INTRODUCCIÓN

Los Estándares de Gestión de Riesgos son el resultado del trabajo de un equipo formado por las principales organizaciones de gestión de riesgos del Reino Unido: El Institute of Risk Management (IRM), la Association of Insurance and Risk Managers (AIRMIC) y ALARM el National Forum for Risk Management in the Public Sector.

Este equipo evaluó además durante un amplio periodo de consulta, los puntos de vista y las opiniones de otras muchas entidades y organismos profesionales interesados en la gestión de riesgos.

La gestión de riesgos es una disciplina que se está desarrollando muy rápidamente y existe un sinfín de puntos de vista y descripciones de lo más variado sobre lo que implica, cómo se debe llevar a cabo y para qué sirve. Se necesita por ello algún tipo de reglas o estándares para consensuar:

- El significado del vocabulario utilizado
- El proceso a través del cual se puede llevar a cabo la gestión de riesgos.
- La estructura organizativa para desarrollar la gestión de riesgos
- Los objetivos de la gestión de riesgos

Es importante que los estándares reconozcan que los riesgos presentan un lado positivo y otro negativo. La gestión de riesgos no está destinada sólo a las multinacionales y empresas que cotizan en bolsa, sino a cualquier actividad, ya sea de corto o de largo plazo. Las ventajas y oportunidades se deben considerar no sólo en el marco de la actividad empresarial en sí misma, sino también en relación con todos los interesados en la empresa (“stakeholders”), numerosos y variados, a los que pueda afectar.

Hay muchos modos de conseguir los objetivos de la gestión de riesgos y resultaría imposible intentar recogerlos todos en un solo documento. Por ello, no se ha pretendido crear lineamientos imperativos que pudieran desembocar en un enfoque rígido ni tampoco establecer un proceso certificable. Al cumplir las diferentes partes

que componen estos estándares, aunque sea de maneras diferentes, las empresas estarán en condiciones de afirmar que se conforman a los mismos. Los estándares representan la mejor práctica con la que las empresas pueden autoevaluarse.

En la medida de lo posible, los estándares han usado la terminología de gestión de riesgos, establecida por la Organización Internacional de Normalización (ISO) en su reciente documento Guía ISO/CEI 73 Gestión de riesgos - Terminología - Líneas directrices para el uso en las normas.

Nota: A fin de evitar confusiones y polémicas en la revisión de la traducción al español de los Estándares, se ha respetado en la medida de lo posible la terminología de la Guía ISO/CEI 73. Se hace notar que la Guía utiliza el término de Gestión de Riesgos tanto para la Gerencia (proceso de diseño, organización y coordinación de las actividades), como para la Gestión propiamente dicha (ejecución material de dichas actividades).

GESTIÓN DE RIESGOS

I. RIESGO.

El riesgo se puede definir como la combinación de la probabilidad de un suceso y sus consecuencias (Guía ISO/CEI 73). En todos los tipos de empresa existe un potencial de sucesos y consecuencias que constituyen oportunidades para conseguir beneficios (lado positivo) o amenazas para el éxito (lado negativo). Se reconoce cada vez más que la gestión de riesgos trata tanto los aspectos positivos como los negativos de los riesgos. Por lo tanto, los presentes estándares consideran el riesgo desde ambas perspectivas. En el campo de la seguridad, se suele admitir que las consecuencias son sólo negativas, por lo que la gestión de riesgos de seguridad se centra en la prevención y en la mitigación del daño.

II. GESTIÓN DE RIESGOS.

La gestión de riesgos es una parte esencial de la gestión estratégica de cualquier empresa. Es el proceso por el que las empresas tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en el conjunto de todas las actividades.

