TONE at the TOP

Proporciona a la alta dirección, juntas directivas y comités de auditoría, información concisa sobre temas relacionados con la gobernanza.

Edición 134 | Abril 2026

¿Qué Deben Saber los Consejos sobre la Supervisión de la Gestión de Riesgos Empresariales (ERM)

En el incierto entorno empresarial actual, los miembros del consejo se ven obligados a mejorar su supervisión de riesgos. Cada vez más las partes interesadas de todo tipo esperan que los consejos de administración adopten un papel proactivo supervisando un panorama de riesgos en constante cambio.

Los riesgos a los que se enfrentan las organizaciones incluyen la disrupción geopolítica, las preocupaciones de ciberseguridad, el impacto de las tecnologías emergentes, los problemas en la cadena de suministro, la escasez de mano de obra y los fenómenos meteorológicos severos, por nombrar solo algunos. "Gestionar el riesgo corporativo no es solo una responsabilidad empresarial y operativa del equipo directivo de una empresa, sino una cuestión de gobernanza y estrategia que recae directamente dentro de la responsabilidad de supervisión del consejo", según el artículo "Risk Management and the Board of Directors" del Foro de Gobierno Corporativo de la Facultad de Derecho de Harvard.

El artículo añade que los tribunales y organismos reguladores se centran en la supervisión ejercida por los consejos y en las respuestas que estos adoptan cuando ocurren crisis. Aunque los directores no deberían participar en la gestión diaria de riesgos, "el papel de supervisión de cada consejo debe incluir la participación activa en el seguimiento de factores clave de riesgo corporativos, incluyendo el uso adecuado de los comités del consejo", señala el artículo..

Este número examina las consideraciones que deben tener en cuenta los consejos en la supervisión de la gestión de riesgos empresariales (ERM) y el papel de la auditoría interna en proporcionar a los consejos aseguramiento y asesoramiento valiosos.

Determinación de la Madurez de la Gestión de Riesgos Empresariales (ERM Maturity).

Una evaluación realista del nivel de madurez de ERM de la organización puede proporcionar a los consejos una mayor comprensión de la situación y de los cambios que pueden ser necesarios. Según la Guía para Directores sobre Fundamentos de ERM de PwC, a un nivel general, las etapas de madurez de ERM de una organización incluyen:

- **Inicial.** Hay algunas prácticas informales, pero no hay políticas ni procesos formales. La organización reacciona ante los problemas.
- **En desarrollo.** Existen sistemas y procesos que son efectivos en algunos aspectos del diseño o funcionamiento. Los enfoques están parcialmente alineados con las operaciones del negocio..
- **Desarrollada.** Existen marcos de referencia y sistemas formales integrados y operando para cumplir con estándares reconocidos.
- **Integrada.** La organización ha integrado sistemas y procesos colaborativos y mejorados que permiten una respuesta estratégica coordinada y eficiente a los riesgos actuales y emergentes.
- **Optimizada.** Los sistemas, procesos y cultura están plenamente-integrados y alineados con las prioridades estratégicas. La tecnología se utiliza para mejorar la gobernanza, la gestión de riesgos y el monitoreo/ elaboración de reportes..

"A medida que el programa de ERM madura, la junta puede promocionar la mejora continua, desafiando a la dirección sobre qué funciona y qué no", indica la guía.

Profundizando

El Resumen Ejecutivo de COSO para la Gestión de Riesgos Empresariales–Integrando la Estrategia y el Rendimiento, sugiere preguntas que los consejos pueden plantear a la dirección sobre ERM, incluyendo:

- ¿Puede toda la dirección — no solo el director de riesgos —explicar cómo se considera el riesgo en la selección de estrategias o al tomar decisiones empresariales?
- ¿Puede la dirección articular claramente el apetito por el riesgo de la entidad y cómo podría influir en una decisión concreta? COSO señala que la respuesta puede revelar una visión de la verdadera mentalidad de la organización respecto a la asunción de riesgos..
- ¿Puede la alta dirección analizar no solo los procesos de gestión de riesgos, sino también cómo la cultura de la organización facilita o inhibe la asunción de riesgos?
- ¿Qué enfoque utiliza la dirección para monitorizar el riesgo y cómo ha cambiado dicho enfoque? Dado el cambio inevitable dentro y fuera de la organización, ¿cómo puede el consejo confiar en una respuesta adecuada y oportuna por parte de la dirección?

