PRÁCTICAS DE BUEN GOBIERNO

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna y gestión de riesgos

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con cerca de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.


AUDITORÍA INTERNA


BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS


OBSERVATORIO SECTORIAL


PRÁCTICAS DE BUEN GOBIERNO

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es

PRÁCTICAS DE BUEN GOBIERNO

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna y gestión de riesgos

Octubre 2021

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Tomás R. Soto García, CIA, CRMA, CFE. IBERDROLA.

Alejandro Bergaz Albarran, CIA. VISCOFAN.

Isabel Casares San José-Martí. CASARES ASESORÍA ACTUARIAL Y DE RIESGOS.

José Ignacio Diez Arocena, CIA, CISA, CFE, CESCOM, COSO. INDRA.

Mónica Gancedo Santamaría, CIA. SANITAS.

Diana Lianes Arcos. PELAYO.

Miguel Losada Tejera. DELOITTE.

Marta Sánchez Jiménez. PWC.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-20099-2021
ISBN: 978-84-122588-4-4

Diseño y maquetación: desdecero, estudio gráfico

Durante años, el despliegue de este marco de gestión integral del riesgo se ha realizado basándose en un modelo de líneas de defensa que requería una explícita separación de las actividades de la gestión de riesgos de las de Auditoría Interna, situación que, dependiendo de las características de la entidad, no siempre era posible. No obstante, el marco normativo del Instituto de Auditores Internos ofrece la posibilidad de que, además de proporcionar aseguramiento respecto de la efectividad de la gestión de riesgos, Auditoría Interna preste servicios de consultoría para potenciar y mejorar la gestión integral del riesgo con una visión *Enterprise Risk Management* (ERM).

El objetivo de este documento es constituir una Guía de Buenas Prácticas que ofrezca a los auditores internos un doble enfoque: disponer de un marco teórico para comprender el papel que Auditoría Interna puede asumir en la gestión de riesgos, y una metodología práctica para evaluar y reforzar el control sobre la gestión de riesgos en cualquier tipo de compañía, salvaguardando la independencia y objetividad en el cumplimiento de su trabajo.

Desde el Instituto agradecemos a la comisión su esfuerzo compartiendo su conocimiento, que ha resultado en un documento que será de gran utilidad para los auditores internos.

Instituto de Auditores Internos de España

Índice

Introducción

La gestión integral del riesgo permite identificar los riesgos y oportunidades y gestionarlos para fortalecer la capacidad de la organización para crear y preservar valor.

El objetivo fundamental de cualquier compañía es generar valor para sus grupos de interés, así como garantizar la protección de éste, una vez creado.

Para lograrlo, las compañías se enfrentan a eventos futuros cuya posible materialización y consecuencias son, a priori, desconocidas. Estas incertidumbres pueden manifestarse en forma de riesgos (consecuencias negativas) y oportunidades (consecuencias positivas), que reducen o generan valor, respectivamente.

Ante este desafío, el consejo de administración (u órgano de gobierno) y la alta dirección (o junta directiva, en el caso de organizaciones sin ánimo de lucro) deben determinar la cantidad y tipo de incertidumbres que están preparados para asumir, de cara a conseguir ese objetivo fundamental.

Mientras que la generación del valor se produce cuando el beneficio excede a los recursos utilizados, la preservación de éste ocurre cuando el valor creado se mantiene en el tiempo, mediante la explotación de las ventajas competitivas de la compañía (calidad superior, eficiencia operativa, satisfacción del cliente, etc.). El valor puede reducirse cuando el liderazgo de la entidad no se mantiene debido, por ejemplo, a una inadecuada elección de la estrategia, a su incorrecta ejecución o a una incorrecta gestión de las incertidumbres que afronta.

La gestión integral del riesgo es la vía por la que la alta dirección puede resolver efectivamente estas incertidumbres (riesgos y oportunidades), de tal modo que se fortalezca la capacidad de la entidad para crear y preservar valor. Para ello, la dirección debe comprender los conceptos de riesgo y de oportunidad y, además, entender los riesgos específicos (y oportunidades) a los que se enfrenta la compañía, con objeto de establecer un marco adecuado para mitigar (y potenciar) su impacto en los objetivos y optimizar su probabilidad de ocurrencia.

Gestión de Riesgos y Auditoría Interna

EVOLUCIÓN DE LA GESTIÓN DE RIESGOS

Es una disciplina que ha evolucionado desde un enfoque reactivo, orientado a la protección de activos, a otro proactivo, centrado en la creación de valor.

En los años 70 del siglo XX, esta disciplina se centró, principalmente, en la transferencia del riesgo "puro" (consecuencias únicamente negativas) mediante pólizas de seguros. En los años 80, la gestión del riesgo financiero se priorizó en muchas empresas, incluidos bancos, entidades aseguradoras y empresas no financieras expuestas a las fluctuaciones de tasas de interés, tipos de cambio y precios de las materias primas. De esta forma, a través de la gestión del riesgo "especulativo" (consecuencias negativas y positivas) mediante el uso de derivados como instrumentos de cobertura contra el riesgo de mercado, se empezó a apreciar un cambio de mentalidad que se consolidó en los años 90, con el inicio de la gestión integral del riesgo.

Se apuntalaron las bases del control interno para la gestión de riesgos, por la introducción de conceptos como la coordinación de actividades de gestión de riesgos y la asignación de responsabilidades a los órganos de gobierno para supervisar esta actividad, fruto de nuevas regulaciones y mejores prácticas.

Por otro lado, esta coordinación habilitó la identificación y análisis del riesgo operacional (pérdidas potenciales originadas por fallos de los procesos, sistemas o personas) y se comenzaron a establecer métodos para gestionarlo de manera preventiva.

Los eventos significativos ocurridos en la primera década del siglo XXI (como los atentados terroristas del 11-S, la crisis financiera asiática o los escándalos de Enron y Worldcom) proporcionaron una nueva dimensión a los conceptos de volatilidad y riesgo. La crisis financiera de 2008 puso en evidencia, en primer lugar, importantes deficiencias en los procesos de control existentes; en segundo lugar, las dificultades del órgano de gobierno y la alta dirección para articular, medir y/o adherirse a un nivel de riesgo considerado aceptable para su compañía; y, por último, en otros casos, la falta de alineamiento entre los objetivos individuales y los objetivos de la entidad.

La gestión de riesgos ha evolucionado desde un enfoque reactivo, orientado a la protección de activos, a otro proactivo, centrado en la creación de valor.

En respuesta a estas situaciones y para evitar otras similares, distintas profesiones, entre ellas Auditoría Interna, han desarrollado y formalizado principios para la gestión integral del riesgo bajo el enfoque *Enterprise Risk Management* (ERM), que se caracteriza por:

- Ser una disciplina estratégica orientada a crear y proteger el valor, en beneficio de todos los grupos de interés de una compañía.
- Establecer una cultura única y coordinar, bajo criterios homogéneos, las actividades de gestión de riesgos de la entidad (capacidades y prácticas).
- Estar enfocada en el impacto que presentan las situaciones que se afrontan, sobre la consecución de los objetivos de la compañía.
- Reconocer el efecto positivo de la incertidumbre (oportunidad), y no solo el negativo.
- Considerar todas las fuentes de riesgo y emplear un enfoque de cartera para compensar las diferentes posiciones de riesgo.

EVOLUCIÓN DE LAS MEJORES PRÁCTICAS DE GOBIERNO CORPORATIVO

El enfoque ERM busca establecer una cultura única y coordinar, bajo criterios homogéneos, las actividades de gestión de riesgos.

Durante las últimas tres décadas han surgido regulaciones y marcos de mejores prácticas en materia de gobierno corporativo, recibiendo una especial atención el marco normativo relacionado con la gobernanza y las responsabilidades de supervisión asignadas al órgano de gobierno de las compañías.

A este respecto, caben destacar los siguientes marcos de referencia:

- *Informe King en Gobierno Corporativo* (Sudáfrica, 1991).
- *Informe del Comité Cadbury* (Reino Unido, 1992).
- Documento *COSO Control Interno - Marco Integrado* (EEUU, 1992) por el *Committee of Sponsoring Organizations* (en adelante, COSO).

La entrada en vigor de la Ley Sarbanes-Oxley de EEUU, en 2002, introdujo las directrices para reformar y fortalecer los sistemas de control interno sobre la información financiera, y amplió las responsabilidades del órgano de gobierno y la alta dirección, incluyendo la obligatoriedad de crear una Comisión de Auditoría para muchas entidades.

El marco normativo ha evolucionado a partir de la introducción de mejores prácticas bajo el principio de "cumplir o explicar" que, en algunos casos, se han incorporado a la legislación local, convirtiéndose en estándares de obligado cumplimiento.

En España, el primer código de buen gobierno se publicó en 1998 con el nombre de *Informe*

Olivencia. Hoy, la referencia de buenas prácticas vigente se recoge en el *Código de Buen Gobierno de las Sociedades Cotizadas,* que se complementa con la *Guía Técnica sobre comisiones de Auditoría de Entidades de Interés Público.* En la legislación española no existe una norma que consolide todos los aspectos de gobierno corporativo, sino que se rige principalmente por lo previsto en la Ley de Sociedades de Capital, la Ley del Mercado de Valores y la Ley de Economía Sostenible.

Esta evolución normativa y de mejores prácticas se caracteriza por la creciente asignación al órgano de gobierno de la responsabilidad de supervisar la Auditoría Interna y la eficacia del control interno y de la gestión integral de riesgos de la entidad.

MARCOS DE REFERENCIA PARA LA GESTIÓN DE RIESGOS

Hay diversos estándares que proponen mejores prácticas para la implementación del enfoque ERM (criterios, metodologías, arquitecturas, procesos, etc.). En general, estos marcos de gestión de riesgos pueden agruparse en tres bloques, conforme al enfoque estratégico con el que fueron diseñados:

- Consecución de los objetivos de la compañía.
- Adhesión a objetivos de control y/o de cumplimiento.
- Cumplimiento con requerimientos regulatorios.

A continuación, se resumen los marcos de gestión de riesgos más utilizados, entre los que destacan COSO-ERM y la norma ISO 31000.

ENFOQUE ESTRATÉGICO	DESCRIPCIÓN	ESTÁNDAR/MARCO
Objetivos de la compañía	Diseñado para mejorar la capacidad de la compañía para cumplir o superar sus objetivos a través de una mejor toma de decisiones y actividades que atienden las incertidumbres clave.	· ISO 31000 · BS 31000 · COSO-ERM · FERMA
Objetivos de control y/o cumplimiento	Busca asegurar la transferencia u otra mitigación de riesgos, principalmente, a través de objetivos y actividades de control y/o de cumplimiento; a menudo basándose en información histórica.	· OCEG "Libro Rojo" · COSO-ERM
Regulatorio	Usado cuando una compañía debe aplicar un estándar y/o práctica diseñada y proporcionar evidencias con el fin de cumplir con requerimientos regulatorios.	· Solvencia · Basilea

Fuente: Adaptado de "Risk and Insurance Management Society, Inc. An overview of widely used risk management standards and guidelines, 2011."

