



ASOCIACIÓN INTERNACIONAL PARA LA COOPERACIÓN EN  
LA PREVENCIÓN DEL FRAUDE

~~LUNES~~  
LAS MARTES CLASS DE ICPF  
~~MIÉRCOLES~~  
~~JUEVES~~  
~~VIERNES~~

# El rol de los consejeros en el Buen Gobierno Corporativo y la lucha contra el fraude

Julia Sáez Torrecuadrada

Fecha: 23/06/26

[asociacionicpf.org](http://asociacionicpf.org)

# Algunos “sonados” terremotos

## El caso Enron

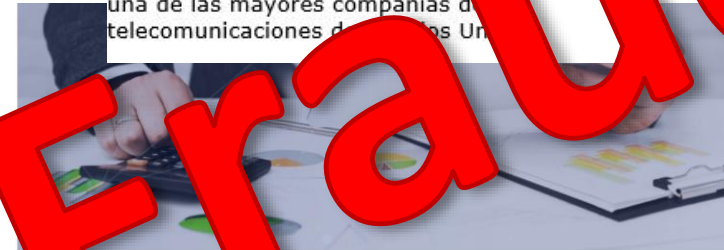
- En el año 2000, tan solo cinco años después de su creación, la eléctrica Enron consiguió aparecer en la lista de la revista Fortune como la séptima mayor compañía de Estados Unidos. Sin embargo, la gloria duró poco, ya que en 2001 se descubrirían numerosas irregularidades en las cuentas de la compañía que acabarían arrastrándola a la quiebra. El mayor escándalo financiero vivido por el país norteamericano hasta el momento ha llenado páginas y páginas en los periódicos de todo el mundo desde que comenzó a salir a la luz.



## Economía Miércoles, 26 de junio de 2002 - 20:55 GMT Caso WorldCom sacude los mercados



Los mercados bursátiles de todo el mundo se desplomaron este miércoles tras difundirse un multimillonario fraude contable en WorldCom, una de las mayores compañías de telecomunicaciones de los Estados Unidos.



WorldCom y el escándalo de fraude contable: reflexiones y recomendaciones para el mundo de la auditoría

## Auge y caída del imperio lácteo Parmalat, el mayor fraude de Europa

## La Audiencia imputa a la matriz de Volkswagen por el fraude de los motores trucados

El juez Moreno investiga a la matriz de la marca alemana por delitos de defraudación, fraude de subvenciones y contra el medio ambiente



## Claves del fiasco de Gowex: quién pagará la factura de su hundimiento

Los delitos por falsear cuentas por los que han denunciado a los administradores pueden suponer hasta seis años de cárcel

Las acciones seguirán suspendidas pero lo probable es un fuerte correctivo para el resto de las pymes que cotizan

El ICO recuerda que no asume el riesgo en sus líneas de crédito y son los bancos los que tendrán que asumir las pérdidas

- \* Falsificó sus cuentas durante años, ocultando un agujero de 14.000 millones
- \* Llegó a tener presencia en 30 países y dar trabajo a 37.000 personas
- \* Tanzi, condenado a 17 años de cárcel, falleció el pasado 2 de enero

# ¿Un mismo patrón?...



## **Supervisión ausente**

El consejo no vio —o no quiso ver— lo que ocurría bajo la dirección.



## **Auditoría debilitada**

Audidores poco independientes o sin medios para confrontar a la dirección.



## **Alertas desatendidas**

Hubo avisos —internos, reguladores o del mercado— que no se atendieron a tiempo.



**El fraude aparece...**

***Cuando el gobierno corporativo falla o es débil***

# El impacto del fraude: cifras que es necesario conocer

**5%**

de ingresos anuales pierden las organizaciones por fraude (est. ACFE)

**\$104K**

Pérdida mediana por caso

**12 m.**

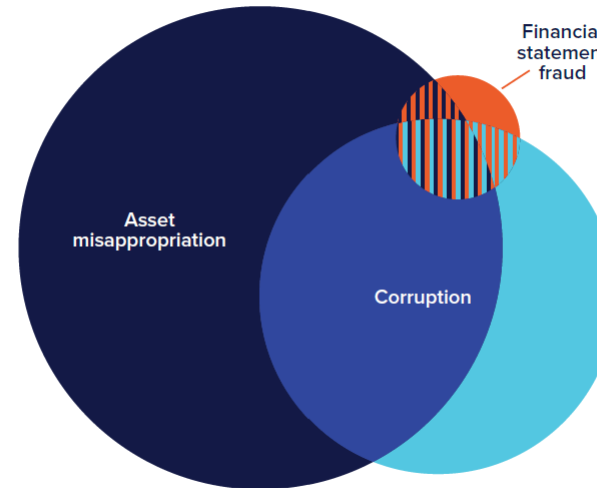
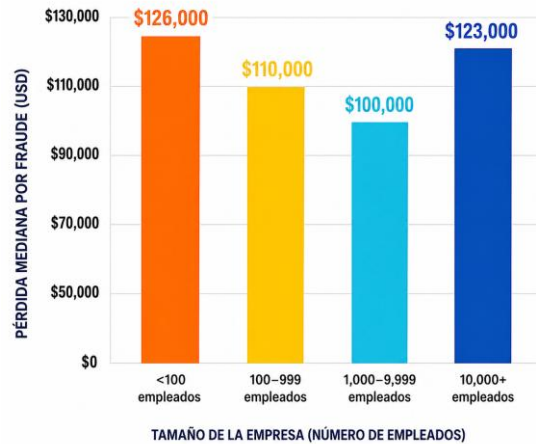
Duración media antes de detectar el fraude

**43%**

de detecciones provienen de denuncias (canal de denuncias)

Origen: Más de la mitad de las denuncias proceden de empleados

**2026**



Asset misappropriation and corruption	53%
Corruption only	33%
Corruption, asset misappropriation, and financial statement fraud	8%
Asset misappropriation and financial statement fraud	3%
Financial statement fraud only	1%
Corruption and financial statement fraud	1%

## LOS FRAUDES HAN ASCENDIDO EN EL ORGANIGRAMA.

	1996	2026
Empleados	58%	41%
Gerentes	30%	41%
Dueños/ejecutivos	12%	16%

# El impacto del fraude...



El fraude representa uno de los principales riesgos para la sostenibilidad de las organizaciones.

**Sus impactos no son únicamente económicos:**



Daño reputacional.



Pérdida de confianza de inversores, clientes y reguladores.



Responsabilidades legales y sanciones.



La experiencia demuestra que las organizaciones con una supervisión activa del Consejo detectan antes los riesgos y reducen la probabilidad de incidentes graves.



