

Instituto de Ciencias del Seguro

Riesgo operacional en el marco de Solvencia II

Ana Belén Herrero Brañas

FUNDACIÓN **MAPFRE**

© FUNDACIÓN MAPFRE

Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o de FUNDACIÓN MAPFRE

FUNDACIÓN MAPFRE no se hace responsable del contenido de esta obra, ni el hecho de publicarla implica conformidad o identificación con la opinión del autor o autores.

Prohibida la reproducción total o parcial de esta obra sin el permiso escrito del autor o del editor.

© 2012, FUNDACIÓN MAPFRE
Paseo de Recoletos 23
28004 Madrid (España)

www.fundacionmapfre.com/cienciasdelseguro
publicaciones.ics@mapfre.com

ISBN: 978-84-9844-270-0
Depósito Legal: M-22642-2012

PRESENTACIÓN

Desde 1975, FUNDACIÓN MAPFRE desarrolla actividades de interés general para la sociedad en distintos ámbitos profesionales y culturales, así como acciones destinadas a la mejora de las condiciones económicas y sociales de las personas y sectores menos favorecidos de la sociedad. En este marco, el Instituto de Ciencias del Seguro de FUNDACIÓN MAPFRE promueve y desarrolla actividades educativas y de investigación en los campos del seguro y de la gerencia de riesgos.

En el área educativa, su actuación abarca la formación académica de postgrado y especialización, desarrollada en colaboración con la Universidad Pontificia de Salamanca, así como cursos y seminarios para profesionales, impartidos en España e Iberoamérica. Estas tareas se extienden hacia otros ámbitos geográficos mediante la colaboración con instituciones españolas e internacionales, así como a través de un programa de formación a través de Internet.

El Instituto promueve ayudas a la investigación en las áreas científicas del riesgo y del seguro y mantiene un Centro de Documentación especializado en seguros y gerencia de riesgos, que da soporte a sus actividades.

Asimismo, el Instituto promueve y elabora informes periódicos y publica libros sobre el seguro y la gerencia de riesgos, con objeto de contribuir a un mejor conocimiento de dichas materias. En algunos casos estas obras sirven como referencia para quienes se inician en el estudio o la práctica del seguro, y en otros, como fuentes de información para profundizar en materias específicas. Dentro de estas actividades se encuadra la publicación de este libro.

Desde hace unos años, Internet es el medio por el que se desarrollan mayoritariamente nuestras actividades, ofreciendo a los usuarios de todo el mundo la posibilidad de acceder a las mismas de una manera rápida y eficaz mediante soportes Web de última generación a través de www.fundacionmapfre.com\cienciasdelseguro

Ana Belén Herrero Brañas, nació en 1987 en Segovia. Es doble licenciada en Administración y Dirección de Empresa y en Ciencias Actuariales y Financieras por la Universidad Pontificia de Salamanca. Su brillante época de estudiante culminó con el Premio Extraordinario de Fin de Carrera 2011 por el proyecto que se presenta en este libro “El riesgo operacional en el marco de Solvencia II”.

Compaginó sus años universitarios con prácticas en distintas entidades del sector asegurador y, en la última etapa, trabajó en el área de Análisis de Balances de la Dirección General de Seguros y Fondos de Pensiones, órgano administrativo que regula y supervisa la actividad aseguradora española.

Actualmente, desarrolla su carrera profesional en el sector asegurador.

PRÓLOGO

El presente Cuaderno contiene el trabajo titulado *El riesgo operacional en el marco de Solvencia II*, que fue presentado por su autora; D^a Ana Belén Herrero Brañas, como Memoria de Fin de Grado para la obtención del Título de Licenciado en Ciencias Actuariales y Financieras por la Universidad Pontificia de Salamanca, en la Facultad de Ciencias del Seguro, Jurídicas y de la Empresa que gestiona el Instituto de Ciencias del Seguro de FUNDACIÓN MAPFRE.

Dicha Memoria fue dirigida por el profesor D. Joaquín Melgarejo Armada, como tutor, habiendo merecido las máximas calificaciones. Conviene indicar que, de acuerdo con las normas académicas aplicables, la calificación de cada memoria se obtiene a la vista de las notas otorgadas por el tutor de la misma y por el supervisor que debe ser nombrado de acuerdo con las citadas normas.

El trabajo referido obtuvo el Premio a la Mejor Memoria de Grado que, por duodécimo año consecutivo, convoca FUNDACIÓN MAPFRE con el fin de favorecer la calidad y la excelencia de los trabajos que los alumnos de Licenciatura han de presentar, obligatoriamente para obtener dicho grado académico, no pudiendo presentarse al premio las memorias cuya calificación sea inferior a 9 sobre 10. En las bases de la convocatoria se establece la posibilidad de que el trabajo sea publicado en la presente colección *Cuadernos de la Fundación*.

El Jurado acordó por unanimidad recomendar la publicación del trabajo que aquí se presenta. El contenido, sobre el que no es oportuno extenderse con el fin de evitar al lector reiteraciones innecesarias, aborda un tema de gran interés para el sector asegurador puesto que analiza la gestión de aquellos riesgos de pérdidas derivados de la inadecuación de procesos internos, de personal o de los sistemas, o de sucesos externos, así como de los cambios normativos. Tal es la importancia que los reguladores conceden a los riesgos operacionales que estos pueden considerarse como el eje principal de los cambios normativos de Basilea II y Solvencia II.

Deseamos transmitir nuestra felicitación a la autora, por el esfuerzo y el resultado final obtenido, así como al tutor del trabajo, por la acertada y valiente elección del tema, por el rigor en la orientación del mismo y por el constante estímulo demostrado para llevar a buen fin su ejecución. Aprovechamos la ocasión para animar a la autora a seguir profundizado en la materia objeto de este estudio con la seriedad y brillantez que ha caracterizado su trayectoria en esta Facultad, en la que además obtuvo su Licenciatura en Administración y Dirección de Empresas.

María José Albert Pérez

Decana

FACULTAD DE CIENCIAS DEL SEGURO, JURÍDICAS Y DE LA EMPRESA

Instituto de Ciencias del Seguro

Madrid, abril de 2012

AGRADECIMIENTOS

No quisiera finalizar este trabajo sin expresar mi agradecimiento al personal docente y no docente de la Facultad de Ciencias del Seguro, Jurídicas y de la Empresa; han sido seis años dónde no sólo me he formado en el plano académico sino también en el personal y muchos de los momentos que recordaré siempre, y que seguramente sirvan para otras circunstancias de mi vida, han tenido lugar en las instalaciones de la universidad.

Muy especialmente, me gustaría agradecer a mi tutor , en primer lugar , que accediera a serlo, así como su ayuda y asesoramiento en la elección del tema a tratar y la predisposición que siempre ha manifestado; no sólo a lo largo del desarrollo del trabajo si no en cada una de sus clases. Es un lujo contar con profesionales de esta categoría que hacen que temas que, a priori, pueden no resultar muy atractivos, al final, acaben siendo tan interesantes.

Finalmente, mi deseo personal es que este documento, independientemente de quien lo lea, contribuya a recalcar la importancia del riesgo operacional, lo necesario que es el adecuado tratamiento del mismo para un exitoso porvenir empresarial y su relevancia dentro del contexto normativo actual.

Si logro esto, habré conseguido el objetivo que me propuse cuando me empecé a interesar por este tema y decidí plasmarlo en mi trabajo de fin de carrera.

Muchas gracias,

Ana Belén Herrero Brañas

INTRODUCCIÓN

El riesgo operacional es un tipo más de riesgo al que las compañías están expuestas en su actividad empresarial. Sin embargo, otros como el riesgo de mercado, de crédito o de liquidez le han quitado protagonismo; las entidades se han preocupado más por protegerse de estos últimos a través de mecanismos de gestión de riesgos adecuados a sus propias necesidades.

No obstante, en los últimos años y como consecuencia de los importantes cambios en los mercados debidos a la globalización y al auge tecnológico, entre otros motivos, se ha producido un cambio en la concepción del riesgo operacional pasando de ser un “cajón de sastre”, donde se reflejaba todo aquello que no era ni riesgo de crédito ni de mercado, a configurarse con un marco de gestión propio donde se identifican eventos y fuentes que pueden dar lugar a pérdidas importantes de tipo operacional.

Tal es su importancia que la actividad bancaria y, posteriormente, la aseguradora -con la entrada en vigor de Basilea II y Solvencia II, respectivamente- ha experimentado un importante cambio normativo cuyo eje principal es el tratamiento del riesgo operacional.

Por todos estos motivos, resulta conveniente realizar un análisis en profundidad que permita el conocimiento del riesgo operacional y la importancia que un adecuado tratamiento del mismo representa dentro de la gestión de riesgos.

A pesar de que es un riesgo inherente a cualquier actividad económica el desconocimiento del mismo ha propiciado que su desarrollo sea relativamente reciente y, debido a esto, resulta imprescindible conocer en qué se basa y cómo se estructura la gestión de riesgos, en general, para poder profundizar en el tratamiento del riesgo operacional.

Así, este trabajo se estructura en tres partes:

- La primera está dedicada al **análisis y gestión del riesgo**. Se tratan temas tan importantes como: su definición, la evolución de la administración de los riesgos y, más en detalle, el Enterprise Risk Management (ERM).

- La segunda parte se refiere, fundamentalmente, al **riesgo operacional** en la actividad aseguradora. Sin embargo, se menciona la actividad bancaria ya que Solvencia II, en la mayoría de sus aspectos, está basada en Basilea II.
- La tercera y última parte contempla una serie de **anexos** que tratan temas importantes en la gestión del riesgo operacional como, por ejemplo, la elaboración de un mapa de riesgo -una de las herramientas más empleadas por las entidades para la gestión de riesgos- o, entre otros, una comparación del tratamiento del riesgo operacional entre Europa y Latinoamérica; la intención de los supervisores de países latinoamericanos es tomar Solvencia II como marco de trabajo para sus exigencias regulatorias.

Personalmente, espero que este trabajo resalte la importancia de una adecuada gestión del riesgo operacional y que ayude a comprender en qué consiste dicho riesgo, cómo se debe tratar adecuadamente en la estrategia empresarial y porqué genera tantos cambios normativos en el panorama europeo.

ÍNDICE

| | |
|--|----|
| I. EL RIESGO. LA GESTIÓN DE RIESGOS | 1 |
| 1. INTRODUCCIÓN | 1 |
| 2. DEFINICIÓN DE RIESGO | 1 |
| 3. TIPOS DE RIESGO | 2 |
| 4. EVOLUCIÓN DE LA ADMINISTRACIÓN DE RIESGOS | 5 |
| 5. LA IMPORTANCIA DEL ERM | 8 |
| 5.1 INTRODUCCIÓN..... | 10 |
| Control Interno. | 11 |
| Informe COSO | 11 |
| Claves para comprender el ERM..... | 14 |
| 5.2 GESTIÓN DE RIESGOS: ENTERPRISE RISK MANAGEMENT (ERM) 16 | |
| Consecución de objetivos. | 17 |
| Proceso de Implantación..... | 18 |
| Componentes de la gestión de riesgos operativos. | 20 |
| Roles y responsabilidades en la gestión de los riesgos..... | 27 |
| 5.3 RELEVANCIA DE LA REINGIENERÍA DE PROCESOS | 31 |
| 6. CONCLUSIONES | 34 |
| II. EL RIESGO OPERACIONAL. TRATAMIENTO EN SOLVENCIA II. | 37 |
| 1. INTRODUCCIÓN | 37 |
| 2. EL RIESGO OPERACIONAL | 38 |
| 2.1. CONCEPTOS BÁSICOS. | 39 |
| Definición de riesgo operacional..... | 39 |
| Fuentes del riesgo operacional..... | 40 |

| | |
|--|------------|
| 2.2. EVOLUCIÓN DEL CONCEPTO DE RIESGO OPERACIONAL..... | 44 |
| 3. EL RIESGO OPERACIONAL EN EL MARCO DE SOLVENCIA II..... | 45 |
| 3.1. ENTENDIENDO SOLVENCIA II..... | 46 |
| Antecedentes | 48 |
| Entorno de Solvencia II..... | 49 |
| Estudios de impacto cuantitativo “QIS” | 54 |
| Directiva de Solvencia II | 56 |
| 3.2. TRATAMIENTO DEL RIESGO OPERACIONAL EN SOLVENCIA II..... | 59 |
| Gestión del Riesgo Operacional | 60 |
| Administración del Riesgo Operacional | 68 |
| Cuantificación del Riesgo Operacional | 81 |
| Evaluación del Riesgo Propio y de Solvencia (ORSA) | 93 |
| 3.3. ROLES Y RESPONSABILIDADES EN EL RIESGO OPERACIONAL | 101 |
| Junta Directiva y Alta Gerencia | 101 |
| Auditoría Interna del Riesgo Operacional | 103 |
| El papel del Gobierno Corporativo | 109 |
| 4. CONCLUSIONES..... | 118 |
| III. REFLEXIONES FINALES..... | 123 |
| REFERENCIAS BIBLIOGRÁFICAS..... | 131 |
| ANEXOS | 135 |
| MAPA DE RIESGO OPERACIONAL..... | 135 |
| COMPARATIVA EUROPA - LATINOAMÉRICA..... | 142 |
| EL RIESGO OPERACIONAL EN PRENSA..... | 156 |
| Colección Cuadernos de la Fundación | |
| <i>Instituto de Ciencias del Seguro.....</i> | <i>163</i> |

EL RIESGO. LA GESTIÓN DE RIESGOS

1. INTRODUCCIÓN

La desregulación y globalización de los servicios financieros junto con la creciente sofisticación de las tecnologías, hacen más complejas las actividades de las entidades financieras y, por lo tanto, aumentan sus perfiles de riesgo (es decir, el nivel de riesgo de las actividades y/o categorías de riesgo de una empresa).

Por otra parte, la alta competitividad en el sector financiero ha impulsado la introducción de las entidades en nuevos mercados; trabajar con nuevos productos no sólo aumenta la complejidad de sus operaciones sino que exige un análisis más profundo de los riesgos. En este sentido, una adecuada administración y supervisión de los riesgos es uno de los desafíos más grandes.

Ésta primera parte explica qué es el riesgo, de forma extensa, y cómo se contextualiza en la realidad empresarial. Se analizan los distintos tipos de riesgos a los que están expuestas las entidades financieras y cómo se deben tratar, globalmente, para su mitigación y control.

2. DEFINICIÓN DE RIESGO

A pesar de que éste documento se centra en el estudio y análisis del riesgo operacional conviene realizar una definición general del riesgo y de su tratamiento en la realidad empresarial para comprender mejor a que se refiere la Gerencia de riesgos.

El Diccionario de la **Real Academia Española de la Lengua** define el riesgo como:

1. Contingencia o proximidad de un daño.
2. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

Desde la óptica de la Gerencia de Riesgos y siguiendo las pautas de la **Guía ISO/CEI 73¹**, el riesgo es la *combinación de la probabilidad de un suceso y de sus efectos*, y una gestión adecuada requiere incluir tanto los aspectos negativos de su definición como los positivos. Por lo tanto, los presentes estándares consideran el riesgo desde ambas perspectivas.

¹ La **Guía ISO/CEI 73** fue publicada en el año 2009 por la *Organización Internacional de Normalización (ISO)* con el objetivo de proporcionar las definiciones de los conceptos generales relacionados con la gestión de riesgos.

De esta forma, ampliar el campo de efecto permite no sólo conservar y proteger el patrimonio empresarial de aquello que lo amenaza, sino preparar a la organización para detectar y aprovechar las oportunidades de negocio que su entorno le presente.

3. TIPOS DE RIESGOS

Toda persona y organización (empresas privadas y públicas, grandes corporaciones, etc.) están expuestas a riesgos de diversa naturaleza que tienen su origen en factores internos y externos.

Así, los riesgos pueden ser:

- **Internos:** son aquellos susceptibles de ser controlados por la empresa o en los que la misma puede influir de alguna manera. Algunos ejemplos de riesgos internos son los relativos al personal o a la investigación y desarrollo de la entidad.
- **Externos:** son aquellos que van más allá del control o de la influencia de la empresa. Destacan, entre otros, los referentes a la competencia o a los cambios en los mercados.

Hay tantas clasificaciones del riesgo como puntos de vista desde los que se abarque el estudio del mismo; por ejemplo, se pueden clasificar como: *ordinarios* y *extraordinarios*, riesgo *inherente* que resulta de la naturaleza de los objetivos y del alcance o *adquirido* que resulta del enfoque, metodologías, herramientas, técnicas, habilidades y de la experiencia que se aplican al proyecto, etc.

Las diferentes modalidades de riesgos que condicionan la consecución de los objetivos empresariales se clasifican como:



Fuente: elaboración propia.

Riesgos financieros

Los riesgos financieros se refieren a la probabilidad de ocurrencia de un evento que tenga consecuencias financieras negativas para una organización e influyan en sus resultados.

Así, destacan los siguientes riesgos financieros:

Riesgo de mercado

El Riesgo de Mercado está asociado a variaciones -o volatilidades- en los precios de los activos y pasivos financieros y se evalúa a través de los cambios en el valor de los mismos. Este riesgo está, a su vez, constituido por otras subcategorías como son:

- **Riesgo de cambio:** surge como consecuencia de la volatilidad del mercado de divisas.
- **Riesgo de tipo de interés:** es el resultado de las variaciones en los tipos de interés.
- **Riesgo de mercado** (en acepción restringida): se refiere específicamente a la volatilidad de los mercados de instrumentos financieros.

Riesgo de crédito

En ocasiones, puede ocurrir que una de las partes de un contrato financiero no cumpla con sus obligaciones; en éste tipo de situaciones surge el riesgo de crédito.

Riesgo de liquidez o de financiación

Se manifiesta cuando una de las partes de un contrato financiero no puede obtener la liquidez necesaria para asumir sus obligaciones, a pesar de disponer de los activos precisos, que no puede vender al precio adecuado ni con la suficiente rapidez, y de la voluntad de cumplir los compromisos adquiridos.

Riesgos estratégicos

Los riesgos estratégicos, según el Diccionario Mapfre de Seguros, son “*aquellos referidos a los objetivos principales o directrices de una empresa u organización, normalmente en el medio y largo plazo*”.

Es decir, son aquellos que destruyen el valor de la empresa por efecto de cambios que ocurren en el entorno país -político, económico y social-, el entorno competitivo de la empresa, la posición estratégica del producto -tendencias tecnológicas y tendencias de consumo-, la implementación de proyectos y el vínculo con los principales stakeholders² de la empresa.

Riesgo operacional

Se define el **riesgo operacional** como la *posibilidad de que se produzcan pérdidas directas o indirectas asociadas a errores humanos, fallos en los sistemas, existencia de políticas, procesos o controles inadecuados y eventos externos*.

Es la clase de riesgo más novedoso de los considerados por los actuales marcos normativos europeos en las entidades financieras. Esta situación se refleja en Basilea II³; acuerdo pionero en establecer mecanismos de cálculo de los requerimientos mínimos de capital para ajustar su valoración a los riesgos reales que soportan las entidades, es decir, plantea modificar las exigencias iniciales de Basilea I para incluir la cobertura del riesgo operacional.

² **Stakeholders:** término inglés. Conjunto de personas y organizaciones que pueden afectar, ser afectadas o percibir por sí mismas que pueden ser afectadas por una decisión, actividad o riesgo.

³ **Basilea II:** acuerdo internacional para homogeneizar la legislación y regulación bancaria en materia de riesgo basado, fundamentalmente, en las buenas prácticas de gestión de riesgos de la industria bancaria. Su objetivo consiste en estimular el desarrollo de unos procedimientos internos de gestión de riesgo adecuados a los riesgos asumidos.

La explicación de un adecuado proceso de gestión y administración del mismo, por parte de las compañías aseguradoras, constituye el tema central del trabajo.

Riesgos fortuito o debido al azar

Un riesgo es fortuito cuando proviene de un acto o acontecimiento ajeno a la voluntad humana de producirlo.

Por ejemplo, tienen tal consideración a aquellos que se deben a circunstancias del medio ambiente o a eventos de la naturaleza.

4. EVOLUCIÓN DE LA ADMINISTRACIÓN DE RIESGOS

La administración de riesgos es uno de los pilares fundamentales del gobierno corporativo; entendiendo este como el sistema mediante el cual las compañías son dirigidas y controladas para el beneficio de los empresarios y de otros interesados claves que sostienen e incrementan el valor de la organización.

En los últimos años, se ha producido un importante cambio en la concepción del riesgo y, como consecuencia, en la forma de concebir la gestión y administración de los mismos.

Así, de forma resumida, se observan los siguientes cambios:

| PASADO | HOY |
|---|--|
| <ul style="list-style-type: none">• El riesgo en forma individual.• Evaluación e identificación de los riesgos.• Enfoque a todos los riesgos.• Mitigación de riesgos.• No dueños de riesgos.• Cuantificación desordenada de riesgos.• El riesgo no es mi responsabilidad.• Evaluado. | <ul style="list-style-type: none">• Riesgo como estrategia de negocio.• Desarrollo de portafolio de riesgos.• Enfoque a riesgos críticos.• Optimización de riesgos.• Responsabilidades definidas.• Mapa de procesos, medición y monitoreo.• Riesgo responsabilidad de cada uno.• Autocontrol. |

Fuente: elaboración propia.

Históricamente, dentro de las organizaciones tanto públicas como privadas la administración de riesgos se ha manejado de forma aislada al resto de ámbitos de la entidad. Sin embargo, como consecuencia de la evolución en la estructura organizacional de las entidades, entre otras circunstancias, la situación ha cambiado; la gerencia de riesgos tiene que estar presente en todas las áreas de actividad de las empresas e informar convenientemente a todos los niveles de la misma.

Gestión de los riesgos y creación de valor

A medida que los riesgos cambian y se multiplican, los gerentes de las compañías se aseguran de que se están valorando convenientemente. No sólo es importante que se tengan en cuenta los riesgos apropiados sino también es importante conocer la cantidad de los mismos que se puede asumir. Como consecuencia, la gestión de riesgo comienza a ser percibida como una nueva forma de administración estratégica de negocio, relacionando la estrategia empresarial con los riesgos cotidianos.