Estos estándares comparten las siguientes características fundamentales:

- Implementación de un enfoque a nivel de empresa, con apoyo a nivel ejecutivo.
- Definición formal de la estructura organizativa y asignación de responsabilidades.
- Establecimiento y comunicación de los objetivos y actividades del proceso de gestión.

- Entendimiento y asignación de responsabilidad en la definición del apetito de riesgo y de los límites de tolerancia aceptables.
- Instauración de procesos estructurados y documentados de identificación, gestión, supervisión y *reporting* de riesgos.

En la práctica, las compañías deben seleccionar el estándar de referencia basándose en los objetivos establecidos y la estrategia de la gestión de riesgos seleccionada para su consecución. Desde la perspectiva de Auditoría Interna, estos estándares constituyen las herramientas para diagnosticar el alineamiento con las mejores prácticas de gestión de riesgos y promover iniciativas de mejora.

El Marco COSO-ERM 2017

En 2004, COSO publicó el estándar *Gestión de Riesgos Corporativos - Marco Integrado,* que amplió el concepto de control interno introducido en 1992, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral del riesgo.

En 2017, respondiendo a mayores exigencias del entorno y a los avances en gestión de riesgos, COSO publicó la actualización del marco bajo el nombre de *Gestión del Riesgo Empresarial – Integrando Estrategia y Desempeño* (COSO-ERM 2017). En esta revisión se reconoce la creciente importancia de la conexión entre riesgo, estrategia y desempeño, enfatizando la integración de la gestión de riesgos no solo en la gestión del negocio y en el control interno, sino también en la creación de valor.

En este marco actualizado, COSO introduce cinco componentes interrelacionados que desagrega en 20 principios:

Fuente: *Coso. Gestión del Riesgo Empresarial. Integrando Estrategia y Desempeño* (2017).

EL MARCO NORMATIVO DE AUDITORÍA INTERNA

Las *Normas Internacionales para la Práctica Profesional de la Auditoría Interna* (Normas) son el marco normativo de la profesión, establecido por el Instituto de Auditores Internos (IAI). Su elaboración y revisión obedece a un proceso de mejora continua, estando vigente su última actualización desde enero de 2017.

Dentro de este marco, Auditoría Interna se define como *"una actividad independiente y objetiva de aseguramiento y consultoría diseñada para agregar valor y mejorar las operaciones de una organización [...]"*, habilitando a Auditoría Interna como prestadora tanto de servicios de aseguramiento como de consultoría.

Los **servicios de aseguramiento** comprenden la evaluación objetiva de las evidencias para emitir conclusiones y recomendaciones con una visión independiente, a partir de la definición de la naturaleza y alcance del trabajo efectuada por Auditoría Interna.

Los **servicios de consultoría** son la respuesta de Auditoría Interna a la solicitud de un cliente, y la naturaleza y alcance del trabajo se definen de común acuerdo, sin que el auditor asuma responsabilidades de gestión.

Indistintamente del tipo de servicios que Auditoría Interna proporcione, las Normas son muy claras al establecer que *"la actividad de auditoría interna debe de ser independiente y los auditores internos deben ser objetivos en el cumplimiento de su trabajo"* (Norma 1100). A este respecto, las Normas reconocen la existencia de impedimentos potenciales a nivel individual y organizativo que pueden afectar esta objetividad e independencia, como *"el conflicto de intereses personales; limitaciones al alcance; restricciones al acceso a los registros, al personal y a los bienes; y limitaciones de recursos (fondos)"*.

El Modelo de las Tres Líneas

La implementación de este modelo es una alternativa por la que las compañías solventan estos impedimentos y garantizan la **objetividad e independencia** requerida por Auditoría Interna.

Con la publicación en 2013 del documento *La Tres Líneas de Defensa en Gestión de Riesgos y Control Efectivo*, el Instituto de Auditores Internos reconoció que la gestión de riesgos era más robusta cuando las tres líneas se encontraban separadas y claramente definidas; por lo que estas líneas deberían existir, de alguna manera, en todas las compañías.

El modelo proponía tres niveles de actividad para garantizar que la gestión y la supervisión de los riesgos se realiza de forma eficaz. Se proponía que la primera línea de defensa tuviera la responsabilidad de identificar, analizar y mitigar los riesgos de la operativa cotidiana; y que la segunda línea facilitara la definición e implementación de los procesos de gestión de riesgos y supervisara su adecuada ejecución. Las responsabilidades de la primera línea se orientaban a procesos o departamentos específicos, mientras que la responsabilidad de la segunda línea era de carácter transversal. Las funciones que proporcionan aseguramiento independiente sobre procesos y controles, tal como Auditoría Interna, constituirían la tercera línea de defensa.

En julio de 2020, el Instituto de Auditores Internos Global publicó la actualización de este

La gestión de riesgos es más robusta cuando las Tres Líneas están claramente definidas y separadas, aunque interactúen coordinadamente entre sí.

modelo, en la que se introducen importantes **novedades:**

- El Modelo de las Tres Líneas (M3L) se orienta a la consecución de objetivos, promoviendo no solo la protección de valor (objetivo fundamental del Modelo de las Tres Líneas de Defensa), sino también a la creación de valor.

- Propone que los roles de la primera[1] y segunda[2] líneas se ubiquen bajo el paraguas de la alta dirección, mientras que los roles de tercera línea (en esencia, Auditoría Interna[3]) se sitúen exactamente al mismo nivel que aquella.

Las Tres Líneas deben colaborar para que las cuestiones operativas, financieras, de riesgo y de aseguramiento estén alineadas.

Mediante la adopción e implantación de los seis principios fundamentales del Modelo, los roles de cada línea deben actuar coordinadamente, colaborando entre ellos y fomentando una comunicación regular y efectiva para que las cuestiones operativas, financieras, de riesgo y de aseguramiento estén alineadas entre sí y, en último término, también lo estén con las expectativas de los *stakeholders* de la entidad.

Se trata de un encargo para la compañía en su conjunto: conseguir que todos los roles trabajen en la misma dirección y que ésta sea la adecuada para obtener unos resultados acordes a los objetivos que se hayan propuesto. Todo ello, sobre el pilar básico de garantizar la independencia y objetividad del auditor interno.

Fuente: El Modelo de las Tres Líneas del IAI 2020; una actualización de las tres líneas de defensa. The IAI Global (2020)

1. Funciones relacionadas con los productos/servicios que la entidad entrega a sus clientes *(front house y back office).*
2. Funciones que ofrecen soporte en el proceso global de gestión del riesgo de la entidad (ERM, Compliance, etc).
3. Si bien tienen cabida, entre otros, roles como los de inspección o investigación, formando parte de Auditoría Interna o funcionando de manera separada.

El rol de Auditoría Interna en la Gestión de Riesgos

La regulación y las mejores prácticas actuales requieren que el órgano de gobierno y la alta dirección asuman la responsabilidad de establecer y mantener un sistema de gestión de riesgos eficaz, tanto a nivel estratégico como operativo. Para lograrlo, las compañías suelen delegar la definición, implementación y monitorización de la gestión de riesgos a una función de Segunda Línea y el aseguramiento a Auditoría Interna, como Tercera Línea.

El papel de Auditoría Interna en la gestión de riesgos lo formalizó el Instituto de Auditores Internos en el año 2004 con la publicación del documento *El papel de Auditoría Interna en la gestión de riesgos ERM,* que establece que *"el rol principal de Auditoría Interna en lo que respecta a ERM es proporcionar aseguramiento objetivo al consejo de administración respecto de la eficacia de las actividades ERM para ayudar a garantizar que los riesgos clave del negocio se están gestionando correctamente y que el sistema de control interno está operando eficazmente".*

A este respecto, la Norma 2120 establece que *"la actividad de auditoría interna debe evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos".* Es decir, que Auditoría Interna debe **proporcionar aseguramiento** sobre el alineamiento de los objetivos de la compañía con su misión y de que, tanto el diseño como el funcionamiento de los procesos de gestión de riesgos (identificación, análisis, gestión y *reporting)*, son eficaces.

Las Normas tienen previsto que Auditoría Interna pueda prestar **servicios adicionales de consultoría** para fortalecer los procesos de gestión de riesgos con un enfoque ERM, pero también establecen cuáles son las actividades que Auditoría Interna nunca debería asumir. De esta forma, se posibilita que las compañías que requieran este tipo de apoyo, típicamente por limitaciones de recursos, puedan hacerlo.

Auditoría Interna proporciona aseguramiento al consejo sobre la eficacia de las actividades ERM para garantizar que los riesgos clave se están gestionando correctamente.

Marco de Relaciones entre Gestión de Riesgos y Auditoría Interna

Auditoría Interna está cualificada para actuar como promotor, e incluso, como líder de un proyecto de ERM, por su amplio conocimiento de la compañía y sus procesos, su posicionamiento organizativo y su *expertise* respecto de las interconexiones entre riesgos y gobernanza.

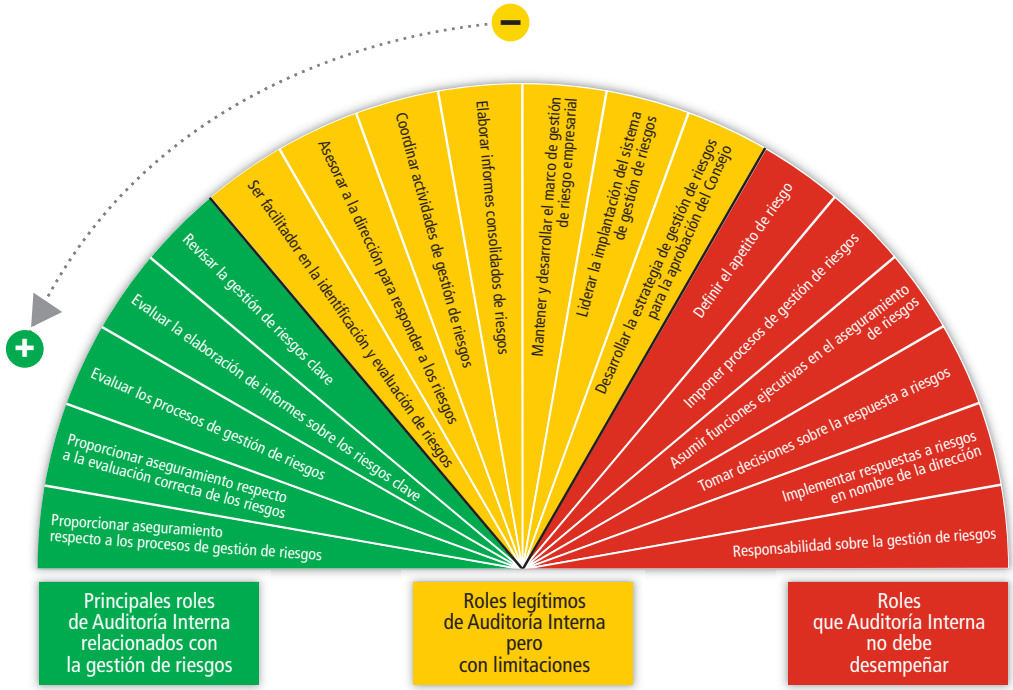
Sin embargo, este rol solo debe desempeñarse cuando Auditoría Interna no asuma la responsabilidad de gestionar los riesgos, actividad que corresponde, en exclusiva, a los actores de la Primera Línea.

