BID | Invest

POLÍTICA DE GOBIERNO Y GESTIÓN DEL RIESGO

GUÍA DE IMPLEMENTACIÓN DE GOBIERNO CORPORATIVO

Corporate Governance

TABLA DE CONTENIDOS

Sobre los Autores | **Cefeidas Group**

Cefeidas Group es una firma de asesoramiento internacional que ayuda a sus clientes a avanzar hacia sus objetivos en América Latina. Cefeidas ha trabajado con BID Invest y el BID durante más de una década. Cefeidas brinda servicios profesionales en Políticas Públicas, Riesgos y Estrategia; Gobierno Corporativo, Stewardship y Sostenibilidad; e Inteligencia e Investigación Estratégicas. www.cefeidas.com

1. FUNDAMENTOS DE LA POLÍTICA DE GOBIERNO Y GESTIÓN DEL RIESGO

¿Qué es y por qué es indispensable?

La Política de Gobierno y Gestión del Riesgo es el documento marco que establece cómo una empresa entiende, organiza y gestiona los riesgos a los que está expuesta en la búsqueda de sus objetivos estratégicos. No se trata simplemente de un manual técnico para tratar incidentes: es la declaración formal del Consejo de Administración sobre cuánto riesgo está dispuesta la organización a asumir, quién decide sobre el riesgo, cómo se identifica, cómo se mide, cómo se responde a él y cómo se comunica a través de la organización.

Toda empresa enfrenta riesgos: financieros, operacionales, estratégicos, regulatorios, reputacionales, tecnológicos, de sostenibilidad y, cada vez más, riesgos derivados del cambio climático y de la transformación digital. La diferencia entre una empresa que prospera frente a la incertidumbre y una que sucumbe a ella no radica en evitar todos los riesgos, sino en la capacidad de tomarlos de manera consciente, informada y dentro de límites previamente definidos. Esta capacidad no surge espontáneamente: requiere un marco formal de gobierno del riesgo, y la Política de Gobierno y Gestión del Riesgo es ese marco.

La política responde a tres preguntas fundamentales que toda empresa madura debe poder contestar con claridad. Primera: ¿cuáles son los riesgos relevantes para nuestra estrategia? Segunda: ¿cuánto de cada riesgo estamos dispuestos a aceptar? Tercera: ¿quién es responsable de cada aspecto de la gestión del riesgo? Sin respuestas formales y documentadas a estas preguntas, las decisiones empresariales se toman sobre supuestos implícitos, los riesgos críticos pasan desapercibidos hasta que se materializan, y los conflictos sobre quién debió actuar emergen tarde y de forma destructiva.

Alcance y aplicación

La Política de Gobierno y Gestión del Riesgo aplica a toda la organización, sin excepciones. Esto incluye al Consejo de Administración y sus comités, a la Alta Gerencia, a todas las unidades de negocio y áreas funcionales, a las subsidiarias y filiales (con las adaptaciones pertinentes), y al personal en todos los niveles. La universalidad del alcance es esencial: el riesgo es transversal y no respeta jerarquías ni fronteras organizacionales.

Concepto clave: Gobierno del riesgo vs. gestión del riesgo

Gobierno del riesgo se refiere a la arquitectura de toma de decisiones sobre el riesgo: quién decide, con qué información, bajo qué parámetros y con qué supervisión. Es responsabilidad última del Consejo de Administración.

Gestión del riesgo se refiere al proceso operativo de identificar, evaluar, tratar, monitorear y reportar riesgos. Es responsabilidad ejecutiva, liderada por la Alta Gerencia y el Jefe de Riesgos.

Una buena política integra ambos planos: define el gobierno (la estructura) y orienta la gestión (el proceso).

La política también aplica, en lo pertinente, a las relaciones con terceros: proveedores críticos, socios estratégicos, contratistas y prestadores de servicios cuya actuación pueda generar exposiciones significativas a la empresa. En estos casos, la política orienta cómo evaluar el riesgo de tercero y cómo trasladar las exigencias de control mediante los acuerdos contractuales correspondientes.

Los roles que se describen a continuación se articulan sobre el Modelo de las Tres Líneas del Instituto de Auditores Internos (ver recuadro), que distribuye las responsabilidades sobre el riesgo en tres planos complementarios. La **primera línea** está conformada por las unidades de negocio y los dueños de procesos, quienes generan y gestionan riesgo en su operación cotidiana e implementan los controles correspondientes. La **segunda línea** está constituida por el Jefe de Riesgos (CRO) y el Departamento de Riesgos, junto con otras funciones de supervisión y soporte como Cumplimiento, Seguridad de la Información y Continuidad de Negocio; su rol es proveer metodología, monitoreo agregado, consultoría y desafío independiente a la primera línea, sin asumir sus responsabilidades operativas. La **tercera línea** es la Auditoría Interna, que proporciona al Consejo un aseguramiento independiente y objetivo sobre la efectividad del marco completo.

Roles principales cubiertos por la política

Consejo de Administración: aprobación de la política, de la Declaración de Apetito de Riesgo, supervisión del marco y rendición final de cuentas.

Comité de Riesgos (o Comité de Auditoría y Riesgo, según la estructura): supervisión especializada y profundización de los temas de riesgo en nombre del Consejo.

CEO y Alta Gerencia: implementación operativa, asignación de recursos y reporte al Comité y al Consejo.

Jefe de Riesgos (CRO) y Departamento de Riesgos: segunda línea, liderazgo metodológico, monitoreo agregado y reporte.

Dueños de procesos y unidades de negocio: primera línea, responsables operativos del riesgo en su ámbito.

Auditoría Interna: tercera línea, aseguramiento independiente sobre la efectividad del marco completo.

Modelo de las Tres Líneas del Instituto de Auditores Internos (IIA, 2020)

El Modelo de las Tres Líneas ayuda a las organizaciones a identificar las estructuras y los procesos que mejor facilitan el logro de los objetivos y promuevan un gobierno sólido y gestión de riesgo. Ver el modelo aquí.

Una política, múltiples niveles de sofisticación

La existencia de una política no implica que la sofisticación deba ser la misma en todas las empresas. Una empresa familiar mediana en proceso de profesionalización puede comenzar con una política breve y enfocada en lo esencial: roles, declaración de apetito básica, taxonomía de riesgos principales y proceso simplificado. Lo crítico es que el Consejo apruebe formalmente el documento y se comprometa con su evolución progresiva. La política puede crecer en sofisticación con la madurez de la empresa.

Objetivo de la política

La política persigue objetivos interrelacionados que, en conjunto, transforman la gestión del riesgo de una práctica reactiva en una capacidad estratégica de la empresa:

- **Establecer una arquitectura clara de gobierno del riesgo,** definiendo roles, responsabilidades y líneas de reporte que eviten vacíos y duplicaciones.
- **Articular el apetito y la tolerancia al riesgo de la empresa,** para que las decisiones estratégicas y operativas se tomen dentro de parámetros conocidos y aprobados.
- **Promover una cultura de riesgo consistente,** donde la identificación, escalamiento y tratamiento de riesgos sea parte natural del trabajo diario.
- **Garantizar la integración del riesgo con la estrategia y el plan de negocio,** evitando que la gestión del riesgo se convierta en una actividad aislada del proceso de toma de decisiones.
- **Asegurar el cumplimiento de marcos regulatorios y mejores prácticas,** incluyendo COSO ERM, ISO 31000, y, cuando aplique, regulación sectorial específica.
- **Habilitar el reporte oportuno y útil al Comité y al Consejo,** con información que permita supervisar y decidir, no solo informar.

Conexión con los pilares del buen gobierno corporativo

La Política de Gobierno y Gestión del Riesgo operacionaliza directamente los cuatro pilares fundamentales del gobierno corporativo, traduciéndolos de principios abstractos a prácticas concretas y verificables:

1. Transparencia (Transparency). La política de gestión de riesgos fortalece la transparencia al definir qué información sobre riesgos debe reportarse, con qué frecuencia y a quién. Asimismo, establece canales formales de comunicación entre la primera, segunda y tercera línea de defensa, y proporciona las bases para la divulgación de riesgos materiales en los informes anuales y en las comunicaciones dirigidas a inversionistas.

2. Rendición de cuentas (Accountability). La política promueve la rendición de cuentas al asignar responsabilidades específicas a cada nivel de la organización, incluidos el Consejo, sus comités, el CEO, el CRO y los dueños de procesos. También establece las consecuencias del incumplimiento de los límites de riesgo y exige documentar las decisiones de aceptación de riesgos, identificando a la persona o instancia responsable de su aprobación.

Principios G20/OECD de Gobierno Corporativo (2023)

Los Principios G20/OCDE de Gobierno Corporativo, en su versión revisada de 2023, dedican una sección específica al **gobierno del riesgo**. Establecen que el Consejo es responsable de aprobar la política de gestión de riesgos, definir el apetito de riesgo, supervisar la integridad de los sistemas de control y asegurar que existan procesos para identificar y reportar oportunamente los riesgos materiales. Los Principios destacan la importancia de que el Consejo cuente con la información, la experiencia y los conocimientos necesarios para ejercer esta función..

Referencias a estándares internacionales

ISO 31000 — Gestión del Riesgo. Define los principios, el marco y el proceso de gestión del riesgo, aplicables a cualquier organización, sector o tipo de riesgo. Enfatiza que la gestión del riesgo debe ser integrada (parte de las actividades organizacionales), estructurada y exhaustiva, personalizada al contexto, inclusiva (involucrando a las partes interesadas), dinámica, basada en la mejor información disponible, considerando factores humanos y culturales, y de mejora continua. Conoce más aquí.

COSO Enterprise Risk Management (ERM). Este marco ofrece una perspectiva completa para integrar la gestión del riesgo con la estrategia y el desempeño organizacional. Conoce más aquí.

3. Responsabilidad (Responsibility). La política reconoce que la gestión de riesgos constituye un deber fiduciario del Consejo de Administración y define los deberes de cuidado y diligencia que deben guiar la toma de decisiones relacionadas con el riesgo. Además, articula el modelo de Tres Líneas para distribuir de manera clara y coherente las responsabilidades en toda la organización.

4. Equidad (Fairness). La política contribuye a la equidad al procurar que las decisiones relacionadas con el riesgo no favorezcan indebidamente a un grupo de interés sobre otro. Asimismo, protege a los accionistas minoritarios al requerir la aprobación formal de las exposiciones materiales y asegura que los conflictos de interés asociados con decisiones de riesgo sean identificados, evaluados y gestionados adecuadamente.

Estándares regulatorios sectoriales

Las empresas en sectores regulados (financiero, asegurador, energético, farmacéutico, telecomunicaciones, entre otros) deben además observar los marcos específicos emitidos por sus reguladores. Por ejemplo, en el sector financiero los principios de Basilea sobre gestión de riesgos son de obligatoria observancia. La política empresarial debe incorporar y armonizar estos requisitos, no contradecirlos.

Ventajas por tipo de empresa

Empresas familiares	En las empresas familiares, la política cumple una función especialmente valiosa de profesionalización e institucionalización. Históricamente, estas empresas han gestionado el riesgo a través de la intuición del fundador o de los miembros de la familia con roles ejecutivos. Esta aproximación, eficaz mientras la empresa es pequeña y los riesgos son conocidos, se vuelve insostenible cuando la empresa crece, se diversifica, incorpora gerentes profesionales no familiares o atrae inversionistas externos. La política permite separar las decisiones de riesgo de las dinámicas familiares, establece criterios objetivos para el escalamiento de exposiciones significativas, y facilita la transición generacional al documentar las prácticas que de otra manera serían tácitas. Adicionalmente, la política protege el patrimonio familiar al prevenir que decisiones individuales expongan a la empresa a riesgos que excedan la capacidad colectiva de absorberlos.
Empresas no familiares no listadas	Para estas empresas, la política es típicamente un facilitador de la profesionalización del Consejo y de la rendición de cuentas hacia inversionistas o socios. Una política bien desarrollada demuestra a financiadores, inversionistas potenciales y aliados estratégicos que la empresa cuenta con un marco maduro de toma de decisiones, lo cual reduce las primas de riesgo en el costo del capital y facilita transacciones futuras como rondas de inversión, adquisiciones o salidas a bolsa.
Empresas listadas (cotizadas)	En las empresas que cotizan en bolsa, la política es frecuentemente una exigencia regulatoria explícita o implícita. Las normas de gobierno corporativo de los reguladores de valores en la región exigen, en grados variables, que las empresas cuenten con un marco formal de gestión del riesgo, una declaración de apetito aprobada por el Consejo, y un Jefe de Riesgos con acceso directo a este. Más allá del cumplimiento, la política es esencial para satisfacer las expectativas de los inversionistas institucionales, agencias calificadoras y analistas, todos los cuales exigen visibilidad sobre cómo se gestionan los riesgos materiales del negocio.
Empresas familiares listadas	Estas empresas combinan los retos de las dos categorías anteriores. La política juega un papel crítico para demostrar que las dinámicas familiares no comprometen la independencia y el profesionalismo del proceso de gestión de riesgos, y que existen mecanismos formales para escalar al Consejo cualquier exposición que exceda los límites aprobados, sin importar quién sea el responsable de la decisión que generó la exposición.