Además, la administración de los riesgos está ligada a la creación del valor. Los riesgos ya no son simplemente peligros que evitar sino que, en muchos casos, son oportunidades que aprovechar. La oportunidad crea valor y, por último, el valor crea riqueza para los accionistas. Por lo tanto, cómo administrar de la mejor forma los riesgos para obtener ese valor se ha convertido en una pregunta crítica.

La administración de los riesgos se debe extender más allá de los peligros tradicionales, financieros y asegurables, para abarcar una amplia variedad de riesgos estratégicos, operacionales, de reputación, regulatorios y de información.

Entender los riesgos y las oportunidades



La necesidad de entender los riesgos y las oportunidades es ineludible cuando se trata de alcanzar el progreso de cualquier empresa. La capacidad de que un negocio prospere al afrontar los riesgos, al mismo tiempo que responde a acontecimientos imprevistos -buenos o malos-, es un indicador de su destreza para competir.

Sin embargo, la exposición al riesgo es cada vez mayor, más compleja, diversa y dinámica. Esto es debido, en gran parte, a los rápidos cambios en la tecnología, la velocidad de la comunicación, la globalización de los negocios y las fluctuaciones en los tipos de cambio dentro de los mercados financieros.

La fuente del riesgo puede situarse dentro de la organización. En este caso, se manifiesta sobre todo en el afán de las empresas por crecer. Así, la adopción de estrategias de expansión, como las adquisiciones de empresas, las inversiones en nuevos mercados internacionales, las grandes reestructuraciones organizacionales, el outsourcing de los procesos clave, los grandes proyectos de inversión y el

desarrollo de nuevos productos, se pueden convertir en elementos que aumenten la exposición al riesgo.

Como consecuencia de la diversidad de riesgos la gerencia requiere un acercamiento más profundo a la administración de los mismos. La mayoría de los accionistas, y los organismos reguladores, solicitan a las juntas directivas una administración de riesgos más comprensiva, rigurosa y sistemática.

Las compañías que consideran la administración de riesgos sólo una cuestión de cumplimiento de los principios contables y legales aumentan bastante su exposición a los mismos, lo que provoca que se reporten estados financieros afectados seriamente por los riesgos.

Crecimiento empresarial a través de los riesgos

El riesgo es inevitable en la actividad empresarial, por lo tanto, una adecuada administración de los mismos reporta importantes beneficios para las entidades.

Es muy raro encontrar una organización, independientemente de su tamaño, en la cual sus accionistas no soliciten que la estrategia empresarial presente una clara conciencia de la administración de riesgos.



Según una investigación realizada por la Unidad de Inteligencia Económica, *Economic Intelligence Unit*, que publica en el año 2006 la revista "The Economist" se descubrió que el 84% de los ejecutivos que respondieron a la encuesta consideran que la administración de riesgos empresarial puede mejorar su razón (ratio) financiero de precio por acción/ganancias y su coste de capital.

Las organizaciones que son más conscientes del riesgo tienen un manejo del mismo más activo, lo que proporciona oportunidades para lograr ventajas competitivas decisivas.

El papel de la junta directiva



La junta directiva, con independencia de la estrategia empresarial, debe decidir qué metas desea alcanzar y cuáles son los riesgos que está dispuesta a soportar para desarrollar las acciones encaminadas a alcanzar estos objetivos.

Por este motivo, la administración del riesgo está experimentando cambios fundamentales; el más destacable es el que aproxima dicha función a la parte más alta de la organización.

El control del riesgo es esencial para mantener la estabilidad y la continuidad en el funcionamiento de los negocios. Sin embargo, una serie de problemas inesperados del gobierno corporativo han conducido al colapso de varias compañías y a otros escándalos en todo el mundo. Los inversores han expresado su preocupación por el nivel bajo de confianza en los estados financieros y el descuido de las juntas directivas en las operaciones corporativas y en el grado de control de la administración de riesgos.

En respuesta a la mala imagen de las juntas directivas por su pobre desempeño y a la carencia de un gobierno corporativo apropiado, en el año 1995, el *Institute of Directors*⁴ publicó los estándares para las juntas directivas. En esta publicación se presentan cuatro tareas principales:

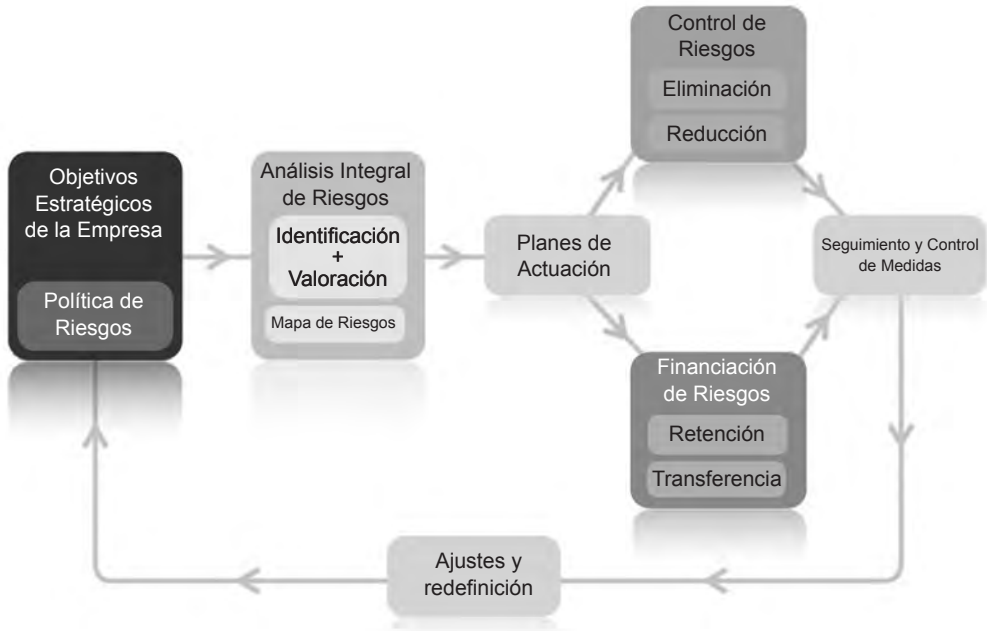
- La junta directiva debe ser emprendedora y conducir al negocio adelante mientras guarda un control prudente.
- Se requiere que la junta directiva esté suficientemente bien informada sobre el funcionamiento de la compañía y sea capaz de responder por sus acciones.
- El consejo directivo debe dar respuesta a corto plazo a los asuntos locales. Sin embargo, debe estar informado más ampliamente de las tendencias y de la competencia de naturaleza internacional.
- El consejo directivo tiene que estar centrado en las necesidades comerciales del negocio mientras que actúa responsablemente hacia sus empleados, sus socios comerciales y la sociedad en su totalidad.

En este contexto, ha surgido el ***Enterprise Risk Management (ERM)***, concepto que se explica más adelante, **como una propuesta disciplinada y estructurada que alinea la estrategia, los procesos, las personas, la tecnología y el conocimiento, con el propósito de evaluar y administrar las incertidumbres que la empresa enfrenta a medida que crea valor.**

5. LA IMPORTANCIA DEL ERM (ENTERPRISE RISK MANAGEMENT)

La Gerencia de Riesgos proporciona un método de gestión y administración del riesgo organizado en fases sucesivas que aportan a la empresa las herramientas necesarias para afrontar sus riesgos.

⁴ *Institute of Director*: organización de Reino Unido fundado en 1903 e incorporada por la carta real en 1906 para apoyar, representar y establecer normas para directores de la empresa.

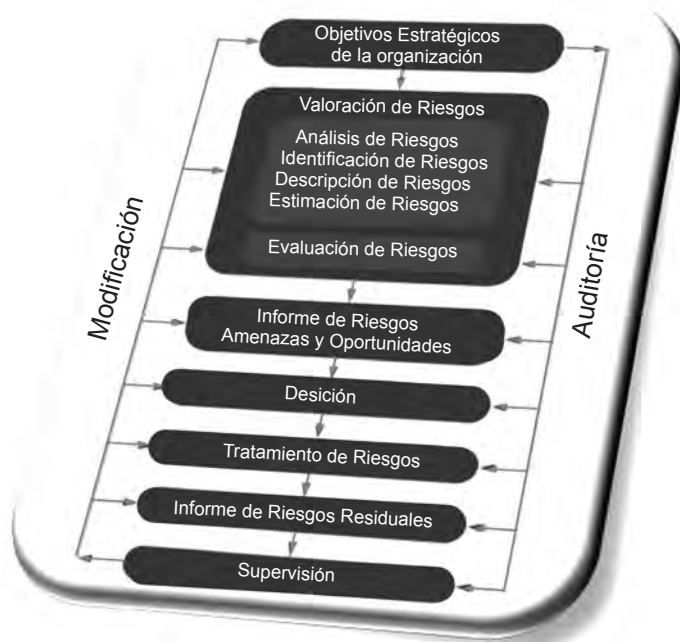


Fuente: FERMA (Federation of European Risk Management).

La gestión y administración de riesgos protege y añade valor a la empresa y sus interesados ("stakeholders") mediante el apoyo a sus objetivos que se fundamenta en:

- **Proveer** una **estructura** que permita 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 de 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.

La Gerencia de Riesgos es un tema complejo que implica la realización de diferentes acciones en el entorno empresarial. Estas se resumen en el esquema siguiente.



En apartados posteriores se analiza todos y cada uno de los aspectos que se tratan en el esquema y que resultan relevantes y necesarios para comprender la adecuada gerencia de los riesgos.

Todas las organizaciones, en cierta medida, gestionan el riesgo. Sin embargo, la norma **ISO 31000:2009**⁵ establece una serie de principios que deben ser satisfechos para que dicha gestión sea adecuada.

Fuente: FERMA (Federation of European Risk Management).

Esta norma internacional recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte cuyo objetivo sea integrar el proceso de gestión de riesgos en el gobierno corporativo de la organización y en su planificación, estrategia, procesos de información, políticas, valores y cultura.

5.1 INTRODUCCIÓN

Para comprender el proceso de Gestión de Riesgos (ERM) es necesario conocer algunos conceptos claves que permiten contextualizar todo lo relativo al marco de la gerencia y administración de los riesgos.

⁵ **ISO 31000:2009**: En noviembre del 2009, la Organización Internacional de Normalización (ISO) publicó la norma "ISO 31000:2009, Gestión de Riesgos - Principios y Directrices", una norma de gestión destinada a ayudar a las organizaciones de todos los tipos y tamaños a gestionar el riesgo con efectividad.

Control Interno

El **control interno** es el proceso que ejecuta la administración con el fin de evaluar operaciones específicas con seguridad razonable en tres principales categorías:

- Efectividad y eficiencia operacional.
- Confiabilidad de la información financiera.
- Cumplimiento de políticas, leyes y normas.

Al concebir el control interno como un proceso se hace referencia a una cadena de acciones extendida a todas las actividades inherentes a la gestión e integrados a los demás procesos básicos de la misma: planificación, ejecución y supervisión. Tales acciones se hallan incorporadas en la infraestructura de la entidad para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad.

Hoy en día, debido a la existencia de un mundo globalizado, surge la necesidad de integrar metodologías y conceptos en todos los niveles de las diversas áreas administrativas y operativas con el fin de ser competitivos y responder a las nuevas exigencias empresariales. Surge así, un nuevo concepto de control interno donde se brinda una estructura común que está documentada en el denominado *Informe COSO*.

Informe COSO

La denominación **COSO** proviene de “*Committee of Sponsoring Organizations of the Treadway Commission*”⁶. Dicho Comité está constituido por representantes de las siguientes organizaciones:

- American Accounting Association⁷ (AAA).
- American Institute of Certified Public Accountants⁸ (AICPA).
- Financial Executives Internacional⁹ (FEI).
- Institute of Internal Auditors¹⁰ (IIA).
- Institute Of Management Accountants¹¹ (IMA).

⁶ **Committee of Sponsoring Organizations of the Treadway Commission:** Comité de organizaciones patrocinadoras de la Comisión Treadway.

⁷ **American Accounting Association:** Asociación Americana de Contabilidad.

⁸ **American Institute of Certified Public Accountants:** Asociación Norteamericana de Contables Públicos.

⁹ **Financial Executives Internacional:** Organización Profesional de Altos Ejecutivos de Finanzas.

¹⁰ **Institute of Internal Auditors:** Asociación Profesional de Auditores.

¹¹ **Institute Of Management Accountants:** Asociación de Contables Administrativos.

El **Informe COSO** es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control interno. Debido a la gran aceptación que tiene desde su publicación en 1992, se ha convertido en el estándar de referencia en todo lo que concierne al control interno.

Existen dos versiones del Informe COSO; la versión de 1992 y la de 2004. Básicamente, la versión del 2004 no es otra cosa que una ampliación del Informe original para dotar al control interno de un mayor enfoque hacia el Enterprise Risk Management o gestión del riesgo.

Informe COSO I

En 1992, se publicó un informe denominado *Internal Control - Integrated Framework (IC-IF)*, conocido también como *COSO I*. Este informe surgió como respuesta a las inquietudes que planteaba la diversidad de conceptos, definiciones e interpretaciones existentes en torno al control interno.

El informe COSO plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la Treadway Commission, *National Commission on Fraudulent Financial Reporting*, creó en Estados Unidos en 1985.

El objetivo prioritario del informe COSO es ayudar a las organizaciones a mejorar el control de sus actividades, estableciendo un marco para los conceptos de control interno que permita una definición común de control interno y de identificación de sus componentes.

Informe COSO II

La preocupación por un adecuado tratamiento de los riesgos puso de manifiesto la necesidad de un marco más potente que permitiera la correcta identificación y coordinación de todos los aspectos que deben estar presentes para una efectiva administración y gestión del riesgo y que, a su vez, este proceso sea reconocido por todas las partes involucradas en dicha administración.

En el 2001, COSO puso en marcha un proyecto, respaldado por Pricewaterhouse Coopers¹², orientado al desarrollo de un marco para evaluar y mejorar la gestión de riesgos corporativos que sea fácil de poner en práctica por la dirección de las empresas.

El nuevo informe *COSO II* describe un *Marco Integrado de Gestión de Riesgos Corporativos (Enterprise Risk Management)* que se fundamenta en principios que incluyen la creación de valor de la empresa para sus shareholders¹³ pero sobre todo para sus stakeholders (donde se incluyen a los anteriores también).

¹² **Pricewaterhouse Coopers:** PwC es la mayor firma de servicios profesionales del mundo. Donde se ofrecen a las empresas y a las Administraciones servicios profesionales especializados en cada sector.

¹³ **Shareholders:** Persona física o jurídica propietaria de acciones de una compañía anónima o comanditaria por acciones.

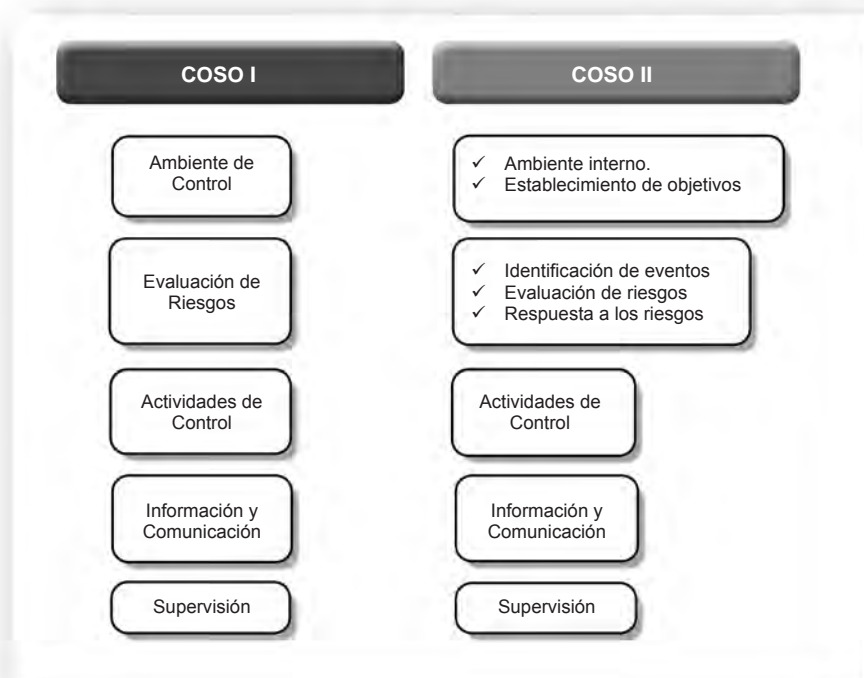
El valor se maximiza cuando se establecen estrategias y objetivos encaminados a un equilibrio entre el crecimiento, el rendimiento y los riesgos relacionados y el despliegue de recursos se realiza de manera eficiente y eficaz.

Dicho informe manifiesta que el ambiente empresarial transcurre en medio de mucha incertidumbre tanto positiva como negativa; positiva en el caso de aprovechar oportunidades y negativa si se convierte en un riesgo que atente contra los objetivos y la entidad en sí.

COSO II detalla en su marco una definición estructurada así como los principios críticos y componentes de un proceso de administración de riesgos efectivo. Además, proporciona pautas para las organizaciones sobre cómo mejorar su gestión de riesgos y criterios para determinar si esta es efectiva y, si no lo es, que se necesita para que lo sea.

Diferencias entre COSO I y COSO II

Las diferencias entre ambos informes se dirigen, fundamentalmente, a dar respuesta a las nuevas necesidades de gestión y administración de los riesgos que surgen en el contexto empresarial.



Fuente: elaboración propia a partir de datos proporcionados por los informes COSO I y COSO II.

COSO II introduce cambios en los apartados que el informe anterior dedicaba al Ambiente de Control y a la Evaluación de Riesgos. En cuanto al **Ambiente de Control** que proponía COSO I, el nuevo informe lo divide en Ambiente Interno y Establecimiento de Objetivos. Por otra parte, la **Evaluación de Riesgos** evoluciona en tres fases diferentes dedicadas a la Identificación, Evaluación y Respuesta a los Riesgos.

Claves para comprender el ERM

El *Enterprise Risk Management (ERM)* hace referencia al proceso de gerencia de riesgos que se ha de llevar a cabo en las entidades siguiendo el marco que establece el informe COSO II.

Sin embargo, antes de explicar cada una de las fases y elementos de la administración del riesgo, conviene resaltar determinados conceptos claves para comprender el entorno del *ERM* y aplicar los principios del mismo a la gerencia de los riesgos.

Así, siguiendo la definición que realiza el informe COSO II, a continuación se explica en qué consiste el Enterprise Risk Management, cuáles son las ventajas que proporciona su implementación a las organizaciones y señala las limitaciones que este proceso puede tener.

Estas claves resultan fundamentales para entender el efecto que la puesta en marcha del ERM tiene en las entidades y analizar cada una de las fases que se llevan a cabo en la gestión de riesgos.

Definición

Según la traducción del informe COSO II *“Enterprise Risk Management es un proceso, efectuado por una entidad delegada por el consejo de administración, la dirección y personal en general, aplicado en el establecimiento de la estrategia y a lo largo de la organización; diseñado para identificar eventos potenciales que puedan afectar a la entidad y gestionar el riesgo de acuerdo a su tolerancia de riesgo, para proporcionar una seguridad razonable en relación con el logro de los objetivos organizacionales.”*

El ERM es un proceso que se aplica en la estrategia de la organización de manera transversal, es decir, en todos los niveles y unidades de la misma. Está diseñado para identificar los eventos potenciales que pueden afectar a la organización y a su manejo del riesgo al delimitar una adecuada tolerancia al mismo.

Por lo tanto, es capaz de proporcionar al consejo de administración un proceso adecuado y eficaz para el control y administración de los riesgos.

Ventajas de una correcta implantación de ERM

La correcta implantación de un proceso de Gestión y Administración de Riesgos (ERM) conlleva una serie de ventajas para la entidad, tales como:

- *Alineación de apetito al riesgo y la estrategia*

La dirección debe considerar la tolerancia al riesgo de la entidad, el establecimiento de objetivos y el desarrollo de mecanismos para gestionar los riesgos.

- *Mejora el tiempo de respuesta*

El ERM proporciona una forma rigurosa de identificar y seleccionar entre las diferentes alternativas de manejar los riesgos, evitarlos, reducirlos, compartirlos, y asumirlos.

- *Reducción operativa de sorpresas y pérdidas*

Las entidades pueden conseguir una mayor capacidad para identificar eventos potenciales que sean perjudiciales y establecer las respuestas, para reducir sorpresas y sus costes asociados.

- *Identificación y gestión de riesgos interrelacionados*

Cada empresa se enfrenta a riesgos que afectan a diferentes ámbitos de la organización. El ERM facilita la gestión eficaz dando respuesta a los impactos de riesgos múltiples y relacionados entre sí, de una manera integral.

- *Aprovechar Oportunidades*

Al considerar una amplia gama de posibles acontecimientos, la dirección está en condiciones de identificar de manera proactiva más oportunidades.

- *Mejora en la distribución del Capital*

Al obtener información sobre los riesgos, la dirección puede evaluar eficazmente las necesidades globales de capital y mejorar la asignación del mismo.

Las ventajas que aporta el ERM ayudan a la dirección a alcanzar sus objetivos y evitar la pérdida de recursos. Esto se debe a que las prácticas que se desarrollan coinciden con las necesidades propias de cada entidad y para implantarlas es inexcusable un profundo autoconocimiento tanto de las fortalezas como de los puntos débiles, que son los que pueden acarrear importantes consecuencias negativas.

Limitaciones del ERM

A pesar de que el ERM proporciona importantes beneficios existen también una serie de limitaciones derivadas, principalmente, de aspectos que involucran el factor humano (por ejemplo, el buen o mal juicio que un directivo tenga en la toma de decisiones en torno al tratamiento de riesgos y la definición de controles). Además, es la propia dirección de la entidad la que tiene la decisión final con respecto al desarrollo del ERM.

Estas limitaciones pueden causar que tanto la dirección como el consejo de administración no tengan una certeza absoluta de la consecución de los objetivos de la entidad.

Otras limitaciones pueden ser:

- Escasos recursos.
- Responsabilidades Indefinidas.
- Ausencia de beneficios tangibles.
- Falta de capacidad y de aptitudes.
- Plan de Implementación difuso.