COMPETENCIAS DE AUITORÍA INTERNA EN GESTIÓN DE RIESGOS

FORTALEZAS	DEBILIDADES
Independencia y objetividad como requerimiento fundamental de la actividad.	Posibles limitaciones derivadas del Modelos de las 3 líneas.
Altos estándares profesionales de ética.	La independencia puede ser un impedimento.
Amplio conocimiento de la organización y sus procesos.	Posicionamiento organizativo puede aislar del resto de la organización.
Expertise en interconexión entre riesgos y gobierno.	No siempre se tiene la *big picture*.
Excelentes capacidades de análisis y comunicación.	Demasiado enfoque en controles (protección de valor) y muy limitado en estrategia (creación de valor).
Desarrollado escepticismo profesional que cuestiona lo "normal".	Posible carencia de experiencia práctica en el negocio.

Fuente: Elaboración propia.

En las primeras etapas de desarrollo del proceso de gestión de riesgos, Auditoría Interna puede apoyar a la compañía sirviendo como catalizador de la iniciativa, asistiendo a la Segunda Línea o asumiendo algunas de sus actividades. Conforme la madurez de la gestión de riesgos aumente, este rol deberá ir disminuyendo y su papel como prestador de servicios de aseguramiento o de Tercera Línea será consolidado.



Fuente: Adaptado de *The Institute of Internal Auditors. The Role of Internal Audit in Enterprise-wide Risk Management,* 2004.

Cuando Auditoría Interna asume un papel activo en las actividades de gestión de riesgos, su objetividad e independencia para identificar y reportar deficiencias de los procesos de gestión de riesgos podría verse comprometida. La publicación en 2016 del documento *Guía Práctica - Auditoría Interna y la Segunda Línea de Defensa* establece unos principios de actuación para mantener la independencia y objetividad de Auditoría Interna mientras realiza actividades de Segunda Línea. En concreto, en este documento se establece que:

- **El Director de Auditoría Interna tiene la responsabilidad de proteger la independencia y la objetividad de la auditoría.** Por lo tanto, si la asunción de las responsabilidades de Segunda Línea pone en riesgo una, otra o ambas, el director deberá comunicarlo a la alta dirección y al órgano de gobierno y corroborar su entendimiento y aceptación de dicho riesgo.
- **Se deberán establecer medidas de salvaguarda y controles adicionales** para proteger esa independencia y objetividad, así como verificar periódicamente qué características existen en el trabajo de Auditoría Interna. Cuando estas salvaguardas no sean posibles y se quiera mantener la independencia y objetividad, las responsabilidades de Segunda Línea se asignarán a otra área de la compañía, o bien se externalizarán.
- Si la asunción de responsabilidades de Segunda Línea por parte de Auditoría Interna es **temporal,** se elaborará e implementará un plan de transición y reasignación de responsabilidades, acordado con el órgano de gobierno y la alta dirección. Si la integración de responsabilidades es **permanente,** éstas deberán ser documentadas en la Norma/Estatuto de Auditoría Interna y aprobadas por la Comisión de Auditoría.

Los conceptos de independencia y objetividad permiten definir, con relativa facilidad, la frontera que divide las responsabilidades de la Tercera Línea y las que corresponden a las otras dos líneas. A continuación, se enumeran algunas actividades de gestión de riesgos que la segunda y la tercera línea suelen asumir.

Si Auditoría Interna asume un papel activo en la gestión de riesgos, su objetividad e independencia para identificar y reportar deficiencias podría verse comprometida.

SEGUNDA LÍNEA · Gestión de Riesgos	TERCERA LÍNEA · Auditoría Interna
Desarrollo y mejora continua del marco de gestión y control de riesgos.	Desarrollar una evaluación independiente respecto de la idoneidad y eficacia del diseño del marco de gestión de riesgos.
Implementar el marco de gestión eficaz de riesgos.	Auditar la implementación del marco de gestión de riesgos.
Asesorar a la dirección respecto al análisis coste-beneficio de la integración de la gestión de riesgos en las operaciones de negocios y sus responsabilidades para hacerla funcionar.	Actuar como revisor independiente para dar aseguramiento razonable respecto de la capacidad y desempeño de la dirección en gestión de riesgos y la vinculación con los objetivos estratégicos.
Asesorar respecto de la asignación de responsabilidades sobre los riesgos, controles y tareas fundamentales.	Auditar si las funciones clave responsables cumplen con sus tareas y responsabilidades y están capacitadas para ejercer las mismas.
Proporcionar información de la situación del proceso de la gestión de riesgos y el desempeño a la Comisión de Auditoría y al Comité de Riesgos.	Dar aseguramiento independiente respecto de la credibilidad y fiabilidad de la información de gestión de riesgos presentada a la Comisión de Auditoría y al Comité de Riesgos.
Asesorar al Comité de Riesgos en relación con actuaciones de gestión de riesgos en curso y destacar riesgos no mitigados que pongan en peligro el patrimonio de la empresa.	Dar aseguramiento respecto de las competencias de la dirección para identificar y atender adecuadamente riesgos vigentes y riesgos no mitigados.
Facilitar el estatus de las prioridades de riesgos y la cobertura de auditoría de estas prioridades.	Dar aseguramiento respecto del alcance y priorización de los riesgos.
Asesorar al consejo de administración y al Comité de Riesgos al respecto del reporting de riesgos interno y externo.	Preparar evaluaciones independientes de los procesos de reporting.

Fuente: Adaptado de *Broadleaf. Relationship between internal audit and risk management,* 2018.

Independientemente del rol que asuma Auditoría Interna, se deben tener en cuenta los principios establecidos en la **Norma 1210 - *Aptitud.*** Esto significa que Auditoría Interna debe reunir u obtener los conocimientos y competencias necesarias para cumplir con sus responsabilidades.

En particular, la publicación *El papel de auditoría interna en la gestión de riesgos ERM* establece que *"cualquier auditor que no pueda demostrar que tiene las aptitudes técnicas y el conocimiento no debería emprender trabajos en el área de gestión de riesgos".* De hecho, esta restricción se eleva al máximo nivel, ya que se establece que *"el Director de Auditoría Interna no deberá prestar servicios de consultoría en este área si las aptitudes técnicas y conocimiento no están disponibles dentro de la función de Auditoría Interna y no pueden ser obtenidas de otras fuentes".*

El alcance de los servicios prestados por Auditoría Interna será contingente a las capacidades existentes y deberá ser formalizado en la norma y aprobado por el órgano competente.

Por tanto, como en cualquier trabajo de auditoría, el alcance de los servicios prestados por Auditoría Interna será contingente a las capacidades existentes y deberá ser formalizado en la norma o estatuto correspondiente y aprobado por el Consejo de Administración a través de la Comisión de Auditoría.

Es necesario hacer una última referencia al concepto de aseguramiento combinado o integrado, que proporcionan las diferentes funciones de aseguramiento presentes en las compañías y, en concreto, a las labores específicas de Gestión de Riesgos y de Auditoría Interna.

Tal y como pone de relevancia el *Marco Internacional para la Práctica Profesional de la Auditoría Interna,* a través de la **Norma 2050 - *Coordinación y confianza,*** *"el DAI debería compartir información, coordinar actividades y considerar la posibilidad de confiar en el trabajo de otros proveedores internos y externos de aseguramiento y consultoría para asegurar una cobertura adecuada y minimizar la duplicación de esfuerzos".*

El nivel de madurez de estas dos funciones determinará las acciones de coordinación y de confianza mutua de las que habla la citada Norma, necesarias para alcanzar ese último objetivo de proporcionar una visión integral y holística de la eficacia del proceso de gestión de riesgos que se encuentra presente en la compañía.

Por medio de actividades frecuentes y eficaces de colaboración, comunicación e intercambio de información entre las áreas de Gestión de Riesgos y de Auditoría Interna, se optimizará la supervisión del gobierno de los riesgos y la eficiencia de los controles adoptados, a la vez que se facilitará y hará más fluida la comunicación con la Comisión de Auditoría y otros órganos de control, en materia de los riesgos que la compañía afronta y/o se encuentra dispuesta a asumir.

El Aseguramiento de la Gestión de Riesgos

El órgano de gobierno de una entidad es el máximo responsable de asegurar que se cumplen las siguientes condiciones:

- Que existe un sistema de gestión de riesgos adecuado.
- Que los procesos de gestión de riesgos implantados funcionan de manera eficaz.
- Que los principales riesgos a los que se enfrenta la compañía se gestionan de acuerdo con el apetito de riesgo definido para apoyar la consecución de sus objetivos estratégicos.

Asegurar el cumplimiento de estas tres condiciones se logra desde una doble perspectiva: delegando a la alta dirección de la entidad, por parte del órgano de gobierno, la definición e implementación del marco de gestión de riesgos, así como el seguimiento de su ejecución; y complementando el primer nivel de aseguramiento mediante una evaluación, objetiva e independiente, llevada a cabo por Auditoría Interna sobre todo ese proceso. Para ello, deberá proporcionarse un nivel de seguridad razonable sobre los siguientes elementos:

- Existen procesos de gestión de riesgos acordes con las necesidades estratégicas y el modelo de negocios de la compañía.
- Estos procesos han sido implementados correctamente y sus elementos son adecuados y suficientes.
- Existen procesos y sistemas para asegurar que todos los riesgos materiales han sido identificados, evaluados y son gestionados eficazmente.
- Los controles clave que soportan estos procesos son adecuados y efectivos.
- Existen procesos de *reporting* para comunicar la efectividad y el estatus del sistema de gestión de riesgos al órgano de gobierno y a la alta dirección.

Para proporcionar este aseguramiento existen tres enfoques distintos, tal y como constan en el documento *Assessing the Adequacy of Risk Management,* publicado por el IIA Global en el 2010:

- **Modelo de Madurez.** Se basa en el principio de que la calidad de la gestión de riesgos de la compañía debe incrementarse con el paso del tiempo. No se emite ningún juicio sobre si el estado de la gestión de riesgos es bueno o malo, solo se establece en dónde se encuentra respecto de una escala de madurez de referencia; de tal forma que el órgano de gobierno y la alta dirección pueden definir el estado deseado e impulsar las iniciativas de mejora necesarias.
- **Enfoque de Elementos del Proceso.** Consiste, fundamentalmente, en verificar si las actividades de gestión de riesgos existentes cumplen con los estándares establecidos conforme a cada uno de los elementos del marco de referencia de gestión de riesgos seleccionado.
- **Enfoque de Principios.** Se basa en el concepto de que la gestión de riesgos es efectiva, siempre y cuando se satisfaga un conjunto mínimo de principios o características de un marco de referencia efectivo.

El punto de partida para proporcionar aseguramiento es realizar un diagnóstico del estatus de la gestión de riesgos existente y un gap analysis respecto de las mejores prácticas.