La cultura de riesgo

La cultura de riesgo es uno de los determinantes más poderosos de la efectividad real del marco de gestión del riesgo, y simultáneamente uno de los más subestimados. Las políticas, los procesos, los KRIs (*Key Risk Indicators*) y los reportes pueden estar perfectamente diseñados sobre el papel, pero si la organización no comparte un conjunto coherente de valores, creencias y comportamientos frente al riesgo, el marco operará de manera defectuosa precisamente cuando más se necesite. En la práctica, las grandes crisis empresariales rara vez se explican por la ausencia de un marco formal: se explican por una cultura que toleró ignorar lo que el marco señalaba.

La responsabilidad de generar y mantener una cultura de riesgo sana es indelegable del Consejo de Administración. Ningún Jefe de Riesgos (CRO), por talentoso que sea, ningún Departamento de Riesgos, por bien dotado que esté, puede sustituir el efecto que tiene el comportamiento, las decisiones y las prioridades del Consejo y de la Alta Gerencia sobre cómo se entiende y se vive el riesgo en toda la organización. La cultura se construye desde arriba: el llamado "tono desde la cima" (*tone at the top*) es el principal mecanismo de transmisión y el principal multiplicador del marco formal.

Qué significa, en concreto, generar cultura de riesgo desde el Consejo

Más allá de las declaraciones formales, generar cultura de riesgo se materializa en comportamientos observables del Consejo de Administración que el resto de la organización lee como señales sobre qué se valora y qué se tolera. Las prácticas que el Consejo asume directamente son:

- **Modelar el comportamiento esperado:** el Consejo demuestra con sus propias decisiones y conductas aquello que la organización debe valorar. Si el Consejo desestima reportes incómodos, la organización aprenderá a maquillarlos; si los exige y los discute con seriedad, la organización aprenderá a producirlos con rigor.
- **Asignar tiempo y atención al riesgo:** el Consejo dedica espacio significativo en sus agendas a la discusión sustantiva de riesgos, no solo a la aprobación formal de documentos. Una sesión anual no es suficiente; se requiere presencia recurrente del tema en las reuniones ordinarias.
- **Formular preguntas difíciles:** el Consejo interroga activamente sobre los supuestos detrás de las evaluaciones de riesgo, los escenarios adversos, los riesgos emergentes y las decisiones que se alejan del apetito aprobado. La calidad de las preguntas modela la calidad de las respuestas.

Auditoría de la cultura

Cada vez más, se espera que la Auditoría Interna no se limite a evaluar procesos y controles, sino que también monitoree la cultura organizacional y la cultura de riesgo. Esta "auditoría de la cultura" provee al Consejo evidencia independiente sobre los tres ejes anteriores, complementando la mirada del CRO. El alcance, la metodología y los reportes de la función de Auditoría Interna se desarrollan en detalle en la Guía de Implementación de Gobierno Corporativo — Reglamento de Auditoría Interna, a la cual se remite para profundizar en este tema.

- **Respaldar a quienes escalan riesgos:** el Consejo apoya públicamente al CRO y a los responsables que reportan exposiciones incómodas, incluso cuando contradicen a la Alta Gerencia. Penalizar al mensajero es la forma más rápida de destruir una cultura de riesgo.
- **Alinear los incentivos:** el Consejo asegura que los sistemas de compensación variable de la Alta Gerencia integren consideraciones de riesgo, no solo de resultado. Un esquema que premia exclusivamente el retorno incentiva la asunción excesiva de riesgo, por más que la Política diga otra cosa.
- **Tolerar el desacuerdo constructivo:** el Consejo crea espacio para que la disensión sobre temas de riesgo sea legítima y bienvenida. Las culturas en las que todos coinciden son las que producen los fracasos más estrepitosos.

Los tres ejes observables de la cultura de riesgo

Para supervisar la cultura de riesgo de manera ordenada, el Consejo y el Comité de Riesgos pueden estructurar su mirada en tres ejes complementarios, que también son los ejes que típicamente analiza la Auditoría Interna cuando emprende una auditoría de cultura:

- **Tono desde la cima:** cómo el Consejo y la Alta Gerencia priorizan, comunican y modelan la gestión del riesgo. ¿Cuál es el apetito declarado y cómo se traduce en las decisiones reales? ¿Las comunicaciones internas son coherentes con la Política aprobada?
- **Gestión del riesgo en el día a día:** qué ocurre operativamente en la organización. ¿Hay reuniones regulares para discutir riesgos? ¿Los gerentes escalan los problemas o los esconden? ¿Cuál es la calidad de los reportes y la profundidad de las conversaciones?
- **Gestión de personas:** cómo los procesos de talento refuerzan o erosionan la cultura. ¿Los programas de incentivos premian el comportamiento responsable frente al riesgo? ¿La evaluación de desempeño incluye criterios de gestión del riesgo? ¿La capacitación es sistemática?

Señales de una cultura de riesgo débil

Algunas señales tempranas de una cultura de riesgo débil que merecen atención del Consejo son:

- ausencia de discusión sustantiva del riesgo en las reuniones del Consejo y del Comité;
- reportes que solo presentan buenas noticias;
- ausencia de eventos reportados o “casi-incidentes” (que sugiere subreporte, no inexistencia);
- rotación frecuente o salida abrupta del CRO o del Jefe de Auditoría Interna;
- resistencia gerencial a las recomendaciones de la segunda y tercera línea;
- compensaciones variables exclusivamente vinculadas al resultado financiero;
- tolerancia silenciosa frente a incumplimientos “menores”.

Cuando varias de estas señales coexisten, el marco formal puede estar operando sobre una base cultural frágil.

2. COMPONENTES CLAVE Y ESTRUCTURA

El siguiente modelo presenta una estructura básica para la redacción de una Política de Gobierno y Gestión del Riesgo. Se invita a las empresas a adaptar este modelo según su realidad específica. Los textos en itálica y fondo gris representan el modelo de redacción sugerido, mientras que las anotaciones en los recuadros laterales o destacados ofrecen orientación práctica para completar cada sección.

[Carátula]

POLÍTICA DE GOBIERNO Y GESTIÓN DEL RIESGO

Índice:

CAPÍTULO I: DISPOSICIONES GENERALES

ARTÍCULO 1 — Objeto

La presente Política tiene por objeto establecer el marco de gobierno y gestión del riesgo de [Nombre de la Compañía], definiendo los principios, la estructura organizacional, los roles y responsabilidades, el apetito de riesgo, y el proceso integral de identificación, evaluación, tratamiento, monitoreo y reporte de los riesgos a los que está expuesta la Compañía en la búsqueda de sus objetivos estratégicos.

ARTÍCULO 2 — Alcance

Esta Política aplica a la Compañía y a todas sus subsidiarias y filiales (las "Compañías"), a su Consejo de Administración y comités, a la Alta Gerencia, a todos los colaboradores, así como, en lo pertinente, a contratistas, proveedores críticos y terceros que actúen en nombre de las Compañías.

Concepto clave

Si la empresa pertenece a un grupo, defina con precisión qué entidades quedan cubiertas por la política. Para subsidiarias en otros países, considere si aplican adaptaciones para reflejar la regulación local. Las exclusiones deben ser explícitas y justificadas.

ARTÍCULO 3 — Definiciones

A los efectos de la presente Política, se entenderá por:

a) Apetito de Riesgo: la cantidad y tipo de riesgo que la Compañía está dispuesta a aceptar en la búsqueda de sus objetivos estratégicos.

b) Tolerancia al Riesgo: el nivel máximo de riesgo que la Compañía está dispuesta a aceptar, incluyendo la variación admisible respecto del Apetito de Riesgo, antes de que se requiera escalamiento o acción correctiva.

c) Capacidad de Riesgo: el máximo nivel de riesgo que la Compañía puede asumir sin comprometer su solvencia, continuidad operacional o cumplimiento normativo.

d) Cultura de Riesgo: el conjunto de valores, creencias, conocimientos, actitudes y comportamientos respecto al riesgo compartidos por todos los colaboradores.

e) Indicador Clave de Riesgo (KRI): métrica utilizada para monitorear la exposición a un riesgo específico y alertar sobre desviaciones.

f) Mapa de Riesgos: representación visual de los riesgos identificados, clasificados por su probabilidad e impacto.

g) Modelo de las Tres Líneas: marco organizacional que distribuye las responsabilidades sobre el riesgo entre las funciones operativas (primera línea), las funciones de supervisión y soporte (segunda línea) y la auditoría interna (tercera línea).

Concepto clave

Las definiciones son críticas para la consistencia interpretativa del documento. Evite crear definiciones propias para conceptos que ya tienen definiciones estándar reconocidas internacionalmente y justificadas.

CAPÍTULO II: PRINCIPIOS Y CULTURA DE RIESGO

ARTÍCULO 4 — Principios Rectores

La gestión del riesgo en la Compañía se rige por los siguientes principios:

a) Integración con la estrategia: la gestión del riesgo es parte integral del proceso de planeación estratégica y de toma de decisiones, no una actividad separada.

b) Liderazgo y compromiso del Consejo: el Consejo de Administración asume la responsabilidad última sobre el marco de gestión del riesgo y demuestra su compromiso a través de su tiempo, atención y decisiones.

c) Proporcionalidad: la sofisticación del proceso de gestión del riesgo es proporcional a la complejidad y materialidad de los riesgos enfrentados.

d) Información oportuna y de calidad: las decisiones de riesgo se toman sobre la mejor información disponible, comunicada oportunamente a quienes deben actuar.

Concepto clave

Los principios articulan la filosofía de la empresa frente al riesgo. Son útiles para resolver dilemas no previstos explícitamente en el resto del documento. Adáptelos a las palabras y prioridades de su empresa.

e) Cultura abierta: se promueve la identificación temprana, el reporte transparente y la discusión constructiva de los riesgos, sin sanción al mensajero.

f) Mejora continua: el marco de gestión del riesgo evoluciona con la experiencia, los cambios en el entorno y la madurez de la organización.

ARTÍCULO 5 — Cultura de Riesgo

La Compañía promueve activamente una cultura de riesgo caracterizada por:

a) La identificación proactiva de riesgos en todos los niveles de la organización.

b) El escalamiento oportuno de exposiciones que excedan los límites aprobados.

c) La rendición de cuentas clara sobre la gestión del riesgo en cada rol.

d) La capacitación continua del personal en gestión del riesgo.

e) El reconocimiento y la incorporación de lecciones aprendidas de incidentes y cuasi-incidentes.

f) La integración de consideraciones de riesgo en los procesos de evaluación de desempeño y compensación.

CAPÍTULO III: ESTRUCTURA DE GOBIERNO DEL RIESGO

ARTÍCULO 6 — Responsabilidades del Consejo de Administración

El Consejo de Administración es el órgano máximo de gobierno del riesgo y, en tal carácter:

a) Aprueba la presente Política y sus actualizaciones materiales.

b) Aprueba la Declaración de Apetito de Riesgo, sus categorías, niveles y métricas asociadas, al menos anualmente.

c) Supervisa la implementación efectiva del marco de gestión del riesgo a través del Comité de Riesgos.

d) Asegura que la Compañía cuente con los recursos, sistemas y personal calificado necesarios para la gestión del riesgo.

e) El CEO designa al Jefe de Riesgos (CRO), sujeto a la aprobación previa o a la no objeción del Consejo de Administración. El Consejo aprueba el mandato y las responsabilidades del CRO, revisa periódicamente su desempeño y deberá ser consultado antes de cualquier decisión de remoción.

f) Recibe y discute reportes periódicos sobre el perfil de riesgo de la Compañía, las exposiciones materiales, los excesos sobre apetito y los riesgos emergentes.

