonable. La cuestión relevante no es ya cuál adoptar, sino con qué profundidad. La diferencia entre las organizaciones que se gestionan “de” riesgos y las que se gestionan “por” riesgos no reside en la sofisticación de su mapa, en la nomenclatura de su comité o en el volumen de su documentación, sino en si las decisiones materiales se acompañan, de forma sistemática, de una valoración explícita del riesgo, con responsable identificado y consecuencias verificables.

Para el consejo de administración, este planteamiento aporta un valor concreto que excede lo metodológico. En primer lugar, le permite ejercer con sustancia sus funciones de aprobación estratégica y de supervisión: las decisiones se toman dentro de un perímetro de riesgo previamente acordado y se documentan dentro de él, lo que refuerza el deber de diligencia que la legislación atribuye a sus miembros y mejora la defensa del consejo ante supervisores, accionistas o terceros. En segundo lugar, anticipa la identificación de los riesgos materiales antes de que se conviertan en pérdidas o sanciones, eleva la calidad de la conversación entre consejo y dirección y reduce la probabilidad de sorpresas costosas. En tercer lugar, dota al consejo de un lenguaje común con auditores, supervisores, inversores y agencias de calificación, lo que disminuye la fricción regulatoria y fortalece la confianza de los terceros con los que la sociedad se relaciona. Por último, asegura que el sistema sobreviva a los cambios en el equipo gestor: el marco institucionaliza el conocimiento del riesgo y reduce la dependencia de personas concretas.

En última instancia, la gestión por riesgos no se justifica por su sofisticación técnica, sino por la calidad de las decisiones que el consejo es capaz de tomar gracias a ella. Esa es la métrica que importa: si las decisiones del consejo son hoy más informadas, más anticipadas y más defendibles que hace un año, el sistema cumple su función; si no lo son, requiere recalibración.

Bibliografía y fuentes

- Basel Committee on Banking Supervision (BCBS), Corporate governance principles for banks, julio de 2015. Bank for International Settlements. Disponible en bis.org.
- Comisión Nacional del Mercado de Valores (CNMV), Código de Buen Gobierno de las sociedades cotizadas, junio de 2020 (revisión).
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management — Integrating with Strategy and Performance, 2017.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control — Integrated Framework, 2013.
- European Banking Authority (EBA), Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), julio de 2021.
- European Central Bank (ECB), SREP methodology booklet (publicación periódica del Mecanismo Único de Supervisión).
- Financial Stability Board (FSB), Principles for an Effective Risk Appetite Framework, noviembre de 2013.
- International Organization for Standardization (ISO), ISO 31000:2018 — Risk management — Guidelines, 2018.
- Ley de Sociedades de Capital (Real Decreto Legislativo 1/2010, de 2 de julio, texto refundido), en particular el artículo 529 ter, sobre facultades indelegables del consejo de administración de las sociedades cotizadas.
- Organisation for Economic Co-operation and Development (OECD) / G20, G20/OECD Principles of Corporate Governance, revisión de septiembre de 2023.
- Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito (CRR), y revisiones posteriores.
- Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial (CRD), y revisiones posteriores.
- Directiva (UE) 2022/2464 del Parlamento Europeo y del Consejo (CSRD), sobre información de sostenibilidad corporativa, diciembre de 2022.
- Banco de España, Memoria de Supervisión (publicación anual).
- Directiva (UE) 2022/2555