El punto de partida para proporcionar aseguramiento conforme a cualquiera de estos tres enfoques es realizar un diagnóstico del estatus de la gestión de riesgos existente en la compañía y un *gap analysis* respecto de las mejores prácticas, tal y como se indica a continuación:

- Seleccionar el marco de referencia respecto del cual se analizará el diseño, la implementación y la ejecución del programa de gestión de riesgos.
- Basándose en el marco de referencia seleccionado, definir el estado "óptimo" deseado, responsabilidad del órgano de gobierno.
- Realizar el diagnóstico para identificar debilidades y fortalezas de ERM.
- La alta dirección debe definir e implementar las iniciativas que impulsen la gestión de riesgos al estado óptimo definido, para lo que puede apoyarse en el conocimiento de los agentes de Segunda y/o Tercera Línea.

La calidad del diagnóstico dependerá del nivel de conocimiento en gestión de riesgos del agente que lo realice, pudiendo ser de la Primera, Segunda o Tercera Línea. Además, la calidad del aseguramiento dependerá directamente del grado de objetividad e independencia de la función que realice el diagnóstico.

Para proporcionar aseguramiento independiente al órgano de gobierno y a la alta dirección sobre la gestión de riesgos, el Marco COSO-ERM 2017 ofrece *"criterios para realizar un diagnóstico para determinar si la cultura, las capacidades y las prácticas de ERM conjuntamente gestionan los riesgos de no lograr la estrategia de la entidad y objetivos empresariales que la apoyan"*.

Si bien es cierto que COSO ofrece estos criterios sobre qué elementos deben existir, no describe el proceso de evaluación de su efectividad a llevar a cabo. Por ello, a continuación, proponemos una metodología para implementar el enfoque de Modelo de Madurez, que se materializa a través de una herramienta Excel que acompaña a esta Guía de Buena Prácticas.

ASEGURAMIENTO SOBRE LA GESTIÓN DE RIESGOS: ENFOQUE DEL MODELO DE MADUREZ

El grado de madurez en la gestión de riesgos representa el estatus de diversos factores que, en su conjunto, son un indicador de la capacidad que tiene la compañía para gestionar los riesgos que amenazan la consecución de sus objetivos establecidos.

Conforme mejora el nivel de competencia en gestión de riesgos de una entidad, la posibilidad de gestionar todo tipo de riesgos también aumenta. La premisa fundamental sobre la que se construye cualquier modelo de madurez reside en que un nivel bajo de madurez lleva aparejado una probabilidad baja de consecución de los objetivos establecidos, mientras que un alto grado de madurez implica una mayor probabilidad de éxito.

Por lo tanto, las iniciativas de fortalecimiento de la gestión de riesgos que puedan surgir del diagnóstico de aseguramiento dependerán de la madurez de los procesos existentes.

Escalas de Madurez

A pesar de que las metodologías más frecuentes establecen diferentes escalas para

mapear el grado de madurez de la gestión de riesgos, todas muestran un gran alineamiento entre sí. En general, parten de una gestión de riesgos que pone énfasis en la protección de los activos, evolucionando hacia una gestión proactiva de una cartera de riesgos, donde el riesgo no solo se considera en términos de pérdidas potenciales, sino como una oportunidad para crear valor y desarrollar una ventaja competitiva.

Esta Guía de Buenas Prácticas no se pronuncia a favor del uso de una escala de madurez en particular, sino que invita a utilizar la escala de madurez que se considere más adecuada, teniendo en cuenta su nivel de conocimiento y la cultura y procesos existentes en cada compañía.

Seleccionada la escala, es importante utilizarla de forma consistente para asegurar la homogeneidad de los criterios de diagnóstico e interpretación de resultados.

La siguiente tabla muestra una escala de madurez de referencia.

ENFOQUE REACTIVO
Cumplimiento y Protección de Valor

MADUREZ DE LA GESTIÓN DE RIESGOS

ENFOQUE PROACTIVO
Estrategia y Creación de Valor

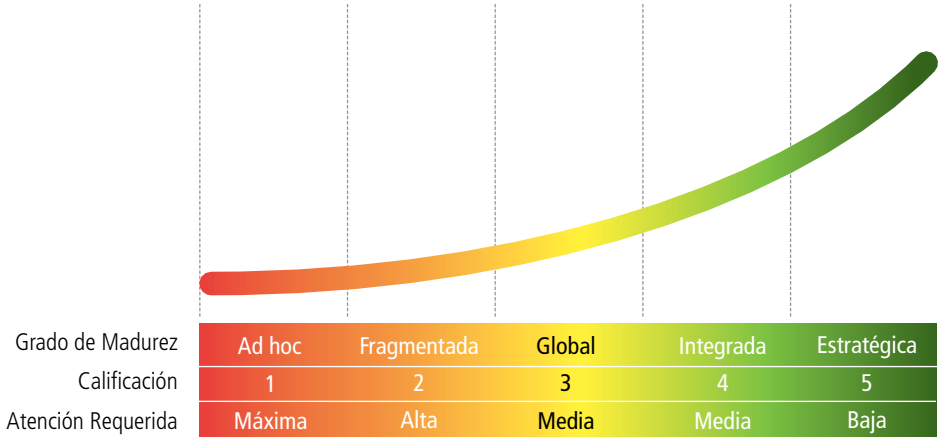
AD HOC	Existen actividades básicas para administrar el riesgo y se llevan a cabo de forma aislada o en silos.	El personal no es consciente de los riesgos a gestionar y únicamente reacciona a los eventos y riesgos conforme se materializan.	La compañía reconoce la necesidad, pero no hay procesos estandarizados. Dependencia en los individuos; falta de capacidad institucional.	El enfoque para determinar los requisitos de control interno y gestión de riesgos es *ad hoc* y desorganizado, sin actividades de comunicación ni de monitorización.
FRAGMENTADA	Se realizan actividades para mejorar la eficacia para estabilizar los procesos y ampliar el alcance.	La mayoría de las actividades de gestión de riesgos las realiza un reducido número de especialistas pertenecientes a las áreas clave de riesgo.	Proceso establecido; sin embargo, predomina la dependencia en las personas.	Existen controles, pero no están documentados. Su funcionamiento depende del conocimiento y la motivación de los individuos.
GLOBAL	Los procesos operativos han alcanzado un estado estable y ahora son efectivos, repetibles y sostenibles.	Las unidades de negocio se coordinan para ciertos tipos de riesgos comunes, pero la exposición al riesgo se mide por separado	Políticas, procesos y estándares definidos e institucionalizados.	Existen controles y están adecuadamente documentados. La efectividad operativa se evalúa periódicamente. Sin embargo, el proceso de evaluación no está documentado.
INTEGRADA	Se ejecutan iniciativas transformadoras para mejorar la conexión entre la gestión de riesgos y los procesos de negocio.	Los riesgos se gestionan como una cartera, según los tipos de riesgos y todas las unidades del negocio.	Riesgo medido y administrado cuantitativamente y agregado en toda la empresa.	Existe un entorno de control interno y de gestión de riesgos efectivo. La evaluación de controles formal y documentada se lleva a cabo frecuentemente. Muchos controles son automatizados con el uso táctico de la tecnología.
ESTRATÉGICA	Los procesos están optimizados y equilibrados por el contexto empresarial y las prioridades del riesgo.	La gestión de riesgos se considera una ventaja competitiva utilizada para identificar y procurar oportunidades de negocio de interés para la compañía.	La gestión de riesgos está integrada en todas las actividades a través de todos los tipos de riesgos y todas las unidades de negocio.	Existe un programa integral de control interno y gestión de riesgos a nivel de empresa. La evaluación del entorno de control es continua, basándose en autoevaluaciones, gap análisis y análisis de causa raíz.

Una gestión de riesgos estratégica tiene gran alcance y máxima madurez y está incluida en los procesos estratégicos de creación de valor de la compañía.

Su lectura, de arriba hacia abajo, indica la evolución lógica de una función de gestión de riesgos. El estadio de madurez más incipiente se representa por una gestión de riesgos *ad hoc* (con una calificación de 1 sobre 5) y se caracteriza por ser una gestión de riesgos reactiva, con la presencia de silos de información y sin unos criterios de aplicación sistemáticos.

Según se avanza hacia la derecha, en cada fase se incorporan elementos que profesionalizan la gestión de riesgos de la entidad, hasta llegar al estadio que presenta la mayor madurez: una gestión de riesgos catalogada como "Estratégica" (con una calificación de 5 sobre 5). Esta última fase se caracteriza por un mayor alcance, presencia y relevancia de las actividades de gestión de riesgos, dando como resultado la inclusión de esta disciplina en los procesos estratégicos de creación de valor de la compañía.

En base a esta escala propuesta, los Componentes y Principios evaluados que presenten un menor grado de madurez requerirán de una mayor atención (y viceversa), según se resume en el siguiente gráfico.



Fuente: Elaboración propia.

Metodología Propuesta

Se propone realizar un diagnóstico en formato de cuestionario, mediante una herramienta Excel que acompaña a esta Guía de Buenas Prácticas[4].

Para cada uno de los 20 principios del marco COSO-ERM 2017 se plantea una serie de cuestiones o "Puntos de Reflexión", que se deben responder asignando una nota que refleje el grado de madurez existente en la compañía (escala de 1-5, de menor a mayor madurez), tomando como referencia el estadio dentro de la escala de madurez elegida que mejor refleje las capacidades de gestión de los riesgos existentes (por ejemplo, ad-hoc, fragmentada, etc.).

4. Descarga el excel aquí: bit.ly/35J76kG

EVALUACIÓN DE LOS COMPONENTES DE LA GESTIÓN DE RIESGOS

Componente 1 – Gobierno y Cultura

Según el Marco COSO ERM 2017, *"el Gobierno y la cultura forman juntos una base para el resto de componentes de la gestión de riesgos corporativos. El gobierno establece el tono de la entidad, reforzando la importancia de la gestión integral del riesgo y estableciendo las responsabilidades de supervisión para ello. La cultura se refleja en el proceso de toma de decisiones".*

Para obtener una evaluación de utilidad sobre *Gobierno y Cultura,* se proponen los siguientes puntos de reflexión asociados a cada uno de los principios que están contemplados en este componente de una gestión de riesgos eficaz.