El Compendio de Ejemplos de COSO incluye observaciones específicas sobre gobernanza. Uno de los ejemplos aborda cómo la ERM puede mejorar la toma de decisiones para obtener mejores resultados, aumentar las oportunidades y minimizar sorpresas negativas.

En el ejemplo, una empresa ha tomado medidas para comprender mejor las capacidades de ERM existentes y deseadas. Por ejemplo, el CEO y el auditor interno asisten a evaluaciones de desempeño empresarial con las divisiones operativas para seguir el progreso en los objetivos de rendimiento y determinar cómo la comprensión de los riesgos afecta a la manera en que se persiguen esos objetivos. Gracias a este esfuerzo, el CEO puede comprender mejor el desempeño del negocio y el auditor interno ha podido desarrollar un plan de auditoría más efectivo.

Orientación sobre Mejores Prácticas

Las organizaciones que buscan mejorar su enfoque de gestión de riesgos pueden elegir entre varios marcos de gestión de riesgos empresariales , incluyendo: *El Marco integrado de Gestión de Riesgos Empresariales de COSO,* la norma ISO 31000 de Gestión de Riesgos, y el Marco Nacional de EE.UU. de Gestión de Riesgos del Instituto de Normas y Tecnología (NIST). Según los "Fundamentos de la Gestión de Riesgos empresariales de Optro," estos marcos suelen compartir cinco componentes clave:

- Cultura de la empresa, gobernanza y valores.
- Planificación estratégica, objetivos y establecimiento de metas.
- Ciclo de gestión de riesgos.
- Monitoreo y mejora continua.
- Transparencia, comunicación e informes.

El Modelo de las Tres Líneas es un modelo de buenas prácticas para la supervisión de la gestión de riesgos por parte de los consejos, mostrando cómo los roles clave trabajan juntos para apoyar una gobernanza sólida. La Herramienta de Riesgos Empresariales y de Procesos de Negocio, alineada con el Modelo, ayuda a las organizaciones a implementar y gestionar un programa estructurado de ERM, proporcionando un enfoque práctico y personalizable para identificar, evaluar, gestionar y monitorear riesgos a nivel empresarial y de procesos..

Colaboración con Auditoría Interna

La auditoría interna puede ser un socio valioso para los consejos en sus esfuerzos por mejorar el ERM. De hecho, el IIA informa que los roles de auditoría interna relacionados con ERM están evolucionando, y un número creciente de DEAs tienen responsabilidad sobre ERM. Según el estudio de la IIA North American Pulse of Internal Audit, el porcentaje de DEAs que declararon ser responsables de los programas de ERM junto con su papel como jefe de auditoría interna aumentó al 34% en 2025.

Un elemento clave que respalda una función eficaz de gestión de riesgos es la colaboración entre las tres líneas. Bajo el modelo de tres líneas del IIA:

- **Primera línea:** La dirección y los responsables de las operaciones que gestionan los riesgos.
- **Segunda línea:** Las funciones de gestión de riesgos y cumplimiento que supervisan y monitorean los riesgos.
- **Tercera línea:** La auditoría interna, que proporciona aseguramiento independiente y asesoramiento para el logro de los objetivos de la organización.

Sobre el IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin fines de lucro que presta servicios a más de 265,000 miembros globales y ha otorgado más de 200,000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Establecido en 1941, el IIA es reconocido globalmente como líder de la profesión de auditoría interna en estándares, certificaciones, educación, investigación y orientación técnica. Para más información, visite **theiia.org.**

El IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA.

Suscripciones gratuitas

Visite **theiia.org/Tone** para obtener la suscripción.

Feedback del Lector

Envíe sus preguntas/comentarios a: **Tone@theiia.org.**

Expectativas para los consejos

Las responsabilidades principales de los consejos relacionadas con el riesgo, incluyen:

- Establecer el apetito y la tolerancia al riesgo de la organización.
- Aprobación y seguimiento del marco ERM.
- Alinear estrategia y exposición al riesgo.
- Supervisar la cultura de riesgos y los controles internos.
- Monitorizar riesgos emergentes y áreas críticas.
- Asegurar roles y responsabilidades claros.