El ERM ayuda a mejorar notablemente la gestión eficaz de presentación de informes y el cumplimiento de leyes y reglamentos, evitar daños a la reputación de la entidad y sus consecuencias pero, para una implantación eficaz, es necesario tener siempre presentes las limitaciones del proceso.

5.2 GESTIÓN DE RIESGOS: ENTERPRISE RISK MANAGEMENT (ERM)

COSO define la **Gestión de Riesgos Corporativos** como un “*un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro*

del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos”.

Así, los aspectos claves del ERM se aprecian en la ilustración. Conviene explicar, ampliamente, cada una de las fases del proceso de Gerencia de Riesgos y cómo interactúan en las organizaciones.



Fuente: COSO Enterprise Risk Management- Integrated Framework. 2004.

Consecución de objetivos

El presente marco de gestión de riesgos corporativos está orientado a alcanzar los objetivos de la entidad. Se clasifican, tal y como se observa en el gráfico, en cuatro categorías:



Fuente: elaboración propia.

- **Estrategia:** objetivos a alto nivel alineados con la misión de la entidad y dándole apoyo.
- **Operaciones:** objetivos vinculados al uso eficaz y eficiente de recursos.
- **Información:** objetivos de fiabilidad de la información suministrada.
- **Cumplimiento:** objetivos relativos al cumplimiento de leyes y normas aplicables.

Estas categorías distintas, aunque relacionadas entre sí, se dirigen a múltiples necesidades de la entidad y pueden ser responsabilidad directa de diferentes ejecutivos.

Dado que los objetivos relacionados con la fiabilidad de la información y el cumplimiento de leyes y normas están integrados en el control de la entidad, puede esperarse que la gestión de riesgos corporativos facilite una seguridad razonable en la consecución de los mismos.

El logro de los objetivos estratégicos y operativos está sujeto a acontecimientos externos, por tanto, la gestión de riesgos proporciona la seguridad de que la dirección y el consejo de administración, en su papel de supervisión, están siendo informados oportunamente del progreso de la entidad hacia su consecución.

Proceso de implantación

Previo a la implantación de un proceso de gestión y administración de riesgos, la dirección debe plantearse cómo instaurarlo en la organización de manera que todos los ámbitos -y todos los niveles- de la entidad estén involucrados.

El tamaño, complejidad, sector, cultura, estilo de gestión y otras características de la entidad afectan al modo de instaurar los principios de la gerencia de riesgos de la manera más eficaz y eficiente posible. Aunque se dispone de una gran variedad de opciones y enfoques, la experiencia muestra que existen determinados puntos en común a todas las organizaciones.

A continuación, se describen las principales etapas seguidas por aquellas entidades que han conseguido completar con éxito la implantación de la gestión de riesgos corporativos.

Grado de preparación del equipo líder

El establecimiento de un equipo líder con representación de las unidades de negocio y funciones de soporte claves -incluyendo la planificación estratégica-, constituye un importante primer paso.

Este equipo se tiene que familiarizar con los componentes, conceptos y principios del marco, de forma que desarrolle un conocimiento y lenguaje común, así como la base fundamental y necesaria para diseñar e implantar un proceso de gestión de riesgos corporativos que aborde de manera eficaz las necesidades específicas de la entidad.

Apoyo de la alta dirección

Aunque el calendario y la forma de instrumentar el apoyo varían según la organización, resulta importante que éste comience pronto y se consolide conforme avanza la implantación.

El liderazgo, al nivel de dirección, articula los beneficios de la gestión de riesgos corporativos y establece y comunica al resto de la organización el proyecto y las necesidades de recursos necesarios para llevarlo a cabo.

El apoyo del consejero delegado y, normalmente, su implicación directa y visible, al menos inicialmente, conduce al éxito.



Desarrollo del plan de implantación

Se elabora un plan inicial para la ejecución de las siguientes etapas estableciendo fases claves del proyecto e incluyendo la definición de flujos de trabajo, hitos, recursos y calendario.

Se identifican las responsabilidades y se establece un sistema de gestión del proyecto, como medio para la comunicación y coordinación del equipo y como base para satisfacer las expectativas de las diferentes unidades y personas. Además, se preocupa por la gestión adecuada del cambio que la nueva situación puede provocar en la organización.

Diagnóstico de la situación actual

Se basa en una evaluación de las políticas y principios de gestión de riesgos corporativos en toda la organización. Implica, generalmente, que se determine si existe una filosofía de gestión de riesgos desarrollada en la entidad así como una comprensión homogénea del riesgo asumido por ella.

El equipo líder identifica las políticas, procesos, prácticas y técnicas formales e informales actualmente presentes así como las capacidades existentes en la organización que permitan aplicar los principios y conceptos del nuevo marco.

Visión de la gestión de riesgos corporativos

El equipo líder desarrolla un enfoque que establece el modo en que se va a aplicar e integrar la gestión de riesgos dentro de la organización para alcanzar los objetivos; incluyendo la forma en que la entidad enfoca sus esfuerzos para situar en línea el riesgo aceptado y la estrategia de riesgos, mejorar las decisiones de respuesta, identificar y gestionar riesgos en toda la empresa, aprovechar las oportunidades y mejorar la utilización del capital.

Desarrollo de capacidades

La evaluación de la situación actual y el enfoque de gestión de riesgos proporcionan la comprensión necesaria de las capacidades personales, tecnológicas y de procesos ya existentes y en funcionamiento, así como de las nuevas capacidades que habrá que desarrollar. Esto implica definir papeles y responsabilidades y adaptar el modelo de organización y sus políticas, procesos, metodologías, herramientas, técnicas, flujos de información y tecnologías.

Plan de implantación

Se actualiza y optimiza el plan inicial añadiéndole amplitud con el fin de determinar la evaluación, diseño y puesta en marcha posterior. Se definen responsabilidades adicionales y el sistema de gestión del proyecto se modifica según sea necesario. El plan abarca, habitualmente, disciplinas generales de gestión de proyectos que forman parte de cualquier proceso de implantación.

Desarrollo de la gestión del cambio

Se desarrollan diferentes acciones para implantar y respaldar el enfoque y las capacidades de gestión de riesgos corporativos incluyendo planes de puesta en marcha, sesiones de formación, formas de motivación y el seguimiento del resto del proceso de implantación.

Seguimiento

La dirección de la organización es la encargada de revisar y reforzar las capacidades de gestión de riesgos como parte de su proceso continuo de gestión.



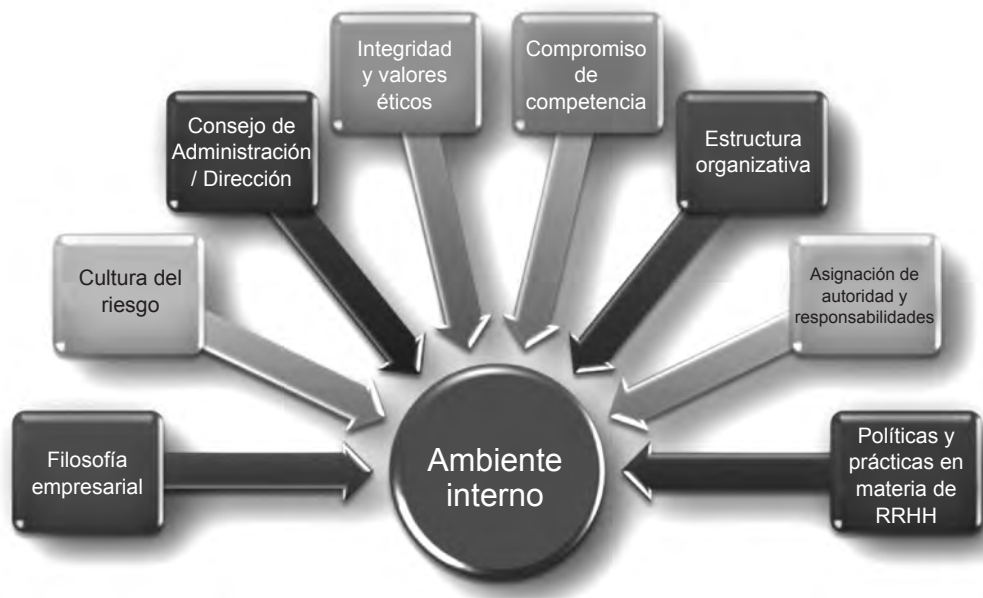
Componentes de la Gestión de Riesgos Corporativos

La gestión de riesgos corporativos está compuesta por ocho elementos relacionados entre sí que se derivan de la manera en la que la dirección conduce la empresa y de cómo se integran dichos elementos en el proceso.

Ambiente interno

El ambiente interno se refiere al talante de una organización que influye en la conciencia de sus empleados sobre el riesgo. Incorpora la filosofía de gestión de riesgos, la supervisión ejercida por el consejo de administración, la integridad, valores éticos y competencia de su personal y la forma en que la dirección asigna la autoridad y la responsabilidad y cómo organiza y desarrolla a sus empleados.

Su importancia reside en que tiene un impacto significativo en el modo en el que se implanta la gestión de riesgos corporativos y en su funcionamiento.



Fuente: elaboración propia.

Establecimiento de objetivos

La gestión de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos que apoyen la misión de la entidad y estén en línea con el negocio. Además, éstos han de ser consecuentes con los niveles de tolerancia establecidos que orientan, a su vez, el riesgo aceptado. Es importante que los objetivos existan antes de que la dirección pueda identificar potenciales eventos que afecten a su consecución.

Las metas que la empresa persigue se fijan a escala estratégica estableciendo una base para los objetivos operativos, de información y de cumplimiento en función del riesgo que se está dispuesto a aceptar. Algunas organizaciones expresan el riesgo aceptado en términos de un mapa de riesgo¹⁴.

Por otra parte, la tolerancia al riesgo es el nivel aceptable de desviación relativa a la consecución de objetivos. Operar dentro de los límites de tolerancia proporciona a la

¹⁴ **Mapa de riesgos:** representación gráfica a través de símbolos de uso general o adoptados, indicando el nivel de exposición (bajo, mediano o alto), de acuerdo a la información recopilada en archivos y los resultados de las mediciones de los factores de riesgos presentes, con el cual se facilita el control y seguimiento de los mismos, mediante la implantación de programas de prevención.

dirección una mayor confianza en que la organización permanece dentro de su riesgo aceptado que, a su vez, aporta más seguridad en la consecución de los objetivos.

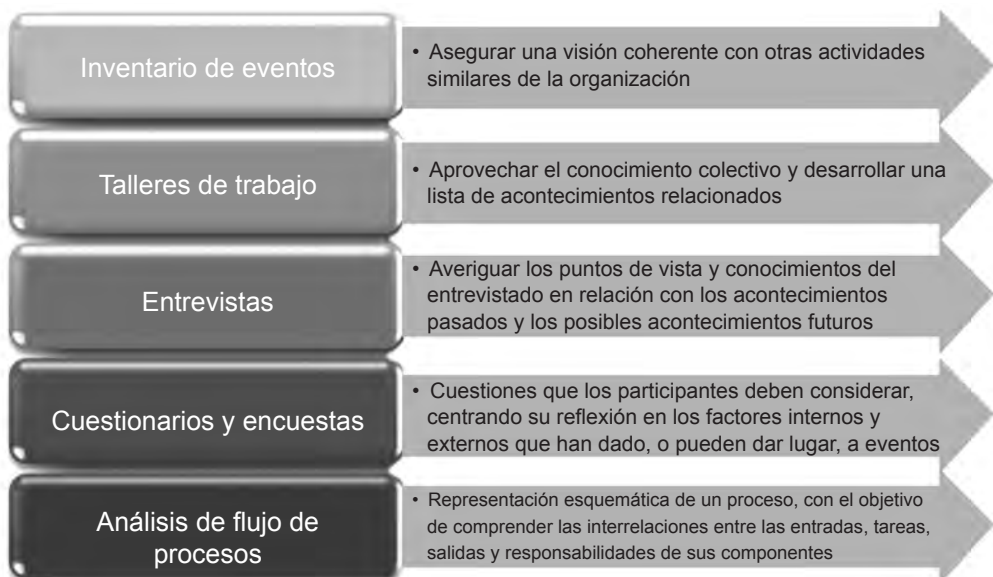
Identificación de eventos

La dirección identifica los eventos potenciales que, de ocurrir, afectarán a la entidad y determina si representan oportunidades o si pueden afectar de forma negativa a la capacidad de la empresa para implantar la estrategia y lograr los objetivos con éxito. Los eventos con impacto negativo representan riesgos que exigen la evaluación y respuesta de la dirección.

Técnicas de identificación de eventos

La dirección utiliza diversas técnicas para identificar acontecimientos que afecten al logro de los objetivos y que permitan diferenciar los posibles riesgos de las oportunidades. Pueden emplearse en línea con la planificación estratégica o al considerar nuevas iniciativas como, por ejemplo, un cambio en la organización.

A continuación, se presentan algunos ejemplos de técnicas comunes de identificación de eventos y su aplicación.



Fuente: Elaboración propia a partir de "COSO Enterprise Risk Management- Integrated Framework. 2004".

Evaluación de riesgos

La evaluación de riesgos permite considerar la amplitud con la que los eventos potenciales impactan en la consecución de los objetivos empresariales. La dirección evalúa estos acontecimientos desde una doble perspectiva: probabilidad e impacto y, normalmente, usa una combinación de métodos cualitativos y cuantitativos.

Los impactos positivos y negativos de los eventos potenciales deben examinarse individualmente o por categoría en toda la entidad. Los riesgos se evalúan con un doble enfoque: riesgo inherente¹⁵ y riesgo residual¹⁶.

Metodologías y técnicas cualitativas y cuantitativas

La metodología de evaluación de riesgos de una entidad consiste en una combinación de técnicas cualitativas y cuantitativas.

La dirección aplica a menudo **técnicas cualitativas** cuando los riesgos no se prestan a la cuantificación o cuando no están disponibles datos suficientes y creíbles para una evaluación cuantitativa o la obtención y análisis de ellos no resulte eficaz.

Las **técnicas cuantitativas** aportan más precisión y se usan en actividades más complejas y sofisticadas para complementar las técnicas cualitativas.

No se explican en detalle cada una de las técnicas de evaluación de riesgos, sin embargo, conviene conocer los métodos de evaluación que existen. Para ello, en el siguiente esquema, se observan los distintos métodos de evaluación de riesgos que se aplican en función de la naturaleza de las técnicas empleadas.

¹⁵ **Riesgo inherente:** aquél al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

¹⁶ **Riesgo residual:** refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente.



Fuente: Elaboración propia a partir de “Gestión de Riesgos Corporativos. Técnicas de Aplicación COSO 2004”.

Riesgo y asignación del capital

Algunas organizaciones, en particular las instituciones financieras, entienden el capital económico como la cantidad de capital requerido para protegerse contra riesgos financieros. Otras, como una medida del capital necesario para hacer funcionar el negocio de la manera planificada. La dirección lo puede utilizar para establecer estrategias, asignar recursos y medir el rendimiento.

Presentación y evaluación de riesgos

Las organizaciones utilizan diversos métodos para presentar la evaluación de riesgos. La presentación de manera clara y concisa resulta especialmente importante en el caso de la evaluación cualitativa dado que, en este caso, los riesgos no se resumen en una cifra o intervalo numérico como sucede en las técnicas cuantitativas. Algunas técnicas incluyen mapas de riesgo y representaciones numéricas.

- **Mapas de riesgo:** es la representación gráfica de la probabilidad de impacto de uno o más riesgos. Los riesgos se representan de manera que los más significativos resalten diferenciándose de los menos significativos.
- **Representaciones numéricas:** dependiendo del contexto del negocio, las mediciones cuantitativas de riesgo pueden presentarse en términos monetarios o porcentuales y con un intervalo de confianza especificado.

Perspectiva al nivel de organización

Como parte de la evaluación de riesgos la dirección puede apoyarse en aquellas realizadas en una unidad de negocio o bien llevar a cabo una evaluación independiente, empleando las técnicas descritas anteriormente, para formar un perfil de riesgo al nivel de toda la organización.

Respuesta al riesgo

Una vez evaluados los riesgos relevantes la dirección determina cómo responder a ellos. Las respuestas típicas son evitar, reducir, compartir o aceptar el riesgo.

Al considerar la respuesta, la dirección evalúa su efecto sobre la probabilidad e impacto del riesgo -así como los costes y beneficios- y selecciona aquella que sitúe el riesgo residual dentro de la tolerancia establecida. La dirección identifica cualquier oportunidad que pueda existir y asume una perspectiva del riesgo global para la entidad o bien una perspectiva de la cartera de riesgos; determinando si el riesgo residual global concuerda con el riesgo aceptado por la entidad.

Finalizadas las acciones de respuesta, la dirección posee una visión completa de los riesgos y de las respuestas individuales así como de su alineación con las tolerancias asociadas.

Costes y Beneficio

Las respuestas al riesgo, en su mayoría, implican algún tipo de coste directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el coste inicial del diseño e implantación de la respuesta -procesos, personal y tecnología- y el coste de mantener la respuesta de manera continua.

Los costes y beneficios asociados pueden medirse cuantitativa o cualitativamente a través de una unidad de medida que sea coherente con la empleada para establecer el objetivo y las tolerancias al riesgo relacionadas.

Actividades de control

Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las respuestas de la dirección a los riesgos. Tienen lugar a través de la organización; a todos los niveles y en todas las funciones.

Incluyen una gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones.

Integración con la respuesta al riesgo

Una vez que la dirección de la entidad selecciona las respuestas adecuadas a los riesgos comienza una segunda fase. En dicha fase se identifican las actividades de control necesarias para asegurar que las respuestas a los riesgos se lleven a cabo correctamente.

Actividades de control como respuesta al riesgo

Las actividades de control se establecen, generalmente, para asegurar que se llevan a cabo de manera apropiada las respuestas a los riesgos. Sin embargo, para ciertos objetivos las propias actividades de control constituyen la respuesta al riesgo. Esto último sucede con frecuencia en riesgos que se refieren a objetivos de control de gestión.

Información y comunicación



La información se identifica, capta y comunica de una forma y en un marco de tiempo que permite a las personas llevar a cabo sus responsabilidades.

Los sistemas de información usan datos generados internamente y otras entradas de fuentes externas, y sus salidas informativas facilitan la gestión de riesgos y la toma de decisiones relativas a los objetivos.

Dentro de la organización también existe una comunicación eficaz que fluye en todas direcciones. La alta dirección insta al personal a que comprendan su función en la gestión de los riesgos corporativos y relacionen su trabajo particular con las acciones de control de los riesgos.

Asimismo, deben tener los medios adecuados para comunicar hacia arriba la información significativa. Y, de la misma forma, debe haber una comunicación eficaz con terceros tales como los clientes, proveedores, reguladores y accionistas.

Supervisión

La supervisión de la gestión de riesgos corporativos se basa en la revisión del funcionamiento de sus componentes a lo largo del tiempo mediante actividades permanentes, evaluaciones independientes o una combinación de ambas técnicas.

Durante el transcurso normal de las actividades de gestión tiene lugar una supervisión continua. El alcance y frecuencia de



las evaluaciones independientes dependerá, fundamentalmente, de la evaluación de riesgos y de la eficacia de los procedimientos de supervisión permanente.

Las deficiencias en la gestión de riesgos corporativos se comunican de forma ascendente trasladando los temas más importantes a la alta dirección y al consejo de administración.

Roles y Responsabilidades en la Gestión de los Riesgos

Todo el personal de una entidad tiene alguna responsabilidad en la gestión de riesgos corporativos.

El consejero delegado es responsable en último lugar y debería asumir su “titularidad”. Otros directivos apoyan la filosofía de gestión de riesgos, promocionan el cumplimiento del riesgo aceptado y la gestión del mismo dentro de sus áreas de responsabilidad, en coherencia con la tolerancia establecida. Otras personas son los encargados de desarrollar la gestión de riesgos corporativos según las directivas y protocolos establecidos. Finalmente, el consejo de administración proporciona un importante papel de supervisión.

Además, conviene destacar la relevancia de algunos terceros que facilitan a menudo información útil para llevarla a cabo aunque no sean responsables de su eficacia.

Consejo de Administración

El consejo de administración juega un papel fundamental en la supervisión de la gestión de riesgos corporativos. Deberá estar informado oportunamente de los riesgos más significativos, la evaluación de la dirección, su respuesta planificada y, lo que es más importante, ha de tener la seguridad de que están en marcha los procesos adecuados y que la dirección está dispuesta a identificar, evaluar y responder al riesgo así como a trasladar la información relevante al consejo.

Pueden delegar las responsabilidades y obligaciones de rendir cuentas sobre aspectos específicos de la gestión de riesgos corporativos a uno a varios comités del consejo para asegurar que se presta atención a las diferentes áreas de riesgo.

Comité de Auditoría

Cada vez es más habitual que la responsabilidad de llevar a cabo la supervisión de la gestión de riesgos corporativos se asigna a un comité de auditoría. Esto se debe a que, aunque la atención del comité de auditoría está centrada en la gestión financiera y en el control interno, dicho comité tiene absoluta capacidad para extender a este tema su ámbito de responsabilidad.

Además, algunos expertos en la materia apuntan determinadas normas que promueven la asignación de dicha responsabilidad a este comité.

Comité de Riesgos

En otros casos, la responsabilidad de supervisar la gestión de riesgos recae en el consejo de administración y lo habitual es que se designen grupos de trabajo diferentes al comité de auditoría. Son muchas las entidades que consideran que asignar a un Comité de Riesgos las tareas de supervisión de riesgos en áreas no financieras excede de la autoridad que se le pretende otorgar y de sus recursos disponibles.

Las responsabilidades del Comité de Riesgos incluyen:

- Supervisar el desarrollo y la participación en un análisis anual de estrategias de riesgos al nivel de empresa.
- Desarrollar y perfeccionar el riesgo aceptado y la tolerancia al riesgo al nivel de empresa.
- Proporcionar guías y supervisión al director del área de riesgos y a los líderes globales de riesgo.
- Evaluar índices de riesgo materiales e informar al consejo.
- Evaluar el informe de índices de riesgo al nivel de empresa.
- Evaluar el informe de tendencias de riesgo de la empresa y garantizar que la estrategia corporativa responde a las cuestiones planteadas.
- Supervisar los papeles y responsabilidades de la auditoría interna.
- Revisar las cuentas consolidadas semestrales y anuales.