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
1. Supervisión de riesgos a través del consejo de administración	· ¿El Reglamento del consejo de administración establece sus competencias en materia de supervisión de gestión de riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Los miembros del consejo de administración reciben formación personalizada para cumplir con sus deberes de supervisión de la gestión de riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Existe una política de gestión de riesgos, aprobada por el consejo de administración, donde se establecen los principales roles, responsabilidades y competencias?	❑ ❑ ❑ ❑ ❑
	· ¿La política de gestión de riesgos es consistente con otros marcos relacionados (p. ej: seguridad, calidad, cumplimiento, etc.)?	❑ ❑ ❑ ❑ ❑
2. Establece estructuras operativas	· ¿La compañía ha articulado un marco formal de gestión de riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿El marco es consistente con otros marcos relacionados (p.ej.: seguridad, calidad, cumplimiento, etc.)?	❑ ❑ ❑ ❑ ❑
	· ¿El marco de gestión de riesgos se comunica ampliamente a través de la compañía?	❑ ❑ ❑ ❑ ❑
	· ¿Están claramente establecidos los flujos de aprobación y reporte en la gestión de riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Existe una función de gestión de riesgos independiente de la gestión?	❑ ❑ ❑ ❑ ❑
	· ¿Están claramente identificados los agentes de 1ª, 2ª y 3ª Línea en las principales áreas de la compañía?	❑ ❑ ❑ ❑ ❑
	· ¿Existe un Comité de Riesgos o se tratan dichos asuntos en alguno de los comités existentes?	❑ ❑ ❑ ❑ ❑
	· ¿Los responsables de riesgos de las áreas/líneas de negocio (p.ej. Seguridad, Cliente, RRHH, Legal, etc.) comparecen periódicamente en dicho comité?	❑ ❑ ❑ ❑ ❑
3. Define la cultura deseada	· ¿Existe un Código Ético?	❑ ❑ ❑ ❑ ❑
	· ¿La compañía personaliza su marco de gestión de riesgos basado en su cultura?	❑ ❑ ❑ ❑ ❑
	· ¿La política de riesgos refleja los principios de comportamiento esperado, conforme a lo previsto en el Código Ético de la compañía?	❑ ❑ ❑ ❑ ❑

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
4. Demuestra compromiso con los valores clave	· ¿Se ponen a disposición del conocimiento público, tanto interno como externo, los principales valores de la compañía?	❑ ❑ ❑ ❑ ❑
	· ¿Demuestra la alta dirección, con su comportamiento, su compromiso con los valores de la compañía *(tone at the top)*?	❑ ❑ ❑ ❑ ❑
	· ¿Demuestra la alta dirección, con su comportamiento, su compromiso con ERM *(tone at the top)*?	❑ ❑ ❑ ❑ ❑
	· ¿Los miembros del Comité de Riesgos promueven activamente la cultura de gestión de riesgos entre el personal de sus áreas de responsabilidad?	❑ ❑ ❑ ❑ ❑
	· ¿El proceso de incorporación de nuevos empleados incorpora un módulo de culturización sobre riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Se realizan mediciones / evaluaciones de forma regular sobre el nivel de cultura de riesgos entre los empleados?	❑ ❑ ❑ ❑ ❑
5. Atrae, desarrolla, y retiene a profesionales capacitados	· ¿Existe un programa de gestión del talento?	❑ ❑ ❑ ❑ ❑
	· ¿Existe una política de la compañía, soportando su compromiso con el desarrollo de los empleados, un sistema de compensación justo, la diversidad y el respeto de los derechos humanos?	❑ ❑ ❑ ❑ ❑
	· ¿El personal de gestión de riesgos dispone de las habilidades y conocimiento necesario para realizar sus tareas?	❑ ❑ ❑ ❑ ❑
	· ¿Los objetivos del personal de gestión de riesgos están alineados con los de la función ERM?	❑ ❑ ❑ ❑ ❑
	· ¿Existe un plan de sucesión para los puestos clave de gestión de riesgos?	❑ ❑ ❑ ❑ ❑

Fuente: Elaboración propia a partir de *COSO ERM Integrating with Strategy and Performance (2017).*

Cada punto de reflexión se evaluará según la calificación 1 a 5 previamente indicada, en función del grado de presencia en la compañía que el auditor interno estime durante la realización del trabajo.

Componente 2 – Estrategia y Definición de Objetivos

Según define el Marco COSO ERM 2017, *"la gestión de riesgos corporativos se encuentra integrada en la planificación estratégica de la entidad mediante el proceso de establecimiento de la estrategia y el establecimiento de objetivos. Con un entendimiento del contexto del negocio, la compañía puede obtener una visión general de los factores internos y externos y sus efectos sobre el riesgo. Una compañía establece su apetito de riesgo de manera conjunta con su estrategia. Los objetivos de negocio permiten poner en práctica la estrategia y dar forma a las prioridades y operaciones diarias de la entidad".*

Para evaluar sobre *Estrategia y Definición de Objetivos,* se proponen los siguientes puntos de reflexión.

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
6. Analiza el contexto empresarial	· ¿Existe un Plan estratégico aprobado por el consejo de administración? · ¿El registro/inventario de riesgos refleja los factores internos y externos que puedan repercutir sobre los objetivos de la compañía (estratégicos, de operaciones, etc.)? · ¿Se analiza de forma sistemática la información externa para identificar los cambios relevantes en el contexto del negocio e identificar riesgos emergentes? · ¿Se analiza de forma sistemática la información interna para identificar los cambios relevantes en el contexto de negocio e identificar riesgos emergentes?	❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑
7. Define el apetito de riesgo	· ¿Existe una "declaración del apetito de riesgo" adecuadamente formalizada? · ¿Es competencia exclusiva del consejo de administración la definición del apetito de riesgo? · ¿Se promueve activamente que la alta dirección y los agentes clave ERM conozcan el apetito de riesgo de la compañía? · ¿Se considera el apetito de riesgo en los procesos de toma de decisiones? · ¿Se involucra al consejo de administración en la toma de decisiones que pudieran implicar incumplir con el apetito de riesgo establecido? · ¿Se monitoriza activamente el cumplimiento con el apetito de riesgo?	❑ ❑
8. Evalúa estrategias alternativas	· ¿La estrategia de la compañía está alineada con su misión, visión y valores? · En el proceso de planificación estratégica, ¿se evalúan estrategias alternativas, analizándose los riesgos y oportunidades asociados basándose en metodologías probadas (p.ej.: técnicas estadísticas, simulación de Montecarlo, matrices de correlaciones, etc.)? · ¿Participan sistemáticamente los agentes clave ERM o el Comité de Riesgos en el proceso de planificación estratégica?	❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑
9. Formula objetivos de negocio	· ¿Los objetivos estratégicos de la compañía están alineados con el apetito de riesgo establecido? · ¿Los objetivos estratégicos son desarrollados en objetivos de operaciones, financieros, cumplimiento, etc.? · ¿Están los objetivos de los empleados alineados a los objetivos estratégicos de la compañía? · ¿Se definen y actualizan los niveles de tolerancia al riesgo para todos los riesgos clave, con la aprobación del consejo de administración? · ¿Se consideran los niveles de tolerancia al riesgo en los procesos de toma de decisiones? · ¿Se monitoriza activamente el cumplimiento con los niveles de tolerancia al riesgo? · ¿Se gestionan caso a caso las excepciones al cumplimiento con la tolerancia al riesgo y requieren aprobación de la alta dirección y/o el consejo de administración?	❑ ❑

Fuente: Elaboración propia a partir de *COSO ERM Integrating with Strategy and Performance.*

Cada punto de reflexión se evaluará según la calificación 1 a 5 previamente indicada, en función del grado de presencia en la compañía que el auditor interno estime durante la realización del trabajo.

Componente 3 – Desempeño

Según el Marco COSO ERM 2017, *"una compañía identifica y evalúa los riesgos que pueden afectar a la habilidad de la entidad de cumplir su estrategia y alcanzar sus objetivos de negocio. Como parte de ese proceso, la compañía prioriza los riesgos de acuerdo con la severidad que presentan y considerando su apetito de riesgo. En base a esto, la compañía selecciona la respuesta al riesgo y supervisa el desempeño para el cambio. En este sentido, desarrolla una visión de cartera de la cantidad de riesgo que ha asumido durante el proceso de consecución de su estrategia y de sus objetivos de negocio".*

Para obtener una evaluación de utilidad sobre *Desempeño,* se proponen los siguientes puntos de reflexión.

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
10. Identifica el riesgo	· ¿Existen procesos para identificar sistemáticamente los principales riesgos y oportunidades que repercuten en la consecución de los objetivos estratégicos y de negocio?	❑ ❑ ❑ ❑ ❑
	· ¿Se identifican y evalúan los riesgos periódicamente, al menos con carácter anual?	❑ ❑ ❑ ❑ ❑
	· ¿Existe una taxonomía de riesgos para catalogar los riesgos por tipología?	❑ ❑ ❑ ❑ ❑
	· ¿Se definen KRIs *(Key Risk Indicators)* para identificar proactivamente riesgos con crecientes o emergentes?	❑ ❑ ❑ ❑ ❑
11. Evalúa la gravedad del riesgo	· ¿Se evalúa el impacto y probabilidad de los riesgos identificados con criterios homogéneos preestablecidos?	❑ ❑ ❑ ❑ ❑
	· ¿Se cuantifica el impacto económico de los riesgos, siempre que sea posible?	❑ ❑ ❑ ❑ ❑
	· ¿Se considera el impacto reputacional de los riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Se determina la gravedad del riesgo con técnicas de análisis determinístico (p. ej.: análisis de sensibilidad)?	❑ ❑ ❑ ❑ ❑
	· ¿Se determina la gravedad del riesgo con técnicas de análisis probabilístico (p. ej.: simulación de Montecarlo)?	❑ ❑ ❑ ❑ ❑
12. Prioriza riesgos	· ¿Los riesgos se priorizan en base a su impacto y probabilidad de ocurrencia?	❑ ❑ ❑ ❑ ❑
	· ¿Los riesgos se representan en un mapa de riesgos (p. ej.: mapa de calor) que habilita su priorización?	❑ ❑ ❑ ❑ ❑
	· ¿Se monitoriza sistemáticamente que la severidad de los riesgos cumple con el apetito de / tolerancia al riesgo establecidos?	❑ ❑ ❑ ❑ ❑

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
13. Implementa respuestas ante los riesgos	· ¿Se definen planes para gestionar todos los riesgos identificados (p. ej.: aceptar, evitar, mitigar, o transferir)?	❑ ❑ ❑ ❑ ❑
	· ¿Se asigna un responsable y fecha de ejecución para gestionar cada uno de los riesgos identificados?	❑ ❑ ❑ ❑ ❑
14. Desarrolla una visión a nivel de cartera	· ¿Existe un registro/inventario de riesgos centralizado a nivel de unidad de negocios?	❑ ❑ ❑ ❑ ❑
	· ¿Se analizan las posibles interdependencias entre los riesgos identificados en cada unidad de negocio, para obtener una visión de cartera a ese nivel?	❑ ❑ ❑ ❑ ❑
	· ¿Existe un registro/inventario de riesgos centralizado a nivel de unidad de la entidad?	❑ ❑ ❑ ❑ ❑
	· ¿Se elabora una visión integrada, a nivel de la entidad, de los riesgos identificados en las distintas unidades de negocio, aplicando metodologías probadas (p. ej.: técnicas estadísticas, análisis de sensibilidad, simulación de Montecarlo, matrices de correlaciones, etc.)?	❑ ❑ ❑ ❑ ❑

Fuente: Elaboración propia a partir de *COSO ERM Integrating with Strategy and Performance.*

Cada punto de reflexión se evaluará según la calificación 1 a 5 previamente indicada, en función del grado de presencia en la compañía que el auditor interno estime durante la realización del trabajo.

Componente 4 – Análisis y Revisión

Según Marco COSO ERM 2017, *"mediante la revisión de las capacidades y prácticas de gestión de riesgos corporativos y del desempeño de la entidad en relación con sus objetivos, una compañía puede considerar cómo han aportado valor las capacidades y prácticas de la gestión de riesgos corporativos a lo largo del tiempo y cómo continuarán impulsando el valor a la luz de cambios sustanciales".*

Para evaluar sobre *Análisis y Revisión,* se proponen los siguientes puntos de reflexión.