**La lucha contra el fraude no es una cuestión operativa; es una responsabilidad de gobernanza.**

# ¿Qué vamos a ver?

01

## Organización

Órganos y reparto de poder: junta, consejo, comisiones, dirección

02

## Gobierno


Principios y mecanismos con los que el consejo dirige y supervisa.

03

## El fraude y el Consejo de Administración

Buenas prácticas y supervisión





# Organización:

Órganos y reparto de poder: junta, consejo, comisiones, dirección

# Los órganos: quién decide qué



PROPIEDAD

## Junta General

- Órgano soberano: expresión de la propiedad.
- Aprobación de cuentas anuales (LSC art. 160.a), Nombramiento y cese de consejeros (LSC art. 160.b), Modificaciones estatutarias (LSC art. 160.c) Operaciones estructurales: fusiones, escisiones (LSC art. 160.g) Política de remuneraciones del Consejo (LSC art. 511 bis) Nombramiento del auditor de cuentas (LSC art. 264)
- Distribución de dividendos (LSC art. 160.a)



SUPERVISIÓN

## Consejo de Administración

**Aprueba la estrategia y supervisa tres ámbitos esenciales: los riesgos —asociados a esa estrategia—, el control interno y la información, financiera y de sostenibilidad.**

**Rinde cuentas a la Junta de Accionistas**



GESTIÓN Y EJECUCIÓN

## Alta dirección

- Ejecución de la estrategia aprobada por el Consejo
- Gestión ordinaria de la sociedad
- Liderazgo del equipo directivo
- Implantación de la cultura y valores corporativos
- Reporte periódico al Consejo
- Tone at the Top: la dirección marca el ejemplo ético y de cumplimiento para toda la organización

## Empleados y terceros

- Los empleados ejecutan procesos y controles: primera línea operativa de la entidad.
- Su actividad se ejecuta sobre los sistemas de información de la entidad
- Su conducta depende de formación, incentivos y canales para alzar la voz.
- Proveedores y terceros críticos: el perímetro de control no termina en la plantilla (externalización, modelos, tecnología).

# Consejos de Administración



## 1. Definición y Naturaleza

- **Órgano colegiado de gobierno**, responsable de tomar **decisiones estratégicas** y **supervisión de la gestión** de una sociedad
- Obligatorio en **Sociedades anónimas cotizadas** (mín. 3 miembros)
- En **Sociedades Limitadas y anónimas no cotizadas** flexible (único, solidario, consejo)
- En **empresas familiares** es menos común, pero aporta ventajas organizativas



## 2. Estructura

- **Presidente:** Convoca, dirige y asegura información
- **Consejeros:** Ejecutivos (gestión), Dominicales (propiedad) e Independientes (criterio)
- **Secretario:** Garantiza la redacción fiel de las actas y asesora en materia de cumplimiento normativo
- **Comisiones obligatorias:** Comisión de Auditoría y Comisión de Nombramientos y retribuciones y Comité de Riesgos (Entidades financieras)



## 3. Funciones esenciales

- **Estrategia:** Aprobación del plan estratégico y de negocio, objetivos, presupuesto, política de inversiones, y financiación, entre otras
- **Supervisión:** de la dirección ejecutiva, del cumplimiento legal y de los sistemas de control interno y gestión de riesgos
- **Nombramientos:** Selección, evaluación y retribución de consejeros y alta dirección. Plan de sucesión del primer ejecutivo
- **Información y transparencia:** Formulación de cuentas anuales, informe de gestión, información financiera periódica y, en su caso, informe de sostenibilidad.



## 4. Deberes de los administradores

- **Diligencia (Art. 225 LSC)** Ordenado empresario. Subordinar interés personal. Dedicación adecuada. Derecho y deber de información. Protección de la discrecionalidad empresarial (Business Judgement Rule)
- **Lealtad (Art.227):** Representante leal en defensa de los intereses de la sociedad. Prohibiciones básicas: no usar el nombre de la sociedad, no aprovechar oportunidades de negocio, no competir, confidencialidad. Evitar conflictos de interés y comunicar los existentes (arts. 228 y 229).

# Comisión de Auditoría: Obligatoria y relevante frente al fraude



## Referencias

- Ley de **Sociedades de Capital**
- Ley de **Auditoría de Cuentas**
- **Código de Buen Gobierno** de las sociedades cotizadas (CNMV)
- **Guía Técnica Comisiones de Auditoría de las entidades de interés público** (CNMV)
- **Normas Globales de Auditoría Interna** (Instituto de Auditores Internos)



## Composición

- **Consejeros no ejecutivos:** Mayoría deberán ser independientes. Al menos uno designado por conocimientos en contabilidad/auditoría
- **Presidente:** Designado de entre los consejeros independientes. Sustitución cada 4 años. Posible reelección tras 1 año de cese
- **Número de miembros:** mínimo 3 miembros (para cotizadas)
- **Estatuto/Reglamento propio**



## Funciones

- Supervisión de la **información financiera y no financiera** (incluida sostenibilidad, CSRD/ESRS)
- Relación con el **auditor externo** (independencia, plan, honorarios)
- Supervisión del sistema de **control interno**
- **Gestión de riesgos** financieros y no financieros
- **Canal de denuncias y cumplimiento normativo**
- Supervisión de la función de **auditoría interna**

# Comisión de Auditoría: Habilidades y Competencias

## 01 Escepticismo

Cuestionamiento activo de datos, procesos y conclusiones de la dirección. Posición propia, sin aceptación automática.

## 02 Diálogo constructivo

Clima que fomente la libre expresión. Diversidad de opiniones. El presidente asegura participación sin presiones externas.

## 03 Comunicación continua

Canal bidireccional y periódico con: dirección, auditoría interna, auditor externo y verificador de sostenibilidad.

## 04 Intervención de expertos

Posibilidad de contratar asesoramiento externo especializado. Presupuesto anual para expertos cuando sea necesario.