Consejero Delegado

Dentro de las responsabilidades del consejero delegado es importante destacar que se encarga de asegurar que todos los componentes de la gestión de riesgos corporativos funcionen correctamente.

El consejero delegado posee la responsabilidad última en la gestión de riesgos corporativos y cumple, normalmente, con esta responsabilidad proporcionando liderazgo y orientación a la alta dirección y estableciendo políticas amplias que reflejen la filosofía de gestión de riesgos de la entidad y su riesgo aceptado.

Además de esta figura, en algunas entidades varios consejeros delegados han decidido identificar a un alto directivo que proporcione pautas a la organización en lo referente a la implantación de la gestión de riesgos corporativos. Otros prefieren establecer un comité para que proporcione estas pautas.

Un nuevo enfoque utilizado por un número creciente de empresas consiste en establecer un director de riesgos que proporcione liderazgo, pautas, apoyo y seguimiento a los directores de línea en la gestión de riesgos corporativos.

Comité Ejecutivo de Gestión de Riesgos Corporativos

En grandes empresas el consejero delegado suele establecer un comité de altos directivos para la gestión de riesgos corporativos. Consiste en un grupo que pertenece a la alta dirección incluyendo directores funcionales como el director financiero, el director de auditoría, el director de comunicaciones y otros.

Las funciones y responsabilidades de este comité incluyen aspectos tales como:

- Responsabilidad global del proceso de gestión de riesgos corporativos; incluyendo los procesos utilizados para identificar, evaluar, responder e informar sobre el riesgo.
- Definición de papeles, responsabilidades y obligaciones de rendir cuenta ante la alta dirección.
- Dotación de políticas, marcos, metodologías y herramientas a las unidades de negocio, para la identificación, evaluación y gestión de riesgos.
- Revisión del perfil de riesgo de la empresa.
- Revisión de las mediciones de rendimiento frente a las tolerancias y la recomendación de acciones correctoras cuando sea necesario.
- Comunicación del proceso de gestión de riesgos al consejero delegado y al consejo.

Responsable de Riesgos

Otra opción consiste en establecer una coordinación centralizada para facilitar la gestión de riesgos corporativos. Esta se realiza a través de un responsable de riesgo, denominado director o gerente de riesgos, que trabaja junto a otros directivos para establecer una gestión eficaz de riesgos corporativos en sus respectivas áreas de responsabilidad.

Dirección

Los responsables de las unidades de negocio, procesos y departamentos funcionales de las distintas líneas son quienes deben identificar, evaluar y responder al riesgo en relación con el logro de sus objetivos. Además, deben asegurar que los procesos empleados cumplan las políticas de gestión de riesgos de la entidad y que sus actividades se encuentren dentro de los niveles de tolerancia al riesgo.

Estos responsables delegan, de manera natural, las actividades específicas de gestión de riesgos corporativos a los gerentes de sus unidades, que tratarán asuntos tales como:

- El cumplimiento de las políticas de gestión de riesgos y el desarrollo de técnicas adaptadas a las actividades de la unidad.
- La aplicación de técnicas y metodologías de gestión de riesgos para garantizar la adecuada identificación, evaluación, respuesta, comunicación y seguimiento de los riesgos.
- La obligación de gestionar los riesgos diariamente.
- La aportación al responsable de una unidad de informes completos y exactos sobre la naturaleza y alcance de los riesgos en las actividades del negocio.

Audidores internos

Los auditores internos juegan un papel fundamental en la gestión de riesgos corporativos; proporcionando un seguimiento objetivo de su aplicación y eficacia. Pueden llevar a cabo revisiones para aportar una evaluación objetiva del proceso completo de gestión de riesgos corporativos o de partes de él.

Dentro de sus funciones destaca el apoyo que prestan a la dirección proporcionando garantías sobre:

- Los procesos de gestión de riesgos corporativos.
- La eficacia y eficiencia de las respuestas al riesgo y actividades de control relacionadas.
- La integridad y exactitud de la información generada sobre la gestión de riesgos.

Los auditores internos adoptan, en ocasiones, un papel de consultoría en el que sugieren mejoras en el proceso de gestión de riesgos de la organización. En el desarrollo de esta función los auditores internos pueden, entre otras actividades, promover el desarrollo de un conocimiento común, formar a la dirección, moderar grupos de trabajo y proporcionar herramientas y técnicas para ayudara los directivos a analizar los riesgos y diseñar actividades de control.

5.3. RELEVANCIA DE LA REINGENIERÍA DE PROCESOS (BPR)

La Reingeniería de Procesos, o BPR (*Business Process Reengineering*), se considera una herramienta más de gestión de riesgos, sin embargo, se trata en un apartado independiente para destacar su relevancia en el panorama actual. Su importancia reside en que es una de las herramientas de gestión de procesos más reciente y eficaz.

La BPR aparece a finales de la década de los ochenta de la mano de *Michael Hammer* y *James Champy*. Surge como reacción a las realidades empresariales y pretende aportar otro tipo de soluciones ante aspectos como los nuevos retos que imponen los clientes, las barreras a la competencia y, sobre todo, los riesgos que implican estos cambios que están aconteciendo en el panorama económico y financiero.

Definición

Hammer y Champy establecen que la reingeniería de procesos es *“la revisión fundamental y el rediseño radical de procesos para alcanzar mejoras espectaculares en medidas críticas y contemporáneas de rendimiento, tales como costos, calidad, servicio y rapidez”*.

Esta definición de la Reingeniería de Procesos supone cuestionar las bases sobre las que se asienta la realidad empresarial, revisando todas las normas preestablecidas que hasta el momento eran incuestionables. La reingeniería determina qué es lo que debe hacer la empresa y cómo debe hacerlo. No se trata de hacer cambios superficiales; estamos ante un proceso de reinención completa del negocio. Por ello, las mejoras que implica deben ser espectaculares y no marginales o incrementales.

Principios

Para entender en qué consiste esta herramienta de gestión de riesgos conviene conocer los principios en los que se basa. Así, *The Boston Consulting Group*¹⁷ estima los siguientes principios clave en los que se basa la BPR:

- Es necesario el compromiso de la gerencia para liderar el programa y la estrategia empresarial debe guiar y conducir los programas de la BPR.
- El objetivo último es crear valor para el cliente y, para ello, hay que concentrarse en los procesos que necesitan cambios.
- Son necesarios equipos de trabajo, responsables y capacitados, a los que hay que incentivar y recompensar con puestos de responsabilidad en la nueva organización que se obtendrá tras el proceso de reingeniería.

¹⁷ **The Boston Consulting Group:** empresa global líder en consultoría estratégica para la Alta Dirección.

- La observación de las necesidades de los clientes y su nivel de satisfacción es fundamental para identificar si se están cumpliendo los objetivos y, para ello, es necesaria la flexibilidad a la hora de llevar a cabo el plan.
- Se requiere el establecimiento de correctos sistemas de medición del grado de cumplimiento de los objetivos.
- Se debe tener en cuenta el factor humano a la hora de evitar o reducir la resistencia al cambio.
- La BPR no tiene que ser vista como un proceso único que se realice una sola vez dentro de la organización; debe contemplarse como un proceso en el que se plantean continuamente nuevos retos.
- La comunicación es esencial a todos los niveles de la organización y traspasando sus fronteras (prensa, comunidad, sistema político, etc.).

Características de la BPR

Todo proceso de reingeniería debe reunir una serie de requisitos para alcanzar reducciones de costes y mejoras en la calidad. A partir de estos requisitos y del servicio prestado al cliente, se determinan unas características comunes a cualquier proceso de este tipo. Éstas son:

- *Unificación de tareas*

La unificación de las tareas en un mismo equipo proporciona una serie de ventajas que permiten una reducción de los plazos. Cuando se concentran en un equipo un conjunto de responsabilidades cabe pensar que se van a eliminar, o reducir en gran parte, las supervisiones; la información va a ser manejada por todos los miembros. Además, la calidad en la realización de las tareas y en la consecución de los objetivos será superior ya que se van a evitar errores.

No se debe olvidar que el enfoque hacia los procesos de la BPR implica una pérdida de entidad de las tareas, es decir, los procesos ganan peso específico en detrimento de las tareas individuales.

- *Participación de los trabajadores en las decisiones*

Son los propios trabajadores los que toman las decisiones y asumen las responsabilidades relacionadas con su trabajo. Para que esto se pueda llevar a cabo son necesarios el esfuerzo, el apoyo, la disciplina, la confianza, la flexibilidad y la capacidad de adaptación. Los beneficios que se derivan de la participación de los trabajadores en las decisiones de la vida empresarial son la reducción de los plazos y de los costes. Éstos son posibles al comprimirse las estructuras tanto vertical como horizontalmente.

- *Diferentes versiones de un mismo producto*

Se realizan diferentes versiones de un mismo producto para conseguir una mayor adaptación a las necesidades y gustos del cliente. Esta idea concuerda con uno de los principios de la BPR; “ofrecer un producto de valor real para el cliente”.

La personalización del producto, a través del lanzamiento al mercado de varias versiones del mismo, contribuye a diferenciarse de los competidores y a cubrir las necesidades de los consumidores a los que va destinada cada una de las versiones de dicho producto.

- *Reducción de las comprobaciones y controles*

Se trata de establecer un plan de evaluación y control que contemple solamente los controles que tienen sentido económico. Con esto se pretende que se agilice y flexibilice la estructura organizativa.

- *Operaciones híbridas*

Las operaciones en todo proceso de reingeniería gozan de una naturaleza dual y se pretende disfrutar de las ventajas que presenta cada una de las opciones. Las distintas unidades pueden trabajar con un elevado grado de autonomía sin perder las ventajas que aporta la coordinación entre las mismas.

- *Instrumentos y técnicas de BPR*

Para llevar a cabo una correcta BPR son necesarios una serie de instrumentos y técnicas entre las cuales destacan las siguientes:

- *Visualización de procesos*

Se trata de realizar un diseño de todos y cada uno de los componentes del proceso objetivo. Se prevén las tareas de cada proceso, los costes y los plazos de cada fase.

- *Investigación operativa*

Es una metodología que proporciona las bases empíricas para la toma de decisiones y ayuda a mejorar la entrega de servicios. Utiliza técnicas sistemáticas de investigación en cinco pasos básicos: identificación del problema, selección de la estrategia de solución, prueba de la estrategia y evaluación, difusión de los resultados y, finalmente, la utilización de los mismos.

- *Gestión del cambio*

Para llevar a cabo un programa de Reingeniería de Procesos es muy importante tener en cuenta el factor humano y la gestión del cambio organizativo. La BPR, normalmente, es un proceso que compete a todos los empleados de la compañía y, por lo tanto,

la gestión del cambio se convierte en una herramienta casi imprescindible para evitar que el proceso fracase por la resistencia que el factor humano presenta.

- *Benchmarking*

Esta técnica se basa en el análisis de los puntos fuertes y débiles de los productos líderes en el mercado, con el fin de obtener la mayor información posible de los procesos operativos en las organizaciones responsables de dichos productos. No obstante, también se aplica a la BPR para estudiar las distintas soluciones adoptadas por la competencia.

- *Infotecnología*

Según Hammer la infotecnología es la herramienta básica de la Reingeniería de Procesos. La mayor parte de las acciones de reingeniería se han fundamentado en la tecnología dejando en un segundo plano al resto de los mecanismos mencionados.

6. CONCLUSIONES

Entender el riesgo, y las consecuencias que pueden derivar de una mala gestión del mismo, resulta fundamental para comprender el contexto en el que operan las entidades financieras, en general, y las aseguradoras en particular. Esto se debe a que la desregularización y la globalización de estos servicios se han producido conforme han avanzado las tecnologías y, por lo tanto, las entidades han visto cómo sus perfiles de riesgo se han visto modificados.

Por otra parte, la alta competitividad ha impulsado la introducción de las entidades en nuevos mercados y productos lo que provoca una mayor complejidad en las operaciones de las entidades y un análisis más profundo de todos los riesgos.

La consecuencia más inmediata ha sido un profundo cambio en la concepción del riesgo y, por tanto, la forma de entender la administración de los riesgos también ha experimentado una importante evolución. Para entender lo sucedido se destacan los siguientes aspectos claves:

- La gestión de los riesgos está ligada a la **creación de valor** para la empresa.
- Hay que entender a qué riesgos está expuesta la entidad para poder comprender cuáles son las **oportunidades** que se pueden aprovechar.
- La empresa crece a través de un **adecuado tratamiento de los riesgos** y, por lo tanto, las empresas tienen que conocer sus propias necesidades y riesgos. Esto resulta clave para aprovechar las oportunidades de negocio que surjan y, lo que es más importante, para poner en marcha mecanismos encaminados a solucionar aquellas debilidades que se detecten.

- La **responsabilidad** en la gestión de los riesgos es de todos y cada uno de los niveles de la entidad y de los individuos que en ella trabajan.

La Gestión de Riesgos (*Enterprise Risk Management -ERM-*) genera un método de gestión y administración organizado en fases sucesivas que proporcionan a la empresa las herramientas necesarias para afrontar, mitigar y controlar los riesgos de manera que se consiga, además del adecuado tratamiento de los mismos, la creación de valor como objetivo último de cualquier entidad.

Sin embargo, aunque una correcta aplicación del método genera numerosas ventajas, también tiene algunas limitaciones que, de presentarse, dificultan el proceso de gestión de riesgos o expresan resultados erróneos o ineficaces pudiendo ocasionar graves problemas para la empresa. Así, el ERM puede asegurar la gestión eficaz de presentación de informes y el cumplimiento de leyes y reglamentos, evitar daños a la reputación de la entidad y sus consecuencias pero para una implantación eficaz se tienen que tener presentes las limitaciones de este proceso.

El ERM indica que para la consecución de una serie de objetivos de diversa índole, previamente establecidos, es necesario que la entidad reúna una serie de características para asegurar su eficacia. Por lo tanto, habrá que adecuar el proceso de gestión de riesgo conforme las necesidades y circunstancias de cada entidad e informar de dicho proceso a todos los niveles de la entidad.

La gestión de riesgos corporativos se basa la interacción de ocho elementos que se derivan de la manera en que la dirección conduce la empresa y de su integración en el proceso de gestión. Estos son:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos
- Evaluación de riesgos
- Respuesta al riesgo
- Actividades de control
- Información y comunicación
- Supervisión

La eficacia del proceso de gestión de riesgos va a depender de las relaciones entre estos componentes y de la importancia que la empresa de cada uno de ellos. Resulta clave para la gestión de riesgos que estos aspectos estén integrados entre si y en cada uno de los niveles de la entidad.

Por otra parte, no se puede olvidar la importancia de la Reingeniería de Procesos (BPR). El hecho de que en la BPR opere de manera muy activa el componente tecnológico no significa que sea un modo de automatizar la empresa; la reingeniería no es igual que la *automatización*, ya que no se trata de mejorar lo deficiente se trata de reinventarlo de forma que comience a ser eficiente desde su concepción.

Tampoco se debe confundir con lo que se denomina *Reingeniería de Software* que no es más que la reconstrucción de sistemas obsoletos de información con tecnología más moderna. No se trata de reestructurar sino de reinventar.

Otro error usual es confundir reingeniería con *reorganización*; la BPR no se centra en la estructura organizacional sino en la estructura de sus procesos. No vale para nada imponer una nueva organización jerárquica con menos niveles y más eficiente si los procesos viejos se mantienen permaneciendo con ellos la ineficiencia en el ciclo productivo.

Los altos cargos de las empresas son los responsables de que el proceso funcione adecuadamente. Así, las empresas pueden protegerse, en la medida de lo posible, de los riesgos y ser conocedoras, convenientemente, de la situación propia a la que están expuestos.

El gobierno corporativo y la auditoría interna, tal y como se analiza en el tratamiento del riesgo operacional, están intrínsecamente relacionados en este proceso de ERM con la adecuada eficacia del mismo.

II

EL RIESGO OPERACIONAL. TRATAMIENTO EN SOLVENCIA II

1. INTRODUCCIÓN

El desarrollo y consolidación de instituciones financieras cada vez más grandes y sofisticadas ha sido impulsado, principalmente, por la desregulación financiera y la globalización. Además, estas instituciones realizan actividades en múltiples mercados y han desarrollado perfiles de riesgo cada vez más complejos.

En respuesta a estos cambios, la administración y gestión de los riesgos está experimentando una constante evolución para adecuarse a las necesidades de las entidades y lograr la consecución de sus objetivos.

La gestión del riesgo es una práctica que garantiza conocer las oportunidades para beneficio de la organización y las amenazas que pueden poner en peligro la no consecución de sus objetivos. Tanto la propia gestión del riesgo como la prevención tienen que formar parte de la cultura y estar impregnadas en la filosofía y en los procesos organizacionales.

Actualmente, la gestión del riesgo se ha configurado como una nueva ciencia social (*Enterprise Risk Management, ERM*) que utiliza métodos científicos para asumir riesgos con conocimiento, disminuyendo las posibilidades de fracaso al tomar decisiones basadas en datos objetivos.

Dentro de los diferentes tipos de riesgos a los que la entidad está expuesta el tratamiento y control del riesgo operacional representa hoy uno de los grandes desafíos.

El concepto de **riesgo operacional** se convierte en un aspecto clave en la comunidad financiera internacional debido al colapso de ciertas instituciones financieras y no financieras provocado, en parte, por problemas de tipo operacional.

La gestión del riesgo operacional tiene como objetivo principal asegurar la actividad de la institución mediante la generación de medidas preventivas a partir de la evaluación del riesgo detectado.

Esta segunda parte se centra en describir las prácticas adecuadas para la gestión y supervisión del riesgo operacional, las cuales desarrollan un conjunto de principios que proveen un marco efectivo para ello.

En primer lugar, resulta conveniente analizar qué se entiende por riesgo operacional y contextualizarlo en el marco de Solvencia II. Para ello, es preciso no sólo definir este concepto si no también observar la evolución que ha experimentado el mismo hasta obtener un tratamiento especial dentro de la gestión de riesgos.

Sin embargo, situar el riesgo operacional en el marco de Solvencia II es una tarea compleja que requiere del estudio en profundidad de numerosos aspectos que rodean al tratamiento de este riesgo en las entidades aseguradoras. Estos aspectos fundamentales son los siguientes:

Estos son:

- **Gestión del riesgo operacional:** en la primera parte se analizó el *ERM (Enterprise Risk Management)* como sistema de gestión de riesgos; ahora se trata de estudiar aquella parte del *ERM* que se encarga de la gestión del riesgo operacional al que se denomina *ORM (Operational Risk Management)*.
- **Administración del riesgo operacional:** se explica en qué consiste el sistema de administración del riesgo operacional y cuáles son las fases de su implantación en la entidad.
- **Cuantificación del riesgo operacional:** se abarca el importante tema del requerimiento de capital por riesgo operacional, analizando tanto el modelo estándar como los modelos internos y los diferentes métodos de cálculo.
- **Evaluación del Riesgo Propio y de Solvencia (ORSA):** esta evaluación es de vital importancia en el tratamiento de los riesgos en general y, particularmente, del riesgo operacional.

Finalmente, no se puede concluir este trabajo dedicado al riesgo operacional en Solvencia II sin mencionar la responsabilidad de la junta directiva en el establecimiento del marco operacional y el papel de la alta gerencia; así como la responsabilidad de la auditoría interna y del gobierno corporativo en el tratamiento y la gestión del riesgo operacional.

2. EL RIESGO OPERACIONAL

El panorama actual y los acontecimientos que han ocurrido en los últimos años han hecho que el concepto de riesgo operacional se convierta en un aspecto clave en la comunidad económico-financiera internacional y decisivo en el entendimiento y tratamiento de los riesgos en el panorama empresarial.

La relevancia que ha adquirido ha intensificado los esfuerzos por agrupar los eventos operacionales bajo una categoría especial de riesgo. Esto ha convencido a las instituciones financieras de la necesidad de poner más atención en el riesgo operacional y dedicar mayores recursos humanos y financieros a su adecuada gestión.

Por ello, entender qué significa el riesgo operacional es importante para comprender los cambios que están acaeciendo en el panorama actual, fundamentalmente en materia normativa.

2.1. CONCEPTOS BÁSICOS

Definición de riesgo operacional

El término “**riesgo operacional**” existe como concepto genérico, al menos, desde 1992 con la publicación del documento “*Internal Control Integrated Framework*”¹⁸ publicado por el COSO (*Committee of Sponsoring Organizations of the Treadway Commission*). Sin embargo, es intrínseco a todas las actividades de negocios y, por lo tanto, ha existido siempre.

Una definición preliminar de riesgo operacional aparece en el segundo documento consultivo (BCBS¹⁹, 2001a), en el texto complementario denominado “*Operational Risk*” (BCBS, 2001b). El proceso de discusión del documento condujo a la inclusión de nuevos aspectos y a la modificación tanto de la definición del riesgo operacional como de los métodos de cuantificación. Estas conclusiones se plasmaron en el documento “*Working Paper on the Regulatory Treatment of Operational Risk*”²⁰ (BCBS, 2001c).

El documento anterior constituyó la base para todas las publicaciones posteriores del Comité de Basilea sobre riesgo operacional así como la difusión de la primera definición consensuada:

“Riesgo operacional es el riesgo de sufrir pérdidas debido a la inadecuación o a fallos en los procesos, personal y sistemas internos o bien por causa de eventos externos”. Lo que incluye el riesgo legal²¹ pero excluye el riesgo reputacional²².

Uno de los mayores avances que se consiguió al consensuar una definición para el riesgo operacional es que, a partir de ella, se establezca una clasificación y determinación de las principales fuentes y eventos de pérdida.

En la siguiente imagen se observa un listado de las principales fuentes y la categorización de eventos que pueden dar lugar a la pérdida financiera por riesgo operacional.

¹⁸ **Internal Control Integrated Framework:** marco conceptual de control interno que provee una visión común e integradora que satisface las demandas de todos los interesados. Publicado en 2001 por el COSO (*Committee of Sponsoring Organizations of the Treadway Commission*).