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
15. Evalúa los cambios significativos	· ¿Existe un proceso de monitorización para identificar periódicamente los cambios del contexto empresarial (p. ej.: los factores internos y externos) con posible impacto en la consecución de los objetivos de la compañía?	❑ ❑ ❑ ❑ ❑
	· ¿Se actualiza periódicamente el registro/inventario de riesgos de la compañía, incorporando temas emergentes o cambios en el contexto de negocio?	❑ ❑ ❑ ❑ ❑
	· ¿El Comité de Riesgos se reúne periódicamente para analizar, concluir y actualizar el perfil de riesgos de la compañía?	❑ ❑ ❑ ❑ ❑
	· ¿Se dispone de un proceso de reporte de urgencia o por excepción (p. ej.: fuera del calendario de reporte formalmente establecido)?	❑ ❑ ❑ ❑ ❑

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
15. Evalúa los cambios significativos	· ¿Existe un proceso de monitorización para identificar periódicamente los cambios del contexto empresarial (p. ej.: los factores internos y externos) con posible impacto en la consecución de los objetivos de la compañía? · ¿Se actualiza periódicamente el registro/inventario de riesgos de la compañía, incorporando temas emergentes o cambios en el contexto de negocio? · ¿El Comité de Riesgos se reúne periódicamente para analizar, concluir y actualizar el perfil de riesgos de la compañía? · ¿Se dispone de un proceso de reporte de urgencia o por excepción (p. ej.: fuera del calendario de reporte formalmente establecido)?	❑ ❑ ❑ ❑ ❑
16. Revisa el riesgo y el desempeño	· ¿La compañía realiza un seguimiento periódico del grado de desempeño para los principales objetivos establecidos?	❑ ❑ ❑ ❑ ❑
17. Persigue la mejora de la gestión del riesgo empresarial	· ¿La compañía revisa la idoneidad y actualiza su marco de gestión de riesgos periódicamente (p. ej.: auditorías)? · ¿Se han implantado mejoras significativas en el proceso de gestión de riesgos en el último año?	❑ ❑ ❑ ❑ ❑

Fuente: Elaboración propia a partir de *COSO ERM Integrating with Strategy and Performance.*

Cada punto de reflexión se evaluará según la calificación 1 a 5 previamente indicada, en función del grado de presencia en la compañía que el auditor interno estime durante la realización del trabajo.

Componente 5 – Información, comunicación y reporte

Según el Marco COSO ERM 2017, "*la comunicación es el proceso continuo e iterativo de obtener información y compartirla a lo largo de toda la entidad. La dirección utiliza información relevante proveniente de fuentes internas y externas para dar soporte a la gestión de riesgos corporativos. La compañía aprovecha los sistemas de información para capturar, procesar y gestionar datos e información. Mediante la utilización de información que afecta a todos los componentes, la compañía reporta sobre los riesgos, la cultura y el desempeño".*

Para poder obtener una evaluación de utilidad sobre *Información, comunicación y reporte,* se proponen los siguientes puntos de reflexión asociados a cada uno de los principios que se encuentran contemplados en este componente de una gestión de riesgos eficaz.

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
18. Aprovecha la Información y la Tecnología	· ¿Los miembros del Comité de Riesgos tienen acceso directo a la información de riesgos que necesitan para cumplir con sus responsabilidades de supervisión? · ¿Se dispone de una herramienta informática de ERM? · ¿Los agentes de 1ª y 2ª Línea tienen acceso directo a la herramienta para la carga, análisis y *reporting* de los riesgos bajo su responsabilidad? · ¿Se hace uso de herramientas de tecnología punta (p. ej.: *data analytics, big data,* inteligencia artificial) para complementar las actividades de ERM?	❑ ❑ ❑ ❑ ❑

PRINCIPIO	PUNTOS DE REFLEXIÓN	GRADO MADUREZ
19. Comunica Información sobre Riesgos	· ¿Están claramente establecidos los flujos de aprobación y reporte de la información en materia de riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Se reportan periódicamente (al menos de forma anual) los principales riesgos de la compañía al consejo de administración vía la Comisión de Auditoría?	❑ ❑ ❑ ❑ ❑
20. Informa sobre el Riesgo, la Cultura y el Desempeño	· ¿Existen procesos de reporting customizados a los diferentes niveles organizativos?	❑ ❑ ❑ ❑ ❑
	· ¿El proceso de gestión de riesgos proporciona la información necesaria para el reporte de información pública (p.ej. Cuentas Anuales, 20F, Informe Anual de Gobierno Corporativo, etc.)?	❑ ❑ ❑ ❑ ❑
	· ¿Se utilizan métricas de monitorización del riesgo (KRIs) para alertar respecto de riesgos crecientes o emergentes?	❑ ❑ ❑ ❑ ❑
	· ¿Se reporta una visión tanto cualitativa (tendencia histórica, perspectiva futura, nivel de aseguramiento, etc.) como cuantitativa (nivel de exposición, nivel máximo, análisis de sensibilidad y test de estrés, etc.) de los principales riesgos?	❑ ❑ ❑ ❑ ❑
	· ¿Se reportan los riesgos materializados y su impacto real sobre los objetivos de la compañía?	❑ ❑ ❑ ❑ ❑
	· ¿Se reporta sobre la cultura de riesgos?	❑ ❑ ❑ ❑ ❑

Fuente: Elaboración propia a partir de *COSO ERM Integrating with Strategy and Performance.*

Cada punto de reflexión se evaluará según la calificación 1 a 5 previamente indicada, en función del grado de presencia en la compañía que el auditor interno estime durante la realización del trabajo.

RESULTADO DEL DIAGNÓSTICO SOBRE LA MADUREZ DE LA GESTIÓN DE RIESGOS

Calificados los Puntos de Reflexión contemplados en los principios asociados a cada componente, y en base a la escala de madurez previamente adoptada, el grado de madurez se determina así:

1) Se calcula como la media aritmética de la valoración obtenida por todos los puntos de reflexión definidos para cada principio.
2) La evaluación de cada componente se determina como la media aritmética de las calificaciones obtenidas por todos los principios de cada componente.
3) La calificación global de la madurez de la Gestión de Riesgos ERM de la entidad es el resultado de calcular la media ponderada de las calificaciones obtenidas en cada uno de los componentes.

Esta ponderación reside en un input que se establece en base al juicio profesional del auditor interno, dependiendo, por ejemplo, de las características de la compañía, del negocio donde opera y de la importancia que cada uno de los componentes aporte a la eficacia del programa de gestión de riesgos de la entidad.

Para facilitar la comprensión de la evaluación efectuada se propone utilizar los siguientes instrumentos que presentan, de forma sencilla y visual, la información generada durante el ejercicio de evaluación:

a) *Mapa de Calor.*

Para relacionar la calificación obtenida por cada principio con la escala de "atención requerida" definida previamente en la escala de madurez utilizada. Este instrumento permitirá identificar rápidamente aquellos ámbitos en los que sea necesario actuar con prioridad, mediante la implementación de las iniciativas oportunas para fortalecer la gestión de riesgos.

ÍNDICE GENERAL DE MADUREZ DEL SISTEMA ERM	3.0	GLOBAL		MÁXIMA	ALTA	MEDIA	LEVE
1. GOBIERNO Y CULTURA	2.8	FRAGMENTADO	35%				
1. Supervisión de Riesgos a través del Consejo de Administración	2,5	Fragmentado			X		
2. Establece Estructuras Operativas	2,5	Fragmentado			X		
3. Define la Cultura Deseada	4,3	Integrado				X	
4. Demuestra Compromiso con los Valores Clave	2,8	Fragmentado			X		
5. Atrae, Desarrolla, y Retiene a Profesionales Capacitados	1,8	Ad hoc		X			
2. ESTRATEGIA Y DEFINICIÓN DE OBJETIVOS	3,8	GLOBAL	20%				
6. Analiza el Contexto Empresarial	3,8	Global					
7. Define el Apetito al Riesgo	3,7	Global					
8. Evalúa Estrategias Alternativas	4,0	Global					
9. Formula Objetivos de Negocio	3,7	Global					
3. DESEMPEÑO	3,0	FRAGMENTADO	15%				
10. Identifica el Riesgo	2,5	Fragmentado			X		
11. Evalúa la Gravedad del Riesgo	2,6	Fragmentado			X		
12. Prioriza Riesgos	4,0	Global					
13. Implementa Respuestas ante los Riesgos	2,5	Fragmentado			X		
14. Desarrolla una Visión a nivel de Cartera	3,3	Global					
4. ANÁLISIS Y REVISIÓN	2,3	FRAGMENTADO	15%				
15. Evalúa los Cambios Significativos	1,8	Ad hoc		X			
16. Revisa el Riesgo y el Desempeño	3,0	Fragmentado			X		
17. Persigue la Mejora de la Gestión del Riesgo Empresarial	2,0	Ad hoc		X			
5. INFORMACIÓN, COMUNICACIÓN Y REPORTE	3,3	GLOBAL	15%				
18. Aprovecha la Información y la Tecnología	3,8	Global					
19. Comunica Información sobre Riesgos	4,5	Integrado				X	
20. Informa sobre el Riesgo, la Cultura y el Desempeño	1,5	Ad hoc		X			

Fuente: Elaboración propia.

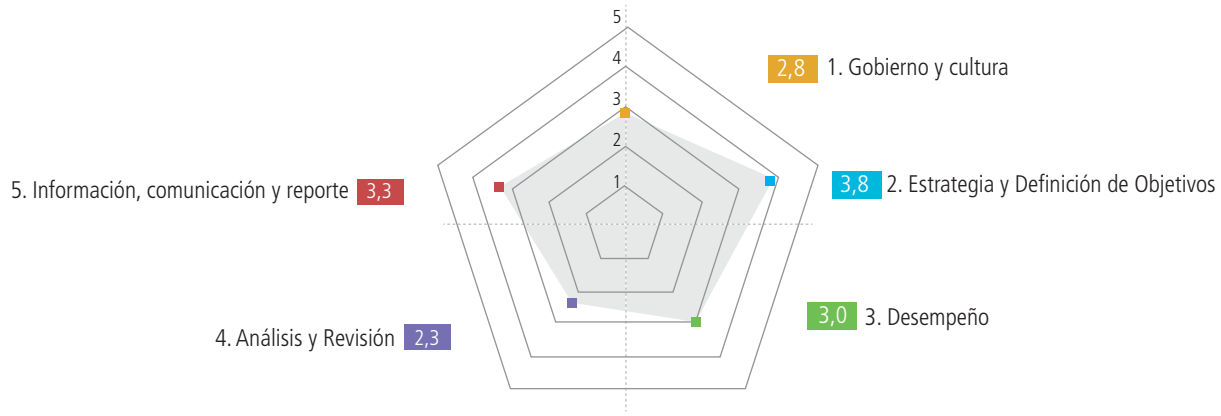
b) Gráfico radial.

Adicionalmente, se propone utilizar un gráfico radial que muestre la calificación integral obtenida por los componentes del ERM. Permitirá comparar el grado de madurez entre cada uno de los componentes y sus principios asociados para identificar fácilmente los ámbitos de priorización y llevar a cabo las iniciativas de mejora del ERM pertinentes.