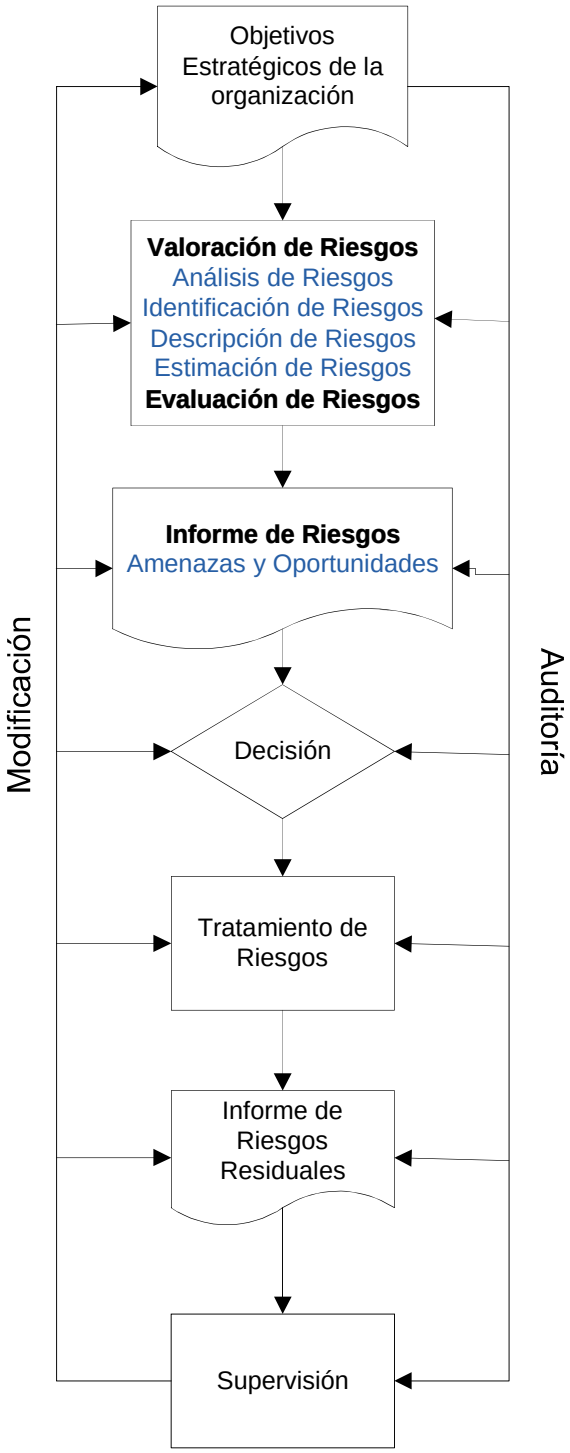
Una gestión de riesgos eficaz se centra en la identificación y tratamiento de estos riesgos. Su objetivo es añadir el máximo valor sostenible a todas las actividades de la empresa. Introduce una visión común del lado positivo y del lado negativo potenciales de aquellos factores que pueden afectar a la empresa. Aumenta la probabilidad de éxito y reduce tanto la probabilidad de fallo como la incertidumbre acerca de la consecución de los objetivos generales de la empresa. La gestión de riesgos tiene que ser un proceso continuo y en constante desarrollo que se lleve a cabo en toda la estrategia de la empresa y en la aplicación de esa estrategia. Debe tratar metódicamente todos los riesgos que rodeen a las actividades pasadas, presentes y, sobre todo, futuras de la empresa. Debe estar integrada en la cultura de la empresa con una política eficaz y un programa dirigidos por la alta

dirección. Tiene que convertir la estrategia en objetivos tácticos y operacionales, asignando responsabilidades en toda la empresa, siendo cada gestor y cada empleado responsable de la gestión de riesgos como parte de la descripción de su trabajo. Respalda la responsabilidad, la medida y la recompensa del rendimiento, promoviendo así la eficiencia operacional a todos los niveles.

A. Factores externos e internos.

Los riesgos a los que se enfrenta una empresa y sus operaciones pueden resultar de factores tanto internos omo externos a la empresa. La tabla que sigue recoge ejemplos de riesgos clave en estas áreas y muestra que algunos riesgos específicos pueden verse afectados por factores internos y externos y, por ello, abarcan las dos áreas. Se pueden clasificar en diferentes categorías de riesgo tales como: de azar, financieros, operacionales, estratégicos, etc.

