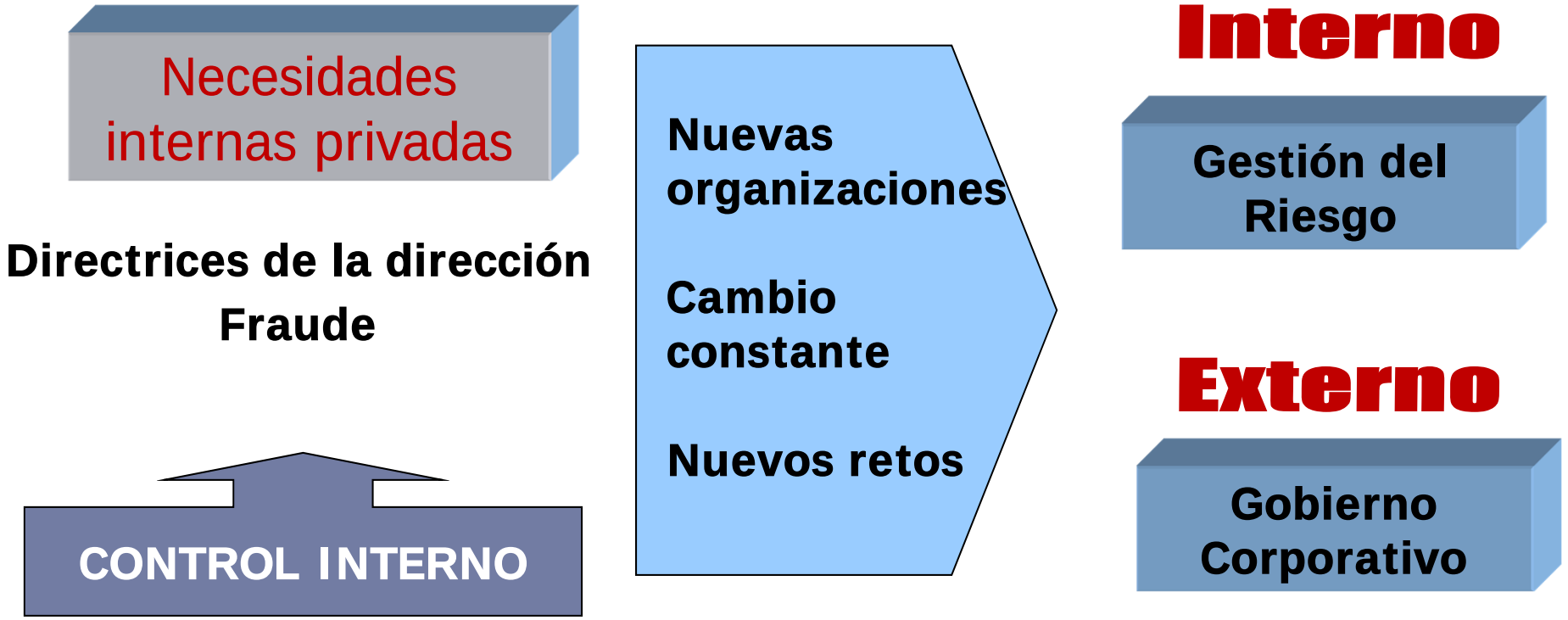
3. Nuevas perspectivas en materia de control interno → Gestión del Riesgo. O Control interno para la gestión empresarial

Evolución de los negocios



Entorno de riesgo actual

- Empresas siempre han debido enfrentarse al riesgo
- Actualmente rapidez del cambio hacen que riesgos parezcan mayores que antes:

  - Globalización ➔ exposición a acontecimientos internacionales
  - Necesidad de aumentar eficiencia, innovación y diferenciación
  - Riesgo de la competencia permanece, pero mayor impacto de los errores que se cometan sobre la posición competitiva
  - Hechos y grandes acontecimiento inesperados
  - Casos de información fraudulenta asociado a crisis empresariales ➔ información financiera como área de riesgo

Gestores

Políticas, procesos y tecnologías que permitan medir, supervisar y controlar los riesgos

Pensar en el futuro:

- **Análisis de escenarios**
- **Planificación de escenarios**

Práctica:

- **Medición cuantitativa de la exposición al riesgo para determinados factores (riesgo de crédito, tipo de interés ...)**
- **Consideración de las respuestas a cada tipo de riesgo**

Necesidad de:

- **Análisis de potenciales/posibles cambios en el entorno económico, político, social ...**
- **Comprensión de cómo interactúan los componentes del negocio**

Gestión del Riesgo- Risk Management

Gestión del Riesgo Empresarial (ERM)

- Maximizar el valor implica establecer unas estrategias y objetivos para llegar a un equilibrio óptimo entre objetivos de crecimiento y beneficio y los riesgos relacionados, y en el uso eficaz y eficiente de los recursos para conseguir objetivos empresariales
- **ERM = Gestión del Riesgo Empresarial implica**:
  - **Alinear la disposición a asumir riesgo con la estrategia**, al evaluar las alternativas, establecer objetivos estratégicos y el desarrollo de mecanismos para gestionar los riesgos.
  - Mejorar la **capacidad de responder a los riesgos** - rigor para identificar y seleccionar respuestas al riesgo: evitarlo, reducirlo, compartirlo o aceptarlo.
  - **Reducir las sorpresas operativas y sus pérdidas** – Identificar riesgos y preparar respuestas.
  - **Identificar y gestionar los riesgos con impactos interrelacionados** que afecten a múltiples partes de la empresa: respuesta integrada a riesgos.
  - **Aprovechar las oportunidades** – identificar y hacer realidad las oportunidades
  - **Mejorar el uso de los recursos** - Información adecuada del riesgo permite a la dirección evaluar eficazmente las necesidades de recursos globales y mejorar la asignación.

Modelos de Gestión del Riesgo / Risk Management

COSO
The Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management — Integrated Framework

AS/NZS 4360:2004

THE AUSTRALIAN & NEW ZEALAND STANDARD ON RISK MANAGEMENT

Standards Australia (Non-government Standards organisation)

EFQM

The EFQM Framework for Risk Management

Driving Excellence in Risk Management

NERAM

Network *for* Environmental Risk Assessment *and* Management

ISO 31000

ISO International Organization for Standardization

Modelos de Gestión del Riesgo / Risk Management

- Existen diferentes modelos surgidos de:
  - Las diferentes aproximaciones al análisis del riesgo y su tratamiento (desde enfoques de control, calidad, excelencia, etc)
  - La consideración de diferentes riesgos
  - En un enfoque particular, ad-hoc, por asuntos, a modo de prever un plan de contingencia en la gestión de un activo/actividad, frente a un enfoque global de segmento de negocio o entidad global.

- **PERO MISMO FIN: ACTUACIÓN PARA EL CUMPLIMIENTO DE OBJETIVOS**

Evolución de la Gestión de Riesgos

- **Ha existido una evolución en el tratamiento y gestión de riesgos ….**
- **GESTIONAR RIESGOS DE …**

ACTIVIDADES
(riesgos concretos en las funciones empresariales: riesgo de crédito de clientes, de instrumentos financieros, de ventas de un producto)

↓

FUNCIONES ORGANIZATIVAS o FUNCIONALES
(función financiera, comercial, industrial)

↓

ÁREAS DE NEGOCIO
(geográfica, innovación …)

↓

EMPRESA / GRUPO
Enterprise Risk Management

Más común

Relevante en entorno actual

Modelos

Modelo	Características
COSO ERM 2004	Primer esfuerzo de marco integral. Con influencias significativas de la profesión contable/auditoría Identifica los elementos, factores e indicadores de un modelo conceptual Para todas las organizaciones, objetivos, estrategias
ISO 31000 2009	Basado en AS/NZS 4360:2004. The Australian & New Zealand Standard On Risk Management Norma para certificación: Más operativo, ya que describe fases, procesos y elementos.
EFQM	Modelo creado como un módulo del Modelo de Gestión de Excelencia, Calidad.

COSO 2004 - Marco para ERM

Gestión del Riesgo

Exige que la entidad adopte una *visión global* del riesgo teniendo en cuenta los diferentes componentes del riesgo.