RESUMEN DE RESULTADOS

	CALIFICACIÓN					
	Componente	Principio 1	Principio 2	Principio 3	Principio 4	Principio 5
1. GOBIERNO Y CULTURA	2,8	2,5	2,5	4,3	2,8	1,8
2. ESTRATEGIA Y DEFINICIÓN DE OBJETIVOS	3,8	3,8	3,7	4,0	3,7	
3. DESEMPEÑO	3,0	2,5	2,6	4,0	2,5	3,3
4. ANÁLISIS Y REVISIÓN	2,3	1,8	3,0	2,0		
5. INFORMACIÓN, COMUNICACIÓN Y REPORTE	3,3	3,8	4,5	1,5		
PROGRAMA ERM	3,0					

CALIFICACIÓN DE LOS COMPONENTES



Fuente: Elaboración propia.

AUDITORÍA INTERNA COMO CATALIZADOR DE LA GESTIÓN DE RIESGOS ERM

Respondiendo al mandato de la Norma 2120 de *"evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos"*, y partiendo de la posibilidad de prestar servicios de consultoría, Auditoría Interna puede asumir el rol de catalizador para potenciar las actividades de gestión de riesgos y orientarlas hacia ERM.

Se propone que, partiendo del resultado del aseguramiento basado en el enfoque del modelo de madurez descrito anteriormente, Auditoría Interna identifique las iniciativas de mejora necesarias y promueva su implementación, ya sea mediante el asesoramiento a la Segunda Línea existente o, en su caso, asumiendo la realización de las actividades de Segunda Línea conforme a los principios de actuación y salvaguardas comentados en esta Guía de Buenas Prácticas.

Metodología Propuesta

El Marco COSO-ERM 2017 se desarrolla a través de 20 principios que representan lo que las compañías deberían hacer como parte de sus prácticas ERM. Sin embargo, no se establecen directrices de cómo llevarlo a cabo, por lo que se presenta a continuación una matriz de iniciativas mínimas necesarias para fortalecer la gestión de riesgos con una visión ERM.

INICIATIVAS PARA FORTALECER LA GESTIÓN DE RIESGOS

1. Gobierno y cultura:
El Gobierno marca el tono de la entidad, reforzando la importancia de la gestión del riesgo empresarial y establece responsabilidades de supervisión al respecto. La cultura hace referencia a los valores éticos, a los comportamientos deseados y a la comprensión del riesgo en la entidad.

PRINCIPIO	ACTUACIÓN
1. Supervisión de riesgos a través del consejo de administración	Definir el **marco de gobernanza** para la gestión de riesgos · Formalizar el **Reglamento o manual del Consejo,** definiendo las competencias y responsabilidades de ERM del Consejo de Administración y, en particular, de la Comisión de Auditoría, gestión de riesgos y Compliance. · Establecimiento de la **Política de Riesgos empresariales** (i.e.; al nivel de la entidad), explicitando los principios fundamentales para llevar a cabo la gestión de riesgos con una visión ERM (asegurando su alineamiento con la misión, visión y valores de la organización), la taxonomía de riesgos, los elementos del sistema de gobierno corporativo que la desarrollan (v.g.; normas, procedimientos), la asignación de las principales responsabilidades, etc. · Seleccionar el **marco de referencia de mejores prácticas ERM** (v.g.; COSO ERM, ISO 31000), customizándolo a las características y necesidades de la organización.
2. Establece estructuras organizativas	Definir la **estructura organizativa y líneas de reporting** para la ejecución de ERM: roles principales de 1ª, 2ª y 3ª Línea de Defensa. · Definir e implementar el **Manual de procedimientos de la Función de Gestión de Riesgos,** asignando competencias y responsabilidades ERM a los agentes de 1ª, 2ª y 3ª Línea de Defensa. · Asignar la **responsabilidad centralizada e integral de ERM** a un Ejecutivo cualificado de la Alta Dirección. · Establecer **Comité de Riesgos** para coordinar y supervisar las actividades de Gestión de Riesgos ERM, formalizando sus principios de actuación en una **Norma del Comité de Riesgos.**
3. Definir la cultura deseada	Establecer los **principios fundamentales** que guiarán la toma de todas las decisiones para ERM, asegurando su alineamiento con la misión, visión y valores de la organización · Asegurar que la **Política de Riesgos** de la entidad explicita los **principios fundamentales de actuación ERM** y que estos están alineados con los principios éticos plasmados en el **Código Ético** de la organización.

PRINCIPIO	ACTUACIÓN
4. Demuestra compromiso con los valores clave	Promover a todos los niveles de la organización los **comportamientos esperados de ERM** y repercusiones por su incumplimiento. · Implementar **iniciativas de comunicación y formación** de los principios clave de ERM. · Establecer un **programa de objetivos e incentivos** que fomente la interiorización de los principios de ERM, asegurando que los objetivos individuales están alineados con los objetivos estratégicos globales. · Promover una **cultura gerencial** que incentive discusiones abiertas de los riesgos de la organización y promueva la toma de decisiones alineada con la cultura de riesgos seleccionada. · Establecer programa de **monitorización del cumplimiento con los valores clave ERM** y divulgación de las medidas disciplinarias por su incumplimiento.
5. Atrae, desarrolla y retiene a profesionales capacitados	Establecer un **programa de gestión del talento** orientado a potenciar las capacidades ERM · Incluir en las Políticas de Recursos Humanos los principios de actuación para atraer, seleccionar y desarrollar los puestos de trabajo necesarios para ejecutar ERM conforme a su diseño. · Definir planes individualizados de formación, desarrollo y sucesión para garantizar la disponibilidad de recursos cualificados para las funciones clave de ERM.

2. Estrategia y establecimiento de objetivos:

La gestión de riesgos empresarial, la estrategia y el establecimiento de objetivos trabajan juntos en el proceso de planificación estratégica. Se establece un apetito de riesgo y se alinea con la estrategia; los objetivos de negocio ponen la estrategia en práctica mientras sirven como base para identificar, evaluar y responder al riesgo.

PRINCIPIO	ACTUACIÓN
6. Analiza el contexto empresarial	Construir y analizar el **"Mapa de Riesgos Clave*** (v.g.; en formato de mapa de calor) de la organización basándose en un análisis "Top Down". · Identificar los objetivos estratégicos de la organización, partiendo del **Plan Estratégico** existente, y desagregarlos en los objetivos clave de operaciones, cumplimiento, etc. · Identificar los **factores externos clave**, incluyendo sus grupos de interés, que puedan repercutir en la consecución de los objetivos clave de la organización. · Identificar los **factores internos clave,** incluyendo los grupos de interés, que puedan repercutir en la consecución de los objetivos clave de la organización.
7. Define el Apetito al Riesgo	Articular el **Apetito al Riesgo** de la organización · Definición del **Apetito al Riesgo,** por el Consejo de Administración, como un elemento estratégico en el contexto de crear y preservar valor. Establecer procesos de monitorización de su cumplimiento.
8. Evalúa estrategias alternativas	Determinar el **Perfil de Riesgos**** resultante de las estrategias consideradas. • Realizar análisis cualitativo de alto nivel (v.g.; mapa de calor, análisis SWOT) de las estrategias consideradas para determinar la tipología y cantidad de riesgo que cada una implica (ver Actuación de Principio 6). • Realizar análisis de riesgos de detalle de las estrategias viables basándose en un enfoque determinístico (v.g.; análisis de sensibilidad) y/o probabilístico (v.g.; análisis Montecarlo) para determinar el binomio riesgo-desempeño óptimo que está alineado con el apetito al riesgo establecido.

* Entendiéndose por "Mapa de Riesgos" como una herramienta de visualización de la información para comunicar los riesgos a los que se enfrenta la organización, con el fin de facilitar su identificación y priorización.

** En donde "Perfil de Riesgos" se refiere al análisis cuantitativo de los riesgos de la organización (i.e.; identificación y evaluación) para obtener un entendimiento objetivo de su impacto en caso de su materialización.

PRINCIPIO	ACTUACIÓN
9. Formula objetivos de negocio	**Alinear estrategia, objetivos y apetito al riesgo.** · Identificar los objetivos de la organización, partiendo del Plan Estratégico existente, así como los objetivos clave de operaciones, cumplimiento, etc. que la soportan. · Corroborar que los objetivos están alineados con la misión, visión y apetito al riesgo. Establecer la **Tolerancia al Riesgo** en la operativa ERM · Establecer métricas de monitorización del riesgo *(Key Risk Indicators* o KRIs) necesarias para alertar de la evolución de los riesgos con impacto en los objetivos de la organización. · Definición por el Consejo, y establecimiento por la Dirección, de la **Tolerancia al Riesgo** (i.e.; límites cualitativos y cuantitativos, de referencia o de obligado cumplimiento). Establecer procesos de monitorización de su cumplimiento. Implementar proceso de actualización para garantizar su aplicabilidad.

3. Desempeño:

Es necesario identificar y evaluar aquellos riesgos que puedan afectar a la consecución de los objetivos estratégicos y de negocio. Los riesgos se priorizan en función de su gravedad en el contexto del apetito al riesgo. Posteriormente, la organización selecciona las respuestas ante el riesgo y adopta una visión a nivel de cartera con respecto al nivel de riesgo que ha asumido. Los resultados de este proceso se comunican a los grupos de interés interesados en el riesgo.

PRINCIPIO	ACTUACIÓN
10. Identifica el riesgo que impacta en el desempeño de la estrategia y los objetivos del negocio. 11. Evalúa la gravedad del riesgo 12. Prioriza riesgos 13. Implementa respuestas ante los riesgos	Definir y formalizar las **directrices y metodologías** del ciclo identificación-medición-gestión e implementarlas en los procesos ERM. · **Identificación:** enfoques *top-down, bottom-up,* auto-evaluación de riesgos y controles (RCSA, Risk and Control Self-Assessment), identificación de eventos de pérdidas (LDB, Loss Data Base), etc. · ***Key Risk Indicators:*** como métricas de monitorización prospectiva para alertar de riesgos crecientes o emergentes. · **Evaluación:** Realizar análisis determinístico (v.g.; análisis de escenarios/sensibilidad) y/o probabilístico (v.g.; análisis Montecarlo) basándose en criterios de probabilidad, impacto, velocidad de materialización, frecuencia de ocurrencia, etc. · **Priorización:** conforme a su severidad en el contexto del apetito y tolerancia al riesgo. · **Gestión:** Aceptar, controlar, evitar, transferir.
14. Desarrolla una visión a nivel de cartera	Definir e implementar las herramientas que soportan la visión cartera de ERM. · Inventario/registro de riesgos. · Mapa de riesgos a nivel de la entidad y mapas individuales al nivel de las unidades de negocios. · Base de datos de eventos de pérdidas operacionales. · Cuadros de mando de KRIs.

4. Revisión y Monitorización:

Al examinar el desempeño de la entidad, una organización puede determinar cómo funcionan los componentes de gestión del riesgo empresarial con el paso del tiempo en un entorno de cambios sustanciales, y qué aspectos son susceptibles de revisar y modificar.