Responsabilidad Fiduciaria

Esta es la responsabilidad fiduciaria más importante del Consejo en materia de riesgo. Asegúrese de que la lista refleje todas las decisiones que solo el Consejo puede tomar (no delegables). Si la empresa cuenta con un **Comité de Riesgos** formal, especifique qué decisiones pueden delegarse al Comité y cuáles permanecen en el pleno del Consejo.

Nota: Las Compañías que, en función de la naturaleza, escala y complejidad de sus operaciones y riesgos, determinen que presentan un perfil de riesgo complejo, podrán adoptar como alternativa que el Jefe de Riesgos (CRO) sea designado directamente por el Consejo de Administración. En tal caso, el literal e) deberá modificarse para reflejar dicha estructura de gobierno.

g) Aprueba cualquier exposición que exceda el apetito de riesgo aprobado, o instruye su mitigación.

h) Promueve activamente la cultura de riesgo, demostrando con su propio comportamiento las expectativas establecidas en la Política.

i) Evalúa anualmente la efectividad del marco de gestión del riesgo, considerando los reportes de la Auditoría Interna y de evaluadores externos cuando corresponda.

ARTÍCULO 7 — Comité de Riesgos

El Comité de Riesgos [o Comité de Auditoría y Riesgo, según la estructura adoptada] es un comité del Consejo de Administración que apoya al Consejo en el ejercicio de sus responsabilidades de supervisión sobre el marco de gestión del riesgo. Sus funciones principales son:

a) Revisar y recomendar al Consejo la aprobación de la presente Política y de la Declaración de Apetito de Riesgo.

b) Supervisar la implementación de la Política y del marco de gestión del riesgo.

c) Revisar el perfil de riesgo de la Compañía y los reportes periódicos del Jefe de Riesgos.

d) Profundizar en categorías específicas de riesgo material (financiero, operacional, cibernético, climático, de cumplimiento, entre otros).

e) Evaluar la adecuación de los recursos asignados a la función de gestión del riesgo.

f) Revisar y validar los indicadores clave de riesgo (KRIs) y sus límites.

g) Analizar los excesos sobre apetito de riesgo y recomendar acciones al Consejo.

h) Coordinar con el Comité de Auditoría (cuando son distintos) sobre temas de riesgo y control.

i) Reportar al Consejo de Administración sobre sus actividades, hallazgos y recomendaciones.

ARTÍCULO 8 — CEO y Alta Gerencia

El CEO es el máximo responsable de la implementación operativa del marco de gestión del riesgo y, en tal carácter:

a) Asegura que la presente Política se implemente efectivamente en toda la organización.

b) Asigna los recursos humanos, financieros y tecnológicos necesarios para la gestión del riesgo.

c) Designa, en coordinación con el Comité y el Consejo, a los responsables de cada categoría de riesgo material.

Comité de Riesgos separado vs. Comité de Auditoría y Riesgo combinado

Las empresas medianas frecuentemente combinan las funciones de auditoría y riesgo en un solo "Comité de Auditoría y Riesgo" para optimizar el uso del tiempo de los Consejeros. La desventaja es que la agenda de auditoría tiende a dominar. Si esta es la opción, sea explícito en la denominación y en la distribución temporal de las agendas.

Las empresas con perfil de riesgo complejo (instituciones financieras, energéticas, infraestructura, listadas grandes) suelen tener comités separados. Su principal ventaja es que permite mayor profundidad en cada agenda.

d) Promueve activamente la cultura de riesgo desde la cúspide ejecutiva ("tono desde la cima").

e) Reporta al Comité y al Consejo sobre el estado de los riesgos materiales y de la implementación de la Política.

f) Aprueba decisiones operativas dentro de su autoridad delegada y dentro del apetito de riesgo aprobado.

g) Escala oportunamente al Comité y al Consejo cualquier exposición que exceda los límites aprobados o cualquier riesgo emergente material.

La Alta Gerencia, en conjunto, es responsable de implementar la Política en sus respectivas áreas y de asegurar que los procesos bajo su responsabilidad operen dentro del apetito de riesgo aprobado.

ARTÍCULO 9 — Jefe de Riesgos (CRO) y Departamento de Riesgos

El Jefe de Riesgos (Chief Risk Officer o CRO) lidera el Departamento de Riesgos y la función de segunda línea. Sus responsabilidades principales son:

a) Diseñar, mantener y actualizar el marco metodológico de gestión del riesgo.

b) Coordinar el proceso anual de identificación, evaluación y priorización de riesgos en toda la Compañía.

c) Mantener el mapa corporativo de riesgos y la matriz de riesgos consolidada.

d) Definir, en coordinación con los dueños de procesos, los indicadores clave de riesgo (KRIs) y monitorear su evolución.

e) Apoyar al Consejo y al Comité en la formulación de la Declaración de Apetito de Riesgo.

f) Reportar periódicamente al Comité de Riesgos y al Consejo sobre el perfil de riesgo, los KRIs, los excesos sobre apetito y los riesgos emergentes.

g) Brindar consultoría a las unidades de negocio sobre la integración del riesgo en sus decisiones.

h) Coordinar con la Auditoría Interna, el área de Cumplimiento y otras funciones de control.

i) Promover la formación en gestión del riesgo en toda la organización.

j) Asistir como participante, sin voto, a las reuniones del Comité de Riesgos cuando se le solicite.

Línea de reporte: el Jefe de Riesgos reporta funcionalmente al Comité de Riesgos (y a través de este al Consejo de Administración) y administrativamente al CEO. Esta línea funcional dual asegura su independencia para reportar oportunamente al Consejo cualquier asunto material, incluso si involucra a la Alta Gerencia.

Concepto clave

La línea de reporte funcional al Comité y administrativa al CEO es la mejor práctica internacional. Garantiza que el CRO no pueda ser silenciado por la Alta Gerencia cuando deba reportar al Consejo.

¿Cuándo se justifica un CRO dedicado?

La práctica internacional sugiere considerar la designación de un CRO dedicado cuando:

- la empresa cotiza en bolsa o tiene planes de hacerlo;
- opera en un sector regulado con exigencias formales (banca, seguros, energía, telecomunicaciones);
- tiene operaciones en múltiples geografías o líneas de negocio;
- maneja exposiciones financieras significativas;
- ha experimentado eventos adversos materiales en los últimos años; o
- los financiadores e inversionistas lo exigen explícitamente.

En empresas medianas que aún no cuentan con un CRO formal, esta función puede ser asumida transitoriamente por el CFO o por un Director de Riesgos con dedicación parcial, hasta que la madurez del marco justifique un cargo dedicado.

ARTÍCULO 10 — Dueños de procesos y unidades de negocio (Primera Línea)

Los dueños de procesos y los líderes de las unidades de negocio constituyen la primera línea del Modelo de las Tres Líneas. Son los responsables operativos de:

a) Identificar los riesgos inherentes a sus procesos y operaciones.

b) Implementar los controles necesarios para mantener los riesgos dentro del apetito aprobado.

c) Monitorear continuamente la efectividad de los controles.

d) Reportar oportunamente al Departamento de Riesgos cualquier evento, incidente o cuasi-incidente material.

e) Participar activamente en los ejercicios anuales de identificación y evaluación de riesgos.

f) Colaborar con la Auditoría Interna en sus revisiones e implementar los planes de remediación acordados.

ARTÍCULO 11 — Auditoría Interna (Tercera Línea)

El Departamento de Auditoría Interna constituye la tercera línea del modelo de gobierno del riesgo y proporciona aseguramiento independiente y objetivo sobre la efectividad del marco de gobierno, gestión del riesgo y control interno. [Sus responsabilidades en relación con la presente Política son:

a) Evaluar periódicamente, a través de sus trabajos basados en riesgos, la idoneidad y efectividad de la implementación de la Política y del marco de gestión del riesgo.

b) Reportar al Comité de Auditoría sus hallazgos, recomendaciones y la conclusión global sobre la efectividad del marco.

c) Coordinar con la segunda línea (Departamento de Riesgos, Cumplimiento, Seguridad de la Información) sin comprometer su independencia ni asumir responsabilidades operativas de aquéllas.

d) Comunicar al Consejo, a través del Comité de Auditoría, cualquier riesgo aceptado por la Dirección que exceda el apetito o tolerancia al riesgo aprobados.]

[El mandato, la independencia organizacional, las líneas de reporte, los recursos, el alcance de los trabajos, el aseguramiento de calidad y demás aspectos de la función de Auditoría Interna se formalizan en el Reglamento de Auditoría Interna aprobado por el Consejo de Administración.]

CAPÍTULO IV: APETITO Y TOLERANCIA AL RIESGO

ARTÍCULO 12 — Apetito, Tolerancia y Capacidad de Riesgo

La Compañía adopta los siguientes conceptos para articular su disposición frente al riesgo:

Reglamento de Auditoría Interna

La presente Política no busca duplicar el contenido del Reglamento de Auditoría Interna. Para el detalle sobre el propósito, la independencia organizacional, las líneas de reporte funcional y administrativo, las responsabilidades del Jefe de Auditoría Interna (JAI), el Plan Anual basado en riesgos, los procesos de comunicación, el aseguramiento de calidad y el modelo operativo (in-house, co-sourced u outsourced) de la función, se remite a la Guía de Implementación de Gobierno Corporativo — Reglamento de Auditoría Interna.

Concepto clave

La articulación entre el Comité de Riesgos y el Comité de Auditoría (cuando están separados) merece especial atención. Idealmente, los presidentes de ambos comités coordinan sus agendas y comparten información. En empresas con un comité combinado, esta coordinación es automática.

- *La Capacidad de Riesgo representa el máximo riesgo que la Compañía puede asumir sin comprometer su solvencia, continuidad operacional o cumplimiento normativo. Es definida en función de los recursos financieros, humanos, operacionales y reputacionales disponibles.*
- *El Apetito de Riesgo es la cantidad y tipo de riesgo que la Compañía está dispuesta a aceptar en la búsqueda de sus objetivos estratégicos, dentro de su Capacidad de Riesgo.*
- *La Tolerancia al Riesgo establece el nivel de variación aceptable respecto al Apetito de Riesgo antes de que se requiera escalamiento o acción correctiva.*

La Declaración de Apetito de Riesgo de la Compañía se encuentra en el Anexo [X] de la presente Política y es aprobada anualmente por el Consejo de Administración a propuesta del Comité de Riesgos.

La **Declaración de Apetito de Riesgo**, que típicamente se incluye como anexo de la política, se encuentra explicada aquí. El Anexo I es un modelo de RAS.

CAPÍTULO V: TAXONOMÍA Y CATEGORÍAS DE RIESGO

ARTÍCULO 13 — Categorías de Riesgo

La Compañía adopta la siguiente taxonomía de riesgos, sin perjuicio de los riesgos emergentes que puedan identificarse:

a) Riesgos Estratégicos: relacionados con la viabilidad del modelo de negocio, decisiones de inversión, fusiones y adquisiciones, y cambios en el entorno competitivo.

b) Riesgos Financieros: incluyendo riesgo de crédito, liquidez, mercado, cambiario, tasa de interés y contraparte.

c) Riesgos Operacionales: derivados de procesos, personas, sistemas o eventos externos. Incluye riesgo de continuidad de negocio.

d) Riesgos de Cumplimiento: incumplimiento de leyes, regulaciones, contratos o estándares aplicables.

e) Riesgos de Reporte: errores u omisiones en la información financiera y no financiera.

f) Riesgos Tecnológicos y Cibernéticos: incluyendo seguridad de la información, ciberataques, uso de la Inteligencia Artificial, dependencia tecnológica y obsolescencia.

g) Riesgos Reputacionales: pérdida de confianza por parte de partes interesadas.

h) Riesgos Ambientales, Sociales y de Gobernanza (ASG/ESG): incluyendo riesgo climático físico y de transición, biodiversidad, derechos humanos y prácticas laborales.

i) Riesgos de Fraude e Integridad: incluyendo corrupción, fraude interno y externo, lavado de activos.

j) Riesgos de Terceros: derivados de proveedores críticos, socios estratégicos y prestadores de servicios.