- La dirección considerará cómo interrelacionan los componentes individuales del riesgo.
- La Dirección desarrollará una visión global desde 2 perspectivas:
  - A nivel de línea o unidad de negocio
  - A nivel de la entidad

RIESGO representa el grado de probabilidad de que un evento impacte significativamente en la capacidad de conseguir los objetivos de la organización ➔

Evento con efecto adverso = **RIESGO**

Evento con efecto positivo = **OPORTUNIDAD**

Vinculación Marco Integrado CI –ERM

- ERM misma filosofía que Marco Integrado de Control Interno (MICI)
- ERM incorpora los mismos objetivos que MICI pero incluye los objetivos estratégicos.
- En el marco ERM, la categoría de objetivos relativa a “Información” es más amplia que la de “Información Financiera” del MICI.
- ERM incluye ocho componentes.
- ERM incluye el establecimiento de objetivos como un componente separado. El MICI considera al establecimiento de objetivos como un prerrequisito antes de aplicar el control interno.
- El marco ERM separa el componente 2 “Evaluación de riesgos” del MICI en tres componentes del ERM.

UN SÓLIDO SISTEMA DE CONTROL INTERNO ES ESENCIAL PARA UNA GESTIÓN DE RIESGOS EFECTIVA EN LA EMPRESA

CI

Información financiera

ERM

Información Global

Marco COSO para ERM (2004)

Deben considerarse los 8 componentes del marco que están interrelacionados…

1. AMBIENTE INTERNO
2. ESTABLECIEMIENTO DE OBJETIVOS
3. IDENTIFICACIÓN DE EVENTOS
4. EVALUACIÓN DE RIESGOS
5. RESPUESTA A LOS RIESGOS
6. ACTIVIDADES DE CONTROL
7. INFORMACIÓN Y COMUNICACIÓN
8. SUPERVISIÓN

Marco COSO para ERM (2004)

Diseñar e implantar 8 componentes interrelacionados…

ALINEADOS CON LOS OBJETIVOS EMPRESARIALES

Los cuales pueden agruparse en 4 tipos de objetivos:

- **Estratégicos**
- **Operativos**
- **Informativos**
- **De cumplimiento**

CONSIDERANDO SU APLICACIÓN A NIVEL:

- **Entidad (organización, empresa o grupo de empresas)**
- **División**
- **Unidad de negocio**
- **Actividades concretas**

Marco COSO para ERM (2004)