*Los miembros deben ser designados atendiendo a sus conocimientos y experiencia en contabilidad y/o auditoría; además, la comisión de auditoría debería contar en su conjunto con conocimientos adecuados del sector:*

### Conocimientos financieros y auditoría

Normativa contable (PGC/NIIF), criterios de auditoría, valoración e interpretación de CCAA

### Control Interno y Gestión de Riesgos

Control interno (COSO/SCIIF), riesgos financieros y no financieros, marcos ERM

### Sostenibilidad (ESG)

Información de sostenibilidad (CSRD), doble materialidad, estándares ESRS

### Tecnología y Ciberseguridad

TI, sistemas de información, ciberseguridad, IA y entornos digitales

# Consejo y Comisión de Auditoría: mismas responsabilidades, distinta regulación

Comparativa de obligaciones clave en España, la Unión Europea y EEUU

FUNCIÓN / OBLIGACIÓN	ESPAÑA	UNIÓN EUROPEA	EEUU
 Estrategia y aprobación de la estrategia	✓ Coincide	✓ Coincide	✓ Coincide
 Supervisión de la dirección (alta dirección)	✓ Coincide	✓ Coincide	✓ Coincide
 Control interno y gestión de riesgos	✓ Coincide	✓ Coincide	✓ Coincide
 Información financiera y cuentas anuales	✓ Coincide	✓ Coincide	✓ Coincide
 Relación con auditor externo y nombramiento	● Consejo nombra; CA informa / propone	● CA propone; Consejo nombra	● CA nombra y gestiona relación (responsabilidad directa)
 Canal de denuncias (whistleblowing)	✓ Coincide	✓ Coincide	✓ Coincide
 Auditoría interna	✓ Coincide	✓ Coincide	✓ Coincide
 Composición e independencia de la Comisión	● Mayoría independiente; presidente independiente	● Independencia; competencia financiera	● 100% independiente; con competencias financieras



## DIFERENCIAS RELEVANTES (EN LA FORMA)



### ESPAÑA

Regulación societaria detallada en la Ley de Sociedades de Capital (LSC) y normativa complementaria.



### UNIÓN EUROPEA

Marco armonizado por Directivas y Reglamento 537/2014; enfoque basado en principios.



### EEUU

Sarbanes-Oxley Act (SOX) y regulación de la SEC/NYSE refuerzan la responsabilidad directa del Audit Committee.



## CONCLUSIÓN

Las tres jurisdicciones coinciden en el fondo: el Consejo establece la estrategia y supervisa; la Comisión de Auditoría profundiza y controla.



Fuentes: LSC arts. 253, 264, 529 ter y quaterdecies; Directiva 2006/43/CE; Reglamento (UE) 537/2014; Sarbanes-Oxley Act §§ 301, 302 y 404; NYSE Listed Company Manual 303A.

En esencia, el **consejo de administración** actúa como el **cerebro estratégico** y debe tomar las decisiones clave que determinarán el rumbo de la compañía a largo de plazo.

La **Comisión de Auditoría** tiene la responsabilidad última de **supervisar la información** (financiera y de sostenibilidad), los **sistemas de control y gestión de riesgos**

# Gobierno Corporativo

Principios y mecanismos con los que el consejo dirige y supervisa



# Definiciones de Referencia

## Principios G20/OCDE (2023)

El gobierno corporativo es el conjunto de relaciones entre la dirección, el consejo de administración, los accionistas y otras partes interesadas, así como la estructura mediante la cual se establecen los objetivos de la empresa, se determinan los medios para alcanzarlos y se supervisa su desempeño

## CBG CNMV (2020) / LSC

El gobierno corporativo es el conjunto de principios, reglas y prácticas que regulan la organización, funcionamiento, supervisión y rendición de cuentas de los órganos de gobierno de una sociedad. En definitiva, el buen gobierno corporativo es un factor clave para la protección de inversores, la eficiencia de los mercados y la confianza empresarial. 64 recomendaciones bajo cumplir o explicar. La LSC configura el marco imperativo para cotizadas (arts. 529 bis a 529 novodecies).

***El gobierno corporativo va más allá del consejo: abarca los comportamientos, canales de información y procesos que determinan cómo una entidad es dirigida, gestionada y controlada.***  
***Implica la supervisión por la que un consejo y un equipo directivo informados orientan a la entidad hacia la ejecución de su estrategia, maximizando el valor a largo plazo de forma ética y dentro del marco legal y regulatorio aplicable***

# Elementos del Gobierno Corporativo



1

## Riesgos (ERM)

Qué riesgo se asume, cuánto y cómo entra en la decisión.

2

## Información

Lo que la entidad reporta, dentro y fuera: financiera y de sostenibilidad.

3

## Control interno

Lo que garantiza que esa información y esos procesos son fiables.

4

## Aseguramiento

Quien verifica todo lo anterior con independencia: auditoría interna y externa.

# Tone at the top y cultura ética



## 1 Tone at the Top

Lo que hace la alta dirección

- ✓ Da ejemplo con sus decisiones y conductas
- ✓ Actúa de forma coherente (“walk the talk”)
- ✓ Reacciona ante incumplimientos, incluso de directivos
- ✓ Habla de ética de forma visible y frecuente
- ✓ Participa activamente en las iniciativas de compliance



## 2 Tone at the Middle

Lo que hacen los mandos intermedios

- ✓ Traducen los valores a la operativa diaria
- ✓ Refuerzan o debilitan la cultura ética del equipo
- ✓ Incorporan criterios éticos en la evaluación del desempeño
- ✓ Reciben formación específica en liderazgo ético
- ✓ Facilitan el escalado de inquietudes sin represalias



## 3 La cultura real se observa en...



**Lo que se premia**

Comportamientos reconocidos



**Lo que se tolera**

Conductas aceptadas



**A quién se promociona**

Referentes de éxito



**Cómo se gestionan los errores**

Reacción ante fallos e incumplimientos



**Indicadores recomendados:** encuestas de cultura, análisis de denuncias, entrevistas de salida y seguimiento de acciones correctivas.



**La integridad y los valores éticos se reflejan en el comportamiento diario de quienes lideran la organización.**

# Entity Level Controls (ELC): Concepto y relevancia

Los Entity Level Controls (ELC) son controles que operan a nivel de toda la organización y establecen el marco dentro del cual funcionan los controles de proceso y transaccionales. Son el primer nivel de defensa en el sistema de control interno y condicionan la eficacia de todos los demás controles.



## 1 Concepto y naturaleza

- ✓ Controles de naturaleza indirecta y persuasiva (no transaccional)
- ✓ Establecen el «tono» y el contexto del control interno
- ✓ COSO IC 2013: componente «Entorno de control» (5 principios)
- ✓ Influyen en la eficacia de todos los controles de proceso
- ✓ Actúan como «controles paraguas» sobre toda la entidad

**Tipos de ELC:** (1) Controles directos a nivel de entidad: previenen o detectan errores (p. ej., cierre contable, conciliaciones corporativas). (2) **Controles indirectos/pervasivos:** crean el entorno para que funcionen otros controles (p. ej., tone at the top, código ético, estructura).



## 2 Relevancia de los ELC

- ✓ PCAOB AS 2201: evaluación obligatoria de ELC en auditoría de ICFR
- ✓ Deficiencias en ELC = posible debilidad material en ICFR
- ✓ SOX §404: la dirección debe evaluar la eficacia del CI incluyendo ELC
- ✓ Los ELC pueden compensar parcialmente debilidades en controles de proceso
- ✓ El auditor externo debe obtener evidencia sobre el funcionamiento de los ELC



**Los ELC son la base del control interno: establecen el entorno, marcan el tono ético y condicionan la eficacia de todos los demás controles.**

La estructura organizativa define cómo se distribuyen las responsabilidades, la autoridad y las líneas de reporte dentro de la entidad. Es un ELC crítico porque determina la segregación de funciones, la cadena de supervisión y la capacidad de escalar incidencias.