La taxonomía será revisada al menos anualmente por el Departamento de Riesgos y aprobada por el Comité de Riesgos.

Concepto clave

La taxonomía de riesgos es el lenguaje común que permite a toda la organización referirse a los mismos conceptos al hablar de riesgo. Cumple tres funciones: facilita la identificación exhaustiva de riesgos, evita duplicaciones (que el mismo riesgo aparezca en dos categorías), y permite la agregación coherente del perfil de riesgo a nivel corporativo.

La estructura recomendada es jerárquica. El primer nivel contiene las categorías principales (estratégico, financiero, operacional, etc.). El segundo nivel desagrega cada categoría en subcategorías más específicas. El tercer nivel, opcional para empresas más maduras, identifica riesgos individuales nombrados.

Ejemplo de jerarquía:

- Riesgo Financiero (Categoría)
  - Riesgo de Crédito (Subcategoría)
    - Concentración de cartera por cliente (Riesgo nombrado)

La taxonomía debe reflejar los riesgos materiales del negocio. Empresas en sectores específicos pueden requerir categorías adicionales (por ejemplo, riesgo de seguridad ocupacional para industrias extractivas).

CAPÍTULO VI: PROCESO DE GESTIÓN DEL RIESGO

ARTÍCULO 14 — Proceso de Gestión del Riesgo

La Compañía implementa un proceso continuo de gestión del riesgo inspirado en la norma ISO 31000 y el marco COSO ERM, que incluye las siguientes etapas:

a) Establecimiento del contexto: comprensión del entorno externo e interno, los objetivos estratégicos y las partes interesadas.

b) Identificación de riesgos: detección sistemática de eventos potenciales que puedan afectar el logro de los objetivos.

c) Análisis de riesgos: comprensión de las causas, consecuencias y probabilidades de cada riesgo.

d) Evaluación de riesgos: comparación del nivel de riesgo con el apetito y los criterios establecidos para priorizar el tratamiento.

e) Tratamiento de riesgos: selección e implementación de respuestas apropiadas (evitar, transferir, mitigar o aceptar).

f) Monitoreo y revisión: seguimiento continuo de la efectividad de los controles y de la evolución de los riesgos.

g) Comunicación y consulta: diálogo permanente con las partes interesadas internas y externas relevantes.

h) Registro y reporte: documentación de los riesgos, decisiones y resultados, y reporte a los órganos de gobierno correspondientes.

ARTÍCULO 15 — Tratamiento del Riesgo

Para cada riesgo identificado, la Compañía selecciona la respuesta más apropiada considerando el costo, la efectividad esperada y el apetito aprobado. Las opciones de tratamiento son:

a) Evitar: descontinuar la actividad que genera el riesgo.

b) Transferir: trasladar el riesgo a un tercero (seguros, contratos, derivados).

c) Mitigar: implementar controles para reducir la probabilidad o el impacto.

d) Aceptar: asumir conscientemente el riesgo, con la aprobación del nivel jerárquico apropiado según la materialidad.

Las decisiones de aceptación de riesgos materiales (por encima del umbral de materialidad definido por el Consejo) son documentadas, justificadas y comunicadas al Comité de Riesgos.

CAPÍTULO VII: REPORTE Y ESCALAMIENTO

ARTÍCULO 16 — Reportes Periódicos

El Departamento de Riesgos prepara y presenta los siguientes reportes periódicos:

Concepto clave

El proceso es cíclico y continuo, no lineal. Sus elementos básicos son:

Identificación de riesgos: Es la base del proceso: un riesgo no identificado no puede gestionarse. Las técnicas de identificación incluyen: talleres con la Alta Gerencia y dueños de procesos; entrevistas estructuradas; revisión de incidentes y cuasi-incidentes; análisis de literatura sectorial y de pares; análisis de escenarios; revisión de auditorías y evaluaciones externas; y monitoreo del entorno regulatorio y competitivo. Debe realizarse de forma continua y, como mínimo, anual.

Evaluación de riesgos: Analiza la probabilidad (que el riesgo se materialice en un horizonte definido) e impacto (qué tan grave sería el efecto) para determinar el nivel de riesgo, representado en una matriz de calor. Distingue entre riesgo inherente (sin considerar controles) y residual (después de aplicar los controles existentes), y algunos modelos incorporan la velocidad de materialización.

Tratamiento de riesgos: La respuesta se define según el costo, la efectividad y el apetito de riesgo: evitar, transferir, mitigar o aceptar el riesgo. La aceptación de riesgos materiales requiere aprobación del nivel jerárquico correspondiente.

Monitoreo continuo: Se realiza mediante KRIs con umbrales y planes de respuesta, reportes periódicos para los órganos de gobierno y auditorías y evaluaciones independientes (de la tercera línea o externas), proporcionando información para una supervisión efectiva.

a) *Reporte [mensual o bimestral] al CEO: resumen ejecutivo de KRIs, eventos materiales y excesos sobre apetito.*

b) *Reporte [trimestral] al Comité de Riesgos: dashboard de riesgos materiales, evolución de KRIs, riesgos emergentes, estado de planes de mitigación, excesos sobre apetito.*

c) *Reporte anual al Consejo de Administración: revisión integral del perfil de riesgo, resultados del proceso anual de identificación y evaluación, evaluación de la efectividad del marco, recomendaciones de actualización de la Política y de la Declaración de Apetito de Riesgo.*

d) *Reportes ad-hoc: ante eventos materiales, riesgos emergentes significativos o excesos críticos sobre apetito que requieran acción inmediata.*

ARTÍCULO 17 — Escalamiento

Los excesos sobre apetito de riesgo se escalan conforme al siguiente esquema:

a) *Excesos dentro de la tolerancia: tratamiento por la primera línea, con notificación al Departamento de Riesgos.*

b) *Excesos sobre la tolerancia pero dentro de la capacidad: notificación al CEO y al Comité de Riesgos para definir plan de acción.*

c) *Excesos materiales que pongan en riesgo la solvencia, continuidad o cumplimiento normativo: escalamiento inmediato al Consejo de Administración.*

Los plazos de escalamiento son definidos por el Comité de Riesgos en función de la materialidad y urgencia, y se documentan en el procedimiento operativo correspondiente.

CAPÍTULO VIII: DOCUMENTACIÓN Y SISTEMAS

ARTÍCULO 19 — Matriz Corporativa de Riesgos

La Compañía mantendrá una Matriz Corporativa de Riesgos como registro maestro consolidado de los riesgos identificados y evaluados. La Matriz contendrá, como mínimo, para cada riesgo:

- *identificador único;*
- *categoría según la taxonomía aprobada;*
- *nombre y descripción (causa, evento y consecuencia);*
- *dueño del riesgo en la primera línea;*
- *evaluación de probabilidad e impacto inherente y residual;*
- *controles existentes;*
- *posición frente al apetito de riesgo aprobado;*
- *indicadores clave asociados;*
- *plan de tratamiento con responsables y plazos; y*
- *fecha de última actualización.*

El Anexo III ayuda a definir responsabilidades con una **Matriz RACI** de gobierno del riesgo.

Concepto clave

La Matriz Corporativa es el instrumento que traduce la Política en operación cotidiana. Su calidad determina la calidad de todo el marco: si la Matriz está desactualizada o incompleta, los reportes al Comité y al Consejo pierden validez. Se recomienda un mecanismo formal de validación por los dueños de riesgo antes de cada consolidación, para evitar que la Matriz refleje únicamente la visión del Departamento de Riesgos. En empresas medianas la Matriz puede residir en una hoja de cálculo estructurada; a mayor madurez, en un sistema dedicado.

El Departamento de Riesgos es responsable de mantener la Matriz Corporativa, con los aportes documentados de los dueños de riesgo. La Matriz se actualizará al menos trimestralmente y de manera extraordinaria ante eventos materiales o cambios significativos del entorno. La Matriz estará disponible en todo momento para el Comité de Riesgos, el Consejo de Administración y la Auditoría Interna.

ARTÍCULO 20 — Indicadores Clave de Riesgo (KRIs)

Para cada riesgo material identificado en la Matriz Corporativa, se definirán Indicadores Clave de Riesgo (KRIs) que permitan monitorear su evolución y alertar oportunamente sobre desviaciones respecto al apetito aprobado. Los KRIs cumplirán con los siguientes criterios:

- *relevancia respecto al riesgo que monitorean;*
- *medibilidad objetiva con fuentes de datos verificables;*
- *carácter prospectivo (predictivo) cuando sea técnicamente posible; y*
- *oportunidad en su producción y reporte.*

Cada KRI contará con:

- *definición precisa y fórmula de cálculo;*
- *fuente de datos y responsable de su producción;*
- *frecuencia de medición y de reporte;*
- *umbrales de tolerancia diferenciados en tres niveles (verde: dentro del apetito; ámbar: cerca del límite; rojo: excede el apetito); y*
- *plan de respuesta ante cada nivel de alerta.*

Los KRIs serán propuestos por el Departamento de Riesgos en coordinación con los dueños de riesgo, validados por el Comité de Riesgos y revisados al menos anualmente. El seguimiento agregado de KRIs se incluirá en los reportes trimestrales al Comité y en el reporte anual al Consejo.

ARTÍCULO 21 — Sistemas, Herramientas y Repositorio Documental

La Compañía dispondrá de los sistemas y herramientas necesarios para soportar los procesos de identificación, evaluación, tratamiento, monitoreo y reporte de riesgos, proporcionales a su tamaño y complejidad. Los sistemas asegurarán la integridad de la información, la trazabilidad de los cambios (audit trail), el control de acceso diferenciado por rol y la continuidad operativa mediante copias de respaldo.

Se mantendrá un Repositorio Documental centralizado del marco de gestión del riesgo, que contendrá al menos:

- *la presente Política vigente y sus versiones anteriores;*
- *la Declaración de Apetito de Riesgo vigente;*
- *la Matriz Corporativa de Riesgos;*

KRI vs. KPI

La distinción entre KRI (Key Risk Indicator) y KPI (Key Performance Indicator) es importante y frecuentemente olvidada. Los KPIs miden desempeño pasado; los KRIs anticipan riesgo futuro. Un KRI útil detecta la presión antes de que se produzca la pérdida. Como referencia, una empresa mediana típicamente monitorea entre 20 y 40 KRIs corporativos; un número mayor tiende a saturar la capacidad de análisis del Comité y del Consejo. Se recomienda revisar la calibración de los umbrales al menos una vez al año, ya que umbrales desactualizados generan tanto falsas alarmas como falsos negativos.

- *los reportes periódicos al Comité y al Consejo;*
- *las actas de las sesiones del Comité de Riesgos en lo pertinente;*
- *los registros de eventos materiales y lecciones aprendidas; y*
- *los informes de la Auditoría Interna sobre el marco.*

El Repositorio estará bajo la custodia del Departamento de Riesgos. Los períodos de retención documental se ajustarán a los requisitos legales y regulatorios aplicables, con un mínimo de [X] años para los documentos que sustenten decisiones materiales.

CAPÍTULO IX: REVISIÓN Y ACTUALIZACIÓN

ARTÍCULO 22 — Revisión anual y ante detonantes

La presente Política será revisada de manera integral al menos una vez al año por el Departamento de Riesgos, con participación del Comité de Riesgos y aprobación final del Consejo de Administración. La revisión anual se calendarizará de manera coordinada con el ciclo de planeación estratégica y presupuestaria de la Compañía.

Adicionalmente a la revisión anual, se realizarán revisiones extraordinarias ante los siguientes detonantes:

a) cambios materiales en la estrategia o el modelo de negocio;

b) reorganizaciones corporativas significativas, incluyendo fusiones, adquisiciones y escisiones;

c) cambios regulatorios relevantes que afecten el marco de gestión del riesgo;

d) eventos adversos materiales que evidencien debilidades del marco vigente;

e) recomendaciones críticas de la Auditoría Interna o de evaluadores externos; y

f) modificaciones sustantivas en los estándares internacionales de referencia adoptados por la Compañía.