PRINCIPIO	ACTUACIÓN
15. Evalúa los cambios significativos	Identificar y analizar periódicamente los **riesgos crecientes y emergentes clave** con una visión a futuro. · De forma sistemática, identificar, analizar y concluir respecto del impacto que los cambios significativos en el entorno empresarial internos y/o externos (i.e.; riesgos crecientes y/o emergentes) puedan tener sobre ERM y la consecución de la estrategia y objetivos de negocio. Llevar a cabo reuniones periódicas del Comité de Riesgos para consensuar la actualización del perfil y registro de riesgos (ver Actuación · Principio 6). · Actualizar periódicamente el perfil de riesgos de la organización (ver Actuación Principios 10 al 13) reflejándolo en el registro de riesgos.
16. Revisa el riesgo y el desempeño	Analizar **desempeño histórico** y concluir respecto de la gestión de riesgos · Determinar periódicamente si el desempeño histórico se desvía del proyectado, identificando las causas raíz, corroborando que éstas están reflejadas en el Perfil de Riesgos actualizado.
17. Persigue la mejora de la gestión del riesgo empresarial	Implementar **proceso de mejora continua.** · Determinar periódicamente la idoneidad del plan de gestión de riesgos existente (i.e.; respuesta a los riesgos), respecto del mapa de riesgos actualizado, y modificar las actuaciones, responsables o fechas de ejecución, conforme sea necesario. · Determinar periódicamente la idoneidad de los procesos ERM (i.e.; identificación, evaluación, priorización, gestión y reporting) y la validez de sus fundamentales (v.g.; apetito al riesgo, cultura, asignación de responsabilidades, metodologías, etc.), así como de los sistemas y de la estructura organizativa, para implementar mejoras considerando los cambios que se originan por los riesgos emergentes y las desviaciones del desempeño histórico.

5. Información, Comunicación y Reporte:

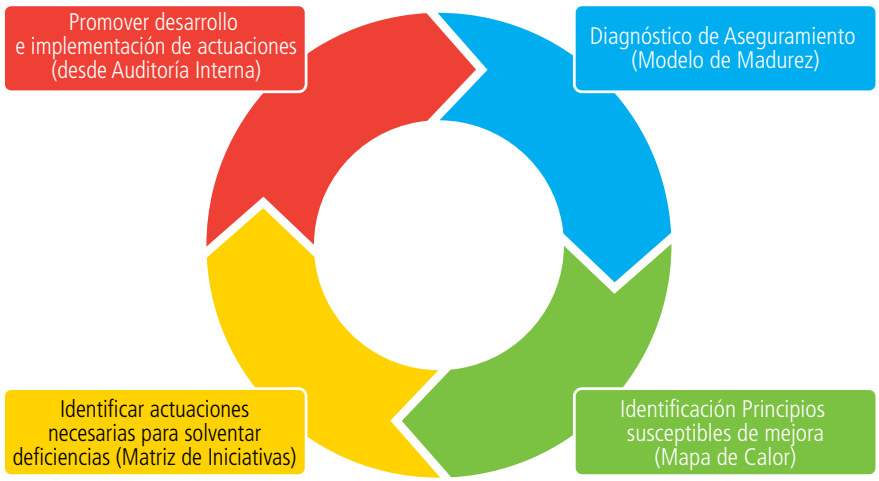
La gestión del riesgo empresarial requiere de un proceso continuo de obtención e intercambio de la información necesaria, tanto de fuentes internas como externas, que fluya hacia arriba, hacia abajo y a lo largo de todos los niveles de la organización.

PRINCIPIO	ACTUACIÓN
18. Aprovecha la información y la tecnología	Incorporar el uso de herramientas de **tecnología de punta** para soportar los procesos de ERM · Sistemas informáticos de gestión de riesgos y reporting. · Bases de datos relacionales y no relacionales. · Herramientas de análisis y visualización de grandes volúmenes datos estructurados y no estructurados (v.g.; data analytics, de big data, l inteligencia artificial, etc.). · Herramientas GRC que soporten la coordinación de las actividades de aseguramiento de las tres líneas de defensa

PRINCIPIO	ACTUACIÓN
19. Comunica información sobre riesgos 20. Informa sobre el riesgo, la cultura y el desempeño	Definir y establecer **procesos de monitorización y reporting** como un elemento integral de la normativa de ERM (v.g.; políticas de riesgos, estatuto de la función, etc.) · Implementar herramientas de monitorización del cumplimiento con el apetito y tolerancia al riesgo y de sistema de gestión basado en KRIs (Key Risk Indicators) o similar. · Determinar las necesidades de información de riesgos (i.e.; tipología, periodicidad, medios) de los grupos de interés internos (v.g.; Comisión de Auditoría, Comité de Riesgos). · Determinar las necesidades de información de riesgos (i.e.; tipología, periodicidad, medios) de los grupos de interés externos (v.g.; Regulador, inversores, etc.). · Implementar reporting periódico de la información necesaria a los grupos de interés internos y externos.

La metodología propuesta para identificar, desde Auditoría Interna, iniciativas de mejora de la gestión de riesgos es relativamente sencilla:

1) Realizar el diagnóstico de aseguramiento en base al enfoque del modelo de madurez.
2) Identificar en el mapa de calor los principios susceptibles de actuaciones de mejora, en base a la evaluación efectuada en el paso 1.
3) Identificar en la matriz de iniciativas aquella actuación necesaria para solventar la deficiencia detectada en el principio correspondiente.
4) Promover, desde Auditoría Interna, el desarrollo e implementación de la actuación de gestión de riesgos que corresponda.



Conclusión

La gestión de la incertidumbre por parte de las compañías ha alcanzado mayor protagonismo durante las últimas décadas. Implementar un sistema de gestión integral de riesgos que permita adoptar decisiones de una manera más ágil y mejor informada constituye un elemento clave para el éxito de las compañías modernas. Afrontar y gestionar riesgos, así como potenciar las oportunidades, se traduce en un mayor número de ventajas competitivas para las entidades, lo que les permite crear más valor, protegerlo de potenciales amenazas y, por ende, hacerlo sostenible en el tiempo.

Los roles que participan en este proceso de gestión integral del riesgo tienen asignadas diferentes responsabilidades: desde la identificación y gestión de la incertidumbre por parte de los agentes de la entidad más ligados al negocio, pasando por las actividades de soporte en gestión de riesgos proporcionadas por agentes especializados, hasta llegar al ente evaluador que proporciona aseguramiento al órgano de gobierno de que existe un sistema de gestión de riesgos adecuado y que los procesos de esa gestión funcionan de manera eficaz.

Estos roles deberían estar desempeñados por funciones o departamentos diferenciados, para garantizar la independencia y objetividad del agente que proporciona el aseguramiento. Independencia y objetividad entendida en relación con los roles ejecutivos y de adopción de decisiones de negocio, desempeñados por otras partes distintas de la compañía.

En la práctica, estos roles y funciones en ocasiones pueden encontrarse concentrados, resultado de la naturaleza, tamaño y características de la compañía. Esta Guía pone de relevancia las buenas prácticas disponibles para que, cuando se requiera que Auditoría Interna asuma un papel más activo en las actividades de gestión de riesgos, se garantice una correcta segregación entre sus actividades fundamentales de aseguramiento y las actividades de consultoría.

Como auditores internos, debemos estar preparados para desempeñar aquel papel que sea más necesario y útil para la compañía. Para ello, esta Guía desarrolla e implementa el enfoque de modelo de madurez con un objetivo doble: proporcionar aseguramiento objetivo sobre la gestión de riesgos existente y promover a Auditoría Interna como catalizador de iniciativas de mejora de la gestión de riesgos con un enfoque ERM.

Bibliografía

- The King Committee on Corporate Governance (South Africa). *The King Report on Corporate Governance,* 1991.
- The Committee on the Financial Aspects of Corporate Governance (Comité Cadbury). *Financial Aspects of Corporate Governance,* 1992.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal control – Integrated framework, 1992.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management - Integrated framework,* 2004.
- The Institute of Internal Auditors – Global. *The Role of Internal Audit in Enterprise-wide Risk Management,* 2004.
- The Institute of Internal Auditors – Global. *Assessing the Adequacy of Risk Management,* 2010:
- Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.
- Risk and Insurance Management Society, Inc. *An overview of widely used risk management standards and guidelines,* 2011.
- Ley 2/2011, de 4 de marzo, de Economía Sostenible.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal Control – Integrated Framework, 2013.
- The Institute of Internal Auditors – Global. T*he three lines of defense in effective risk management and control,* 2013.
- Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores
- The Institute of Internal Auditors – *Global. International Professional Practices Framework: Internal Audit and the Second Line of Defense,* 2015.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management – Integrating strategy and performance,* 2017.
- The Institute of Internal Auditors – Global. *Marco Internacional para la Práctica Profesional de la Auditoría Interna,* 2017.
- The Institute of Internal Auditors – Global. The IIA's Three Lines Model; An update of The Three lines of Defense, 2020.

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA EN LA ESTRATEGIA DE NEGOCIO

Definir, desarrollar y hacer un seguimiento de la estrategia es uno de los procesos más importantes de cualquier compañía. Este documento recoge el trabajo de Auditoría Interna en la definición y seguimiento de la estrategia, describe los posibles roles que puede desempeñar respecto a la estrategia de negocio, y aporta una visión práctica de cómo ejecutar dichos roles en las distintas fases del proceso estratégico.

AUDITORÍA INTERNA DEL PROCESO DE INVERSIÓN EN TECNOLOGÍAS EMERGENTES

Se ofrecen los aspectos clave para comprender mejor qué son y cómo evolucionan las tecnologías emergentes. Se analiza el posicionamiento de Auditoría Interna frente a esas nuevas tecnologías. Y se incluye un análisis de riesgos en una auditoría interna de inversiones en tecnologías emergentes.

AUDITORÍA INTERNA DE LA GESTIÓN DE PROYECTOS

Gestionar un proyecto implica planificar, organizar y dirigir el conjunto de procesos y operaciones diseñados para manejar el proyecto de inicio a fin. Este documento, basado en la metodología PMBOK del Project Management Institute (PMI), ayudará al auditor interno a afrontar la auditoría de un proyecto en sus diferentes fases, áreas de conocimiento y procesos.

AUDITORÍA INTERNA DEL GOBIERNO DEL DATO

Aborda los problemas existentes y las mejores prácticas para resolverlos en lo referente a la definición de un buen gobierno del dato. Se analizan a fondo varios aspectos, desde el ciclo de vida del dato –incluyendo su trazabilidad y calidad– hasta metodologías y normativas aplicables en el proceso de gobierno del dato. Todo desde la perspectiva de Auditoría Interna.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

La gestión de la incertidumbre por parte de las compañías ha alcanzado mayor protagonismo durante las últimas décadas. Implementar un sistema de gestión integral de riesgos que permita adoptar decisiones de una manera más ágil y mejor informada constituye un elemento clave para el éxito de las compañías modernas.

Esta guía desarrolla un enfoque de modelo de madurez y desvela buenas prácticas para que Auditoría Interna tenga un papel más activo en las actividades de gestión de riesgos, se garantice una correcta segregación entre sus actividades de aseguramiento y las de consultoría.

Instituto de Auditores Internos de España

The Institute of Internal Auditors