## 1 Estructura organizativa (ELC)

- ✓ Estructura clara con responsabilidades definidas por escrito
- ✓ Segregación de funciones incompatibles (aprobación / ejecución / registro)
- ✓ Matrices de autoridad y límites de delegación
- ✓ Organigrama actualizado y accesible
- ✓ Revisión periódica ante cambios de negocio o crecimiento



## 2 Líneas de reporte (ELC)

- ✓ Reporting funcional y jerárquico claramente diferenciados
- ✓ Funciones de control con reporte directo al Consejo/Comité de auditoría
- ✓ Canales de escalado para incidencias y excepciones
- ✓ No subordinación de funciones de control a áreas operativas
- ✓ Documentación de las delegaciones y subdelegaciones



**Una estructura organizativa y líneas de reporte adecuadas aseguran la segregación de funciones, la supervisión efectiva y la capacidad de escalar incidencias.**

# Estructura organizativa y líneas de reporte: Modelo de tres líneas (IIA 2020)



**PRINCIPIOS CLAVE**

- Responsabilidad**  
Cada línea tiene roles y responsabilidades definidos.
- Independencia**  
La tercera línea es independiente. La segunda línea debe ser objetiva.
- Colaboración**  
Las tres líneas colaboran y comparten información.
- Enfoque en valor**  
Orientadas a la consecución de los objetivos y a la creación de valor sostenible.

*La primera línea gestiona, la segunda supervisa y apoya y la tercera proporciona aseguramiento independiente sobre la eficacia del sistema de gobierno, riesgos y control*

**HABILITADORES DEL MODELO**

- Cultura ética y tono desde arriba
- Información y datos de calidad
- Tecnología y herramientas adecuadas
- Competencias y desarrollo del talento
- Comunicación y transparencia

# “Accountability” en el gobierno corporativo

En el gobierno corporativo, la “accountability” establece **quién responde ante quién y por qué**. Es el mecanismo que **conecta el poder de decisión con la obligación de rendir cuentas**, asegurando que la **delegación de autoridad no diluya la responsabilidad última**.

## Cadena de accountability

### Accionistas → Consejo:

El Consejo es “*accountable*” ante la junta de accionistas. Mecanismos: voto, «say on pay», revocación.

### Consejo → Alta dirección:

El CEO y el Comité de dirección son “*accountable*” ante el Consejo. Mecanismos: evaluación, retribución variable, destitución.

### Alta dirección → Organización:

Cada directivo es “*accountable*” de su área. Mecanismos: objetivos, KPIs, evaluación del desempeño.

## “Accountability” colectiva vs. individual

El Consejo es colectivamente accountable, pero cada consejero tiene además una accountability individual: el deber de diligencia y el deber de lealtad. En regímenes como el de UK, la accountability individual se formaliza con «statements of responsibilities» que asignan funciones específicas a personas concretas, con consecuencias regulatorias individuales.

## ¿Qué exige la “accountability” efectiva?

**Roles y responsabilidades claros** (quién hace qué y ante quién responde) | **Evaluación periódica del desempeño** (del Consejo, de la dirección, de los auditores) | **Consecuencias efectivas** (cese, clawback, sanciones, responsabilidad penal) | **Transparencia informativa** (IAGC, proxy statements, informes de sostenibilidad) | **Supervisión independiente** (auditoría interna, auditor externo, regulador).

**Principios OCDE (2023): un marco de gobierno corporativo eficaz debe asegurar la “accountability” del Consejo ante la empresa y los accionistas.**

Ref.: OCDE, *Principios de Gobierno Corporativo (2023)*, caps. II, V, VI; UK Corp. Governance Code 2024, Sec. 1; LSC, arts. 225-232; CBG CNMV 2020

LSC = Ley de Sociedades de Capital | KPI = Key Performance Indicator

# La función de cumplimiento (Compliance)

## El concepto

- Función que asegura el **cumplimiento de las normas externas**, la **normativa interna** y los **compromisos voluntarios**.
- Segunda línea: **independiente del negocio**, con **acceso directo al consejo**.
- No sustituye al negocio: **cada área** sigue siendo **dueña de su riesgo** de cumplimiento.

## Qué hace la función

- Define el **marco común**: políticas, formación, evaluación de riesgos de cumplimiento.
- **Asesora** antes decisiones clave (nuevos productos, nuevos mercados, M&A) y **monitoriza** después.
- **Independencia funcional**: Reporta al consejo y actúa como interlocutor único ante los supervisores.

## Por qué transversal y no por “silos”

### Las normas cruzan los negocios

Una misma obligación (sanciones, datos, conducta, blanqueo) afecta a todas las unidades y países a la vez: gestionarla por silos multiplica huecos e incoherencias.

### Criterio único y especialización

La interpretación normativa exige expertos; una compañía necesita un solo criterio aplicado igual en todas las unidades y jurisdicciones.

### Independencia e interlocución

El que vende no puede ser quien decida si se puede vender; y el supervisor espera un interlocutor único con visión de grupo.

### La prueba de eficacia

No es el manual: es si la función tiene voz antes de las decisiones y datos después de ellas (DOJ, guía ECCP; ISO 37301).



La gestión de riesgos es una necesidad para cualquier organización y está incluida como requerimiento en la mayoría de las regulaciones europeas y americanas. Dota al **Consejo/Comisión Auditoría** de los elementos necesarios para **supervisar la ejecución de la estrategia** y provee a los ejecutivos de **herramientas de gestión y alerta temprana**.

## Hacia la gestión por riesgos

### 1 · El consejo define el apetito

Cuánto riesgo y de qué tipo se acepta para ejecutar la estrategia. Decisión indelegable.

### 2 · El apetito se traduce en límites

Tolerancias y métricas vinculantes por negocio y proceso, fijadas antes de decidir (ex ante).

### 3 · La decisión incorpora el riesgo

Cada decisión relevante (inversión, producto, mercado, M&A) lleva su análisis de riesgo dentro, no después.

### 4 · El consejo supervisa en base a métricas

Seguimiento de perfil frente a apetito, excepciones y escalado. Además de Mapas de riesgos actualizados

## Tres estadios de madurez

### Control interno

Fiabilidad de la información, cumplimiento, eficacia operativa. Necesario, no suficiente.

### Gestión de riesgos (ERM)

Inventario, evaluación, apetito, respuestas, reporte y seguimiento (COSO ERM 2017, ISO 31000). El riesgo, aún como función paralela.

### Gestión por riesgos

El riesgo integrado en el proceso de decisión. Es el estadio que los marcos actuales persiguen.