OBJETIVOS EMPRESARIALES

ELEMENTOS

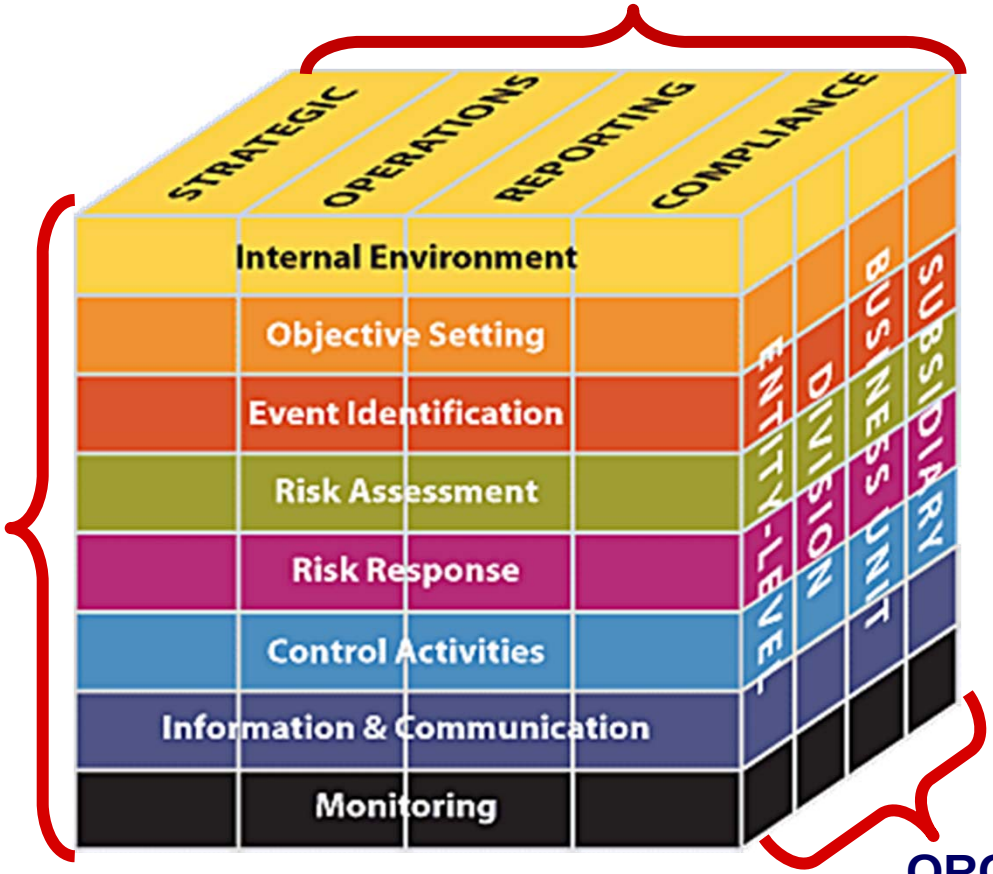


Figura utilizada en el Informe COSO –ERM ó COSO 2 (2004)

NIVEL ORGANIZATIVO

Debe buscarse la integración de todos los elementos para que todo funcione como un sistema

Marco ERM -COSO 2004

1. AMBIENTE INTERNO

Tiene que ver con:

- **La concienciación** del personal respecto del riesgo y el control
- **En el establecimiento de las estrategias y objetivos, y en la determinación de las actividades de negocio** deben tenerse en cuenta **la Filosofía relativa a la Gestión del Riesgo adoptada por los máximos responsables**

Cultura del riesgo de la entidad = que debe guiar las acciones de la entidad con respecto al riesgo.

Marco ERM

1. AMBIENTE INTERNO

Debe definirse:

- Visión del Administradores: Combinación Objetivos – Riesgo que se está dispuesto a asumir para conseguirlo
- Filosofía de la gestión del riesgo: Propenso o adverso al riesgo ➔ Apetito de riesgo = Riesgo que se está dispuesto a asumir para conseguirlo
- Considerar el riesgo de Integridad y valores éticos
- Compromiso de competencia/capacidad profesional para ser elementos del sistema de gestión de riesgos
- Estructura organizativa adecuada, capaz de captar información sobre riesgos, y adaptativa para afrontarlos.
- Asignación de autoridad y responsabilidad
- Diseño coherente de Políticas y prácticas de recursos humanos

Marco ERM

2. ESTABLECIMIENTO DE OBJETIVOS

Dirección debe considerar la estrategia frente al riesgo al establecer sus objetivos ➔ Debe establecer

APETITO DE RIESGO = Determinación del nivel de riesgo que la Dirección y los Administradores consideran aceptable/están dispuestos a asumir

TOLERANCIA AL RIESGO: margen aceptable de variación de los objetivos seleccionados y relacionados, considerando la disposición de asumir riesgos.

- **Objetivos Estratégicos ➔** Objetivos alineados con metas estratégicas para crear valor: misión-visión-valores
- **Objetivos Seleccionados ➔** Concreción de los objetivos directivos que van a permitir cumplir los objetivos estratégicos, identificando eventos y riesgos/oportunidades
- **Objetivos Relacionados ➔** operativos, de confiabilidad de la información y cumplimiento, alineados con estrategia y apetito de riesgo deseado.

Marco ERM

3. IDENTIFICACIÓN DE ACONTECIMIENTOS

Identificar eventos potenciales con impacto en objetivos en condiciones de incertidumbre: causas y fuente de riesgo.

Diferenciar riesgos y oportunidades.

- Riesgo: Acontecimientos que puedan tener impacto negativo
- Oportunidad: contecimientos que pueden tener un impacto positivo, que la Dirección debe incorporar a los canales de establecimiento de estratagias.

Factores

Incluye identificar acontecimientos internos como externos, que pueden afectar a la estrategia y el logro de objetivos.

Considerar cómo se combinan e interactúan los factores para influir en el perfil de riesgo.