¹⁹ **BCBS (Basel Committee on Banking Supervision):** Comité de Supervisión Bancaria de Basilea, organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros.

²⁰ **Working Paper on the Regulatory Treatment of Operational Risk:** documento publicado en septiembre del año 2001 por el BCBS dónde se regulan los requerimientos de capital por riesgo operacional.

²¹ **Riesgo legal:** posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos privados entre las partes.

²² **Riesgo reputacional:** posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.



Fuente: elaboración propia.

Fuentes del riesgo operacional

Tal y como lo plantea el Comité de Basilea el riesgo operacional presenta las siguientes fuentes.



Fuente: elaboración propia.

Procesos internos

Los procesos internos hacen referencia a la *“posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos”*.

Podrán considerarse, entre otros, los riesgos asociados a los fallos en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la incorrecta compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones así como el incumplimiento de plazos y presupuestos planeados.

Personas

Son las posibles pérdidas financieras asociadas a *“negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, blanqueo de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal (...)”*, entre otros factores.

Se incluyen pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación.

Tecnología de la Información



La posibilidad de que se produzca una pérdida financiera surge como consecuencia del *“uso de inadecuados sistemas de información y tecnologías relacionadas que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atender contra la confidencialidad, integridad, disponibilidad y oportunidad de la información”*.

Las instituciones pueden considerar incluir en este área los riesgos derivados de fallos en la seguridad y continuidad operativa de los sistemas TIC's²³, errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información y fallos para alinear las TIC's con los objetivos de negocio, entre otros aspectos.

Eventos externos

El Comité de Basilea define como evento externo la *“posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el de-*

²³ TIC's: “Tecnologías de la Información y de la Comunicación”.

sarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información”.

Entre otros factores se podrán tomar en consideración los riesgos que implican las contingencias legales, los fallos en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como los fallos en servicios críticos provistos por terceros.

Otros riesgos asociados con eventos externos incluyen el rápido cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

Categorización de eventos de pérdida por Riesgo Operacional

Comité de Basilea, en coordinación con el sector financiero, ha identificado una serie de eventos que pueden desembocar en pérdidas sustanciales por riesgo operacional.

Fraude interno

Se refiere a “pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna a la empresa”.

Dentro de este evento no se consideran aquellos asociados con la discriminación en el trabajo. Aunque sí incluye eventos tales como: fraudes, robos con participación de personal de la empresa, sobornos, etc.

Fraude externo

Son las “pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero”.

Esta categoría incluye eventos como: robos, falsificación o ataques informáticos entre otros.

Relaciones laborales y seguridad en el puesto de trabajo

Las pérdidas que acontecen como consecuencia de este evento son aquellas “derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con discriminación en el trabajo”.

Clientes, productos y prácticas empresariales

Este tipo de eventos se corresponde con las “pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto”.

Daños a activos materiales

Los daños a activos materiales son aquellos que se producen cuando las entidades se enfrentan a “*pérdidas derivadas de daños o perjuicios a activos físicos como consecuencia de desastres naturales u otros eventos de fuentes externas*”.

Interrupción del negocio y fallos en los sistemas

Son las “*pérdidas derivadas de incidencias o interrupciones en el negocio y de fallos en los sistemas*”.

Ejecución, entrega y gestión de procesos

La ejecución, entrega y gestión de procesos se refiere a las “*pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores*”.

Esta categoría incluye eventos asociados con: captura de transacciones, ejecución y mantenimiento, monitoreo y reporte, entrada y documentación de clientes, gestión de cuentas, contrapartes de negocio, vendedores y proveedores.



Fuente: elaboración propia.

2.2. EVOLUCIÓN DEL CONCEPTO DE RIESGO OPERACIONAL

Realizar las acciones necesarias para el adecuado tratamiento del riesgo operacional no es una tarea fácil. Esto explica las complicaciones que han tenido lugar hasta lograr el consenso en su definición que ha marcado la perspectiva regulatoria.

El riesgo operacional se ha asociado siempre a fallos operativos y errores de control interno, es decir, era todo aquello que no era ni riesgo de mercado ni riesgo de crédito. Hasta la década de los noventa, se consideraba un área caracterizada por pequeños, predecibles y frecuentes sucesos tales como errores en el procesamiento de operaciones, rupturas al conciliar cuentas o fallos técnicos del sistema, además de alguna gran pérdida que acontecía ocasionalmente cada diez años.

Situaciones como la quiebra del Banco Barings²⁴ (1995), Daiwa²⁵ (1984-1995) y Enron²⁶ (2001), entre otros muchos -algunos de los cuales se tratan en un anexo especial- han alertado sobre la necesidad de controlar los sucesos que se relacionan con el fraude de empleados, fallos de control interno, eventos externos, trato a los clientes, etc.

Además, otros factores como la diversificación de actividades y complejidad de nuevos productos, nuevos canales de venta, la globalización, fusiones y adquisiciones a gran escala, automatización de procesos, externalización de actividades y, sobre todo, cambios regulatorios, han contribuido al auge de estas incertidumbres.

La preocupación por este riesgo motivó que la Asociación Bancaria Británica (*British Banker Association*) emprendiera en 1999 un proyecto que reunió también al ISDA²⁷ (*Internacional Swaps and Derivatives Association*), al RMA²⁸ (*Robert Morris Associated*) y PricewaterhouseCoopers, a través de la realización de una encuesta de ámbito mundial, y del que surgió la primera definición formal que considera al riesgo operacional como “*riesgo de pérdidas directas o indirectas resultantes de procesos inadecuados o fallidos, personal, sistemas o como resultado de acontecimientos externos*”.

²⁴ **Banco Barings:** Inglaterra, febrero de 1995. Este banco inglés quiebra como resultado de tremendas pérdidas en sus posiciones de futuro del índice de acciones japonesas. El ejecutivo Nick Leeson había comprado ocho mil millones de dólares en futuros, apostando al alza del índice Nikkei de la bolsa de Tokio. Pero el índice se desplomó, en parte por el terremoto de Kobe. En sólo un mes, Baring perdió 1.200 millones de dólares y terminó en la quiebra.

²⁵ **Daiwa Bank:** durante once años se falsificaron documentos para ocultar pérdidas de la oficina en NY por ventas de bonos, propiedad del banco y de clientes, sin contar con las autorizaciones expresas. La pérdida fue de 1.1 billones de dólares y \$340 millones de dólares de multa.

²⁶ **Enron:** el ocultamiento de deudas y registro de utilidades mayores a las reales, para generar un mayor flujo de efectivo, y la inadecuada aplicación de principios contables, alterando de manera intencional las cifras del negocio, condujeron a pérdidas superiores a los 500 millones de dólares.

²⁷ **ISDA (*International Swaps and Derivatives Association*):** “Asociación Internacional de Swaps y Derivados”. Es una organización profesional que agrupa a los mayores actores del mercado de derivados.

²⁸ **RMA (*Robert Morris Associated*):** Asociación cuyo objetivo es promover la capacidad para identificar, evaluar y gestionar los impactos del riesgo de crédito, riesgo operacional y riesgo de mercado en los negocios y clientes.

Después de muchas consideraciones, el segundo documento consultivo para el Nuevo Acuerdo de Capitales de Basilea aprobado en junio de 2004 establece una definición causal, “*riesgo de pérdida que deriva de procesos internos inadecuados o fallidos, gente o sistemas o de eventos externos*”, incluyendo el riesgo legal pero excluyendo los riesgos estratégico, sistemático y reputacional, así como el coste de oportunidad asociado con fallos operativos y las pérdidas indirectas, por su difícil cuantificación.

Por tanto, el riesgo operacional puede proceder de sucesos internos (relativos a errores de los procesos, sistemas y personas), o externos.

Establecer una definición común supone un gran avance hacia el consenso y la homogeneización de términos. Basilea II, en este sentido, aporta un punto de partida básico y un marco de referencia para el tratamiento del riesgo operacional.

Siguiendo las palabras de José Antonio Núñez y José Juan Chávez, en su artículo “*Riesgo operativo: esquema de gestión y modelado del riesgo*”, del riesgo operacional destacan las siguientes características:

- Es **antiguo** y está presente en cualquier clase de negocio.
- Es **inherente a toda actividad** en que intervengan personas, procesos y plataformas tecnológicas.
- Es **complejo**, como consecuencia de la gran diversidad de causas que lo originan.
- Las grandes pérdidas que ha ocasionado en varias empresas, ha mostrado el desconocimiento que de él se tiene y la **falta de herramientas** para gestionarlo. Aunque esta situación está cambiando gracias a los grandes avances normativos que acontecen en los últimos años.

Este trabajo centra el tratamiento del riesgo operacional en la actividad aseguradora, es decir, en Solvencia II; pero conviene destacar la importancia de Basilea II ya que representa el punto de partida en el tratamiento de este tipo de riesgo. Por lo tanto, Solvencia II sigue las líneas que Basilea II está implantando en la actividad bancaria pero para el sector asegurador.

3. EL RIESGO OPERACIONAL EN EL MARCO DE SOLVENCIA II

El tratamiento del riesgo operacional en el marco de Solvencia II constituye el apartado más relevante de todo el documento ya que es dónde se explica cómo se realiza la gestión del mismo en el ámbito asegurador.

Sin embargo, para entender cómo establece Solvencia II que las compañías tienen que gestionar el riesgo operacional conviene explicar, previamente, qué es Solvencia II, cuáles son sus antecedentes, en qué entorno surge y sobre qué pilares se asienta.

A continuación, se analiza el tratamiento del riesgo operacional en el entorno empresarial, y, para ello, es necesario explicar detalladamente la gestión, administración y cuantificación de dicho riesgo en el contexto financiero europeo.

Finalmente, se dedica un apartado especial a la responsabilidad de los distintos órganos de las entidades aseguradoras en el tratamiento del riesgo operacional. Serán los responsables de los diferentes ámbitos de la organización los encargados de poner en marcha adecuadas prácticas de gestión del riesgo y de informar convenientemente a todo el personal involucrado en la administración del mismo para que la gestión de riesgos forme parte de la cultura empresarial.

3.1. ENTENDIENDO SOLVENCIA II

La función de toda entidad aseguradora es la de mediar en el sistema financiero recogiendo el ahorro presente de los asegurados para indemnizar, en el futuro, a aquellos que sufran las consecuencias desfavorables de un riesgo asegurado.

El creciente proceso de globalización y creación de un mercado financiero único requiere la homogeneización de los criterios establecidos por la Unión Europea. Al mismo tiempo, el lanzamiento de nuevos productos con un componente financiero significativo exige la aplicación de similares criterios de solvencia a los establecidos para la banca.

En este entorno cambiante se manifiesta la necesidad de poner en marcha sistemas de supervisión de carácter preventivo y dinámico.

La solvencia de una entidad no debería estar basada únicamente en datos financieros; deberían considerarse, adicionalmente, otros aspectos tales como su exposición al riesgo, su tamaño, estrategias, políticas de protección en reaseguro, etc.

Desde un punto de vista normativo, la preocupación por garantizar la protección del asegurado implica establecer requisitos de solvencia. Sin embargo, es tarea de la comunidad científica, dedicada a la investigación en materia de seguros, estudiar y desarrollar los medios que garanticen la estabilidad de los aseguradores y, por tanto, la de los asegurados que de ellas dependen.

Actualmente esta investigación debe realizarse dentro de un ámbito internacional, centrado en el proyecto europeo elaborado por la *Asociación Internacional de los Supervisores de Seguros* (IAIS²⁹) en colaboración con la *Asociación Internacional de Actuarios* (IAA³⁰). Aunque conviene destacar que no se trata de un sistema homogéneo en los Estados Miembros de la UE.

²⁹ **IAIS** (*International Association of Insurance Supervisors*): la "Asociación Internacional de Supervisores de Seguros" fue establecida en 1994 con el propósito de promover la cooperación entre los reguladores de seguros, así como de otros sectores financieros.

³⁰ **IAA** (*International Actuarial Association*): Asociación Internacional Actuarial.

Solvencia II describe cómo deberá estructurarse el sistema de valoración de la solvencia del asegurador a partir del análisis de sus riesgos. Su principal objetivo es la armonización de las actuaciones de las entidades aseguradoras a nivel europeo, estableciendo formas de actuación comunes y adecuadas a economías cambiantes que, cada vez más, necesitan mayor cobertura para sus riesgos.

Por otra parte, para las compañías de seguros europeas supone un cambio profundo en su sistema de gestión, cuantificación y control efectivo del riesgo basado en la implementación de un proceso que se adapte a las necesidades reguladoras y de mercado.

La preocupación de CEIOPS³¹ por la gestión del riesgo operacional se puso de manifiesto cuando dicho organismo incluyó, en su cuarto estudio de impacto (QIS4), un cuestionario relacionado con la gestión del mismo en las compañías de seguros, en el que resaltaba lo siguiente:

“Actualmente, la implantación de estrategias, políticas y procedimientos, en muchas compañías de seguros concernientes a la gestión del riesgo operacional, es un pre-requisito necesario para asegurar que cualquier empresa identifique, analice, trate y controle de una forma adecuada el riesgo operacional, no siendo suficiente detener el proceso en la gestión de los riesgos propios de negocio que están llevando a cabo”.

En España, las compañías de seguros que operan en este territorio se han visto motivadas a avanzar en esta dirección ante la aparición y modificación del artículo 110 del Reglamento de Ordenación y Supervisión de los Seguros Privados (ROSSP), en el que se destaca:

“Las entidades aseguradoras establecerán sistemas de gestión de riesgos adecuados a su organización, que les permitan identificar y evaluar sus riesgos internos y externos a los que están expuestas.

Para ello, se establecerán estrategias respecto a los mismos, ajustadas a la naturaleza e incidencia de tales riesgos, incorporando procesos que permitan una medición de los riesgos identificados, incluyendo la probabilidad de ocurrencia e impacto en el perfil de riesgo de la entidad.

Asimismo, las entidades deberán tener establecidos planes de contingencia que permitan anticipar situaciones adversas que puedan poner en peligro su viabilidad”.

³¹ **CEIOPS** (Committee of European Insurance and Occupational Pensions Supervisors): Comité Europeo de Supervisores de Seguros y de Pensiones de Jubilación. Actualmente, desde el 1 de enero de 2011, la Autoridad Europea de Seguros y Planes de Pensiones (EIOPA, *European Insurance and Occupational Pensions Authority*) reemplaza a CEIOPS.

El artículo 110 surge, por tanto, en el marco de este importante reto regulatorio al que se enfrentan las compañías de seguros europeas, con el objetivo de orientar y ayudar en dicho proceso para la construcción de un modelo de gestión del riesgo operacional (ORM) óptimo que permita un control eficaz de los riesgos en un entorno dinámico.

Antecedentes

Para entender el proyecto de Solvencia II es preciso explicar de dónde nace la necesidad de controlar estos aspectos en las entidades aseguradoras y cómo evoluciona hasta llegar a la regulación actual.

La *Directiva 73/239/CE*³², de 24 de julio de 1973 estableció que las empresas de seguros dispusieran, además de las reservas técnicas suficientes para hacer frente a

los compromisos contraídos, de una reserva complementaria denominada margen de solvencia para hacer frente a los riesgos de explotación.

Por su parte, la *Directiva 2002/83/CE*³³ de 5 noviembre del 2002, por la que se refunden las directivas sobre los seguros de vida, dan al margen de solvencia, reserva complementaria, la función de actuar como amortiguador frente fluctuaciones adversas de la actividad.

El margen de solvencia supuso, en los años 70, el reconocimiento de la necesidad de que las entidades aseguradoras contaran con un margen de seguridad por encima de sus activos que pudiera hacer frente a la realidad del negocio asegurador, caracterizado por una serie de elementos de carácter imprevisible que constituyen los riesgos.

Con la apertura de mercados en los 90, estas normas aumentan su importancia a partir de la tercera generación de Directivas comunitarias en 1994 sobre seguros con las cuales se abolieron los controles de precios y productos en toda la UE.

Estas Directivas encomendaron a la Comisión Europea liderar un proceso de revisión de los requerimientos de solvencia que culminaría con la puesta en marcha del conocido como marco de **Solvencia I**.

Han transcurrido más de treinta años desde que se estableció la necesidad de disponer de esta reserva complementaria, y el debate se produce en otras circunstancias y en un ámbito más ambicioso, pero la esencia del mismo sobre la actividad asegurado

³² Primera Directiva del Consejo de 24 de julio de 1973 sobre coordinación de las disposiciones legales, reglamentarias y administrativas relativas al acceso a la actividad del seguro directo distinto del seguro de vida, y a su ejercicio.

³³ Directiva 2002/83/CE del Parlamento Europeo y del Consejo de 5 de noviembre de 2002 sobre el seguro de vida.

ra como un negocio cargado de riesgos de carácter múltiple y sobre la necesidad de establecer los requisitos comunes y armonizados en todos los Estados Miembros del Espacio Económico Europeo, permanece.

Finalmente, las bases que reflejan las diferencias entre Solvencia I y Solvencia II, son las siguientes:

| Solvencia I | Solvencia II |
|--|--|
| <ul style="list-style-type: none">• Regulación desde los 70s.• Valoración de activos pasivos no armonizada.• Requerimientos de capital basados en medidas de volumen no sensibles al riesgo.• Insensible a mecanismos de reducción del riesgo.• No anima a la medición ni a la gestión.• Grandes diferencias en las medidas de supervisión.• Sistema estático y retrospectivo. | <ul style="list-style-type: none">• Planteamiento basado en riesgo.• Probabilidad explícita de ruina (margen de fallo).• Divergencia entre solvencia y contabilidad.• Dos requerimientos de capital: SCR y MCR.• Activos: carga de capital en función del riesgo asumido.• Producción Notmativa: Lamfalussy y tres pilares. |

Fuente: DGSFP.

Entorno de Solvencia II

Es conveniente analizar cuál es el entorno en el que se ha desarrollado Solvencia II para comprender este cambio normativo y los factores por los que se le ha otorgado la importancia actual a la gestión del riesgo operacional.

Contexto económico

La consecución del mercado único europeo, en todos los sectores, está dentro de las prioridades y objetivos fundamentales de la UE.

Se espera que las reformas que introduce Solvencia II puedan contribuir a lograrlo en el ámbito del seguro, fortaleciendo la función de las aseguradoras como inversores institucionales, poniendo en vigor una normativa que permita lograr un adecuado nivel de protección para los asegurados y fomentando la estabilidad del sistema financiero en su conjunto.

El sector asegurador contribuye al crecimiento económico de muy diversas formas. Desde un punto de vista macroeconómico, permite un mayor grado de eficiencia facilitando la transferencia de riesgos de unos agentes a otros, mientras que desde un punto de vista microeconómico, ayuda a que los individuos minimicen el impacto de acontecimientos ni esperados ni deseados, lo cual les permite organizar con mayor certidumbre.

Adicionalmente, el negocio asegurador ofrece la posibilidad de colocar los excedentes financieros y satisfacer necesidades tales como las pensiones de jubilación.

La creciente globalización de los servicios es una de las características más importantes del contexto del sector asegurador. Algunos de los retos para entidades y supervisores son los siguientes:

- Permitir una adecuada integración que permita lograr el crecimiento económico.
- Asegurar que el sector de servicios financieros dé la respuesta adecuada a los nuevos cambios.
- Garantizar que el sector de servicios financieros siga siendo competitivo.

Como se ha explicado anteriormente, la regulación sobre la solvencia de entidades aseguradoras surge en los años 70 del pasado siglo, época en la que el sector era menos abierto, competitivo y dinámico de lo que lo es hoy. Desde entonces, muchas cosas han cambiado, en especial las innovaciones financieras. En el sector asegurador los cambios se resumen en:

- **Aumento de la competencia:** las compañías se han expandido más allá de sus fronteras nacionales y se ha acelerado la integración en los servicios financieros con bancos que ofrecen productos de seguro.
- **Desarrollo de los mercados financieros**, entendido bien como aparición de nuevos productos o como un mayor grado de integración. Ambos factores han mejorado el acceso de las aseguradoras a mercados más profundos y también han mejorado su habilidad para evaluar correctamente los riesgos.
- Mejoras en la **modernización del riesgo** y en la gestión, especialmente con la introducción y uso de modelos del tipo VaR³⁴.
- **Cambios en la distribución**, fomentados por el desarrollo de las ventas por canales tales como el teléfono o internet.
- **Reforma del Estado del Bienestar** motivada por los cambios demográficos, los cuales presionan sobre los sistemas públicos de pensiones y están consiguiendo un aumento en la demanda de productos tales como los planes de pensiones.

³⁴ **Valor en Riesgo** (VaR, *Value at Risk*) es una medición de riesgo frecuentemente utilizada en el riesgo de pérdida de una cartera específica de activos financieros.

Desde comienzos de este siglo, la Comisión Europea viene trabajando en la reforma del sistema de fijación del nivel de capital en las entidades aseguradoras. Los objetivos buscados son:

- Protección de los asegurados.
- Establecimiento de unas exigencias de capital más acordes con los riesgos soportados.
- Establecimiento de principios de gestión de los riesgos.

El sistema trata de llevar al ámbito del seguro lo que es Basilea en el sector bancario. Por ello, se articula en tres pilares que se detallan posteriormente.

Otros aspectos destacables de Solvencia II, desde el punto de vista económico, serán los siguientes:

- Articulación en torno a dos cifras de capital: capital económico³⁵ y capital legal³⁶.
- Armonización de los métodos cuantitativos y cualitativos de supervisión.
- Incorporación de desarrollos internacionales para promover una mayor convergencia con organizaciones como la IAIS, IAA y la IASB³⁷, en cuestiones tales como el establecimiento de normas relativas al nivel de capital adecuado.

El elemento fundamental del nuevo sistema es el cambio de criterio para calcular la cantidad de capital de solvencia; se pasa de fijar éste como una función del riesgo de suscripción de primas a hacerlo depender del nivel de riesgo soportado en todas y cada uno de las esferas en las que se desarrolla la actividad de una aseguradora.

Contexto político y normativo

Dentro del contexto político y normativo de Solvencia II conviene destacar, de manera resumida, las siguientes cuestiones:

- Su papel dentro de las demás reformas de la UE.
- Relación con la regulación bancaria de solvencia.
- Las *NIC*.

³⁵ **Capital económico:** cantidad asociada al riesgo que se soporta.