B. El proceso de gestión de riesgos.



La gestión de riesgos protege y añade valor a la empresa y sus interesados (“stakeholders”) mediante el apoyo a los objetivos de la empresa a través de:

- *Proveer una estructura que permite que las actividades futuras se desarrollen de forma consistente y controlada.*

- *Mejorar la toma de decisiones, la planificación y el establecimiento de prioridades mediante una visión integrada y estructurada del negocio, su volatilidad y*
- *las oportunidades y amenazas del proyecto.*

- *Contribuir a una asignación más eficiente del capital y los recursos dentro de la organización.*

- *Reducir la volatilidad en las áreas no esenciales del negocio.*

- *Proteger y mejorar los activos y la imagen de la compañía.*

- *Desarrollar y apoyar a los empleados y la base del conocimiento de la organización.*

- *Optimizar la eficiencia operacional.*

III. VALORACIÓN DE RIESGOS.

La valoración de riesgos está definida en la Guía ISO/CEI 73 como el proceso general de análisis y de evaluación de riesgos *(Ver apéndice).*

IV. ANÁLISIS DE RIESGOS.

Comprende la identificación, descripción y estimación de riesgos.

A. Identificación de riesgos.

La identificación de riesgos se propone identificar la exposición de una empresa a la incertidumbre. Ello requiere un conocimiento detallado de dicha

empresa, del mercado en el que opera, del entorno legal, social, político y cultural que le rodea, así como el desarrollo de una visión común coherente de su estrategia y de sus objetivos operacionales, incluyendo los factores críticos para su éxito y las amenazas y oportunidades relacionadas con la consecución de estos objetivos. Hay que enfocar la identificación de riesgos de forma metódica para asegurarse de que se han identificado todas las actividades importantes de la organización y que se han definido todos los riesgos que implican dichas actividades. La volatilidad relacionada con estas actividades debe ser identificada y categorizada.

Las actividades y decisiones empresariales pueden clasificarse en distintas categorías, que incluirían las siguientes:

- *Estratégicas: Se refieren a los objetivos estratégicos a largo plazo de la empresa. Pueden estar condicionadas por áreas como la disponibilidad de capital, los riesgos políticos y soberanos, los cambios legales y de regulación, la reputación y los cambios en el entorno físico.*

- *Operacionales: Se refieren a los problemas cotidianos a los que se enfrenta la empresa al esforzarse por conseguir sus objetivos estratégicos.*

- *Financieras: Se refieren a la gestión efectiva y al control de las finanzas de la empresa así como a los efectos de factores externos como la disponibilidad de crédito, los tipos de cambio de las divisas, los movimientos de los tipos de interés y otras exposiciones al mercado.*

- *Gestión del Conocimiento: Se trata de la gestión efectiva y del control de los recursos del conocimiento, la producción, protección y comunicación de los mismos. Los factores externos pueden incluir el uso sin autorización o el abuso de la propiedad intelectual, los fallos en las áreas de energía y la competencia tecnológica. Entre los factores internos se pueden incluir el mal funcionamiento de los sistemas o la pérdida de personal clave.*

- *Conformidad: Se refiere a temas como salud y seguridad, medioambiente, descripción comercial, protección del consumidor, protección de datos, prácticas de empleo y temas de regulación.*

Mientras que la identificación de riesgos pueden llevarla a cabo consultores externos, es muy probable que un enfoque interno con procesos y herramientas coherentes, coordinadas y bien comunicadas, resulte más eficaz. La "propiedad" interna del proceso de gestión de riesgos es esencial.

B. Descripción de riesgos

El objetivo de la descripción de riesgos es mostrar los riesgos identificados de una forma estructurada, por ejemplo, utilizando una tabla. La tabla de descripción de riesgos que figura a continuación, se puede utilizar para facilitar la descripción y valoración de riesgos. El uso de una estructura bien diseñada es necesario para asegurar un proceso exhaustivo de identificación, descripción y valoración de riesgos. Al tener en cuenta la consecuencia y probabilidad de cada uno de los riesgos que constan en la tabla, debería ser posible dar prioridad a los riesgos clave que tienen que ser analizados con más detalle. La identificación de los riesgos asociados a las actividades empresariales y la toma de decisiones se pueden calificar como estratégica, táctica u operacional. Es importante incorporar la gestión de riesgos en la fase de concepción de los proyectos así como a lo largo de la vida de un proyecto específico.