Ejemplos de Riesgos considerados en ERM

- Riesgo estratégico
- Riesgo operativo
  - Riesgo de Procesos Operativos, de mercados, y abastecimiento
  - Riesgo legal y de litigios
  - Riesgo de seguridad informática
  - Riesgo de fraude
  - Riesgo asociado al personal
  - Riesgo de cambio

- Riesgos financieros
  - Riesgo de liquidez
  - Riesgo de crédito
  - Riesgo de mercado
  - Riesgo de tipo de cambio

- Riesgo de regulación y de cumplimiento

- Riesgo Reputacional
- Riesgo de continuidad del negocio
- Riesgo medioambiental y social
- Riesgo de actividad internacional
- Riesgo geopolítico / Riesgo país
- Otros

Marco ERM

3. IDENTIFICACIÓN DE ACONTECIMIENTOS

Técnicas de Identificación de Eventos: No existe un método específico

Sirve cualquier mecanismo que sirva para conseguir información que permita clasificar y evaluar riesgos y oportunidades.

Ejemplos:

- Inventarios de eventos y listas de verificación
- Análisis de información histórica (de la empresa/sector)
- Indicadores de excepción
- Entrevistas y sesiones grupales guiadas por facilitadores y expertos, metodología Delphi
- Análisis de flujos de procesos
- Técnicas de razonamiento inductivo, tormenta de ideas…

Fuentes COSO (2004), ISO 31000 (2009)

Marco ERM

4. EVALUACIÓN DEL RIESGO

Debe permitir a la entidad comprender el grado en que los acontecimientos potenciales pueden tener impacto sobre los objetivos

- Analizar las consecuencias si se declara el riesgo
- Controles ya presentes y su efectividad para las circunstancias

Evaluar los riesgos tanto cuantitativa como cualitativamente desde dos perspectivas:

- Probabilidad
- Impacto

Usado para revisar riesgos y se usa para medir los objetivos relacionados.

Debe emplearse una combinación de metodologías cuantitativas y cualitativas de evaluación del riesgo.

Debe considerarse el horizonte temporal de los objetivos.

Hay que llegar a una conclusión sobre los riesgos inherentes y residuales (aquellos que no se van a gestionar)

- Debe existir un proceso continuo y supervisión
- Necesidad de documentación.
- La selección de técnicas dependerá de:
  - Lo apropiado y justificado para la organización
  - Las necesidades de información para la toma de decisiones (tipo y frecuencia de información)
  - Tipo e importancia de los riesgos
  - Grado de pericia del personal implicado, disponibilidad de apoyo tecnológico
  - Disponibilidad de datos
  - Lo cambiante que sea el entorno de riesgo de la empresa: grado de incertidumbre y complejidad

Algunas Herramientas y técnicas de Evaluación de Riesgos

Fuente: ISO 31000 - IEC/FDIS 31010:2009(E)

- Tormenta de ideas
- Entrevistas estructuradas o semiestructuradas
- Método Delphi
- Listas de verificación
- Análisis primario de riesgo
- Estudios de riesgo y operabilidad (HAZOP)
- Análisis de Riesgos y Puntos de Control Crítico (HACCP)
- Evaluación del riesgo del entorno
- Estructura «¿Qué pasa si? »(SWIFT)
- Análisis de escenarios
- Análisis de causa-efecto
- Árbol de decisión
- Índices de riesgo
- Matriz Consecuencia / probabilidad
- Análisis de costo / beneficio
- Análisis de decisión multicriterio (MCDA)
- Métodos estadísticos

Marco ERM

5. RESPUESTA AL RIESGO

Se debe identificar y evaluar las respuestas posibles al riesgo ➔ El objetivo es obtener un riesgo residual alineado con el nivel de tolerancia definido.

Para ello , se evalúan opciones con relación al "apetito" de riesgo, coste-beneficio de las respuestas potenciales al riesgo, y el grado en que la respuesta va a reducir el impacto y/o la probabilidad.

Se seleccionan y ejecutan las respuestas basándose en la evaluación del conjunto de riesgos y respuestas posibles.

Categorías de respuesta:

Evitarlo: Llevar a cabo acciones para evitar las actividades que generan riesgo.

