



# Gestión del riesgo en las empresas. ¿Hasta dónde llegar?

Los riesgos son inherentes a los negocios, las empresas y los mercados. Sin embargo, quien nos iba a decir que una de las cinco grandes firmas de auditoría, Arthur Andersen, cesaría en sus actividades tras el caso Enron por falta de gestión y control del riesgo en sus actividades, o que Lehman Brothers quebraría en septiembre de 2008 por su riesgo incontrolado en los créditos subprime.

Tras situaciones como las descritas grandes empresas como EADS pusieron en marcha políticas de gestión del riesgo destinadas a supervisar aspectos como los riesgos de divisas, de financiación de las ventas, los asociados a la cartera de inversiones, la dependencia de determinados proveedores y subcontratistas o la disponibilidad de financiación.

## La norma ISO 31000, que aborda los principios de gestión del riesgo en las organizaciones, está de actualidad al desarrollar un marco que integra la gestión del riesgo en todas las políticas de la empresa

Pero no todas las empresas tienen la misma exposición al riesgo en sus operaciones. Existen sectores de actividad en los que las empresas que lo conforman están especialmente expuestas a riesgos que comprometen su supervivencia. De esta manera, las entidades financieras españolas son supervisadas por los reguladores para el control de su riesgo de liquidez, de solvencia o de divisas, las empresas del sector salud están expuestas a importantes riesgos de pérdida de reputación derivados de su actividad diaria y en el sector de la alimentación los riesgos relacionados con alertas sanitarias o de consumidor exigen de gran control de la calidad de sus productos. Pero también existen riesgos

generales a toda organización como el recientemente introducido en la reforma del Código Penal español que ha venido a sumar un riesgo de gran importancia para todas las empresas de todos los sectores, ya que incluye la responsabilidad penal de las personas jurídicas, tanto por las actuaciones realizadas por sus representantes y directivos como por el resto del personal intermedio de la empresa.

Así que, ¿cómo podemos conocer el nivel de exposición de nuestra empresa a los riesgos derivados de su actividad? Y es más, ¿qué efectos tendría en el futuro de la misma la ocurrencia de alguno de estos riesgos?

Hay dos parámetros que dan respuesta a estas preguntas; la probabilidad de que se produzca alguno de estos incidentes o riesgos y el impacto que esto produce en la organización. Así, si la probabilidad de ocurrencia de un incidente es elevada y/o el impacto de este incidente puede ser de gravedad entonces la empresa tiene gran exposición al riesgo (ver figura 1).

Los objetivos que deben guiar las políticas internas de gestión del riesgo son dos: la reducción de la probabilidad del riesgo (mediante procedimientos de control interno) y la mitigación del impacto del riesgo a través de planes de contingencia preestablecidos.

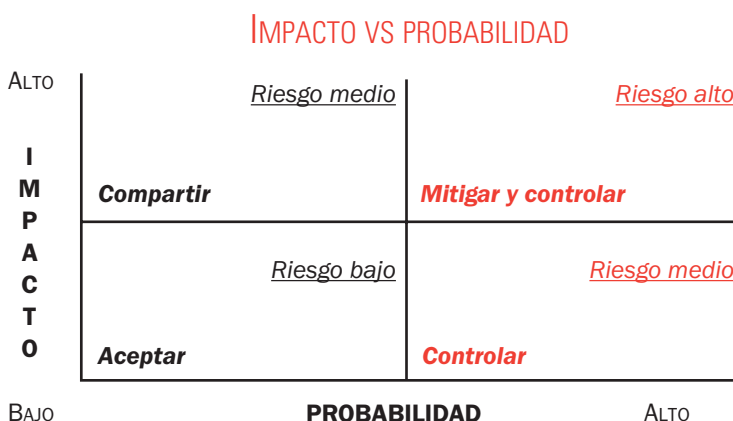
Así llegamos a la siguiente pregunta clave en este aspecto tan difuso en las empresas, ¿cómo se gestiona el control del riesgo en las organizaciones empresariales? Y todavía más allá, ¿a qué coste para que sea rentable dicho control? O como decía un reconocido empresario con gran criterio "que no nos cueste más el entierro que la abuela".

En este ámbito, la Organización Internacional de Estandarización (ISO) publicó en noviembre de 2009 la norma ISO 31000 que aborda los principios de gestión del riesgo en organizaciones. Este estándar internacional recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de gestión cuyo propósito sea la integración de los procesos de gestión del riesgo en las políticas de gobernabilidad, estrategia, planificación, gestión y reporte de la empresa.

De esta manera, la ISO 31000 establece las principales guías para implementar una gestión del riesgo exitosa y eficiente, y en ella se marcan los once objetivos básicos que guían esta práctica:

1. Creación y protección del valor de la compañía.
2. Integración de la gestión del riesgo en los procesos operativos.

FIGURA 1



3. Integración en los procesos de decisión de la gestión.
4. Control de la incertidumbre.
5. Establecimiento de un marco de control sistemático, estructurado y planificado.
6. Fundamentado en la mejor información disponible.
7. Mediante el desarrollo a medida para cada organización.
8. Implicación de los factores humanos y culturales.
9. Transmite transparencia en la organización
10. Es dinámico, iterativo y sensible a los cambios.
11. Facilita la mejora continua de la Organización.

**FASES EN LA GESTIÓN DEL RIESGO**

Bajo estos principios la norma propone una serie de fases y estructura para la gestión del riesgo y sugiere los siguientes pasos para su implementación (ver figura 2):

1. Establecimiento de los principios de riesgo y la comunicación con stakeholders (accionistas, consejeros, clientes,..). Esta primera fase pretende involucrar a los stakeholders en el proceso de gestión del riesgo y determinar sus expectativas y necesidades en cuanto al nivel de exposición al riesgo de la empresa.

2. Establecimiento del marco de gestión del riesgo. En este punto se determina lo que se denomina apetito por el riesgo y se define el grado de exposición y control del riesgo que se desea en la sociedad. Puede aplicarse en este punto un análisis PEST (Político, Económico, Socio-cultural y Tecnológico) que identifique los factores externos de riesgo.

3. Identificación de riesgos. Proceso en el que se identifican, analizan y evalúan los riesgos. Se recomienda el uso de las técnicas de identificación de riesgos definidas en la ISO/IEC 31010:2009 como son sesiones de brainstorming, entrevistas estructuradas, check lists, etc... En este punto también se evalúa cada riesgo a través de la probabilidad e impacto del mismo y el establecimiento de un mapa de los riesgos existentes.

**“La metodología propuesta por la norma asegura el control y la exposición a los riesgos de la empresa mediante la consecución de objetivos realistas”**

4. Tratamiento de los riesgos. Allá donde el nivel de riesgo sea intolerable (riesgos ubicados en la zona de Riesgo Alto de la figura 1) es necesario introducir procedimientos de control interno o planes de contingencia que mitiguen el impacto o reduzcan la probabilidad de ocurrencia del mismo. El riesgo resultante debe adaptarse a la tolerancia al mismo de la sociedad.

5. Monitorización y control. La monitorización regulada y periódica de los riesgos es necesaria para la adaptación a los cambios externos y las nuevas necesidades que se generen en el devenir de la empresa. En este sentido es de gran interés la realización de auditorías periódicas que aporten información objetiva del cumplimiento del modelo de gestión del riesgo.

Esta metodología propuesta por la ISO asegura el control y la exposición a los riesgos de la empresa mediante la consecución de objetivos realistas sin perder de vista que “el mayor riesgo que pueden asumir los gestores es no asumir riesgo alguno”.



FIGURA 2