**La prueba de madurez no es tener un mapa de riesgos: es poder señalar qué decisión reciente cambió por lo que decía el riesgo. El riesgo debería ser una dimensión de cada decisión relevante**

# Riesgos complejos: gobernar sin invadir la gestión



El consejo no domina la técnica ni debe hacerlo: gobierna el marco, exige métricas y asegura el escalado.

## Inteligencia artificial y modelos

- **Riesgo de asimetría:** Las compañías adoptan IA rápidamente, pero los marcos de control y gobernanza van muy por detrás. Esta asimetría es la mayor fuente de riesgo sistémico oculto.
- Marco de **supervisión proactivo:**
  1. Inventario de usos de IA en la organización
  2. Evaluar riesgos e impacto regulatorio (AI Act UE)
  3. Gap Analysis: controles actuales vs. obligaciones
  4. Plan de preparación y hoja de ruta de gobernanza
  5. Garantizar calidad e integridad de datos de entrenamiento

## Ciberseguridad

- Riesgo de negocio, no asunto solo del área técnica: métricas de parcheo, detección y respuesta hasta el consejo.
- Previsión 2026: inversores priorizarán ciberseguridad e IA. El Comisión de auditoría debe asegurar información sobre gestión de riesgos en estos ámbitos.

## Blanqueo de capitales

Integración efectiva de filiales y adquisiciones en el marco AML del grupo, con plazo y verificación.

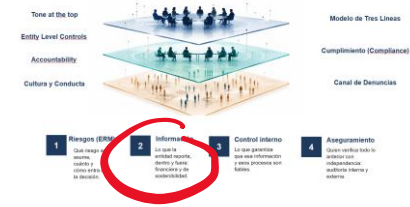
Marco en refuerzo continuo (UE: nuevo reglamento y autoridad únicos, AMLR/AMLA).

## Geopolítica

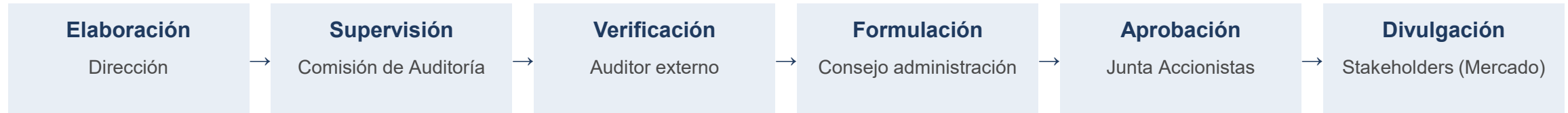
- Riesgo país catalogado y supervisado desde la matriz: sanciones, fragmentación, acceso a divisa y a corresponsalía.
- Escenarios prospectivos en la decisión estratégica, no solo en el mapa de riesgos.

**Transversal a todos: la incertidumbre regulatoria —sostenibilidad, IA, divergencia entre jurisdicciones— se gobierna como riesgo, no se padece como trámite.**

## 2 Información (financiera y sostenibilidad)



La responsabilidad del consejo de administración/Comisión auditoría es supervisar el proceso que genera la información y responder por el resultado.



### Responsabilidad de la Comisión Auditoría: supervisar la información

- El consejo **supervisa el proceso de elaboración** —a través de la comisión de auditoría— y los **controles internos que lo sostienen** (LSC art. 529 quaterdecies).
  - Revisar que las cuentas se elaboran conforme a normativa contable
  - Analizar estimaciones contables significativas y sus hipótesis
  - Controlar la adecuación del perímetro de consolidación
  - Revisar coherencia entre cuentas anuales y otra información corporativa
  - Verificar información en web corporativa y CNMV actualizada
- La formulación y firma de las cuentas (LSC art. 253) es el acto final de esa supervisión, con responsabilidad de los administradores (arts. 236-241). EE. UU.: certificación personal del CEO y el CFO (SOX secciones 302 y 906), con sanciones penales.
- Velar por la integridad de la información periódica
- Aclarar salvedades del auditor externo en la junta general de accionistas

### El perímetro se ha ampliado

- Información Sostenibilidad bajo CSRD/ESRS (UE): Mismo estándar de rigor: la información no financiera también genera responsabilidad.
  - Supervisar el proceso de elaboración del informe de sostenibilidad
  - Revisar control interno de la información de sostenibilidad
  - Coordinar con verificador de sostenibilidad
  - Supervisar el proceso de doble materialidad
  - Coordinar con comisión de sostenibilidad (si existe)



## Controles a nivel de entidad (ELC)

Tono desde arriba, supervisión del consejo, código ético, políticas corporativas. Condicionan la eficacia de todo lo demás.

## Controles de proceso

Cierre contable, conciliaciones, estimaciones, métricas de sostenibilidad. Donde se fabrica la fiabilidad del dato.

## Controles de aplicación

Validaciones automáticas, interfaces, configuraciones de los sistemas que procesan las transacciones.

## Controles generales de TI (ITGC)

Accesos, gestión de cambios, operaciones y seguridad. La base: sin ITGC fiables, nada de lo anterior es confiable.

## Cuando algo falla: la escala de gravedad

- **Deficiencia de control:** el control no está bien diseñado o no opera como se diseñó.
- **Deficiencia significativa:** merece la atención del consejo.
- **Debilidad material:** probabilidad razonable de error material no detectado. La evalúan dirección y auditor externo.

## El consejo debe supervisar la eficacia del sistema de control interno de la entidad



## SELECCIÓN

- Responsable del proceso de selección y cese
- Propuesta motivada con  $\geq 2$  alternativas (EIP cotizadas)
- Criterios: calidad, independencia, capacidades sectoriales, honorarios
- No discriminar auditores de menor tamaño

## INDEPENDENCIA

- Recibir declaración anual de independencia
- Emitir informe sobre independencia previo al informe de auditoría
- Aprobar servicios distintos a la auditoría (límites RUE art. 4.2)
- Establecer política interna de contratación

## COMUNICACIÓN

- Reuniones periódicas sin presencia de ejecutivos
- Plan de auditoría: riesgos, materialidad, alcance
- Cuestiones significativas: estimaciones, juicios, control interno
- Seguimiento de recomendaciones post-auditoría

## EVALUACIÓN

- Evaluar calidad del trabajo al cierre
- Revisar informe adicional para la Comisión (art. 36 LAC)
- Considerar resultados inspecciones ICAC
- Valorar continuación o cambio de auditor

**Principio de independencia: ni el auditor ni el verificador participan en la toma de decisiones de la comisión de auditoría.**



## De quién es y de quién depende

**Recurso del consejo**, no del management: dependencia funcional de la comisión de auditoría.

La comisión aprueba estatuto de auditoría y:

- Proponer **nombramiento/cese** del **Director de Auditoría Interna (DAI)**
- **Aprueba el Plan Anual**: cobertura de riesgos financieros y no financieros. La Comisión puede —y debe— pedirle revisiones específicas cuando algo no cuadra
- Garantiza **recursos humanos, tecnológicos y financieros** suficientes, así como **acceso irrestricto** a información, sistemas y personas.
- **Mantiene reuniones periódicas** con el DAI sin la dirección presente.
- **Evalúa anualmente** desempeño del área. Recibe **evaluación externa de calidad** de la función al menos cada cinco años (normas del IIA).
- Recibe **informe anual de actividades** con seguimiento de hallazgos

## Qué asegura

- Los **tres pilares de la supervisión**: riesgos, control interno e información (financiera y de sostenibilidad).
- El **cierre real de los hallazgos**, no su cierre administrativo.
- **Alertas tempranas**: degradación de controles y riesgos emergentes antes de que estallen.
- **Visión transversal completa** de la organización: ningún otro órgano la tiene.
- **Aseguramiento** también sobre la **segunda línea**: riesgos, compliance y control financiero.

## Qué debe exigirle el consejo

- **Plan basado en riesgos** conectado con la estrategia: su aprobación es una conversación estratégica, no un trámite.
- **Opinión periódica de conjunto** sobre gobernanza, riesgos y control.
- **Coordinación** con el auditor externo y las funciones de control, sin huecos ni duplicidades.
- **Capacidad, tecnología y presupuesto** a la altura del perímetro.
- **Respuesta de la dirección a cada hallazgo**, con plazo: lo que no se remedia, se escala.

**No es un departamento más de la dirección:  
es el mejor aliado de la Comisión de Auditoría.  
Auditoría Interna es el instrumento que permite a la comisión cumplir sus  
obligaciones de supervisión de forma eficaz y fundamentada.**

# El fraude y el Consejo de Administración



# El Patrón Común: ¿Por Qué Ocurren los Fraudes?



## 1. TRIÁNGULO DEL FRAUDE

(Donald R. Cressey)



El fraude ocurre cuando coinciden estos tres factores.

## 2. DIAMANTE DEL FRAUDE

(Añade la CAPACIDAD)



Además de los tres elementos del triángulo, se requiere que la persona tenga la capacidad para llevarlo a cabo.

## 3. PENTÁGONO DEL FRAUDE

(Añade la ARROGANCIA)



A los cuatro elementos del diamante se suma la arrogancia, que puede llevar al individuo a creer que no será castigado.



### 3 ELEMENTOS CLAVE

Presión + Oportunidad + Racionalización



### 4 ELEMENTOS CLAVE

Triángulo del fraude + Capacidad

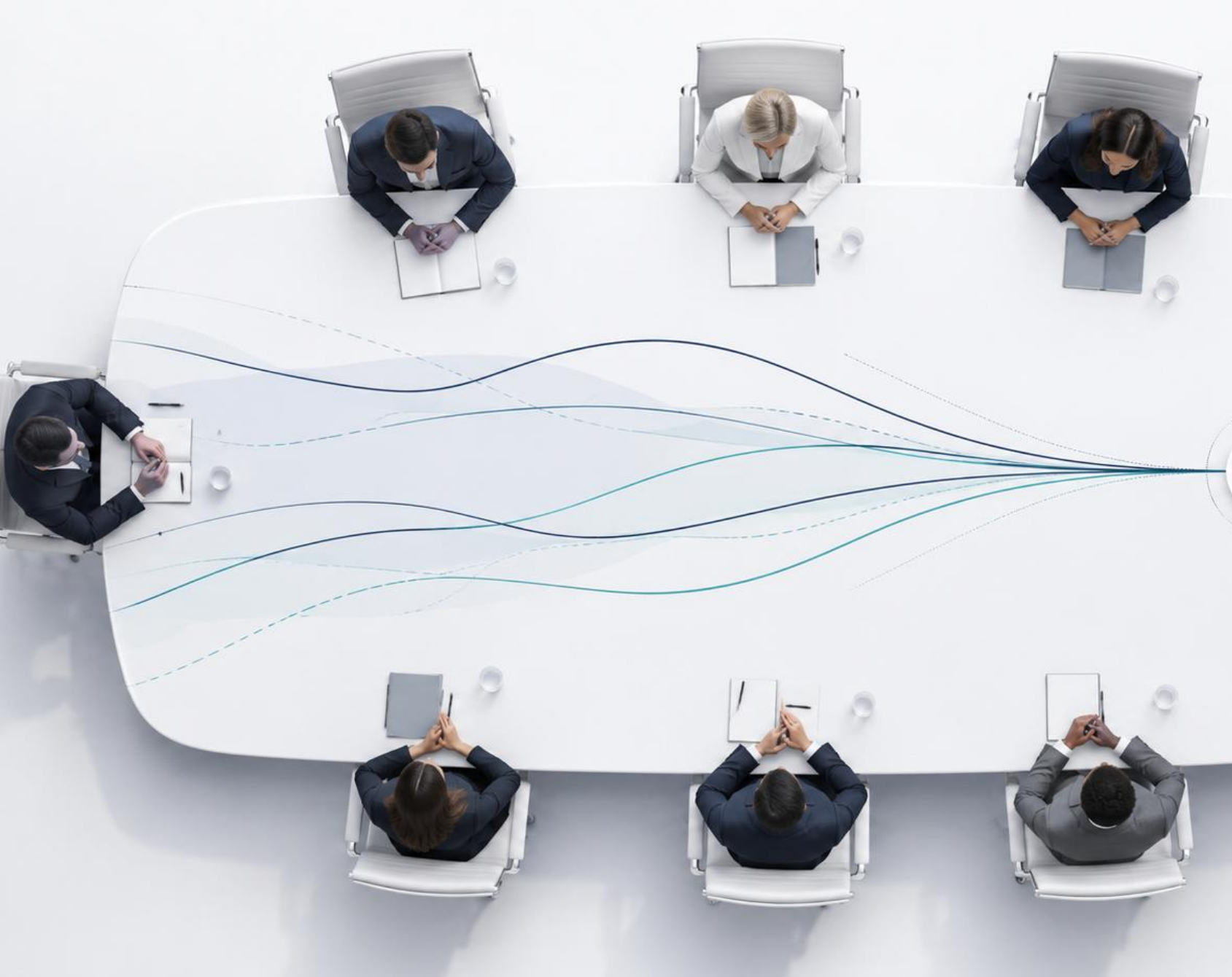


### 5 ELEMENTOS CLAVE

Diamante del fraude + Arrogancia

Ref.: Cressey, D.R. (1953) *Other People's Money*; Wolfe, D.T. & Hermanson, D.R. (2004) *The Fraud Diamond*. CPA Journal

Ref.: Crowe Horwath (2011) *Why the Fraud Triangle is No Longer Enough*. IN Crowe Horwath LLP; Marks, J. (2012) *The Mind Behind the Fraudsters Crime*. Crowe Horwath.