Tabla (1) - Descripción de riesgos

1. Nombre del riesgo	
2. Alcance del riesgo	Descripción cualitativa de los sucesos, su tamaño, tipo, número y dependencias.
3. Naturaleza del riesgo	Ej. Estratégicos, operacionales, financieros, de gestión del conocimiento y de conformidad.
4. Interesados	Interesados y sus expectativas

5. Cuantificación del riesgo	Importancia y probabilidad
6. Tolerancia del riesgo / Apetito	Potencial de pérdida e impacto financiero del riesgo Valor en riesgo Probabilidad y tamaño de las pérdidas/ganancias potenciales Objetivo(s) del control de riesgo y nivel deseado de rendimiento
7. Tratamiento del riesgo y mecanismos de control	Medios primarios por los que se gestiona el riesgo actualmente Niveles de confianza en el control existente Identificación de protocolos de supervisión y revisión
8. Acción potencial de mejora	Recomendaciones para reducir riesgos
9. Política y estrategia a desarrollar	Identificación del responsable de la función de desarrollo de la política y la estrategia.

C. Estimación de riesgos.

La estimación de riesgos puede ser cuantitativa, semi-cuantitativa o cualitativa en términos de probabilidad de ocurrencia y de sus posibles consecuencias.

Por ejemplo, las consecuencias en términos de amenazas (riesgos negativos) y oportunidades (riesgos positivos) pueden dividirse en altas, medias o bajas (Ver tabla 2). La probabilidad puede clasificarse como alta, media o baja pero requiere diferentes definiciones respecto a las amenazas y las oportunidades (Ver tablas 3 y 4.).

Los ejemplos aparecen en las tablas. Algunas empresas opinaran que se adecuarán mejor a sus necesidades medidas de consecuencia y probabilidad diferentes. Por ejemplo, muchas empresas opinan que clasificar las consecuencias y probabilidades como altas, medias o bajas, se adapta

bastante bien a sus necesidades y se pueden presentar en una matriz 3 x 3. Otras empresas creen que usar una matriz de 5 x 5 para evaluar las consecuencias y las probabilidades les proporciona una mejor valoración.

Tabla (2) Consecuencias - Amenazas y oportunidades

Altas	El impacto financiero en la empresa es susceptible de superar $x. Fuerte impacto en la estrategia o en la operatividad de la empresa. Alta preocupación de los interesados.
Medias	El impacto financiero en la empresa es susceptible de situarse entre $x y $y. Impacto moderado en la estrategia o en la operatividad de la empresa. Moderada preocupación de los interesados.
Bajas	El impacto financiero en la empresa es susceptible de situarse por debajo de $y. Bajo impacto en la estrategia o en la operatividad de la empresa. Baja preocupación de los interesados.

Tabla (3) Probabilidad de ocurrencia - Amenazas

Estimación	**Descripción**	**Indicadores**
Alta (Probable)	Susceptible de ocurrir cada año o más del 25% de probabilidad de que ocurra.	Posibilidad de que suceda varias veces en el período de tiempo (por ejemplo, diez años). Ha ocurrido recientemente.
Media (Posible)	Susceptible de ocurrir en un período de diez años o menos del 25% de probabilidad de que ocurra.	Podría suceder más de una vez en el período de tiempo (por ejemplo, diez años). Podría ser difícil de controlar debido a varias influencias externas. ¿Hay un historial de ocurrencia?
Baja (Remota)	No es susceptible de ocurrir en un período de diez años o menos del 2% de probabilidad de que ocurra.	No ha sucedido. Poco probable que suceda.

Tabla (4) Probabilidad de ocurrencia - Oportunidades

Estimación	Descripción	Indicadores
Alta (Probable)	Es probable que se alcancen resultados favorables en un año o más del 75% de probabilidad de que ocurra.	Oportunidad clara, que se puede barajar con razonable certeza y conseguir a corto plazo basándose en los procesos de gestión actuales.
Media (Posible)	Perspectivas razonables de resultados favorables en un año o del 25% al 75% de probabilidad de que ocurra.	Oportunidades alcanzables pero que requieren una gestión cuidadosa. Oportunidades que pueden surgir fuera de lo previsto
Baja (Remota)	Cierta posibilidad de resultados favorables a medio plazo o menos del 25% de probabilidad de que ocurra.	Oportunidad posible que aún tiene que ser investigada completamente por la dirección. Oportunidad en la que la probabilidad de éxito se considera baja, partiendo de los recursos de gestión que se están aplicando en este momento.