La revisión evaluará la vigencia y adecuación de los principios, la estructura de gobierno, la Declaración de Apetito de Riesgo, la taxonomía, los KRIs, el proceso de gestión del riesgo y los flujos de reporte.

ARTÍCULO 23 — Proceso y responsables de la actualización

Las modificaciones a la presente Política se sujetarán al siguiente proceso:

1) el Jefe de Riesgos (CRO) elabora la propuesta de modificación, con la justificación técnica y el análisis de impacto correspondiente;

2) la propuesta se somete a consulta previa con el CEO, la Alta Gerencia, la Auditoría Interna y las áreas de Cumplimiento y Legal, cuyos comentarios se documentan formalmente;

3) el Comité de Riesgos revisa la propuesta y las observaciones recibidas, y emite recomendación al Consejo;

Concepto clave

La revisión anual es un ejercicio de aseguramiento del marco, no una reescritura. En condiciones normales, la mayoría de los elementos permanecerán estables y solo se ajustarán componentes específicos (calibración de umbrales, incorporación de riesgos emergentes, ajustes al RAS).

Los cambios estructurales frecuentes en la Política son en sí mismos una señal de advertencia, ya sea de un diseño original deficiente o de falta de estabilidad estratégica.

Documentar formalmente que la revisión concluyó sin cambios materiales es tan valioso como documentar los cambios: acredita ante auditores externos, reguladores y financiadores que el ejercicio se realizó efectivamente.

4) el Consejo de Administración aprueba la modificación e instruye su comunicación e implementación.

Las modificaciones materiales de la Política (aquellas que alteran la estructura de gobierno, la Declaración de Apetito de Riesgo, la taxonomía principal o los procesos críticos de escalamiento) requieren siempre aprobación del Consejo en pleno. Las modificaciones menores de carácter aclaratorio o formal podrán ser aprobadas por el Comité de Riesgos, con reporte informativo al Consejo.

Toda modificación aprobada se comunicará formalmente a la Alta Gerencia y a los responsables involucrados en un plazo no mayor a [30] días hábiles desde su aprobación, y se incorporará al Repositorio Documental con la actualización del control de versiones.

ARTÍCULO 24 — Mejora continua

La Compañía adopta el principio de mejora continua sobre el marco de gestión del riesgo. A tal efecto, incorporará sistemáticamente al proceso de revisión las siguientes fuentes de aprendizaje:

a) las lecciones aprendidas de eventos adversos, cuasi-incidentes y excesos sobre apetito ocurridos en el período;

b) los hallazgos y recomendaciones de la Auditoría Interna en sus revisiones del marco;

c) los resultados de evaluaciones externas independientes cuando se realicen;

d) las prácticas emergentes en empresas comparables y en la evolución de los estándares internacionales; y

e) los aportes de partes interesadas relevantes, incluyendo inversionistas, financiadores y reguladores.

El Departamento de Riesgos mantendrá un registro documentado del proceso de mejora continua, que incluirá las fuentes consideradas, las decisiones de incorporación o descarte, y las acciones implementadas. Este registro será reportado anualmente al Comité de Riesgos.

CAPÍTULO X: DISPOSICIONES FINALES

ARTÍCULO 25 — Aprobación, vigencia y control de versiones

La presente Política entra en vigor a partir de su aprobación por el Consejo de Administración, previa recomendación del Comité de Riesgos, y reemplaza cualquier versión anterior o documento equivalente. La Política tendrá vigencia indefinida hasta su modificación o derogación por el Consejo.

Se mantendrá un control de versiones que documente, para cada versión aprobada: número de versión, fecha de aprobación por el Consejo, número de acta correspondiente, síntesis de los cambios respecto a la versión anterior, y responsable de la custodia del documento.

ARTÍCULO 26 — Disposiciones transitorias

[En aquellos casos en que la Compañía no cuente al momento de aprobación de la presente Política con la totalidad de las estructuras y funciones aquí previstas, se aplicarán las siguientes disposiciones transitorias:

- *Cuando el Comité de Riesgos no se encuentre formalmente constituido, sus funciones serán ejercidas por el Consejo de Administración en pleno o, si existiese, por el Comité de Auditoría. La Compañía se compromete a constituir formalmente el Comité de Riesgos, o a formalizar un Comité combinado de Auditoría y Riesgo, en un plazo no mayor a [doce (12)] meses desde la aprobación de la presente Política.*
- *Cuando la Compañía no cuente con un Jefe de Riesgos (CRO) dedicado, sus responsabilidades serán asumidas transitoriamente por [el Director Financiero (CFO) / el Director de Cumplimiento / el CEO], preservando en lo posible la línea de reporte funcional al Comité correspondiente. La designación de un CRO dedicado se realizará en un plazo no mayor a [dieciocho (18)] meses o cuando lo justifique la evolución del perfil de riesgo.*
- *Cuando la Declaración de Apetito de Riesgo no cuente aún con métricas cuantitativas por categoría, se aprobará una primera versión cualitativa que se enriquecerá progresivamente en ciclos anuales sucesivos.*
- *Los procedimientos operativos derivados de la presente Política se elaborarán y aprobarán en un plazo no mayor a [seis (6)] meses desde la vigencia del presente documento.]*

Concepto clave

Las disposiciones transitorias son especialmente relevantes en empresas medianas que aprueban su primera Política de Gobierno y Gestión del Riesgo sin contar aún con toda la infraestructura ideal. Reconocer explícitamente estas brechas y comprometer plazos concretos para cerrarlas es preferible a redactar una Política aspiracional que no refleja la realidad. Los plazos indicados son referenciales; cada empresa debe calibrarlos a su capacidad efectiva de ejecución. Sin plazos, las disposiciones transitorias tienden a volverse permanentes.

ARTÍCULO 27 — Custodia, publicación y comunicación

La custodia formal de la presente Política corresponde a [el Secretario Corporativo / el Jefe de Riesgos], quien asegurará que la versión vigente esté disponible en el Repositorio Documental y que las versiones históricas se conserven conforme al régimen de retención aplicable.

La Política será comunicada formalmente a la Alta Gerencia, a los mandos medios con responsabilidades de gestión del riesgo y a todo el personal cuya función se vea afectada por sus disposiciones. La comunicación incluirá una sesión de sensibilización cuyo alcance se ajustará al rol del destinatario.

La Política se incorporará al programa de inducción de nuevos colaboradores con responsabilidades relevantes. [En el caso de empresas de oferta pública, la Política, o un resumen ejecutivo de la misma, se publicará en el sitio web corporativo y se referenciará en el informe anual de gobierno corporativo.]

Concepto clave

La comunicación es la actividad que transforma un documento aprobado en una política efectivamente vigente. Se recomienda diferenciar el contenido y la profundidad según el destinatario: sesiones detalladas para la Alta Gerencia y responsables directos; sesiones sintéticas para el personal general; incorporación al *onboarding* de nuevos ingresos. En empresas listadas, la publicación externa refuerza la rendición de cuentas ante inversionistas y mercado.

ARTÍCULO 28 — Anexos

Los siguientes documentos forman parte integrante de la presente Política y se consideran vigentes con ella:

a) *[Anexo I: Declaración de Apetito de Riesgo aprobada por el Consejo de Administración.*

b) *Anexo II: Taxonomía Corporativa de Riesgos.*

c) *Anexo III: Matriz RACI de gobierno del riesgo (asignación de responsabilidades por actividad).*

d) *Anexo IV: Plantilla de la Matriz Corporativa de Riesgos.*

e) *Anexo V: Glosario de términos.]*

Los [Anexos I y II] podrán ser actualizados por el Consejo de Administración a propuesta del Comité de Riesgos sin necesidad de reformar el cuerpo principal de la Política, dado su carácter dinámico. Los demás anexos podrán ser actualizados por el Comité de Riesgos con reporte informativo al Consejo. Toda actualización de un Anexo se comunicará conforme al Artículo 27.

Concepto clave

La separación entre el cuerpo principal (más estable) y los anexos (más dinámicos) permite mantener la Política vigente sin necesidad de someter al Consejo cambios menores. Es una práctica útil en empresas medianas que están en proceso de calibración y esperan realizar ajustes frecuentes durante los primeros ciclos. Es crítico, sin embargo, que las reglas sobre quién puede modificar qué queden claramente establecidas para evitar que la separación se preste a modificaciones no autorizadas.

Concepto Clave: La Declaración de Apetito de Riesgo (RAS)

La Declaración de Apetito de Riesgo (*Risk Appetite Statement* o RAS) es típicamente un anexo de la Política, pero merece tratamiento separado por su importancia. La RAS traduce la estrategia y los valores de la empresa en parámetros operacionales que orientan las decisiones del día a día.

Una RAS bien construida tiene tres componentes interrelacionados: una **declaración cualitativa** que articula la filosofía general de riesgo de la empresa; un **conjunto de declaraciones por categoría de riesgo** que especifican la postura para cada tipo (estratégico, financiero, operacional, etc.); y un **conjunto de métricas cuantitativas y cualitativas con sus respectivos límites**, que permiten monitorear el cumplimiento de la declaración.

Niveles de apetito recomendados: Una práctica eficaz consiste en utilizar una escala de cinco niveles de apetito por categoría de riesgo:

- Averso ("Risk Averse"): no se aceptan riesgos en esta categoría salvo en circunstancias excepcionales.
- Mínimo ("Minimal"): preferencia clara por opciones de bajo riesgo, asumiendo solo riesgos residuales muy bajos.
- Cauto ("Cautious"): preferencia por opciones seguras con bajo nivel de riesgo residual y limitada oportunidad de ganancia.
- Abierto ("Open"): disposición a considerar todas las opciones, eligiendo aquella con mayor probabilidad de lograr el objetivo, considerando el riesgo.
- Hambriento ("Hungry"): disposición a considerar opciones innovadoras o más riesgosas que ofrecen retornos superiores, asumiendo conscientemente el riesgo asociado.

Fuente de la clasificación: HTM Orange Book (2023)

Concepto Clave: La Declaración de Apetito de Riesgo (RAS) (continuado)

Ejemplo de Declaración por Categoría:

Riesgo Reputacional: La Compañía adopta una postura aversa al riesgo reputacional. No se aceptarán acciones que puedan generar daño reputacional material, incluso si ofrecen oportunidades de retorno significativas. Las decisiones que involucren impacto reputacional potencial deben ser escaladas al Comité de Riesgos.

Riesgo Financiero - Liquidez: La Compañía adopta una postura cauta. Mantiene una posición de liquidez que cubre al menos [X] meses de necesidades operativas en escenarios de estrés. Cualquier desviación material requiere aprobación del Comité de Riesgos.

Riesgo de Innovación: La Compañía adopta una postura abierta. Acepta inversiones en innovación que puedan no generar retorno positivo en el corto plazo, dentro del [X]% del presupuesto anual de I+D, con seguimiento trimestral por el Comité de Estrategia.

Errores frecuentes al redactar la RAS:

Tres errores son comunes al redactar la primera Declaración de Apetito de Riesgo:

i. declaraciones genéricas que aplican igual a cualquier empresa ("buscamos minimizar el riesgo manteniendo retornos atractivos"), que no orientan ninguna decisión real;

ii. declaraciones sin métricas asociadas, que impiden monitorear el cumplimiento; y

iii. declaraciones inconsistentes con la estrategia aprobada (declarar aversión al riesgo cuando la estrategia es de crecimiento agresivo).

Una buena RAS es específica, medible y coherente con la estrategia. Ver un modelo de RAS en el Anexo I.

3. GUÍA PASO A PASO PARA LA IMPLEMENTACIÓN

Desarrollar e implementar la Política de Gobierno y Gestión del Riesgo es un proyecto que típicamente se ejecuta en un horizonte de seis a doce meses, aunque las empresas con marcos previos pueden hacerlo en menos tiempo y las que parten desde cero pueden requerir más tiempo.

Fase de preparación

1

Mes 1

Acción 1: Designar al líder del proyecto y obtener mandato del Consejo

El primer paso es designar al líder del proyecto (idealmente el CRO o, en su ausencia, un miembro de la Alta Gerencia) y obtener un mandato formal del Consejo de Administración. Este debe definir el alcance, plazos, recursos, un Consejero como punto focal y los entregables esperados: la Política de Gestión de Riesgos, la Declaración de Apetito de Riesgo y el plan de implementación. Sin este mandato, el proyecto pierde prioridad y autoridad para coordinar con las distintas áreas.