³⁶ **Capital legal:** importe mínimo que una compañía debería tener.

³⁷ **IASB** (*International Accounting Standards Board*): Consejo de Normas Internacionales de Contabilidad.

Solvencia II dentro de las reformas comunitarias

Desde que, en los años 90, surgiera la idea de modificar la normativa sobre solvencia se han producido múltiples cambios; no sólo en el ámbito de la UE sino también en otros países. Lo mismo ocurre con la normativa contable y con la supervisión bancaria. De todos estos cambios los principales son:

El llamado *Plan de Acción en los Servicios Financieros (FSAP)*³⁸ en el que se incluye el desarrollo del llamado *enfoque Lamfalussy*³⁹.

- La Directiva de Requisitos de Capital en la que se incluyen los acuerdos de Basilea II para el ámbito de la UE y cambios en la regulación de conglomerados financieros.
- El desarrollo de los *Estándares Internacionales de Información Financiera (IFRS)*.
- Desarrollos normativos en algunos estados miembros de la UE.

Las actuales directivas dan soporte a una legislación para los Estados Miembros y permiten que las aseguradoras tengan un marco establecido para poder prestar sus servicios en otros países de la UE. Sin embargo, existen múltiples áreas en las cuales la legislación, lejos de fijar criterios y normas claras y precisas, da pie a múltiples interpretaciones. Esta situación ha conducido a una fragmentación de la regulación en la Unión Europea que ha desarrollado barreras entre los Estados y ha impedido la formación de un mercado único.

Consistencia con la regulación bancaria

La Directiva de Requisitos de Capital (*CRD*) actualiza el sistema de regulación bancaria de la UE. En líneas generales, permite a los bancos una respuesta flexible a las exigencias del mercado siempre que tengan plenamente identificados los riesgos y un nivel adecuado de capital y sistemas de control para manejar los riesgos.

³⁸ En marzo de 2000 el Consejo Europeo de Lisboa aprobó el *FSAP*, conjunto de 42 medidas destinadas a completar el mercado único en servicios financieros.

³⁹ El proceso Lamfalussy se utiliza en la Unión Europea para el desarrollo regulatorio de los servicios financieros. Está constituido por cuatro niveles, cada uno de ellos centrado en un estadio específico de la implementación de la legislación financiera: En el primer nivel, se encuentran las Directivas y Reglamentos del Parlamento Europeo y del Consejo; en el segundo nivel, se sitúan las Directivas y Reglamentos de la Comisión; en el tercer nivel, los Comités específicos de nivel 3 que asesoran acerca de los detalles técnicos que son acordados por votación de los representantes de los Estados Miembros; y en el cuarto nivel, la propia Comisión Europea realiza el seguimiento y vigilancia de la aplicación de la normativa comunitaria por los Estados Miembros.

Este sistema pretende lograr interpretaciones más consistentes de la legislación comunitaria, mayor convergencia en las prácticas supervisoras nacionales, y calidad técnica en la legislación de servicios financieros.

La Comisión ha propuesto que las aseguradoras sigan un esquema similar al desarrollado por Basilea II, basado en tres pilares:

- **Pilar I. Requisitos mínimos de capital:** fijación de unas normas comunes para la valoración de activos y pasivos y para el cálculo de los requisitos de capital.
- **Pilar II: Procesos de supervisión** que ayuden a garantizar que las aseguradoras tengan adecuados sistemas de gestión y control de riesgos, además de un nivel de capital óptimo.
- **Pilar III: Información y disciplina de mercado:** fijación de requisitos que permitan la comparación de capitales entre entidades.

Un aspecto fundamental en el proceso es garantizar que, Solvencia II, sea capaz de adoptar adecuadamente la estructura de los tres pilares a la vez que permite recoger las peculiaridades del negocio asegurador.

Normas Internacionales de Contabilidad –NIC–

En los últimos años, se han producido avances significativos en la normativa contable internacional (NIC). Las empresas de la UE que cotizan en Bolsa se han visto obligadas a llevar su contabilidad usando las *Normas Internacionales de Información Financiera (NIIF)* desde el 1 de enero de 2005, lo cual incluye la *IFRS4* que, por primera vez, incorpora los contratos de seguros en este ámbito.

Los requisitos de la *IFRS4* reflejan los resultados de la primera fase de los trabajos de la *IASB* sobre contratos de seguros.

La *IASB* ha dado algunas indicaciones sobre la estructura posible de los modelos contables que está desarrollando, especialmente en los contratos de no vida. Estos principios son consistentes con el enfoque establecido por *IAIS* y fijan el marco establecido por la Comisión para Solvencia II.

Desarrollos internacionales en la regulación de solvencia en seguros

La Comisión ha establecido que el marco de Solvencia II se ajuste a los principios de la *IAIS*, agrupados en tres bloques:

- **Bloque 1: Reconocimiento de los riesgos**
 - Espera lograr la robustez del asegurador para cumplir con sus compromisos tanto de corto como de largo plazo.
 - Ha de ser sensible al riesgo indicando, explícitamente, qué riesgos individuales o combinación de ellos han de ser regulados y cómo esos riesgos se recogen en las exigencias.
 - Para cada uno de esos riesgos se ha de indicar cómo se recoge la prudencia.

- **Bloque 2: Valoración de los compromisos**
 - Se necesita una metodología que haga un uso óptimo y consistente de la información suministrada por los mercados financieros.
 - Se debe incluir la definición de las provisiones técnicas, las cuales han de ser prudentes, realistas, objetivas y han de permitir la comparación entre aseguradoras.
 - Se debe determinar el *mejor estimador* del coste de hacer frente a los compromisos incorporados en la cartera de seguros, teniendo en cuenta el valor temporal del dinero y considerando como tipo de descuento el tipo relevante libre de riesgo.
- **Bloque 3: Estimación de los requisitos de solvencia y control de la solvencia**
 - Se ha de establecer un rango de niveles de control y los instrumentos asociados con cada uno de esos niveles.
 - Se permite el uso de un conjunto de enfoques normalizados para determinar los requisitos de solvencia, posibilitándose el uso de modelos internos, si resultase apropiado.

Estudios de impacto cuantitativo “QIS”

Según el *Diccionario Mapfre de Seguros*, el término “QIS” se utiliza en el marco de Basilea II y Solvencia II para referirse a las “pruebas propuestas por el organismo supervisor para evaluar el impacto cuantitativo que produciría en las empresas supervisadas la adopción de un determinado modelo de requerimiento de capital de solvencia”.

El CEIOPS, es el organismo encomendado por la Comisión Europa encargado de realizar los estudios técnicos necesarios para desarrollar y estudiar la viabilidad e impacto cuantitativo de Solvencia II.

Para poder elaborar Solvencia II, el CEIOPS ha solicitado la cooperación de las aseguradoras europeas. Dicha cooperación ha sido canalizada mediante los trabajos conocidos como QIS, siglas de “Quantitative Impact Study”, en los que se ha diseñado un modelo cuantitativo de aplicación general para calcular las cifras de SCR⁴⁰ y MCR⁴¹.

⁴⁰ **SCR:** (*Solvency Capital Requirement*) término acuñado en el marco del proyecto Solvencia II que hace referencia al nivel de fondos propios exigible por parte de las autoridades supervisoras a las empresas de seguros y de reaseguros destinado a absorber pérdidas significativas y ofrecer a los tomadores y beneficiarios de seguros una garantía razonable de que se efectuarán los pagos al vencimiento. Su fórmula de cálculo está orientada a recoger el verdadero perfil de riesgo de las empresas, teniendo en cuenta la incidencia de las posibles técnicas de reducción del riesgo, así como los efectos de la diversificación. Sustituirá al margen actual de solvencia.

⁴¹ **MCR:** (*Minimum Capital Requirement Solvency*) término acuñado en el marco del proyecto Solvencia II que hace referencia al nivel de fondos propios por debajo del cual los tomadores y los beneficiarios, en caso

Estos modelos se han elaborado con la colaboración de las compañías y, a partir de los resultados obtenidos, se llega al modelo actual. Hasta la fecha, se han llevado a cabo cinco pruebas sucesivas conocidas como QIS1, QIS2, QIS3, QIS4 y QIS5.

El principal objetivo de los QIS es dar una visión clara y concisa de los resultados, informando sobre la capacidad de las entidades al realizar los cálculos requeridos y determinar el nivel de evaluación de las provisiones técnicas.

Se evalúa la solvencia de las instituciones de seguros calculando los requerimientos de capital mediante el empleo de una fórmula estándar. Por otra parte, valora el impacto cuantitativo que tendría la implementación de Solvencia II en términos del balance general y de solvencia. Además, evalúa la factibilidad de los cálculos manteniendo el principio de proporcionalidad.

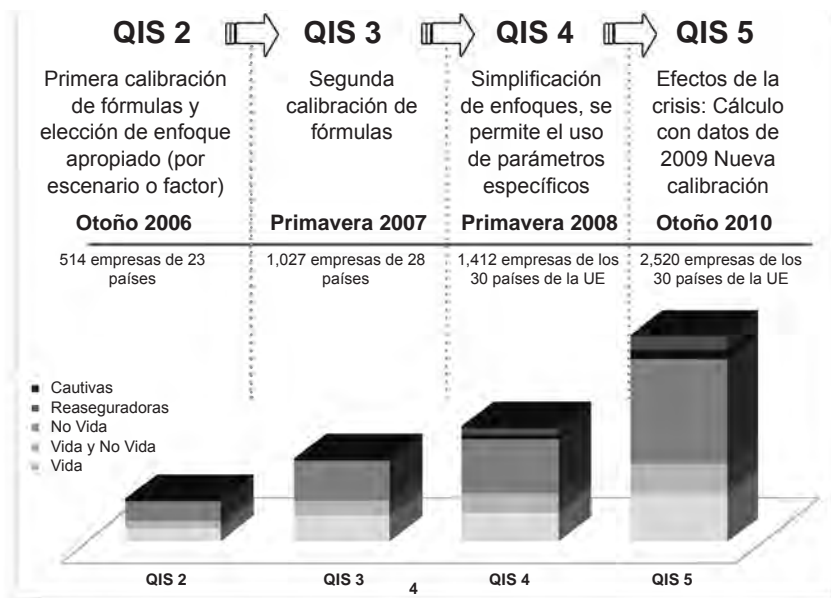
- En el primer estudio (QIS 1), llevado a cabo en el año 2006, participaron 312 entidades de 19 países.
- En el segundo estudio (QIS 2), se evaluaron las necesidades de capital y la consideración de la diversificación de los riesgos. Año 2006.
- En el tercer estudio (QIS 3), se calibran las fórmulas estándar para el cálculo del MCR -Capital Mínimo Obligatorio- y SCR -Capital de Solvencia Requerido-. Año 2007.
- En el cuarto estudio (QIS 4), se completa la calibración de las fórmulas estándar. Año 2008.
- En el quinto estudio (QIS 5), se afina la calibración de las fórmulas estándar. Año 2010.

Los resultados de estos estudios han servido para confeccionar una base de datos que permita asesorar sobre el desarrollo del nuevo sistema de solvencia.

Finalmente, es importante conocer que los datos obtenidos no pueden considerarse representativos del EEE porque no todos los países han participado en los diferentes estudios.

Gráficamente, la evolución de los estudios de impacto cuantitativo “QIS” están representados en el siguiente cuadro dónde aparece la fecha en la que se han publicado, las entidades, los países que han participado y lo que se han concluido en los mismos.

de continuar las empresas de seguros y de reaseguros su actividad, estarían expuestos a un nivel de riesgo inaceptable. La insuficiencia del capital mínimo obligatorio activa la intervención en última instancia de las autoridades de supervisión. Sustituirá al vigente fondo de garantía.



Fuente: Mazars Auditores, S.L.P.
"Solvencia II, notas sobre QIS 5".

Directiva de Solvencia II

Solvencia II es el *proyecto de revisión y modificación de las normas sobre la supervisión y la valoración de la situación financiera de las aseguradoras, en el marco de la Unión Europea, de modo que las compañías aseguradoras operen dentro de sus ámbitos de responsabilidad con un nivel de solvencia adecuado.*

Es un proyecto llevado a cabo por la Comisión Europea y está enfocado a que cada empresa aseguradora conozca su posicionamiento frente a los distintos riesgos que está asumiendo y a exigir un sistema de gestión adecuado.

Solvencia II busca definir la información que las aseguradoras deben aportar al mercado y el nuevo papel que tienen que desempeñar los supervisores. Un enfoque basado en la verificación, por parte del supervisor, de los procedimientos utilizados por las entidades en la evaluación interna de los recursos propios que precisan para respaldar el conjunto de los riesgos asumidos.

La implantación de Solvencia II supone una mejor estimación de los riesgos reales asumidos por cada aseguradora, así como un reto para los supervisores que deberán

prever situaciones de crisis, evaluar los mecanismos de control de las entidades y adoptar medidas cuando se incrementa el riesgo.

Esta normativa afecta además a la transparencia, a la disciplina de mercado y a como las aseguradoras deben informar sobre su nivel de solvencia, exposición al riesgo y mecanismos de control interno.

Es importante destacar la influencia de Basilea II sobre Solvencia II. Por un lado, aparece como referente y estímulo para la actualización de la supervisión de las compañías aseguradoras. Por otra parte, resulta fundamental que a riesgos semejantes se dé una respuesta regulatoria similar; en un entorno económico caracterizado por la creciente existencia de conglomerados financieros y por la participación, cada vez mayor, de las entidades de crédito en el negocio asegurador.

La estructura de tres pilares desarrollada bajo Basilea II va a ser recibida por Solvencia II como un modelo que desarrolla, además, sus propias características.

En resumen, la aprobación de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo -de 25 de noviembre de 2009- sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), ha supuesto el paso definitivo en el proceso de renovación de los principios, esquemas y procedimientos de supervisión prudencial y de mercado para el sector asegurador europeo.

Estructura de los tres pilares

Solvencia II se ajusta al enfoque de los **tres pilares** desarrollado en el acuerdo de Basilea (*BIS II*) para la regulación internacional de las entidades financieras (*Comité de Supervisión Bancaria de Basilea, 2004*). Cada uno de los pilares mencionados en dicho acuerdo, ajustados a las características específicas del mercado asegurador, hace referencia a (*IAA, 2004*):

Pilar I. Necesidades financieras mínimas o requerimientos mínimos de capital

Este pilar es cuantitativo y se basa en el mantenimiento de provisiones técnicas adecuadas, activos apropiados que soporten las obligaciones asumidas y una cuantía mínima de capital, definida a partir de un conjunto de elementos de capital disponibles y necesarios para cada asegurador. Así, como lo referente a las inversiones y las reservas de las entidades.

Serán permitidos modelos internos para calcular el nivel capital. Se desarrollará un criterio de aprobación para la UE en cooperación con el grupo consultivo de la IAS, la IAIS y tomando en consideración la experiencia en el sector bancario.

Serán admisibles modelos parciales para facilitar la introducción de modelos internos. Resultarán útiles los modelos de fuentes externas (reaseguradores, bancos, consultores, etc.).

Pilar II. El proceso de examen supervisor

El segundo pilar analiza los principios básicos del proceso de evaluación por parte del órgano de supervisión, de la efectividad de los sistemas de gestión de riesgos y de control interno, incluyendo la revisión de la exposición al riesgo de cada entidad.

En dicha revisión se incluirá el programa de reaseguro, los modelos internos de gestión de riesgos y el buen gobierno corporativo así como la posibilidad de requerir, por parte de los supervisores, capitales adicionales a los calculados de acuerdo a los modelos aplicados en casos individuales.

Con la definición del Pilar II se garantiza que las compañías aseguradoras dispongan de un capital adecuado, que les permita soportar todos los riesgos derivados de sus negocios y desarrollar y utilizar técnicas de gestión que reflejen el perfil concreto de los riesgos del asegurador, los supervisen y gestionen.

- Se elaborarán principios para el control interno de las empresas de seguros.
- Se debería exigir que las empresas de seguros sigan los principios para la gestión prudente de riesgos (especialmente en suscripción, reservas, manejo de siniestros).
- Se exigirá que las empresas fortalezcan su gestión financiera presentando un plan sobre su política de inversiones.

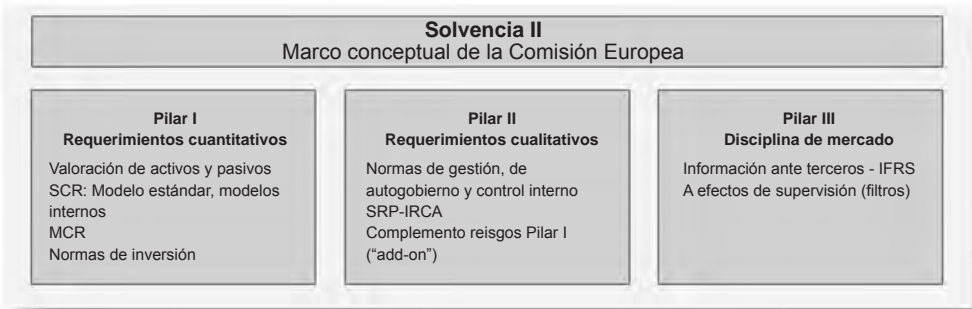
Pilar III. Medidas para fomentar la disciplina del mercado

El tercer pilar complementa a los dos pilares anteriores fomentando la disciplina de mercado, a través del establecimiento de un conjunto de requisitos de divulgación que permitan a los agentes del mercado evaluar información esencial referida al ámbito de aplicación, al capital, a las exposiciones al riesgo, a los procesos de evaluación del riesgo y, con todo ello, a la suficiencia del capital de la institución.

El Pilar III introduce requisitos de acceso al mercado con el objetivo de que mejoren las prácticas de la industria aseguradora y que se fomente la transparencia en el mercado. Las exigencias de presentación de información dependerán de los métodos y medidas adoptados en los pilares anteriores.

Dentro de lo posible, los reportes de *IAS/IFRS* deberían ser la base de la supervisión para reducir la carga administrativa a las empresas.

En determinadas ocasiones, por ejemplo en empresas que están atravesando momentos económicos o financieros complicados, con el fin de evitar agravar la situación habría que tener en cuenta que no toda la información puede hacerse pública.



Fuente: EIOPA.

3.2. TRATAMIENTO DEL RIESGO OPERACIONAL EN SOLVENCIA II

El sistema de gestión y tratamiento del riesgo operacional se explica a través de cuatro aspectos fundamentales. Para que el tratamiento del mismo sea adecuado cada uno de los elementos que lo componen tienen que funcionar correctamente y acomodarse a las necesidades propias de cada entidad.



Fuente: EIOPA.

El estudio de estos aspectos permite el conocimiento del tratamiento del riesgo operacional en el marco de Solvencia II y, a su vez, facilitan a las entidades aseguradoras el establecimiento de los mecanismos apropiados para implementar aquellos procesos necesarios para una adecuada gerencia del mismo.

Para ello, las entidades cuentan con diferentes métodos y herramientas que permiten un control y gestión del riesgo operacional mucho más efectivo.

Gestión del Riesgo Operacional (ORM)

La gestión del riesgo operacional (*Operational Risk Management*, ORM) se define como un *proceso integral que implica y afecta en su aplicación y desarrollo a toda la organización y a todos los niveles comprendiendo la identificación, el análisis, la evaluación, el tratamiento, la mitigación y el control de los riesgos considerados operacionales*. Es parte integrante del ERM pero referida, exclusivamente, al riesgo operacional.

El objetivo principal de este proceso es la minimización de las pérdidas operacionales a las que está sometida la entidad aseguradora y la mejora continua en los controles. Por ello, la gestión de los riesgos operacionales resulta de suma importancia para la evolución, crecimiento y supervivencia de cualquier compañía de seguros tanto desde un punto de vista global como en cada una de sus unidades estratégicas de negocio.

En este sentido, CEIOPS ha desarrollado un marco común de valoración del riesgo y de la solvencia para el sector asegurador europeo. Fruto de la implementación de este marco de trabajo las entidades deberán establecer una infraestructura robusta para la identificación, valoración, revisión, control y publicidad de todos los riesgos a los que una empresa aseguradora está expuesta, tanto en el corto como con medidas de medio y largo plazo.

El impacto en términos de coste asociado a la falta de gestión de riesgo operacional por parte de las compañías aseguradoras puede ser enorme.

CEIOPS, en su informe *Lessons to be learned from the crisis: Solvency II and beyond 2009*⁴², considera que una de las lecciones aprendidas a raíz de la crisis financiera que se está viviendo en la actualidad es, precisamente, que tanto los supervisores como la industria del seguro son conscientes de la relevancia del riesgo operacional al que, en el pasado, no se le ha prestado la suficiente atención.

La gestión de riesgos es un proceso que debe expandirse por toda la organización y, para ello, es necesario crear una unidad de riesgo específica que defina el marco de

⁴² *Lessons to be learned from the crisis: Solvency II and beyond 2009*: Documento publicado por CEIOPS (actualmente EIOPA) que recoge las lecciones de esta crisis financiera y en qué afecta a Solvencia II y a las entidades aseguradoras.

gestión e informe a la alta dirección de los resultados derivados del proceso de gestión del riesgo. Para llevar a cabo esta función es fundamental la existencia de una auditoría como mecanismo interno que permita contrastar y validar los procedimientos seguidos.

El ORM es un proceso continuo que no finaliza una vez alcanzada la última fase. Los resultados conducen a decisiones estratégicas y diarias que inciden sobre la operativa del negocio, en el que resulta básico un adecuado proceso de retroalimentación.

Los puntos clave del mismo son las causas, las consecuencias (pérdidas monetarias, incidencias en el negocio, daños en la reputación de la entidad, etc.), la política de límites establecida (tolerancia al riesgo) y los controles definidos sobre el mismo.

Una vez implementado un sistema efectivo de ORM los responsables de las líneas de negocio reportarán y validarán la información de riesgos a través de una infraestructura informática y los responsables del departamento de riesgos o auditoría realizarán una validación cruzada. Un aspecto crítico será el análisis de la efectividad de los controles internos y la monitorización de los planes de mitigación de riesgos.