Reducirlo: Acciones para reducir el impacto, la probabilidad de ocurrencia del riesgo o ambos.

Compartirlo: Acciones para reducir el impacto o la probabilidad de ocurrencia al transferir o compartir una porción del riesgo.

Aceptarlo: No se llevan a cabo acciones que afecten el impacto y probabilidad de ocurrencia del riesgo, se deja que el riesgo se manifieste.

Marco ERM

6. ACTIVIDADES DE CONTROL

Si se ha decidido controlar la probabilidad, el impacto, o ambos

Integración con Respuesta al Riesgo

Es necesario implantar las políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo, y otras directrices son llevadas a cabo.

Ëstos tienen lugar a través de la organización, en todos los niveles y funciones.

Incluyen los controles de aplicación y los controles de tecnología de la información generales.

Tipos de Actividades de Control

- Preventivas / detectivas,
- Manuales / Automatizados / Informátizados
- Controles de la Dirección / Controles de empleados
- Controles contables / Financieros y No financieros / Controles cuantitativos y cualitativos, controles de gestión

Marco ERM

7. INFORMACIÓN Y COMUNICACIÓN

- La Dirección identifica, capta y comunica la información pertinente en la forma y tiempo que permita a las personas cumplir con sus responsabilidades.
- Comunicación tiene lugar en sentido amplio, con flujos descendentes, transversales y ascendentes en la organización.
- Información interna y externa (clientes, proveedores, reguladores, accionistas, otros grupos de interés, prensa …).

Marco ERM

8. SUPERVISIÓN

Objetivo

Comprobar que el proceso de Gestión de Riesgos mantiene su efectividad a lo largo del tiempo y que todos los componentes del marco ERM funcionen adecuadamente

Procedimientos

- Actividades continuas de supervisión, durante el curso normal de las operaciones.
- Evaluaciones puntuales realizadas por personal no responsable directo de la ejecución de las actividades. Su alcance y frecuencia depende de los resultados de la evaluación de riesgos y de la efectividad de las medidas de control continuo.
- Combinación de ambas.

Gestión de Riesgos y Control Interno

- El control interno es el proceso efectuado por el consejo de administración, la dirección y demás personal de la organización con el objetivo de proporcionar seguridad razonable en la consecución de:
  - la eficacia y eficiencia de las operaciones,
  - fiabilidad de la información financiera,
  - cumplimiento de normas aplicables y
  - salvaguarda de los activos.

- El **control interno forma parte íntegra de la gestión de riesgos corporativos** y sus cinco componentes básicos, (…), que deben estar relacionados a través de un proceso integrado, son los siguientes: (i) entorno de control; (ii) evaluación de riesgos; (iii) actividades de control; (iv) información y comunicación; y (v) supervisión.

Fuente: CNMV (2010): Control interno sobre la información financiera en las entidades cotizadas

Consecuencias para el Control Interno

- La empresa debe prever una infraestructura (sistemas, procesos, equipos de trabajo) para la:

  – Captación de eventos que pueden derivar en riesgo/oportunidad
  – Convertir datos en información y conseguir el conocimiento de las circunstancias
  – Evaluación de los impactos y de las posibles respuestas
  – Comunicación efectiva y oportuna a lo largo de toda la organización
  – Previsión de una respuesta oportuna (cambios) en toda la organización ante la confirmación del riesgo/oportunidad
  – Supervisión de todo el proceso de gestión de riesgos

➔ CONTROL INTERNO ENFOCADO HACIA LA GESTIÓN DE RIESGOS

Responsabilidad del ERM

INTERNOS

- **Todo el personal en una entidad** tiene algún tipo de responsabilidad en la Gestión de Riesgos.
  - **Administradores**
  - **Dirección - Gestores**
  - **Gestor de Riesgo**
  - Directores Financieros
  - **Auditores Internos**
  - Resto de Personal

EXTERNOS

- Proporcionan información útil para una adecuada gestión de riesgos.
  - **Auditores externos**
  - **Legisladores y reguladores**
  - **Clientes, proveedores**
  - **Analistas financieros, calificadoras**
  - **Medios de comunicación**