D. Métodos y técnicas de análisis de riesgos.

Se pueden usar diversas técnicas con el fin de analizar riesgos. Estas pueden ser específicas para riesgos positivos o negativos o capaces de tratar ambos tipos.

E. Perfil de riesgos.

El resultado del proceso de análisis de riesgos puede utilizarse para crear un perfil de riesgos que proporcione una valoración de la importancia de cada

riesgo y aporte una herramienta para priorizar los esfuerzos de tratamiento de riesgos. De este modo se clasifica cada riesgo identificado, facilitando una visión de su importancia relativa. Este proceso permite situar a cada riesgo en un mapa de la zona afectada de la empresa, describir los procedimientos de control primarios que se aplican e indicar las zonas en las que se debe aumentar, disminuir o reajustar el nivel de la inversión en el control de riesgos. La valoración contribuye a asegurar el reconocimiento de la "propiedad" del riesgo y la asignación de los recursos de gestión apropiados.

V. EVALUACIÓN DE RIESGOS.

Cuando el proceso de análisis de riesgos se ha llevado a cabo, es necesario comparar los riesgos estimados con los criterios de riesgo establecidos por la empresa. Los criterios de riesgo pueden incluir costos y beneficios asociados, requisitos legales, factores socioeconómicos y medioambientales, preocupaciones de los interesados, etc. Por tanto, se usa la evaluación de riesgos para tomar decisiones acerca de la importancia de los riesgos para la empresa y sobre si se debe aceptar o tratar un riesgo específico.

VI. TRATAMIENTO DE RIESGOS.

El tratamiento de riesgos es el proceso que consiste en seleccionar y aplicar medidas para modificar el riesgo. El tratamiento de riesgos incluye, como principal elemento, el control o mitigación del riesgo, pero también se extiende más allá, por ejemplo, a la elusión de riesgos, a la transferencia de riesgos, a la financiación de riesgos, etc.

NOTA: En estos estándares, la financiación de riesgos se refiere a los mecanismos (ej. programas de seguros) destinados a costear las consecuencias financieras del riesgo. Por lo general, la financiación de riesgos no se considera una provisión de fondos para sufragar el coste derivado de la aplicación del tratamiento de riesgos (en contra de lo expuesto en la Guía ISO/CEI 73).

Cualquier sistema de tratamiento de riesgos debe proporcionar como mínimo:

- *Un funcionamiento efectivo y eficiente de la organización.*
- *Controles internos efectivos.*
- *Conformidad con las leyes y reglamentos.*

El proceso de análisis de riesgos asiste al funcionamiento efectivo y eficaz de la empresa al identificar aquellos riesgos que requieren mayor atención por parte de la dirección. Esta deberá priorizar acciones de control de riesgos en función de su potencial para beneficiar a la empresa.

La efectividad del control interno constituye el grado en que el riesgo será eliminado o reducido mediante las medidas de control propuestas. La rentabilidad de los controles internos está relacionada con el coste del control, comparado con los beneficios esperados de la reducción de riesgos.

Los controles propuestos tienen que medirse según el posible efecto económico en caso de que no se tome ninguna acción, comparado con el coste de la(s) acción(es) propuesta(s) y necesariamente requieren más información detallada e hipótesis que las que están disponibles inmediatamente.

En primer lugar, hay que fijar el coste de la puesta en práctica. Este debe calcularse con precisión, ya que se convertirá rápidamente en la referencia con la que se medirá la rentabilidad. También hay que calcular la perdida que se debe prever si no se toma ninguna medida, y, al comparar los resultados, la dirección puede decidir si poner o no en práctica las medidas de control de riesgos.

La conformidad con las leyes y regulaciones no es opcional. Una empresa debe entender las leyes aplicables y debe aplicar un sistema de control para lograr la conformidad. Solo ocasionalmente se dispone de cierta flexibilidad cuando el coste de reducción de un riesgo es totalmente desproporcionado con relación a ese riesgo.