Implantar un proceso ORM

Para la implantación adecuada de un proceso ORM según los principios del marco de gestión de riesgos operacionales, se deben tener en cuenta los siguientes aspectos tanto desde el punto de vista organizativo como directivo:

- *Definición de la estrategia*

El marco global de la gestión del riesgo se inicia con la definición de la **estrategia** a seguir compuesta por los objetivos y políticas de riesgo dentro del modelo de gobierno corporativo. Se deben definir de forma clara tanto la actitud frente al mismo como su política de retención y de transferencia.

- *Aprobación del Plan Estratégico*

Se debe solicitar la aprobación por parte del consejo de administración del plan estratégico y del plan táctico correspondiente a dicha gestión. La dirección tiene la responsabilidad de implementar el marco de gestión de riesgo operacional, a todos los niveles, e involucrar a toda la organización para lograr una cultura de gestión responsable.

- *Identificar los riesgos operacionales*

La entidad debe identificar los riesgos operacionales asociados a sus productos, actividades, procesos y sistemas.

- *Planes de contingencia y continuidad del negocio*

Para la compañía de seguros es fundamental disponer de planes de contingencia y de continuidad del negocio que aseguren su capacidad para operar. Con esto se evitará una posible interrupción de la actividad.

- *Adaptación de la estructura organizativa*

Adaptar la estructura organizativa a las nuevas circunstancias de gestión del riesgo resulta muy importante. El organigrama considerado servirá para marcar los pasos generales de la implantación del ORM. Por otra parte, es necesario conocer el grado de preparación del equipo líder, para cada una de las unidades de negocio, y llevar a cabo la designación de los responsables de cada área en materia de riesgo.

- *Implicación de la organización*

En todo proceso de implantación de un ORM la dirección debe plantearse involucrar a toda la organización. Para ello, resulta básico analizar las diferentes unidades o líneas de negocio así como los departamentos principales de la entidad.

- *Límites de tolerancia*

En el estudio de los riesgos de una empresa se deben establecer los límites de tolerancia a pérdidas económicas que puede soportar cada entidad, en valores referenciados, frente a determinados parámetros financieros.

Los límites o umbrales de tolerancia que conviene determinar son las pérdidas económicas totales de todo tipo de riesgos soportables por la empresa en un periodo de tiempo normalmente anual, las pérdidas económicas de cada tipo de riesgos soportables por la entidad en un periodo de tiempo y, por último, las pérdidas económicas soportables por el impacto de un único siniestro.

- *Bases de datos de pérdidas operacionales*

Los datos de pérdidas operacionales para calcular el riesgo de la firma deben provenir de fuentes internas y externas.

Las **fuentes internas** de datos partirán de la información de la compañía y de un estudio de sus procesos y procedimientos. Será importante disponer de una base de datos que incluya tanto datos públicos como privados. Los datos públicos se obtienen, generalmente, a través de organismos creados para dicha función y que disponen de mecanismos de validación de la información. Los datos privados, de carácter externo, se obtienen a través de la cooperación de diferentes instituciones que estén de acuerdo en compartir sus datos internos.

En España, el sector **carece de una base de datos privada externa**. En este sentido queda todavía mucho por hacer; no sólo es necesario que las compañías tengan su

base de datos de pérdidas operacionales interna, deben disponer de datos históricos sobre las mismas de, al menos, cinco años para que dicha base de datos proporcione información significativa para la creación de escenarios futuros lo más acertados posibles. Un paso importante sería la creación de una base de datos nacional para la comparativa sectorial de las entidades, así como para el enriquecimiento de la información interna para el análisis predictivo del riesgo operacional.

Con este objetivo, se creó en Inglaterra en el año 2004 la base de datos de pérdidas operacionales externas privada de las compañías que operan en ese mercado y que se conoce como *Operational Risk Insurance Consortium* (ORIC). Surgió como consecuencia de que las organizaciones registrasen pérdidas de más de 20 millones de dólares y, por lo tanto, su objetivo es la reducción de las pérdidas potenciales futuras en la industria aseguradora.

En dicho consorcio participan las principales compañías de seguros inglesas. ORIC fue promovida por la *Association British Insurance*⁴³ (ABI) y *SAS Business Intelligence*⁴⁴.

En este sentido, España (y el resto de Europa) tendrá que tomar ejemplo de este consorcio con vistas a crear una base de datos de riesgo operacional que permita modelizar sus pérdidas. Una vez determinado el proceso de obtención de datos de pérdidas habrá que categorizarlos, es decir, agruparlos por categorías. Dicho proceso ayudará al tratamiento y comprensión del riesgo con vistas a la optimización de su control.

Para agrupar los datos consideran diferentes atributos o criterios. La cuestión clave es determinar qué constituye una buena categorización estándar. En principio, las categorías pueden establecerse de forma que se puedan identificar las personas o grupos de personas responsables (supervisores o controladores del riesgo) y deben definirse de forma que el gerente de riesgos comprenda cómo puede reducir la probabilidad y severidad de ocurrencia de una pérdida.

En resumen, las entidades financieras tienen que contar con una estrategia aprobada por la dirección estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operacional.

Las estrategias y políticas deberían ser implementadas por la Función de Gestión de Riesgo, responsable de identificar y gestionar todos los riesgos. La Función de Gestión de Riesgo puede incluir sub-unidades especializadas por riesgos específicos.

Las entidades financieras deberían desarrollar su propio enfoque y metodología para la gestión de riesgos de acuerdo con su objeto social, tamaño, naturaleza y complejidad de operaciones y otras características. La implementación del sistema de gestión

⁴³ **Association British Insurance (ABI):** la Asociación de Aseguradoras Británicas o ABI es una asociación comercial formada por las compañías de seguros en el Reino Unido.

⁴⁴ **SAS Business Intelligence:** empresa encargada de la creación de bases de datos para generar informes y análisis.

de riesgo operacional debería considerar todas las etapas de gestión de riesgo descritas anteriormente.

Identificación

La identificación efectiva del riesgo considera que tanto los factores internos como los externos pueden afectar de forma negativa al logro de los objetivos institucionales.

Durante este proceso la unidad del riesgo operacional recoge y utiliza una amplia gama de información como datos internos y externos de pérdida, indicadores del riesgo y resultados de los ejercicios de la evaluación del riesgo. La unidad del riesgo operacional analiza las pérdidas posibles y emprende el análisis sistemático de procesos y de sistemas, con el objetivo de considerar el potencial del riesgo para todas las categorías definidas como riesgo operacional.

Simultáneamente, las unidades de negocio individuales utilizan los mismos datos para ampliar su comprensión de fuentes de error del proceso de negocio, de las áreas del alto coste y del esfuerzo excesivo de trabajo. Por lo tanto, estas unidades de negocio realizan sus procesos internos para identificar las oportunidades de mejora en la eficiencia operativa.

Resulta obvio que sin una identificación de riesgos apropiada es muy difícil alcanzar una gestión exitosa. Desde un punto de vista metodológico, en el marco ORM destaca la dinámica de sistemas que permite pasar de un enfoque cualitativo a un enfoque más cuantitativo, y establecer un sistema integral basado en realimentación que facilita el control de los procesos y la minimización de las pérdidas operacionales.

Evaluación

Para todos los riesgos operacionales materiales que han sido identificados la entidad debería decidir si usa procedimientos apropiados de control y/o mitigación o los asume. Esta decisión depende de la estrategia de riesgos de la entidad y de su propensión al mismo.

Para aquellos riesgos que no pueden ser controlados la entidad financiera debería decidir si los acepta, reduce el nivel de actividad del negocio expuesta o se retira de esta actividad completamente. Todos los riesgos materiales deberían ser evaluados por probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de la entidad a los mismos.

Cuando sea posible, la entidad debería usar controles internos apropiados u otras estrategias de mitigación. Estos procesos internos incluyen el cálculo de pérdidas indirectas, la evaluación cualitativa de su potencial del riesgo y la evaluación empleando indicadores.

Mientras que se establece el marco de riesgo operacional, las unidades de negocio individuales participan, junto con el personal responsable, en los análisis de desarrollo

de escenarios para identificar la frecuencia y las consecuencias de los riesgos potenciales. Los escenarios son apropiados para la entidad y se modifican con el tiempo a medida que la actividad evoluciona, así como la calidad y la cantidad de datos de pérdida de negocio.

Medición

Las entidades financieras deberían estimar el riesgo inherente en todas sus actividades, productos, áreas particulares o conjuntos de actividades o portafolios, usando técnicas cualitativas basadas en análisis expertos, técnicas cuantitativas que estiman el potencial de pérdidas operativas a un nivel de confianza dado o una combinación de ambos.

Monitoreo

Un monitoreo regular de las actividades puede ofrecer la ventaja de detectar rápidamente y corregir deficiencias en las políticas, procesos y procedimientos de gestión del riesgo operacional. Además, fomenta la identificación temprana de cambios materiales en su perfil, así como la aparición de nuevos riesgos.

Su alcance incluye todos los aspectos de la gestión del riesgo operacional en un ciclo de vida consistente con la naturaleza de sus riesgos y el volumen, tamaño y complejidad de las operaciones.

Control

Después de identificar y medir los riesgos a los que está expuesta la entidad financiera debería concentrarse en la calidad de la estructura de control interno. El control del riesgo operacional puede ser conducido como una parte integral de las operaciones a través de evaluaciones periódicas separadas, o de ambas formas. Todas las deficiencias o desviaciones deben ser reportadas a la gerencia.

El control es la base de la gestión del proceso. A través de éste el equipo de riesgo operacional y los líderes de la unidad de negocio pueden determinar la eficiencia de su marco de trabajo, identificar áreas de debilidad de la administración del riesgo y volver a dirigir el esfuerzo de la entidad para crear un ambiente de control más exhaustivo.

Reporte

Debe existir un reporte regular de la información pertinente a la alta gerencia, a la dirección, al personal y a partes externas interesadas, como clientes, proveedores, reguladores y accionistas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

El análisis de la información y la administración de esfuerzos del negocio y del equipo del riesgo operacional se combinan para desarrollar los protocolos de divulgación, que sirven al negocio individual y al equipo central de la administración.

El equipo central del riesgo operacional proporciona la información que cubre una visión de arriba hacia abajo del mismo incluyendo datos reales de pérdida, posibles pérdidas, causas de la pérdida (y de las posibles pérdidas), la evaluación de riesgo, escenarios de datos e indicadores claves del riesgo.

La entidad reporta las pérdidas acumuladas y las tendencias, los resultados de la evaluación del riesgo, los resultados de indicadores claves, el capital económico y el marco regulatorio a todas las partes relevantes involucradas.

La divulgación también debe tener una perspectiva de abajo hacia arriba que se dirige a las necesidades de la administración de la unidad de negocio. Estos informes se deben modificar requisitos particulares para que la unidad de negocio facilite la disminución del riesgo, la mejora de proceso y la política de contención de costes.

Plan Director para la Implantación del Proceso ORM

El plan director es un *documento oficial en el que los responsables de una organización reflejan sus intenciones para con el futuro de su compañía en el largo plazo, definiendo generalmente un período no inferior a 5 años.*

Para una adecuada implantación del proceso de gestión del riesgo operacional, es necesario un plan director que refleje las acciones a realizar en la compañía para la consecución de sus objetivos. Este se divide en tres fases:

- Construcción del marco general basado en el modelo estándar.
- Implementación y desarrollo de modelos internos.
- Orientar lo anterior a un enfoque avanzado y dinámico.

El proceso ORM se localiza principalmente en el Pilar II, aunque será necesario que la información obtenida a raíz del mismo se utilice en los modelos internos y en el cálculo del capital económico⁴⁵.

- *Primera Fase*

Se establecen los objetivos, estrategias, asignación de responsabilidades, estudio de las relaciones causa-efecto y el lugar donde la dinámica de sistemas tendrá una especial relevancia.

⁴⁵ **Capital económico:** nivel de capital acorde con los riesgos que la entidad tenga con independencia de la existencia de activos. Es la cuantificación probabilística del importe de pérdidas futuras potenciales.

Para todo ello, la entidad analiza detalladamente los procesos y procedimientos de las posibles fuentes de riesgo. Se construye el mapa de riesgos y, una vez fijados o analizados los controles existentes, se procederá a la obtención del mapa residual.

En esta primera fase, se habrá determinado la política de retención y transferencia de la entidad frente al riesgo.

- *Segunda Fase*

Respecto a la fase segunda, correspondiente al Pilar II, se finaliza el diseño del proceso ORM y se aplican modelos avanzados para la gestión y cuantificación del riesgo operacional, stress testing, planes de continuidad de negocio y gobierno corporativo.

- *Tercera Fase*

En la tercera fase del Pilar III, el proceso ORM se ejecuta concentrándose el modelo general en la creación de valor y en la optimización de la política de reaseguro.

Un plan director describe las responsabilidades y acciones que la compañía de seguros debería desarrollar en relación a los riesgos a los que está expuesta. Los planes de acción incluyen, fundamentalmente, las siguientes medidas o acciones en cuanto al riesgo operacional:

- **Reducir:** la entidad podrá optar por la reducción de la frecuencia de la pérdida o/e intensidad de la misma.
- **Evitar:** se establecen las medidas necesarias para evitar la ocurrencia del riesgo llevando a cabo una óptima prevención y reduciendo su frecuencia a cero.
- **Retener:** hay dos tipos de retenciones: total o parcial.

La **total** está basada en la reposición del valor intrínseco de la pérdida producida. Por ello, la entidad aseguradora asumirá las posibles pérdidas imputando dichas pérdidas directamente a la cuenta de resultados, estableciendo una o varias líneas de crédito y/o un fondo interno o externo a la empresa.

La **retención parcial** puede hacer referencia directamente al reaseguro con las diferentes modalidades que éste ofrece.

Una vez implementado este plan, la organización deberá comprobar si los controles son efectivos y si, al cabo del tiempo, la frecuencia y severidad del riesgo se reducen. Para ello, se implementan informes específicos de revisión de la efectividad de los planes de acción. Este aspecto es clave puesto que los potenciales beneficios de la implementación de un ORM son directamente proporcionales a su efectividad para mejorar los controles y reducir el riesgo.

Administración del riesgo operacional

La administración del riesgo operacional no puede convertirse en un proceso eficaz dentro de la institución a menos que los líderes articulen y apoyen una visión de alto nivel, y los encargados de las unidades de negocio entiendan y aprecien los beneficios que se derivan de implementar los cambios en los procesos culturales y del negocio, requeridos por el nuevo marco de trabajo.

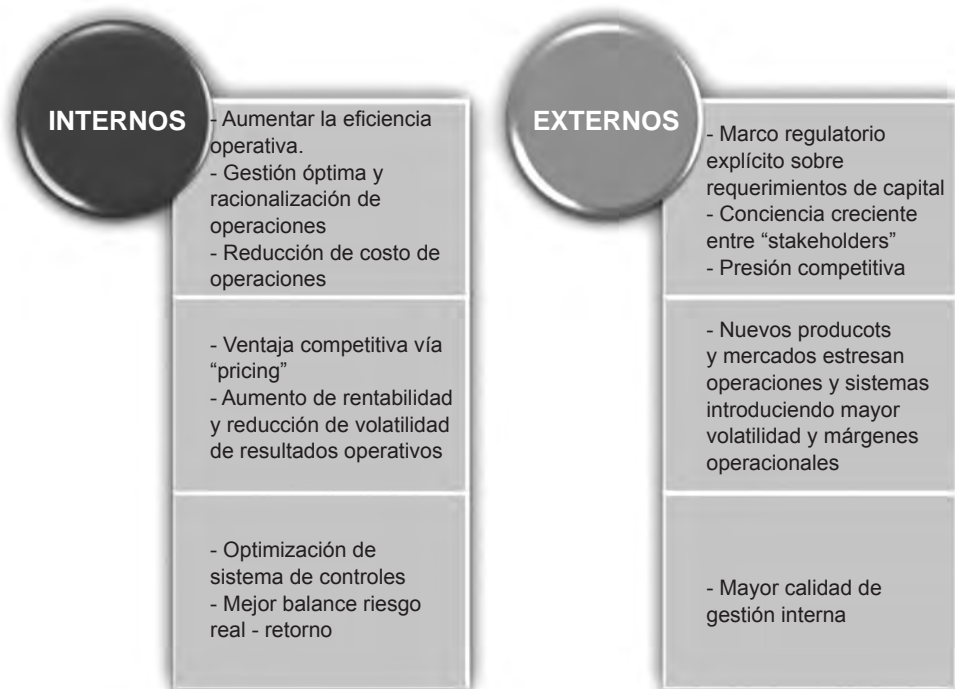
Este proceso reflejará otros empleados para áreas del riesgo diferentes tales como riesgo de mercado o de crédito. A través del riesgo operacional, los vínculos, las estructuras, la evaluación de riesgo, los indicadores claves, la base de datos de pérdida y el marco de trabajo, se provee a la administración de información relevante para emprender un programa de control riguroso.



Fuente: Elaboración propia.

Sistema para la Administración del Riesgo Operacional

El sistema de administración del riesgo operacional puede resultar muy complejo si no se conocen cuáles son los factores determinantes que intervienen en él. Éstos pueden ser tanto internos como externos.



Fuente: Elaboración propia.

Se define el **sistema de administración del riesgo operacional** como una *aproximación estructurada y disciplinada para alinear la estrategia, procesos, gente, tecnología y conocimiento con el propósito de evaluar y manejar la incertidumbre de la entidad, buscando siempre crear valor.*

Las entidades, que deberán estar involucradas en la administración del riesgo operacional y decidir qué mecanismo se va a emplear durante el proceso, pueden optar por una metodología por etapas para administrar el riesgo operacional.

Las acciones que se desarrollan en cada una de las fases de la administración por etapas, se reflejan en el cuadro siguiente:



Fuente: Informe KPMG “Metodologías de valoración de la posición financiera global de una entidad aseguradora desde la perspectiva de una supervisión prudencial”.

FASE 1. Evaluación y Planeación

La primera fase refleja el análisis de un proceso corriente de riesgo operacional. La entidad evalúa cómo administra dicho riesgo incluyendo las tareas y las responsabilidades correspondientes.

En esta fase se revisan la estructura, el contenido y los criterios de las metodologías de evaluación. Además, se estudia su frecuencia, estructura de reportes y aumento en los límites de esfuerzos comunes en la divulgación de riesgo.

El análisis de los indicadores existentes claves del riesgo y de los procesos que apoyan la recolección de datos es, también, parte de esta fase.

FASE 2. Marco de trabajo de diseño e implementación

En la fase 2 se establecen varios equipos para tratar aspectos específicos del riesgo operacional incluyendo su estructura organizacional, definiciones, vínculos y estructuras, recolección de información de pérdida, evaluación de riesgo, indicadores claves del riesgo (ICRs), divulgación, definición del capital, y tecnología de información.

Es necesario que los equipos se enfoquen para definir las necesidades de información, diseñando las estructuras organizacionales, procesos y sistemas. Con esto se persigue mejorar la administración de riesgo operacional y la evolución del plan.

Desarrollar y ejecutar el plan de acciones ayuda a los equipos de trabajo a tratar consideraciones de organización tales como comunicaciones, entrenamiento y aseguramiento de la calidad.

FASE 3. Pruebas y aprobación

En esta fase se lleva a cabo una metodología piloto en la cual las compañías pueden probar su diseño. El equipo realiza las revisiones oportunas con base en los resultados y, a continuación, se lo da a conocer a todos los miembros de la organización.

FASE 4. Monitoreo y Control

En esta fase la administración del riesgo operacional adquiere una mayor importancia, tanto de forma interna como externa a la organización. Las entidades necesitan establecer la supervisión de los procesos y de los sistemas que satisfagan las expectativas de sus propias organizaciones y de sus reguladores; este proceso se coordina con la propia gestión del riesgo operacional.

Aunque la duración de un proyecto del riesgo operacional depende de las circunstancias individuales de cada organización no suele ser inferior a dos años.

Herramientas de administración del riesgo operacional

Los altos cargos de las instituciones financieras suelen ser cautelosos ante las iniciativas corporativas que impliquen costes financieros con retornos poco tangibles. Por ello, en ocasiones, resulta difícil demostrar que la implementación de un programa de administración del riesgo operacional agrega valor a la institución. En este sentido, es importante estimar de forma precisa el riesgo operacional.

De acuerdo con el *Principio 4º del documento sobre buenas prácticas del Comité de Basilea*, los bancos y, por extensión, las entidades aseguradoras deben usar las herramientas pertinentes para identificar, evaluar, controlar y mitigar el riesgo operacional inherente en todos los productos, actividades, procesos y sistemas.

Existen herramientas específicas para estas tareas que permiten realizar un análisis más completo del riesgo operacional y disminuir su dependencia en mecanismos de control interno dentro de las líneas de negocios. La coordinación con la función de auditoría interna y el reporte adecuado de la información obtenida resultan elementos imprescindibles para un tratamiento eficaz de este riesgo.

El documento del BIS ⁴⁶ titulado “*Buenas Prácticas para la Gestión y Supervisión del Riesgo Operativo*”, identifica varios ejemplos de tales herramientas que incluyen: auto-evaluaciones, mapas de riesgo, indicadores clave, análisis de escenarios y la medición o cuantificación de la exposición al riesgo operacional a través de una variedad de enfoques.

Se distinguen dos tipos de herramientas de administración del riesgo operacional:

- **Herramientas cuantitativas**
- **Herramientas cualitativas**

A continuación, se explica en qué consisten cada uno de los tipos de herramientas, cuáles son los procedimientos más utilizados de medición y cuantificación del riesgo en función de las diferentes tipologías, y cuándo se utilizan unas u otras herramientas de administración del riesgo operacional.

Herramientas cuantitativas de gestión del riesgo operacional

En la utilización de las herramientas cuantitativas de gestión del riesgo operacional son fundamentales los registros históricos sobre incidencias y eventos de pérdida, es decir, el conocimiento de una serie de datos que permitan hallar la repercusión de determinados factores en este riesgo de forma fiable.

BASES DE DATOS

Para el cálculo del riesgo operacional existen numerosas técnicas cuantitativas. Sin embargo, la gran mayoría de las entidades que utilizan herramientas de cálculo de carácter cuantitativo lo hacen a través de las bases de datos.