Acción 2: Diagnóstico del estado actual del marco de riesgo

Antes de redactar la Política, es necesario evaluar la situación actual para identificar prácticas existentes, estructuras de gobierno, documentos relacionados y brechas frente a las mejores prácticas. El diagnóstico se realiza mediante entrevistas, revisión documental, benchmarking y, opcionalmente, apoyo de consultores externos, culminando en un informe que prioriza las principales áreas de mejora.

Fase de diseño

2

Meses 2 a 4

Acción 3: Definir la estructura de gobierno del riesgo

Antes de redactar la Política, deben definirse aspectos clave como la estructura de comités, la designación del CRO, la aplicación del modelo de Tres Líneas y la relación con cumplimiento, ética y auditoría interna, con la participación del Consejo.

Acción 4: Redactar la Política

Con la gobernanza definida, se redacta una Política clara, práctica y adaptada a la empresa. Es recomendable elaborar primero un borrador completo y perfeccionarlo en sucesivas revisiones para

"Quick wins"

La mayoría de las empresas ya cuenta con prácticas de gestión de riesgos distribuidas en distintos documentos. El objetivo es consolidarlas y armonizarlas en un marco coherente, aprovechando lo existente para ahorrar tiempo y reducir la resistencia al cambio.

detectar inconsistencias y vacíos, sobre todo cuando, en paralelo, el Consejo defina el RAS (ver acción 5).

Acción 5: Redactar la Declaración de Apetito de Riesgo

En paralelo a la acción 4, el Consejo debe definir el nivel de riesgo aceptable por categoría y establecer métricas y límites cuantitativos mediante talleres, análisis históricos y de escenarios, para luego validar y formalizar la Declaración.

Fase de validación y aprobación

3

Meses 5 a 6

Acción 6: Consulta con stakeholders clave

Antes de presentar el borrador al Comité de Riesgos para su revisión formal, debe consultarse con los stakeholders clave, que aportarán perspectivas que enriquecen el documento: el CEO y los miembros de la Alta Gerencia (asegurar la viabilidad operativa); el responsable de Auditoría Interna (alineación con la tercera línea y con el plan de auditoría); el responsable legal (alineación regulatoria); el responsable de Cumplimiento; y los auditores externos (a título informativo).

Las observaciones identifican problemas materiales antes de que el documento llegue al Consejo, lo que ahorra tiempo y evita el desgaste de las revisiones tardías. Cada comentario debe ser considerado y, si no se acepta, debe documentarse el motivo.

Acción 7: Revisión por el Comité de Riesgos y aprobación por el Consejo

Con el borrador validado por los stakeholders, se presenta formalmente al Comité de Riesgos (o al Comité que haga sus veces) para su revisión. El Comité típicamente requiere una o dos sesiones para profundizar en los temas más críticos: la Declaración de Apetito de Riesgo, las responsabilidades del CRO y el proceso de escalamiento. Tras incorporar los comentarios del Comité, este recomienda al Consejo la aprobación del documento.

La aprobación por el Consejo se documenta formalmente en acta. Se recomienda que la sesión incluya una presentación ejecutiva del documento (no solo su entrega), permitiendo a los Consejeros formular preguntas y comprender plenamente el marco que están aprobando. La aprobación es el hito que da vida formal a la Política.

Fase de implementación

4

Meses 6 a 9

Acción 8: Comunicación y capacitación

Una Política aprobada pero desconocida no genera cambio. La comunicación debe ser sistemática y multicapa: una comunicación formal del CEO o del Presidente del Consejo a toda la organización anunciando la aprobación; sesiones de capacitación diferenciadas para distintos públicos (Alta Gerencia, mandos medios, dueños de procesos, equipo del Departamento de Riesgos); incorporación del contenido en los programas de inducción de nuevos colaboradores; y disponibilidad permanente del documento en los repositorios documentales de la empresa.

Acción 9: Integración con políticas y procesos existentes

La Política no opera en el vacío. Requiere integrarse con: el reglamento del Comité de Riesgos (o de Auditoría y Riesgo); los términos de referencia del Jefe de Riesgos; los manuales operativos y procedimientos de las distintas áreas; los procesos de planeación estratégica y presupuestaria; los procesos de aprobación de inversiones, contratos y compromisos; las políticas de compensación variable (incorporando consideraciones de riesgo); el plan anual de auditoría interna.

Fase de monitoreo y mejora continua

5

Continuo, a partir del mes 9

Acción 10: Establecer el ciclo de monitoreo, reporte y mejora continua

La implementación culmina con el establecimiento del ciclo recurrente de operación: el cronograma anual de identificación y evaluación de riesgos; la cadencia de reportes al Comité y al Consejo (típicamente trimestral para el Comité, anual integral para el Consejo); el calendario de revisión de la Política (anual, como mínimo); y el proceso de revisión y actualización de la Declaración de Apetito de Riesgo (anual, alineado con el ciclo de planeación estratégica).

El primer año de operación es el más importante: pone a prueba todos los elementos del marco y revela qué funciona y qué requiere ajustes. Es recomendable que al cabo del primer año el Comité de Riesgos realice una evaluación formal de la implementación y proponga al Consejo las modificaciones que correspondan.

Cronograma variable

Empresas que ya cuentan con elementos previos de gestión del riesgo (un Comité que cubre temas de riesgo, un mapa de riesgos previo, alguna política dispersa) pueden ejecutar el proyecto en cuatro a seis meses. La diferencia se concentra en las fases 1 y 2.

4. CONSIDERACIONES DE TIEMPO

La gestión del riesgo es por naturaleza dinámica, y la política debe acompañar esa dinámica sin perder estabilidad.

Detonantes para desarrollar o reformar la política

Más allá de la conveniencia general de contar con una política formal, existen detonantes específicos que aumentan la urgencia de desarrollarla o reformarla. Reconocer estos detonantes oportunamente permite anticipar la decisión y evitar desarrollar la política en condiciones de presión.

Detonantes estratégicos y de negocio

- **Reforma de gobierno corporativo:** cuando la empresa decide profesionalizar su gobierno (incorporación de Consejeros independientes, formación de comités, separación de los roles del fundador) es el momento natural para desarrollar la política.
- **Cambio en la estrategia:** una nueva estrategia (entrada a nuevos mercados, lanzamiento de líneas de negocio, transformación digital) genera nuevos perfiles de riesgo que requieren formalización.
- **Crecimiento o transformación corporativa:** fusiones, adquisiciones, escisiones o reorganizaciones requieren actualizar el marco de gestión del riesgo.
- **Preparación para una salida a bolsa (OPA):** los reguladores de valores y los inversionistas institucionales exigen un marco formal antes de la cotización. Desarrollarlo con anticipación reduce el costo y evita retrasos.
- **Llegada de un inversionista institucional o financiero externo:** fondos de inversión, bancos de desarrollo como BID Invest y otros inversionistas institucionales típicamente exigen el marco como condición de su inversión.
- **Transición generacional en empresas familiares:** el paso de una generación a otra es el momento idóneo para institucionalizar prácticas que dependían de las personas.

Detonantes regulatorios y externos

- **Cambio regulatorio:** nuevas exigencias de gobierno corporativo o de gestión del riesgo emitidas por reguladores sectoriales (valores, banca, seguros, energía, telecomunicaciones, salud) que aplican a la empresa.
- **Eventos adversos materiales:** fraudes significativos, fallos operacionales graves, sanciones regulatorias, daño reputacional o crisis financieras revelan debilidades del marco previo y exigen su revisión.

Mejor anticiparse que reaccionar

La peor situación para desarrollar una política es bajo presión externa: un regulador que exige el documento en treinta días, un inversionista cuyo cierre depende de su existencia, o una crisis que reveló su ausencia. En estas circunstancias, el documento se desarrolla apresuradamente, no captura las particularidades de la empresa, y termina siendo letra muerta. Anticiparse a los detonantes permite un desarrollo metódico que genera un documento útil y duradero.

- **Recomendaciones de auditores externos o internos:** hallazgos materiales sobre deficiencias del marco de gestión del riesgo.
- **Cambios materiales en el entorno:** crisis macroeconómicas, pandemias, cambios geopolíticos significativos, transformaciones tecnológicas disruptivas o intensificación de los riesgos climáticos.

Frecuencia de revisión y actualización

La Política debe revisarse periódicamente para mantener su vigencia sin afectar la estabilidad necesaria para su implementación.

La práctica recomendada es realizar una **revisión integral anual**, alineada con el ciclo de planificación estratégica, para verificar que la Política, el Apetito de Riesgo, la taxonomía de riesgos, los KRIs, los procesos y los reportes continúen siendo adecuados. La revisión suele ser liderada por el CRO, validada por el Comité de Riesgos y, cuando corresponda, aprobada por el Consejo.

Además, deben realizarse **revisiones extraordinarias** cuando ocurran eventos relevantes, como cambios estratégicos, reorganizaciones, crisis, modificaciones regulatorias o el ingreso a nuevos mercados, actualizando únicamente los componentes afectados.

En organizaciones con una gestión de riesgos más madura, algunas **categorías de riesgo** pueden revisarse con frecuencias diferenciadas según su nivel de dinamismo, por ejemplo, de forma trimestral, semestral, anual o bianual.

Integración con el calendario anual de gobierno corporativo

La Política y sus componentes asociados deben articularse con el resto del calendario anual de gobernanza para evitar duplicaciones, generar sinergias y asegurar que las decisiones se tomen sobre información actualizada y consistente:

- **Q1:** Cierre del año anterior: revisión del perfil de riesgo del año, evaluación de KRIs, lecciones aprendidas. Inicio del proceso anual de identificación y evaluación de riesgos..
- **Q2:** Consolidación del mapa anual de riesgos. Propuesta de actualización de la RAS. Revisión por el Comité de Riesgos. Coordinación con el plan anual de auditoría interna.
- **Q3:** Aprobación por el Consejo de la Declaración de Apetito de Riesgo actualizada. Definición de KRIs y umbrales para el año siguiente. Revisión integral de la Política y propuesta de actualizaciones materiales.
- **Q4:** Aprobación por el Consejo de las actualizaciones a la Política. Integración con el ciclo presupuestario y de planeación estratégica. Capacitación al Consejo y Comité sobre cambios materiales. Preparación del cierre anual.

5. DESAFÍOS DE IMPLEMENTACIÓN Y ESCENARIOS CRÍTICOS

Señales de advertencia de implementación deficiente

Problemas en la fase de desarrollo.

La primera señal de problemas surge cuando el desarrollo del documento **se delega completamente a un consultor externo o al equipo de control sin involucrar activamente al Consejo y a la Alta Gerencia.** El resultado es un documento técnicamente correcto pero desconectado de la realidad estratégica de la empresa, que la cúpula no siente como propio y, por tanto, no defiende ni implementa con convicción.

Cómo abordarlo: La respuesta pasa por rediseñar el proyecto como un ejercicio de co-construcción, no de externalización. Incluso cuando se contrate apoyo externo especializado, el liderazgo del proyecto debe recaer en una figura interna con peso institucional, respaldada por un mandato explícito del Consejo. El consultor aporta metodología y benchmarking; la empresa aporta contexto estratégico y decisiones. Cuando la Alta Gerencia percibe que ha construido el documento, lo defiende; cuando percibe que lo ha recibido, lo tolera.

Otra señal preocupante es el **copia-pega regulatorio**, particularmente común en empresas que enfrentan presión regulatoria. La política se construye copiando el modelo de empresas comparables (frecuentemente del sector financiero), sin adaptación al contexto. Un marco diseñado para una entidad bancaria con miles de empleados será completamente inadecuado para una empresa industrial mediana familiar, y viceversa.