– Diligente, "Comprendiendo la Supervisión del Consejo de Administración sobre la Gestión de Riesgos Ahora y en el Futuro"

El Modelo "deja claro que, si bien la independencia de la auditoría interna respecto a la dirección asegura que esté libre de obstáculos y sesgos en la planificación y ejecución de su trabajo, la independencia no implica un aislamiento total", según el informe Colaboración Sin Concesiones: Perspectivas de los Profesionales sobre Auditoría Interna, Gestión de Riesgos y Prácticas de Gobernanza, de Baker Tilly, la Fundación de Auditoría Interna y Wolters Kluwer TeamMate. Las crecientes responsabilidades de la auditoría interna en varias áreas, incluida la gestión integral de riesgos (ERM), ofrecen oportunidades para consolidar su papel como evaluador independiente de la eficacia de la gobernanza y la gestión de riesgos.

El informe señala que el 90% de los encuestados ve beneficios en la coordinación entre la segunda y la tercera línea, incluyendo:

- Mejor cobertura de riesgos.
- Reducción de la duplicación de esfuerzos.
- Mayor alineación organizacional.
- Mejora de la comunicación con la junta y una elaboración de informes más eficiente.

El 39% de los encuestados afirma haber visto una mayor integración de las funciones de auditoría interna y gestión de riesgos en los últimos cinco años, y el 60 % afirma que esta cifra aumentará en los próximos cinco años. "Cuando se diseñan cuidadosamente mediante el intercambio de información, actividades coordinadas y prioridades alineadas, estos enfoques ayudan a garantizar que los consejos reciban datos fiables para una toma de decisiones fundamentada", señala el informe.

Una Visión Clara

Por encima de todo, ERM trata de reconocer o anticipar el cambio y decidir qué significa para la organización. COSO señala que una visión clara del cambio permite a las organizaciones tomar decisiones acertadas sobre cuestiones difíciles, como si es mejor hacer nuevas inversiones o retirarse. Como afirma COSO, "La gestión de riesgos empresariales proporciona el marco adecuado para que los consejos evalúen riesgos y adopten una mentalidad de resiliencia."

Tecnología y ERM

Existe un gran potencial para que la inteligencia artificial (IA) desempeñe un papel más importante en ERM. Menos de uno de cada diez encuestados informa usar IA con frecuencia para ayudar a identificar riesgos (6%) o afirma que la utiliza intensamente para el ingreso de datos en actividades de gestión de riesgos (3%), según Enhanced Enterprise Risk Management and Strategic Decision-Making, de Baker Tilly y la Internal Audit Foundation.

Las plataformas integradas de gobernanza, riesgo y cumplimiento (GRC) pueden soportar procesos ERM. Una encuesta de madurez ERM de Baker Tilly y la Internal Audit Foundation revelan que solo el 21% de los profesionales que respondieron los utilizan. Los programas de ERM de muchas organizaciones se basan en herramientas sencillas, como procesamiento de textos y hojas de cálculo (59%) o herramientas tecnológicas internas (20%).

"En una época en la que la transformación digital ha acelerado la dependencia de la tecnología en todos los aspectos de las operaciones y ha redefinido las estrategias, es peligroso que ERM no siga el ritmo", advierte el informe de Enhanced Enterprise Risk Management.

Teniendo esto en cuenta:

- El software como servicio (SaaS) y las herramientas GRC pueden mejorar los programas básicos de ERM y promover una comprensión más profunda de los riesgos a nivel empresarial. Pueden centralizar datos, automatizar flujos de trabajo y facilitar la identificación de riesgos, lo que permite una mejor toma de decisiones y minimiza la exposición al riesgo.
- El informe aconseja a las organizaciones que apoyen, faciliten y supervisen la exploración del uso seguro de la IA dentro de la organización e identifiquen formas de poner la IA en funcionamiento en los procesos de ERM.

"Avanzar desde los enfoques tradicionales de ERM con la ayuda de herramientas colaborativas, escaneo externo de riesgos, integración multifuncional y tecnologías de vanguardia debería ser el objetivo de todos los programas de ERM", afirma el informe.

Entre los expertos globales encuestados, el 50% espera una perspectiva de riesgo global turbulenta o tormentosa en los próximos dos años, creciendo hasta el 57% en los próximos 10 años." Solo el 1% predice una perspectiva tranquila.

– Informe de Riesgos Globales del Foro Económico Mundial 2026.