## ¿El fraude es competencia del Consejo de Administración?

**La prevención y detección del fraude es una función de supervisión indelegable.**

Es una función de supervisión, articulada a través de la Comisión de Auditoría, sobre el sistema de control interno y de gestión de riesgos diseñado y operado por la dirección ejecutiva.

# Buenas prácticas del consejo en la gestión del fraude

Compromiso del Consejo y del Comité de Auditoría para una organización íntegra y resiliente

## 01 Tono desde arriba



- Política de tolerancia cero al fraude aprobada por el Consejo.
- Mensajes periódicos de la presidencia como modelo de conducta.
- La integridad como criterio en la evaluación del desempeño directivo.

## 02 Evaluación periódica de riesgos



- Revisión anual del mapa de riesgos de fraude por el Comité de Auditoría.
- Incluir management override como riesgo explícito.
- Validar con asesores externos (auditores forenses, expertos independientes).

## 03 Canal de denuncias efectivo



- Accesible para empleados, proveedores y terceros (43% de detección, ACFE 2024).
- Reportes directos al Comité de Auditoría, independiente de la dirección.
- Protección robusta al denunciante (ISO 37002 y Directiva UE 2019/1937).

## 04 Controles internos robustos



- >50% de fraudes: falta o anulación de controles (ACFE 2024).
- Segregación de funciones, autorizaciones duales, data analytics continuo.
- Revisión periódica de eficacia y plan de remediación de deficiencias.

## 05 Formación y cultura ética



- Formación anual obligatoria: empleados, directivos y consejeros.
- Encuestas de cultura ética e indicadores conductuales.
- Reconocimiento de señales de alerta (fraud red flags) a nivel de Consejo.

## 06 Plan de respuesta e investigación



- Protocolo de investigación independiente predefinido (no ad hoc).
- Acceso directo del Comité de Auditoría al equipo investigador.
- Comunicación oportuna a reguladores (CNMV, SEC) cuando proceda.



Una gestión eficaz del riesgo de fraude requiere liderazgo del Consejo, evaluación rigurosa de riesgos, controles robustos, cultura ética, un canal de denuncias efectivo y una respuesta rápida y coordinada.



Prevenir



Detectar



Responder

# Los 5 principios COSO/ACFE de gestión del riesgo de fraude

FRMG 2ª edición (mayo 2023)

## LOS 5 PRINCIPIOS COSO/ACFE DE GESTIÓN DEL RIESGO DE FRAUDE

FRMG 2ª edición (mayo 2023)



## RESPONSABILIDADES



### Consejo y Comité de Auditoría

- Supervisión última del control interno y del programa antifraude.
- Integridad de la información financiera.
- Miembros independientes con competencia financiera.
- Asesoramiento legal ante alegaciones.
- Intervención directa si el fraude involucra a la alta dirección.



### Tono desde arriba

- El CEO establece el tono ético de toda la organización.
- Coherencia entre discurso y conducta observable.
- Políticas de compensación alineadas con valores.
- Código de conducta y declaración de compromiso.
- Formación antifraude periódica y obligatoria.



### Canal de denuncias

- Ley 2/2023 reguladora de protección de informantes.
- Múltiples canales (teléfono, web, email, app). Accesible 24/7, multilingüe.
- Alcance: empleados, consejeros, accionistas, proveedores, contratistas y terceros.
- Garantizar confidencialidad y, en su caso, anonimato. Comunicación bidireccional y anónima.
- Supervisión: informes periódicos al Comité; analizar número, tipología y resultados de denuncias.
- La ACFE demuestra que la mayoría de los fraudes se descubren mediante denuncias; aproximadamente la mitad proceden de empleados.

## EVALUACIÓN DEL RIESGO DE FRAUDE Y ELUSIÓN DE CONTROLES



### Identificación y evaluación de riesgos

- 4 categorías: información financiera, no financiera, activos y corrupción.
- Esquemas específicos por sector, estructura y geografía.
- Probabilidad: remota / razonablemente posible / probable.
- Significatividad: intrascendente / más que intrascendente / material.
- Heat maps para priorización.



### Elusión de controles por la dirección (management override)

- Riesgo más crítico y difícil de detectar.
- La alta dirección tiene conocimiento de los controles y autoridad para eludirlos.
- Puede crear proveedores ficticios, manipular estimaciones contables o registrar transacciones fraudulentas cerca del cierre.
- Los fraudes de alta dirección son los más dañinos en importe y duración.
- Los empleados difícilmente denuncian a un superior.

### Mitigantes específicos:

- Componente obligatorio en toda evaluación de riesgo de fraude.
- Controles de supervisión independientes del Consejo.
- Canal de denuncias con acceso directo al Comité de Auditoría.

# Estándares ISO: Marco Internacional de Compliance e Integridad

## ISO 37001:2025

Anti-Bribery  
Management Systems

- Sistema de gestión certificable para prevenir, detectar y responder al soborno (activo y pasivo).
- El Consejo debe supervisar el diseño e implementación del sistema y recibir informes directos.
- La dirección debe demostrar liderazgo: recursos adecuados, cultura ética, acceso directo del compliance officer al Consejo.
- Revisión 2025: refuerza cultura de compliance y gestión de conflictos de interés entre otros aspectos.
- Aplica a organizaciones públicas, privadas y sin ánimo de lucro de cualquier tamaño.

## ISO 37002:2021

Whistleblowing Management  
Systems — Canales de  
Denuncia

- Marco para establecer, implementar y mejorar sistemas de gestión de denuncias (canales internos y externos).
- Principios clave: confianza, imparcialidad, protección robusta del denunciante frente a represalias.
- Coherente con la Directiva (UE) 2019/1937 (Whistleblower Protection) y su transposición española.
- Asegura que las alertas de fraude lleguen al nivel correcto de supervisión (Comisión de Auditoría / Consejo).

## ISO 37003:2025

Fraud Control Management  
Systems — NOVEDAD 2025

- Guía específica para gestión integral del riesgo de fraude: prevención, detección, respuesta y mejora continua. Su objetivo es asegurar que las investigaciones se desarrollen de forma objetiva, imparcial, competente y documentada, permitiendo a las organizaciones responder eficazmente ante incumplimientos éticos, normativos o legales y adoptar las medidas correctivas correspondientes
- Cubre fraudes internos, externos y la colusión entre ambos. Aplica a toda tipología de organizaciones.
- Complementa ISO 37001 (soborno) e ISO 37301 (compliance) con un enfoque exclusivo en fraude.
- Promueve un enfoque proactivo y basado en riesgo, alineado con COSO FRMG 2023.