Una forma de obtener protección financiera contra el impacto de los riesgos consiste en la financiación de riesgos, la cual incluye el seguro. No obstante, debe resaltarse que algunas pérdidas o elementos de una perdida no podrán asegurarse, como por ejemplo algunos costes asociados a la salud, la seguridad en el trabajo o los incidentes medioambientales, que pueden incluir daños a la moral de los empleados o a la reputación de la empresa.

VII. INFORME Y COMUNICACIÓN DE RIESGOS.

A. Informe interno

Los diferentes niveles de una empresa necesitan diferentes tipos de información del proceso de gestión de riesgos.

El Consejo de Administración debe:

- *Conocer los riesgos más importantes a los que se enfrenta la empresa.*
- *Conocer los posibles efectos en el valor de la empresa para los accionistas de las desviaciones con respecto a los márgenes de rendimiento previstos.*
- *Asegurar niveles apropiados de toma de conciencia en toda la empresa.*
- *Saber cómo la empresa gestionará una crisis.*
- *Ser consciente de la importancia de la confianza de los interesados en la empresa.*
- *Tener claro cómo gestionar las comunicaciones con los inversores cuando sea pertinente.*
- *Estar seguro de que el proceso de gestión de riesgos funciona de forma efectiva.*
- *Divulgar una clara política de gestión de riesgos que abarque las responsabilidades y la filosofía de gestión de riesgos.*

Las unidades de negocios deben:

- *Ser conscientes de los riesgos que comprenden sus áreas de responsabilidad, los impactos posibles que estos pueden ejercer en otras áreas y las consecuencias que otras áreas pueden provocar en ellas.*
- *Disponer de indicadores de rendimiento que les permitan supervisar las actividades de negocio y financieras clave, el progreso hacia la consecución de los objetivos e identificar los desarrollos que requieran intervenciones (ej. previsiones y presupuestos).*
- *Disponer de sistemas que adviertan de las variaciones en las previsiones y en los presupuestos con la debida frecuencia para que sea posible tomar las medidas apropiadas.*
- *Informar rápida y sistemáticamente a la alta dirección de cualquier nuevo riesgo o cualquier fallo en las medidas de control existentes que perciban.*
- Los individuos deben:
- *Comprender su responsabilidad respecto a riesgos individuales.*
- *Ser conscientes de cómo pueden mejorar continuamente la respuesta de la gestión de riesgos.*
- *Entender que la gestión y la conciencia de riesgos son una parte fundamental de la cultura de la empresa.*
- *Informar rápida y sistemáticamente a la alta dirección de cualquier nuevo riesgo o cualquier fallo en las medidas de control existentes que perciban.*

B. Comunicación externa.

Las empresas tienen que informar regularmente a sus interesados explicando sus políticas de gestión de riesgos y la efectividad con la que está consiguiendo sus objetivos.

Cada vez más, los interesados esperan que las empresas den muestras de una gestión eficaz en cuanto al rendimiento no financiero de la empresa en áreas como asuntos comunitarios, derechos humanos, prácticas laborales, salud, seguridad y medioambiente.

Un buen gobierno corporativo requiere que las compañías adopten un enfoque metódico respecto a la gestión de riesgos que:

- *Proteja los intereses de sus interesados.*
- *Asegure que el consejo de administración desempeña sus deberes de dirigir la estrategia, crear valor y supervisar el rendimiento de la empresa.*
- *Asegure que los controles de gestión existen y que funcionan bien.*

Las medidas relativas a los informes a cumplimentar sobre la gestión de riesgos deben quedar establecidas claramente y ser puestas a disposición de los interesados.

Los informes deben tratar:

- *Los métodos de control, especialmente de las responsabilidades de la dirección sobre la gestión de riesgos.*
- *Los procesos para identificación de riesgos y cómo son conducidos por los sistemas de gestión de riesgos.*
- *Los sistemas de control primarios implantados para gestionar riesgos importantes.*
- *La supervisión y revisión del sistema implantado.*

Cualquier deficiencia importante que no esté cubierta por el sistema, o que se dé en el propio sistema, debe ser notificada junto con las medidas que se han tomado para tratarla.

VIII. LA ESTRUCTURA Y LA ADMINISTRACIÓN DE LA GESTIÓN DE RIESGOS.

A. Política de gestión de riesgos

La política de gestión de riesgos de una empresa debe definir su enfoque y apetito del riesgo, así como su enfoque de la gestión de riesgos. La política también debe establecer las responsabilidades de la gestión de riesgos en toda la empresa.