Cómo abordarlo. El diagnóstico inicial del estado actual es la barrera natural contra este problema, y debe realizarse antes de mirar cualquier modelo externo. El diagnóstico responde tres preguntas: qué riesgos son realmente materiales para nuestro

Equipos multidisciplinarios y auditores invitados

Dada la velocidad de cambio del entorno, los equipos de Auditoría Interna deberían combinar formaciones diversas (contabilidad, TI, ingeniería, ASG, derecho). Cuando una auditoría específica requiere *expertise* que el equipo no tiene, una práctica interesante es la figura del "auditor invitado" (*guest auditor*): un profesional especializado, contratado puntualmente o tomado en préstamo de otra área, que se integra al equipo bajo la dirección del JAI únicamente para ese encargo. Es particularmente útil para empresas medianas con presupuestos acotados.

negocio; qué prácticas de gestión del riesgo ya existen en la empresa aunque no estén formalizadas; y qué capacidad efectiva tenemos para operar el marco que aprobemos.

La **ausencia de la Declaración de Apetito de Riesgo o su redacción genérica** es otra señal crítica. Si la política habla extensamente del proceso de gestión del riesgo pero no contiene declaraciones específicas y medibles sobre cuánto riesgo está dispuesta a asumir la empresa por categoría, el documento tiene un agujero estructural que lo convierte en operativamente inútil.

Cómo abordarlo. Cuando el Consejo se resiste a comprometerse con métricas cuantitativas, la respuesta no es renunciar a la RAS sino secuenciarla en dos fases. La primera versión de la RAS puede ser cualitativa: articula la postura por categoría de riesgo utilizando la escala de cinco niveles (averso, mínimo, cauto, abierto, hambriento) sin obligar a definir umbrales numéricos. Esta versión es menos amenazante y permite construir el hábito de la conversación sobre apetito en el Consejo. En la revisión anual siguiente se introducen métricas cuantitativas, comenzando por las categorías más medibles (financieras) y progresando hacia las menos cuantificables (estratégicas, reputacionales). Adicionalmente, para cada declaración cualitativa se exige documentar el sustento: qué evidencia interna o de mercado la fundamenta, y qué decisiones concretas cambiarían si la postura fuera diferente. Este ejercicio convierte declaraciones vacías en compromisos operativos.

Problemas en la fase de implementación.

La señal más común de implementación deficiente es la **persistencia de prácticas previas a la política**. Pasados varios meses de la aprobación, las decisiones se siguen tomando como antes, los reportes al Comité no incluyen información de riesgo, los KRIs no se monitorean, la Declaración de Apetito de Riesgo no se utiliza como criterio de decisión. Cuando esto ocurre, el documento existe en el repositorio pero no en la operación.

Cómo abordarlo. La política solo desplaza las prácticas anteriores cuando se integra activamente en los procesos de decisión en los que dichas prácticas se materializan. Concretamente, esto exige modificar los procesos de aprobación existentes: los memorandos de inversión, las propuestas de crédito, los contratos materiales y las decisiones estratégicas deben incorporar una sección de riesgo, con la opinión del Departamento de Riesgos y la verificación de la consistencia con el apetito aprobado. En paralelo,

los reportes al Comité y al Consejo se rediseñan para incluir sistemáticamente información de riesgo, con un dashboard de KRIs, la evolución respecto al apetito y los riesgos emergentes. Una técnica eficaz consiste en fijar una fecha de corte a partir de la cual ningún expediente relevante avance sin la sección de riesgo formalizada. Adicionalmente, el CEO debe incorporar el estado de implementación de la política como punto recurrente en sus reuniones ordinarias con la Alta Gerencia durante los primeros seis a doce meses. Sin este empuje sostenido desde la cúpula ejecutiva, la inercia organizacional vuelve a las prácticas anteriores.

Otra señal crítica es el **aislamiento de la función de gestión del riesgo.** Si el Departamento de Riesgos opera como un silo, sin interacción con las unidades de negocio, sin participar en las decisiones estratégicas y sin presencia en los foros directivos clave, su capacidad de influencia es nula y la implementación de la política se limita a la elaboración de reportes formales que nadie utiliza.

Cómo abordarlo. La respuesta estructural consiste en integrar al Departamento de Riesgos en los foros donde se toman las decisiones, no solo en los foros donde se supervisa el riesgo. Esto significa la presencia formal del CRO (o de su delegado) en el Comité Ejecutivo o su equivalente, en el comité de inversiones o de crédito, en las revisiones estratégicas trimestrales y en la elaboración del plan de negocio y del presupuesto. La presencia debe darse con voz consultiva y con opinión escrita cuando corresponda, no solo como observador. Complementariamente, el modelo operativo del Departamento debe combinar dos ejes: un núcleo central que mantiene la metodología, la matriz corporativa y el reporte agregado; y una red de “risk champions” distribuidos en las unidades de negocio, que actúan como enlace con la primera línea y aseguran que la conversación sobre riesgo se dé donde efectivamente se generan las exposiciones. Sin esta red distribuida, incluso un Departamento central técnicamente sólido termina aislado.

La **falta de escalamiento oportuno** es una señal especialmente peligrosa. Cuando los excesos sobre apetito de riesgo no se reportan al Comité y al Consejo en los plazos previstos, o cuando se reportan diluidos en información menos relevante, la supervisión se compromete y el riesgo material crece silenciosamente hasta su materialización.

Cómo abordarlo. El escalamiento eficaz requiere reglas explícitas, canales protegidos y responsabilidad personal identificada. En primer lugar, la política debe definir con precisión los umbrales que activan el escalamiento automático, los plazos máximos entre la detección y la comunicación (típicamente de 24 a 72 horas, según la severidad) y los destinatarios obligatorios en cada nivel. En segundo lugar, deben existir canales que no dependan de la Alta Gerencia para funcionar: la línea de reporte funcional del CRO al Comité de Riesgos, las sesiones privadas (executive sessions) del Comité con el CRO, sin presencia de la Alta Gerencia, al menos una vez al año, y el derecho documentado del CRO a acceder al Presidente del Comité o al Consejo, en caso necesario. En tercer lugar, la responsabilidad por el escalamiento debe estar personalmente asignada: el CRO es responsable de escalar exposiciones materiales que detecte, y el incumplimiento de este deber tiene consecuencias explícitas en su evaluación. Finalmente, el Comité debe reforzar el comportamiento correcto respaldando públicamente al CRO cuando escala información incómoda; el momento en que la organización aprende que escalar es seguro es también el momento en que la cultura de escalamiento se consolida.

Escenarios "¿Qué pasaría si...?"

“¿Qué pasaría si el Consejo no aprueba la Declaración de Apetito de Riesgo?”

Algunos Consejos, especialmente en empresas familiares o con prácticas de gobierno aún incipientes, pueden mostrarse reticentes a definir un apetito de riesgo explícito. En estos casos, se recomienda un enfoque gradual: comenzar con una Declaración de Apetito de Riesgo cualitativa, que establezca la postura general frente a cada categoría de riesgo, e incorporar progresivamente métricas cuantitativas en las revisiones posteriores, a medida que la organización fortalece su madurez en gestión de riesgos.

“¿Qué pasa si el CRO reporta un riesgo material que la Alta Gerencia minimiza?”

Este escenario, lamentablemente común, pone a prueba la integridad del marco de gobierno del riesgo. La línea de reporte funcional del CRO al Comité de Riesgos (no solo al CEO) es la respuesta estructural: el CRO tiene el deber y la facultad de reportar directamente al Comité y, si es necesario, al Consejo, sin mediación de la Alta Gerencia. La política debe ser explícita sobre este derecho y deber.

Adicionalmente, la práctica recomendada incluye sesiones privadas ("*executive sessions*") del Comité de Riesgos con el CRO, sin presencia de la Alta Gerencia, al menos una vez por año. Estas

Trampas comunes

- **Confundir la política con los procedimientos:** La política debe definir principios, responsabilidades y lineamientos generales, mientras que los procedimientos describen cómo ejecutar las actividades. Mantener ambos documentos separados facilita su comprensión y actualización.
- **Subestimar la RAS:** Una declaración genérica no orienta la toma de decisiones. Debe definir claramente el nivel de riesgo aceptable por categoría y evolucionar hacia métricas concretas alineadas con la estrategia.
- **Nombrar un CRO sin recursos ni respaldo:** La función de gestión de riesgos requiere recursos adecuados, acceso al Comité o al Consejo y una estructura organizacional que le permita desempeñar eficazmente sus responsabilidades.
- **Generar reportes demasiado extensos:** Los informes al Comité y al Consejo deben ser ejecutivos, claros y centrados en la información crítica, complementados con anexos cuando sea necesario.
- **Asignar funciones de segunda línea a Auditoría Interna:** La Auditoría Interna debe preservar su independencia como tercera línea de defensa. La Política debe definir claramente la separación de responsabilidades entre gestión de riesgos y auditoría interna.

sesiones permiten conversaciones francas sobre tensiones que de otra manera no se ventilarían.

“¿Qué pasa si ocurre un evento material que excede el apetito aprobado?”

El protocolo de respuesta debe estar previsto en la Política. Como mínimo, debe contemplar: notificación inmediata al CEO y al CRO; reunión extraordinaria del Comité de Riesgos en plazos breves (24 a 72 horas, según la severidad); evaluación de la materialidad y de la necesidad de comunicación al Consejo; definición de un plan de acción correctivo; comunicación a partes interesadas externas (reguladores, inversionistas, auditores) cuando corresponda; y registro formal del evento para análisis ex-post y lecciones aprendidas.

La política también debe prever que las decisiones de aceptación de exposiciones que excedan el apetito aprobado solo pueden tomarse por el órgano apropiado según la materialidad: la Alta Gerencia puede aceptar excesos menores dentro de la tolerancia; el Comité aprueba excesos materiales dentro de la capacidad; el Consejo aprueba excesos críticos.

“¿Qué pasa si el Comité de Riesgos identifica una debilidad estructural del marco?”

El Comité, en su rol de supervisión, ocasionalmente identificará que el marco actual presenta debilidades estructurales que la implementación operativa no puede resolver: ausencia de recursos suficientes, inadecuación del CRO para el rol, deficiencias del proceso de identificación de riesgos, brechas en la taxonomía. La respuesta es elevar al Consejo la recomendación de modificar la Política o sus componentes asociados, presentando un diagnóstico claro y un plan de remediación. El Consejo, como aprobador final, decide y asigna los recursos correspondientes.

“¿Qué pasa si un nuevo riesgo emergente requiere atención inmediata?”

Riesgos emergentes (cibernético, climático, de inteligencia artificial, geopolítico) frecuentemente surgen entre ciclos anuales de revisión. La Política debe prever que el Comité de Riesgos puede incorporar nuevas categorías o KRIs sin esperar a la revisión anual, con notificación al Consejo. Esta agilidad es esencial: un marco rígido que solo se actualiza una vez al año puede no detectar a tiempo cambios materiales del entorno.

Alerta: el riesgo de la falsa sensación de control

Una de las consecuencias más peligrosas de un marco mal implementado es la falsa sensación de control: el Consejo asume que los riesgos están gestionados porque existe una política, pero la implementación es deficiente y los riesgos materiales no son detectados ni reportados oportunamente. Las consecuencias se revelan cuando un evento material ocurre y se descubre que las defensas eran ilusorias. La supervisión activa del Comité, las evaluaciones independientes de la Auditoría Interna y, cuando corresponda, evaluaciones externas periódicas son las herramientas que previenen este escenario.

6. ANEXOS Y RECURSOS

Glosario de Términos

A continuación, presentamos un glosario comprehensivo de los términos utilizados en este documento, incluyendo las variaciones terminológicas empleadas en los principales países de América Latina y el Caribe.