# Tendencias y riesgos emergentes

## 1. DIGITALIZACIÓN Y FRAUDE TECNOLÓGICO



### Inteligencia Artificial

Uso indebido o manipulación de algoritmos y modelos.



### Deepfakes

Suplantación de identidad mediante audios, vídeos o imágenes generadas por IA.



### Suplantación de identidad

Aumento de ataques de phishing, smishing y vishing más sofisticados.



### Fraude en pagos electrónicos

Riesgos en transferencias, pagos instantáneos y monederos digitales.

## 2. RIESGOS DE TERCEROS



- **Proveedores:** riesgos de fraude, corrupción o incumplimiento en la cadena de suministro.
- **Socios de negocio:** alineación de valores y diligencia adecuada continua.
- **Contratistas y agentes:** actuaciones en nombre de la organización que pueden generar responsabilidades.

## 3. FRAUDE ESG (AMBIENTAL, SOCIAL Y DE GOBERNANZA)



### Manipulación de información de sostenibilidad

Datos ESG inexactos o falsos para mejorar la percepción del desempeño.



### Greenwashing

Comunicar compromisos ambientales que no se materializan en acciones reales.



### Falseamiento de indicadores no financieros

Riesgo de fraude en métricas sociales, de diversidad, seguridad o gobernanza.



Los inversores, reguladores y la sociedad exigen transparencia y veracidad en la información no financiera.



Los riesgos evolucionan. La supervisión del Consejo también debe hacerlo.  
La preparación hoy es la mejor defensa frente al fraude mañana.



# ¿Qué información debe pedir el consejo y cómo supervisa?

## Diseño del programa

- Política antifraude aprobada y actualizada
- Inventario de esquemas de fraude por proceso (fraud risk assessment)
- Mapa de controles preventivos y detectivos asociados
- Recursos (FTE, presupuesto) de las 2.<sup>a</sup> y 3.<sup>a</sup> líneas

## Operación y métricas

- Incidentes detectados, en investigación y cerrados
- Origen de la detección (canal, auditoría, control, otros)
- Pérdidas brutas, recuperaciones, impacto neto
- Tiempo medio de detección y de resolución

## Cultura y canal

- Resultados de la encuesta de cultura ética
- Volumen y tipología de denuncias; Respuestas
- Cobertura de formación obligatoria
- Hallazgos relevantes de auditoría interna y externa

## Gobierno y agenda

- Aprobar y revisar anualmente la política antifraude y el apetito de riesgo asociado.
- Punto fijo en el orden del día de la Comisión de Auditoría: estado del programa antifraude.
- Sesión ejecutiva (sin presencia de la dirección) con el auditor externo, al menos una vez al año.
- Acceso directo y sin filtros del responsable de auditoría interna y del responsable de cumplimiento a la Comisión de Auditoría.

## Operación y revisión

- Revisión del diseño y operación del canal de denuncias y de la independencia de su instructor.
- Revisión de incidentes relevantes y de las acciones correctivas: lecciones aprendidas formalizadas.
- Evaluación periódica de la eficacia del programa (autoevaluación + revisión independiente).
- Diálogo con el auditor externo sobre riesgos de fraude considerados (NIA-ES 240) y su impacto en el plan de auditoría.

# Ejemplo de preguntas que el Consejo Debe Formular a la Dirección

**1** ¿Cuándo fue la última evaluación formal de riesgo de fraude y qué nuevos riesgos se identificaron?

**3** ¿El canal de denuncias es accesible para empleados, proveedores y terceros? ¿Cuántas alertas se han resuelto?

**5** ¿Cuál es el estado de los controles clave y existe un plan de remediación para las deficiencias identificadas?

**7** ¿Ha habido señales de presión financiera, cambios culturales o rotación inusual de personal relevante?

**9** ¿La formación en ética y fraude cubre a todos los niveles, incluyendo alta dirección y consejeros?

**2** ¿Qué porcentaje de ingresos estimamos que podríamos perder por fraude no detectado?

**4** ¿Existe riesgo de anulación de controles por parte de la alta dirección (management override)?

**6** ¿Se realizan análisis de datos (data analytics) de forma continua para detectar anomalías y patrones de fraude?

**8** ¿Tenemos un plan de respuesta a fraude predefinido, con roles claros y protocolo de comunicación a reguladores?

**10** ¿El programa antifraude está alineado con COSO, ISO 37001/37003 y la normativa vigente (LSC, CBG, SOX)?

# Algunas Conclusiones



# Cinco ideas clave para el consejo

## El fraude representa uno de los principales riesgos para la sostenibilidad de las organizaciones

Las organizaciones pierden de media el 5% de sus ingresos anuales y el fraude tarda unos 12 meses en detectarse (ACFE 2026). No es un riesgo hipotético: el Consejo debe dimensionar la exposición. Sus impactos no son solo económicos: daño reputacional, pérdida de confianza de inversores, clientes y reguladores y posibles responsabilidades legales y sanciones.

## La responsabilidad del Consejo es indelegable

Prevenir y detectar el fraude es una función de supervisión indelegable del Consejo, articulada vía Comisión de Auditoría (LSC arts. 529 ter y quaterdecies). La ignorancia no exime de la responsabilidad solidaria (art. 237 LSC).

## Supervisar es cuestionar, no recibir informes

El rol del Consejo es activo: preguntar, validar y exigir evidencia de la eficacia real de los controles, con escepticismo y diálogo constructivo (Guía Técnica CNMV 1/2024).

## El riesgo está también en la cumbre

El management override —la anulación de controles por la dirección— es el fraude más dañino y difícil de detectar (NIA 240). Exige auditoría interna con reporte funcional al Consejo y acceso directo a la Comisión de Auditoría.

## La importancia de la cultura, el “tone at the top” y el canal de denuncias

Las denuncias detectan el 43% de los fraudes (ACFE 2026), una parte sustancial se asocia a falta o anulación de controles. Sin un tone at the top coherente, ningún sistema de control es suficiente.



El **fraude** no es únicamente un problema de **control interno**; es un **problema de gobernanza**.

El **Consejo de Administración** debe actuar como **garante de la integridad de la organización**, impulsando una **cultura ética**, **supervisando los riesgos** y asegurando que existen mecanismos eficaces de **prevención, detección y respuesta**.

**“La mejor defensa frente al fraude comienza en la sala del Consejo: con liderazgo, supervisión y compromiso ético.”**

**MUCHAS GRACIAS**

**¿Preguntas?**



Julia Sáez Torrecuadrada  
[j.saezt@gov-a.com](mailto:j.saezt@gov-a.com)  
LinkedIn: [juliasaeztorrecuadrada](#)