Además, debe referirse a cualquier requerimiento legal para los principios de la política, por ejemplo, en el campo de la salud y la seguridad.

Vinculado al proceso de gestión de riesgos, debe existir un conjunto integrado de herramientas y técnicas para usar en las diferentes fases del proceso empresarial. Para trabajar de forma efectiva, el proceso de gestión de riesgos requiere:

- *El compromiso por parte del presidente y los altos ejecutivos de la empresa.*
- *La asignación de responsabilidades dentro de la empresa.*
- *La asignación de los recursos apropiados para la formación y el desarrollo de una conciencia de riesgos mejorada por parte de todos los interesados.*

B. Papel del consejo de administración.

El consejo de administración tiene la responsabilidad de determinar la dirección estratégica de la empresa y de crear el entorno y las estructuras necesarias para que la gestión de riesgos opere de forma eficaz. Esta tarea se puede realizar a través de una dirección ejecutiva, una comisión no ejecutiva, un comité de auditoría o cualquier otra función que se ajuste al modo de operar de la organización y que sea capaz de actuar como "promotor" de la gestión de riesgos.

Al evaluar su sistema de control interno, el consejo debe, como mínimo, tener en cuenta:

- *La naturaleza y extensión de los riesgos negativos aceptables por la compañía que puede absorberlos en su negocio particular.*
- *La probabilidad de que esos riesgos se conviertan en realidad.*
- *Cómo deben tratarse los riesgos inaceptables.*
- *La habilidad de la compañía para minimizar la probabilidad y el impacto en el negocio.*
- *Los costes y beneficios del riesgo y la actividad de control llevada a cabo.*
- *La efectividad del proceso de gestión de riesgos.*
- *La implicación en los riesgos de las decisiones del consejo de administración.*

C. Papel de las unidades de negocios / seguridad.

El papel de las unidades de negocio / seguridad incluye lo siguiente:

- *Las unidades de negocios / seguridad tienen la responsabilidad primaria de gestionar los riesgos en el día a día.*
- *La dirección de las unidades de negocios / seguridad es responsable de promover la conciencia del riesgo en sus operaciones; deben introducir objetivos de gestión de riesgos en su actividad.*
- *La gestión de riesgos debe ser un tema habitual en las reuniones de la dirección para considerar las exposiciones y fijar nuevas prioridades en el trabajo a la luz de un análisis de riesgos efectivo.*
- *La dirección de las unidades de negocios / seguridad debe asegurar que la gestión de riesgos está incorporada en la fase conceptual de los proyectos, así como a lo largo de la vida de los mismos.*

D. El papel de la función de gestión de riesgos.

Dependiendo del tamaño de la empresa, la función de gestión de riesgos puede variar desde un simple defensor de la gestión de riesgos, pasando por un gestor de riesgos a tiempo parcial, hasta un departamento de gestión de riesgos completo.

El papel de la función de gestión de riesgos incluye lo siguiente:

- *Establecer la política y la estrategia de gestión de riesgos.*
- *Primer defensor de la gestión de riesgos en los niveles estratégico y operacional.*
- *Crear una cultura consciente de riesgos dentro de la empresa, incluyendo la formación apropiada.*
- *Establecer la política y estructuras de riesgos internas para las unidades de negocios.*
- *Diseñar y revisar los procesos de gestión de riesgos.*
- *Coordinar las diversas actividades funcionales que informan de los temas de gestión de riesgos dentro de la empresa.*
- *Desarrollar procesos de respuesta al riesgo, incluyendo planes de contingencia y de continuidad del negocio.*
- *Preparar los informes de riesgos para el consejo de administración y los interesados.*

E. El papel de la auditoría interna.

El papel de la auditoría interna puede variar de una empresa a otra.

En la práctica, este papel puede incluir todas o alguna de las siguientes tareas:

- *Enfocar el trabajo de la auditoría interna sobre los riesgos importantes, identificados por la dirección, y revisar los procesos de gestión de riesgos en toda la empresa.*
- *Producir confianza en la gestión de riesgos.*
- *Proporcionar un apoyo activo y participar en el proceso de gestión de riesgos.*
- *Facilitar la identificación y valoración de riesgos y formar al personal de operaciones en la gestión de riesgos y el control interno.*
- *Coordinar los informes de riesgos al consejo de administración, al comité de auditoría, etc.*

Al determinar el papel más apropiado de una empresa en particular, la auditoría interna debe asegurar que no se infringen los requisitos profesionales de independencia y objetividad.