Término Utilizado	Definición
Apetito de Riesgo	Cantidad y tipo de riesgo que la organización está dispuesta a aceptar en la búsqueda de sus objetivos. Variante: "Apetito al Riesgo" (uso intercambiable). En inglés: Risk Appetite.
Capacidad de Riesgo	Máximo nivel de riesgo que la organización puede asumir sin comprometer su solvencia, continuidad o cumplimiento. En inglés: Risk Capacity.
Comité de Riesgos	Comité del Consejo especializado en supervisión del marco de gestión del riesgo. En empresas medianas frecuentemente combinado como "Comité de Auditoría y Riesgo".
Consejo de Administración	Órgano colegiado elegido por los accionistas para supervisar la gestión de la empresa. Conocido también como Junta Directiva (Colombia, Venezuela), Directorio (Chile, Perú, Argentina, Uruguay), o Consejo (México, España).
Cultura de Riesgo	Valores, creencias, conocimientos, actitudes y comportamientos compartidos sobre el riesgo. En inglés: Risk Culture.
Declaración de Apetito de Riesgo (RAS)	Documento aprobado por el Consejo que articula la postura cualitativa y cuantitativa sobre el riesgo. En inglés: Risk Appetite Statement.
Departamento de Riesgos	Unidad organizacional bajo el CRO. Variantes: Dirección de Riesgos, Gerencia de Riesgos, Área de Riesgos, Función de Riesgos.
Escalamiento	Proceso formal por el cual una exposición o evento se eleva al nivel jerárquico apropiado para su atención. Variante: Reporte ascendente.
Jefe de Riesgos (CRO)	Responsable máximo de la función de gestión del riesgo. Variantes: Director de Riesgos, Gerente de Riesgos, Oficial Principal de Riesgo, Chief Risk Officer (CRO).
KRI (Indicador Clave de Riesgo)	Métrica utilizada para monitorear la exposición a un riesgo y alertar sobre desviaciones. En inglés: Key Risk Indicator. Distinto del KPI (Key Performance Indicator).
Mapa de Riesgos	Representación visual de los riesgos identificados según probabilidad e impacto. Variantes: Matriz de Riesgos, Mapa de Calor (heat map).
Modelo de las Tres Líneas	Marco organizacional del IIA (2020) que distribuye responsabilidades de riesgo entre primera línea (operativa), segunda línea (supervisión y soporte) y tercera línea (auditoría interna). Sustituye al anterior "Modelo de las Tres Líneas de Defensa".
Primera Línea	Funciones que generan y gestionan riesgo en su operación cotidiana: unidades de negocio, procesos operativos, dueños de procesos.
Riesgo Emergente	Riesgo nuevo o evolutivo cuyo perfil aún no es completamente comprendido. Ejemplos: ciberseguridad avanzada, riesgos climáticos de transición, IA generativa, geopolíticos.
Riesgo Inherente	Nivel de riesgo en ausencia de controles. En inglés: Inherent Risk.
Riesgo Residual	Nivel de riesgo después de aplicar los controles existentes. En inglés: Residual Risk.
Segunda Línea	Funciones de supervisión y soporte sobre la primera línea: Gestión del Riesgo, Cumplimiento, Seguridad de la Información, entre otras.
Taxonomía de Riesgos	Clasificación estructurada de las categorías de riesgo de la organización.
Tercera Línea	Auditoría Interna, que provee aseguramiento independiente sobre la efectividad del marco completo.
Tolerancia al Riesgo	Variación aceptable respecto al apetito antes de requerir escalamiento. En inglés: Risk Tolerance.
Tono desde la Cima	Comportamiento y comunicaciones del Consejo y la Alta Gerencia que modelan la cultura organizacional. En inglés: Tone at the Top.

Anexo I: Modelo de RAS

La siguiente plantilla puede ser adaptada por cada empresa para construir su Declaración de Apetito de Riesgo. El siguiente modelo debe revisarse con asesoría legal local antes de su utilización.

DECLARACIÓN DE APETITO DE RIESGO — [Nombre de la Empresa]

Aprobada por el Consejo de Administración en sesión del [fecha]. Vigente hasta su próxima revisión, prevista para [fecha], salvo modificaciones excepcionales aprobadas por el Consejo.

1. Declaración Cualitativa General

[Nombre de la Compañía] desarrolla sus actividades [describir brevemente la actividad principal] con el objetivo de [objetivo estratégico de la empresa]. En la búsqueda de estos objetivos, asume riesgos de manera consciente, informada y dentro de los límites aprobados por el Consejo de Administración.

La Compañía mantiene una postura general [conservadora/moderada/agresiva — seleccionar] frente al riesgo, privilegiando [objetivos prioritarios: solvencia / crecimiento / retorno / continuidad / reputación] sobre [aspectos relativizables]. Las decisiones de toma de riesgos se enmarcan en el Modelo de las Tres Líneas y son supervisadas por el [Comité de Riesgos] del Consejo.

2. Apetito por Categoría de Riesgo

Se utiliza la siguiente escala de cinco niveles:

- Averso: no se aceptan riesgos en esta categoría salvo en circunstancias excepcionales aprobadas por el Consejo.
- Mínimo: preferencia clara por opciones de bajo riesgo. Solo se asumen riesgos residuales muy bajos.
- Cauto: preferencia por opciones seguras con bajo riesgo residual y oportunidad limitada de retorno.
- Abierto: disposición a considerar todas las opciones, eligiendo aquella con mayor probabilidad de éxito considerando el riesgo.
- Hambriento: disposición a considerar opciones innovadoras o de mayor riesgo que ofrecen retornos superiores.

CATEGORÍA	NIVEL	DECLARACIÓN ESPECÍFICA	MÉTRICA / LÍMITE
Estratégico	[Abierto]	Acepta inversiones estratégicas con horizonte de retorno de mediano plazo	ROI mínimo: [X]% en [Y] años
Financiero — Liquidez	[Cauto]	Mantiene cobertura para escenarios de estrés	Liquidez ≥ [X] meses
Financiero — Crédito	[Cauto]	Limita concentración por cliente y sector	Concentración cliente: ≤ [X]%
Operacional	[Mínimo]	No tolera fallos materiales en procesos críticos	Pérdidas operacionales: ≤ [X]% ingresos
Cumplimiento	[Averso]	No tolera incumplimientos materiales	[Cero] sanciones materiales
Reputacional	[Averso]	No acepta acciones que dañen la reputación	[Cero] eventos materiales/año

CATEGORÍA	NIVEL	DECLARACIÓN ESPECÍFICA	MÉTRICA / LÍMITE
Cibernético	[Mínimo]	Inversión continua en ciberseguridad	Madurez NIST: nivel [X]
ASG/ESG	[Cauto]	Cumple compromisos ambientales y sociales	Métricas ESG por sector
Innovación	[Hambriento]	Acepta inversiones que pueden no generar retorno corto plazo	Hasta [X]% del presupuesto I+D

3. Tolerancias y umbrales de escalamiento

Para cada métrica anterior, se establecen tres niveles de tolerancia:

- Verde: dentro del apetito. Gestión normal por la primera línea.
- Ámbar: cerca del límite. Notificación al CRO y al CEO. Plan de acción definido.
- Rojo: excede el apetito. Escalamiento inmediato al Comité de Riesgos. Si la materialidad lo amerita, escalamiento al Consejo dentro de [X] días hábiles.

4. Vigencia y revisión

Esta Declaración será revisada al menos anualmente, y antes ante: cambios materiales en la estrategia, eventos adversos significativos, cambios regulatorios relevantes, o reorganizaciones corporativas materiales. Las modificaciones serán propuestas por el Comité de Riesgos y aprobadas por el Consejo de Administración.

Anexo II: Plantilla de matriz de riesgos

La matriz de riesgos es la herramienta operativa que consolida los riesgos identificados, su evaluación y los planes de tratamiento. La plantilla siguiente es una estructura mínima recomendada que cada empresa puede expandir según su madurez.

Las escalas siguientes son referenciales. Cada empresa debe calibrar los umbrales financieros a su tamaño y estructura.

Escala de probabilidad (ejemplo)

NIVEL	DESCRIPCIÓN
1 — Raro	Probabilidad < 5% en el horizonte considerado. Evento muy improbable.
2 — Improbable	Probabilidad > 5 y ≤ 25%. Podría ocurrir en ciertas circunstancias.
3 — Posible	Probabilidad > 25 y ≤ 50%. Podría ocurrir bajo circunstancias normales.
4 — Probable	Probabilidad > 50 y ≤ 75%. Ocurrirá probablemente en el horizonte.
5 — Casi cierto	Probabilidad > 75%. Se espera que ocurra.

Escala de impacto (ejemplo)

NIVEL	DESCRIPCIÓN
1 — Insignificante	Impacto financiero < 0.1% ingresos; sin efecto reputacional o regulatorio.
2 — Menor	Impacto financiero > 0.1% y ≤ 1% ingresos; impacto reputacional local y temporal.
3 — Moderado	Impacto financiero > 1% y ≤ 5% ingresos; impacto reputacional regional; advertencia regulatoria.
4 — Mayor	Impacto financiero > 5% y ≤ 15% ingresos; impacto reputacional nacional; sanción regulatoria.
5 — Catastrófico	Impacto financiero > 15% ingresos; impacto reputacional internacional; crisis de continuidad.

Plantilla de Matriz

CAMPO	DESCRIPCIÓN	EJEMPLO
ID del riesgo	Identificador único	R-FIN-001
Categoría	Categoría según taxonomía	Financiero — Crédito
Nombre del riesgo	Denominación específica	Concentración cliente principal
Descripción	Causa, evento, consecuencia	Pérdida del cliente principal por...
Dueño del riesgo	Responsable primera línea	Director Comercial
Probabilidad inherente	Escala 1-5	3 — Posible
Impacto inherente	Escala 1-5	4 — Mayor
Nivel inherente	Producto P × I	12 — Alto
Controles existentes	Lista de controles	Diversificación cartera; SLAs...
Probabilidad residual	Después de controles	2 — Improbable
Impacto residual	Después de controles	3 — Moderado
Nivel residual	Producto P × I residual	6 — Medio
Apetito	Nivel apetito categoría	Cauto
Estado vs. apetito	Verde / Ámbar / Rojo	Verde
KRIs asociados	Métricas de monitoreo	Concentración cliente >X%
Plan de tratamiento	Acciones, responsable, plazo	Diversificar a 5 nuevos clientes en 12 meses
Última actualización	Fecha	[YYYY-MM-DD]
Próxima revisión	Fecha programada	[YYYY-MM-DD]

Anexo III: Matriz RACI de gobierno del riesgo

La matriz RACI distribuye con precisión las responsabilidades sobre las actividades clave del marco de gestión del riesgo. Las convenciones son:

R (Responsible) — responsable de la ejecución;

A (Accountable) — rinde cuentas;

C (Consulted) — consultado;

I (Informed) — informado.

Esta matriz es un punto de partida: cada empresa debe adaptarla a su estructura organizacional. En empresas con Comité combinado de Auditoría y Riesgo, las columnas "Comité de Riesgo" y "Auditoría Interna" se ajustan en consecuencia. En empresas sin CRO formal, las responsabilidades del CRO recaen transitoriamente en el CFO o en quien designe el Consejo. Lo crítico es que cada actividad tenga claramente identificado **un único responsable de rendir cuentas (A).**

ACTIVIDAD	Consejo	Comité Riesgo	CEO	CRO	1ª Línea	Aud. Interna
Aprobar la Política	**A**	**R**	C	C	I	I
Aprobar la RAS	**A**	**R**	C	**R**	I	I
Definir taxonomía de riesgos	I	**A**	C	**R**	C	I
Identificar riesgos materiales	I	C	**A**	**R**	**R**	C
Evaluar probabilidad e impacto	I	I	**A**	**R**	**R**	I
Definir tratamiento	I	C	**A**	C	**R**	I
Implementar controles	I	I	**A**	C	**R**	I
Monitorear KRIs	I	C	**A**	**R**	C	C
Reporte trimestral al Comité	I	**A**	C	**R**	C	I
Reporte anual al Consejo	**A**	**R**	C	**R**	I	I
Escalar excesos materiales	**A**	**R**	C	**R**	C	I
Aprobar excesos al apetito	**A**	**R**	C	C	I	I
Auditar el marco	**A**	C	I	C	I	**R**
Aprobar plan auditoría	I	C	I	I	I	**R**
Capacitar en riesgo	I	C	**A**	**R**	C	I
Revisar la Política anual	**A**	**R**	C	**R**	C	C

Fuentes

BID Invest, “IDB Invest Corporate Governance Tool” (2024)

Corporate Governance Development Framework, “Corporate Governance Progression Matrix” (2024)

Good Governance Institute, “Board guidance on risk appetite” (2020)

IIA, “The IIA’s Three Lines Model” (2020)

Institute of Risk Management (IRM), “Risk Appetite and Tolerance — Guidance Paper” (2011)

OECD, “G20/OECD Principles of Corporate Governance” (2023)

PSOJ, “Navigating Corporate Governance” (2024)

UK Government, “Risk Appetite Guidance Note” (2021)

UK Government, “The Orange Book Management of Risk – Principles and Concepts” (2026)