F. Recursos y aplicación.

Los recursos necesarios para llevar a cabo la política de gestión de riesgos de la empresa deben establecerse claramente a todos los niveles de gestión y en cada unidad de negocios. Además de otras funciones operacionales que puedan tener, las personas involucradas en la gestión de riesgos deberán tener claramente definidos sus papeles en la coordinación de la política y de la estrategia de gestión de riesgos. Se requiere la misma definición clara para aquellas personas involucradas en la auditoría y la revisión de controles internos y que faciliten el proceso de gestión de riesgos. La gestión de riesgos debe estar integrada en la empresa a través de los procesos estratégicos y presupuestarios. Es necesario destacarla en la iniciación y en toda la formación y desarrollo, así como en los procesos operacionales, por ejemplo, los proyectos de desarrollo de productos o servicios.

IX. Supervisión y revisión del proceso de gestión de riesgos

Una gestión de riesgos efectiva requiere una estructura de informe y revisión para asegurar que los riesgos están identificados y evaluados eficazmente, que se llevan a cabo los controles oportunos y que las reacciones son las apropiadas. Se deben efectuar con regularidad auditorías de la política y de conformidad con los estándares, así como revisiones del rendimiento de los estándares para identificar las oportunidades de mejora. Hay que recordar que las empresas son dinámicas y que operan en entornos dinámicos. Es imprescindible identificar los cambios en la empresa y en el entorno en el que opera, y efectuar las modificaciones apropiadas en los sistemas.

El proceso de supervisión debe asegurar que existen los controles apropiados de las actividades de la empresa y que se entienden y se siguen los procedimientos

establecidos. Es imprescindible identificar los cambios en la empresa y en el entorno en el que opera, y efectuar las modificaciones apropiadas en los sistemas.

Cualquier proceso de supervisión y revisión debe determinar también si:

- *Las medidas adoptadas dan el resultado previsto.*
- *Eran apropiados los procedimientos adoptados y la información recogida para la valoración.*
- *Un mayor conocimiento habría ayudado a tomar mejores decisiones y a identificar qué lecciones deberían aprenderse para la valoración y gestión de riesgos en el futuro.*

APÉNDICE

X. Apéndice

Técnicas de identificación de riesgos - ejemplos

- Tormenta de ideas
- Cuestionarios
- Estudios empresariales que se centren en cada proceso de negocio y describan tanto los procesos internos como los factores externos que puedan influir en estos procesos.
- Establecimiento de criterios de competencia comparativa (“benchmarking”) en la industria.
- Análisis de distintos escenarios
- Talleres de valoración de riesgos
- Investigación de incidentes
- Auditoría e inspección
- Método HAZOP (Hazard & Operability Studies -Estudios de Azar y Operatividad-)

Métodos y técnicas de análisis de riesgos - ejemplos

Riesgo positivo

- Estudios de mercado
- Prospección
- Pruebas de mercado
- Investigación y desarrollo
- Análisis de impacto en el negocio

Ambos

- Establecimiento de modelos de dependencia
- Análisis SWOT (Strengths, Weaknesses, Opportunities, Threats -puntos fuertes, puntos flacos, oportunidades y amenazas-)
- Análisis del árbol de sucesos
- Planes de continuidad del negocio

- Análisis BPEST (Business, Political, Economic, Social, Technological -de negocio, político, económico, social, tecnológico-)
- Establecimiento de modelos de opción real.
- Toma de decisiones en condiciones de riesgo e incertidumbre
- Inferencia estadística
- Medidas de tendencia central y dispersión
- PESTLE (Political, Economic, Social, Technical, Legal, Environmental -político, económico, social, técnico, legal, medioambiental-)

Riesgos negativos

- Análisis de amenazas
- Análisis del árbol de fallos
- Análisis FMEA (Failure Mode & Effects Análisis -análisis de los modos de fallos y sus efectos-)