En el Marco de Solvencia II las instituciones aseguradoras deben desarrollar sus bases de datos a partir de un proceso homogéneo y bien estructurado de recolección de pérdidas, que incluya su asignación o clasificación en función de las distintas áreas de negocios o apoyo y de los diferentes tipos de riesgos.

Un proceso estructurado no sólo tiene el fin de registrar las pérdidas, sino también analizarlas adecuadamente y poder entender sus causas. Este paso representa uno de los mayores desafíos y tareas pendientes a los que se enfrentan las entidades.

⁴⁶ **Banco de Pagos Internacionales (BIS):** “*Bank for International Settlement*”. Es el banco central de bancos centrales con sede en Basilea (Suiza). Organización internacional que fomenta la cooperación financiera y monetaria internacionales y sirve de banco para los bancos centrales. En febrero del 2003 el Comité de Supervisión Bancaria de Basilea publicó el documento “*Buenas Prácticas para la Gestión y Supervisión del Riesgo Operativo*”.

Una vez finalizada la construcción de las bases de datos de pérdidas las entidades deben abordar el desarrollo de un modelo de medición del riesgo operacional.

En este sentido, el Nuevo Acuerdo de Capital (*Basilea II*) ha marcado la pauta y presenta tres métodos para el cálculo de los requerimientos de capital asociados al riesgo operacional. Estos métodos, que se explican con mayor extensión en el apartado dedicado a la cuantificación del riesgo operacional, son:

- Método del Indicador Básico.
- Método Estándar.
- Métodos de Medición Avanzada (AMA por sus siglas en inglés).

Los dos primeros, método básico y estándar, no se caracterizan por ser sensibles al riesgo; estos métodos se han convertido en procedimientos de transición hasta que las entidades desarrollen otros métodos más avanzados.

A las herramientas cuantitativas no se les dedica mayor explicación ya que cada entidad podrá emplear sus herramientas propias en función de la información de la que disponga; siempre que el método de cálculo que emplee haya sido aprobado.

Herramientas cualitativas de gestión del riesgo operacional

El uso de técnicas cualitativas se emplea, cada vez más, en la identificación y evaluación de los riesgos operacionales. Las decisiones que toman las entidades afectan al perfil de riesgos de diversas maneras, estas herramientas ofrecen una respuesta más completa antes las situaciones que se puedan plantear.

Algunas de las técnicas cualitativas más destacadas en la gestión del riesgo operacional son: la auto-evaluación, el mapa de riesgos, los indicadores de riesgo clave (en inglés KRIs), los procesos de asignación del riesgo, las tarjetas de puntaje (*scorecards*), y el análisis de escenarios.

Estas técnicas son relativamente nuevas y las modalidades que adoptan en la práctica dependen en gran medida de las características que presenta cada entidad y de sus objetivos.

AUTOEVALUACIONES

Las autoevaluaciones son las herramientas que se consideran más útiles en el control del riesgo operacional.

La **autoevaluación de riesgos** se define como un *proceso de identificación y evaluación de los riesgos existentes en la entidad, sumado a una evaluación de los controles establecidos para su administración y mitigación.*

Se puede aplicar a todos los riesgos pero es un componente crítico en la gestión del riesgo operacional; ya que permite que la entidad compruebe la vulnerabilidad de sus operaciones y actividades ante este riesgo.

Es importante adecuar este proceso al tamaño e importancia del riesgo para la entidad ya que, por ejemplo, un riesgo específico puede ser crítico para una organización pequeña pero de muy bajo impacto o de complejidad diferente para una entidad más grande.

La autoevaluación es interna e incorpora información reportada tanto por la alta gerencia como por el personal de la entidad. Esta información está referida a procesos, actividades, funciones y proyectos, tanto a nivel de unidades de negocio como de toda la organización. Además, se puede mantener actualizada a través de hojas de trabajo, reuniones y / o cuestionarios realizados con determinada frecuencia.

La implementación de esta técnica se facilita a través de una función específica encargada de coordinar el proceso para la identificación de los riesgos y los controles correspondientes. Esto se realiza a través de distintas etapas: identificación, evaluación, control y seguimiento).

- *Beneficios de la auto-evaluación*

Entre los principales beneficios de la auto-evaluación de riesgos destacan los siguientes:

- Permite entender los riesgos inherentes en los procesos de negocio.
- Evalúa la efectividad de los controles internos.
- Revela áreas prioritarias de trabajo.
- Acuerda planes de acción para tratar riesgos que excedan el nivel de riesgo tolerable. Por ejemplo, a través del tratamiento de debilidades identificadas en los controles internos.
- Permite adjudicar la propiedad de los riesgos y controles al personal mejor preparado para administrarlos.

MAPAS DE RIESGOS

La asignación o mapa de riesgos ("*risk mapping*") es el *proceso a través del cual se agrupan por tipo de riesgo las diferentes unidades de negocio, funciones organizativas o procesos*. Esta técnica puede dejar al descubierto ámbitos que presenten deficiencias así como ayudar a determinar las prioridades para su gestión.

Se puede ejecutar de forma indistinta a un nivel alto o bajo con el objetivo de identificar qué falla en un proceso determinado y sus resultados pueden ser representados visualmente a través de un diagrama de flujo de proceso o de un mapa de riesgos.

En la siguiente ilustración, se observa un gráfico conocido como “heat map”. Los colores se representan en función de la tolerancia al riesgo de la entidad y el resultado es una herramienta gráfica muy simple que permite resaltar aquellos riesgos que requerirían ser rápidamente mitigados.

FRECUENCIA

| | | | | |
|------------------------|---------------------------|---------------------|-------------------|-------------------------|
| CASI SEGURO (4) | 4 | 8 | 12 | 16 |
| PROBABLE (3) | 3 | 6 | 9 | 12 |
| RARO (2) | 2 | 4 | 6 | 8 |
| CASI NULA (1) | 1 | 2 | 3 | 4 |
| | INSIGNIFICANTE (1) | MODERADO (2) | FUERTE (3) | SIGNIFICANTE (4) |

SEVERIDAD

Fuente: UNESPA. Congreso “Riesgo Operacional”.

El objetivo del mapa de riesgos es revisar y diagnosticar el sistema de control interno existente en la entidad mediante la identificación de los principales riesgos a los que están expuestas las actividades realizadas, los controles existentes para mitigarlos y las oportunidades de mejora en el proceso de gestión del riesgo.

Para su construcción se fijan dos ejes de forma bidimensional: uno asociado a la frecuencia y otro a la intensidad o severidad de ocurrencia de los riesgos. La determinación de ambas variables se realiza a partir de la opinión de expertos o de datos históricos y se calcula para cada riesgo un par ordenado de frecuencia en intensidad. Con ello se obtiene el mapa de puntos que constituirá el mapa de riesgos.

Una vez identificados los puntos de riesgo, se procede a la construcción del “heat map” en base a la estimación del riesgo de cada punto numerado y con un código de color.

La dificultad reside en que es necesario disponer de unos adecuados programas informáticos que permitan el control efectivo en tiempo real. Para ello, dicho proceso se verá apoyado por los *Key Risk Indicators* (KRI), que se explican a continuación.

Una vez obtenido el mapa de riesgos residual se aplicará la política de planes de acción que establezca la entidad para su tratamiento.

Debido a la importancia que en la gerencia, especialmente del riesgo operacional, tiene el mapa de riesgos se dedica un anexo especial a la elaboración y desarrollo del mismo. Con ello se persigue comprender en qué consiste esta herramienta cualitativa y cómo se lleva a la práctica empresarial ya que es una técnica de administración muy empleada en cualquier entidad financiera y, particularmente, en el sector asegurador.

VENTAJAS DEL MAPA DE RIESGOS

El mapa de riesgos, además de ser una herramienta de gestión y control eficiente aporta otras ventajas a la organización entre las que destacan las siguientes:

- **Potencia la cultura de riesgos y controles** en la organización promoviendo en los empleados la comprensión de los riesgos del negocio y su responsabilidad en el proceso de mitigación a través del control interno.
- **Promueve una continua reflexión crítica** motivando a las unidades de negocio al diseño, construcción y mantenimiento de mejores sistemas de controles efectivos.
- **Contribuye a aumentar la cantidad y calidad de información** fiable sobre la situación de control de los riesgos existentes.
- Contribuye a dar **solidez al sistema de control interno** y, con ello, a minimizar la desconfianza sobre auditorías a posteriori requeridas por los sistemas de control.
- Permite poner el **enfoque en los riesgos más significativos** para la entidad y a disminuir los costos en revisiones recurrentes.
- Un sólido sistema de identificación y gestión de riesgos puede contribuir también a **reducir costes**.

CONDICIONES PREVIAS A LA ELABORACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos se elabora una vez que se han cumplido unas condiciones previas y necesarias para asegurar la efectividad de la herramienta y que la situación reflejada en se corresponda con la realidad.

- **Establecer el ámbito en el que se va a desenvolver el análisis:** identificar el alcance del trabajo en dos vertientes; la correspondiente a la clasificación por áreas de la entidad objeto de análisis y la referente a la tipología de riesgos presentes en las actividades desarrolladas por la entidad.

- **Identificar los riesgos** a los que están expuestas las distintas actividades, considerando no sólo la experiencia histórica de aquellos eventos que se hayan materializado en un problema económico sino cualquier posibilidad de sufrir alguno.
- **Evaluar los riesgos:** una vez identificados todos los riesgos potenciales, se establece una valoración que permita priorizar según su relevancia. Dicha evaluación tiene que ir acompañada de un análisis de los controles establecidos para mitigar los riesgos con el objeto de conocer la verdadera exposición de la entidad a los mismos.
- **Gestionar los riesgos:** se establecen, por un lado, las prioridades necesarias y, por otro, planes con las medidas correctoras que se consideren adecuadas para los riesgos más relevantes.

INDICADORES DE RIESGO CLAVES (KRI)

Los *KRI* (*Key Risk Indicator*) son *parámetros o indicadores que permiten predecir los cambios en el perfil de riesgos de la compañía de seguros*. Por lo tanto, propician la realización de las correcciones necesarias, favoreciendo el proceso de realimentación y control.

Los componentes de un *KRI* están constituidos por una determinada variable de riesgo a controlar, una unidad de medida y un intervalo que permita mostrar la posición de alarma o no frente a un determinado riesgo. Para todo ello, será básico un adecuado *reporting* de los riesgos con el objetivo de medir, controlar y solucionar posibles desviaciones en los márgenes fijados.

Los indicadores de riesgo se clasifican en dos categorías:

- **Indicadores específicos** que se asocian directamente a un proceso dentro de un área de actividad en concreto.
- **Indicadores generales** que afectan a la entidad en su conjunto y que se reflejan, por ejemplo, en el volumen de negocio.

Para la construcción de un indicador de riesgo se parte bien de datos históricos de pérdidas operacionales obtenidos a partir de procesos de autoevaluación de riesgos o de auditorías internas o externas.

Una vez implementados los niveles de alerta de un *KRI* los baremos suelen recalibrarse de manera periódica, hasta que se garantice su efectividad.

VENTAJAS DE LOS KRI

Los indicadores de riesgo presentan numerosas ventajas, entre las cuales destacan las siguientes:

- Permiten establecer **niveles de riesgo actuales**, a través de medidas precisas del estado de un riesgo identificado y la efectividad para su control.
- Son útiles para el **control del riesgo operacional** permitiendo acciones preventivas o que minimicen pérdidas materiales al posibilitar una acción temprana.
- Posibilitan **detectar tendencias y cambios** en el nivel de riesgo.
- Ofrecen **señales de alerta temprana** al hacer resaltar los cambios en el entorno, eficiencia de los controles y exposición a riesgos potenciales antes que se materialicen.

Los KRI contribuyen a la toma de decisiones a través del establecimiento de umbrales mínimos y rangos de tolerancia para los diversos riesgos; ambos deberían ser definidos por las máximas autoridades. Estos límites se ajustan, posteriormente, para ser alineados con la dinámica del entorno de negocios.

TARJETAS DE PUNTUAJE O “SCORECARDS”

La técnica de tarjetas de puntaje (“scorecards”) se refiere a un *conjunto de sistemas para la medición del riesgo operacional que tienen en común la evaluación de los generadores de riesgo, la evaluación de la amplitud y calidad del ambiente interno de controles de riesgos, todo ello a través del uso de cuestionarios.*

La metodología de tarjetas de puntaje también suele ser conocida como “Risk Drivers and Control Approaches” (RDCA). Estos cuestionarios consisten en una serie de preguntas ponderadas y basadas en el nivel de riesgo de la línea de negocio consultada; permiten trasladar evaluaciones cualitativas a una métrica cuantitativa.

El cuestionario está diseñado de tal manera que refleja el perfil de riesgos único de la entidad lo que se logra a través del diseño de preguntas específicas para la organización, la calibración de las respuestas y la aplicación de ponderadores y puntajes alineados con la importancia relativa del riesgo para la entidad. Las tarjetas son, habitualmente, completadas por personal de línea y están sujetas a revisión por una función centralizada de control de riesgos.

Asimismo, su participación potencia el desarrollo colectivo del conocimiento del riesgo operacional al involucrar también a los especialistas de los riesgos clave. Además, suele ser muy útil ya que motiva a cada unidad de negocios a pensar en los riesgos operacionales a los que se ven expuestas.

Un aspecto importante es que evalúa el riesgo operacional al momento de detectarse las debilidades y vulnerabilidades, es decir, cuando la probabilidad de ocurrencia es alta.

Por otra parte, el RDCA responde rápidamente a cambios en el entorno de negocios o a la aparición de nuevos riesgos operacionales permitiendo acomodar los nuevos riesgos a medida que van surgiendo; agregando preguntas o cambiando otras sin necesidad de esperar a que se materialicen las pérdidas. Por su diseño, las metodologías

RDCA están totalmente alineadas con el marco de gestión de la entidad, vinculando en consecuencia la medición con el seguimiento del mismo.

Las entidades podrían utilizar esta técnica para asignar el nivel de capital económico que corresponde a cada línea de negocio dependiendo de los resultados de la gestión y control de diversos aspectos del riesgo operacional. La directa vinculación entre el capital económico y el desempeño de las gerencias ofrece fuertes incentivos para realizar mejoras en la gestión del riesgo operacional, al centrar los esfuerzos de las unidades de negocio en mitigar el riesgo y mejorar los controles internos.

Las tarjetas de puntaje pueden ser utilizadas como una herramienta de seguimiento del riesgo operacional facilitando una serie de controles al combinar KRIs en la evaluación, reporte de impacto de nuevos controles y otros cambios en el ambiente operativo de la entidad.

PRUEBA DE ESTRÉS:

PRUEBA DE SENSIBILIDAD Y ANÁLISIS DE ESCENARIOS

Este tipo de pruebas permiten a la organización comprender mejor sus riesgos y actuar de forma más eficaz ante situaciones potenciales extremas.

El stress testing o pruebas de estrés hace referencia a la variación o cambio de los parámetros individuales que pueden afectar a la posición financiera de la entidad. Un ejemplo de una prueba de estrés es una elevada rotación en los empleados.

Las pruebas de estrés son herramientas aplicadas en instituciones financieras y de seguros con el objetivo de valorar su nivel potencial de vulnerabilidad económica y financiera cuando se producen determinados eventos excepcionales, pero factibles. A través de ellas, las compañías de seguros pueden mejorar la gestión de sus riesgos para mantener los recursos financieros adecuados mediante la identificación y la cuantificación de diferentes escenarios complejos sobre posiciones financieras futuras esperadas.

Dichas pruebas estiman el impacto que la ocurrencia de perturbaciones adversas excepcionales, pero posibles, puede tener sobre aquellas variables que afectan a los resultados y a la solvencia de un asegurador o un grupo de compañías de seguros.

Esta herramienta comprende dos tipos de análisis, uno de sensibilidad y otro de escenarios, cuyo objetivo es que los aseguradores dispongan de un mayor número de datos que les permitan entender las vulnerabilidades a las que han de hacer frente en situaciones atípicas, con baja probabilidad de ocurrencia, derivadas de riesgos, en este caso operacionales, que pueden tener un impacto económico negativo para el asegurador.

PRUEBAS DE SENSIBILIDAD

Las pruebas simples de sensibilidad se utilizan para determinar el impacto en una unidad de negocios de la aseguradora, derivado de un movimiento adverso en el factor

que define un determinado riesgo o en un pequeño número de factores de riesgo que presentan una elevada correlación entre sí, sobre las condiciones financieras futuras del asegurador.

ANÁLISIS DE ESCENARIOS

El análisis de escenarios cuantifica el efecto de una variación simultánea en diversos factores de riesgo. Los escenarios definidos para llevar a cabo estas mediciones pueden basarse en eventos significativos ocurridos en el pasado (escenario histórico), o en la estimación de las consecuencias de un evento que aún no hayan ocurrido (escenario hipotético).

Los primeros reflejan los cambios en los factores de riesgo que se han producido en determinados momentos de la historia. La forma más simple de definir estos escenarios es identificando periodos específicos de tiempo que fueron, particularmente, extremos en términos de volatilidad o variabilidad de los factores de riesgo y observando los efectos que ocasionaron en las aseguradoras. De esta manera, una vez valoradas todas las consecuencias derivadas del shock ocurrido en el pasado, se traslada al presente y se aplica a la situación actual de la entidad cuantificando el efecto y las consecuencias, tanto en la entidad como en la totalidad del mercado asegurador analizado.

Los escenarios hipotéticos, en cambio, están basados en un conjunto de situaciones que se sabe que pueden producirse pero que todavía no han ocurrido.

Para llevar a cabo un diseño óptimo de esta herramienta, el asegurador debe demostrar que los riesgos incluidos en el riesgo operacional han sido considerados y que existen planes y procedimientos apropiados para un manejo adecuado de los mismos.

Es importante desarrollar estas medidas ya que permiten llevar a cabo una evaluación del impacto, financiero y no financiero, asociado a elevadas pérdidas no esperadas pero posibles.

La importancia de implementar estas técnicas reside en que:

- Se vinculan, directamente, con el proceso de gestión y promueven una sana administración del riesgo.
- El proceso de evaluación y análisis de los factores de riesgo permite una mayor comprensión de los riesgos operacionales y proveen información importante para mejorar la gestión y el control.
- Capturan cambios en el perfil de riesgos de la entidad y/o en la estructura organizacional.
- Evalúan el impacto financiero y no-financiero de eventos extremos con grandes pérdidas inesperadas.

- Ayudan a determinar el perfil global de riesgos de la entidad y a establecer el apetito por riesgo dada su capacidad de asumirlo.
- Permiten validar modelos y los análisis estocásticos realizados, como así también la calibración de las hipótesis del modelo.
- Proveen información para la determinación del capital económico y son un elemento integral del marco de administración de riesgos de la entidad.

Cuantificación del Riesgo Operacional

La cuantificación del riesgo operacional en el sector asegurador europeo es un aspecto de vital importancia y envergadura, tanto por su aplicación en el ámbito de Solvencia II como en la evaluación de la efectividad de los sistemas de control interno en las entidades.

La implantación gradual de la de gestión y cuantificación del riesgo operacional requiere una infraestructura que permita recopilar eventos históricos, tanto individuales como sectoriales, en un horizonte temporal prolongado.

Diariamente, en la industria bancaria se procesan millones de transacciones; por lo tanto, el número de datos disponibles sobre pérdidas derivadas de fallos operacionales es muy elevado. Este tamaño muestral posibilita el desarrollo de un modelo de frecuencia e intensidad que permite evaluar la función de distribución de las pérdidas provocadas por este riesgo y las necesidades de capital para cubrir las.

Desde el punto de vista asegurador, como se ha definido en ocasiones anteriores, el riesgo operacional se asocia a los fallos derivados de la falta de adecuación de los procesos internos, de las personas, de los sistemas, o como consecuencia de eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional.

En este sentido, a pesar de no incluir el riesgo reputacional en la definición, en muchas ocasiones las pérdidas operacionales elevadas provocan la aparición, el desarrollo y la intensificación de este tipo de riesgo.

Así, es evidente la importancia del riesgo operacional en el sector asegurador. Sin embargo, a causa de la falta de suficientes datos cuantitativos, es complejo identificar este tipo de riesgo dentro de los datos de experiencia de pérdidas recogidos típicamente para los riesgos de suscripción, crédito y mercado.

El tratamiento del riesgo operacional en el marco de Solvencia II implica obligaciones cuantitativas de capital, a través del cálculo de los requerimientos de capital o SCR (*Solvency Capital Requirement*) y de los requerimientos cualitativos, relativos al proceso de revisión supervisora enmarcados en el Pilar II.

Cálculo del Requerimiento de Capital de Solvencia -SCR-

El CEIOPS ha elaborado un modelo de SCR siguiendo un esquema de identificación de los distintos riesgos a los cuales se enfrentan las aseguradoras. De esta forma, se estima convenientemente el requerimiento de capital global de cada compañía.

La determinación del *Solvency Capital Requirement* se debe realizar teniendo en cuenta los principales riesgos de la actividad aseguradora y la aproximación de la pérdida máxima posible que, en su conjunto, podría manifestarse en un horizonte temporal de un año con una probabilidad de un 99,5%. Esto se recoge en el cuarto estudio de impacto cuantitativo “QIS 4”.

El objetivo de este requerimiento es, básicamente, cubrir las pérdidas inesperadas; las esperadas ya deben estar adecuadamente recogidas en el valor de las reservas técnicas. De no cumplirse con el nivel exigido se le demandará a la compañía restablecer su capital hasta el nivel óptimo de SCR, de acuerdo a un plan de adecuación que necesita ser aprobado por los supervisores.

En sus comienzos, el CEIOPS sugirió el uso de intervalos al 99,5% con un horizonte de un año equivalente a una probabilidad de impago del 0,50% y proponía en una primera instancia el uso del TVaR⁴⁷.

El TVaR presenta las siguientes ventajas respecto al VaR:

- Considera no sólo la probabilidad de insolvencia sino también la pérdida esperada por la **insolvencia**.
- En el VaR las pérdidas más allá del umbral de confianza no se contemplan a la hora de dotar el capital.
- El TVaR es subaditivo, es decir, las exigencias de capital por dos o más riesgos combinados son menores que las exigencias asociadas a cada uno por separado. Esta propiedad no se da con generalidad en el VaR, sobre todo en casos de colas muy pesadas o en distribuciones muy asimétricas.

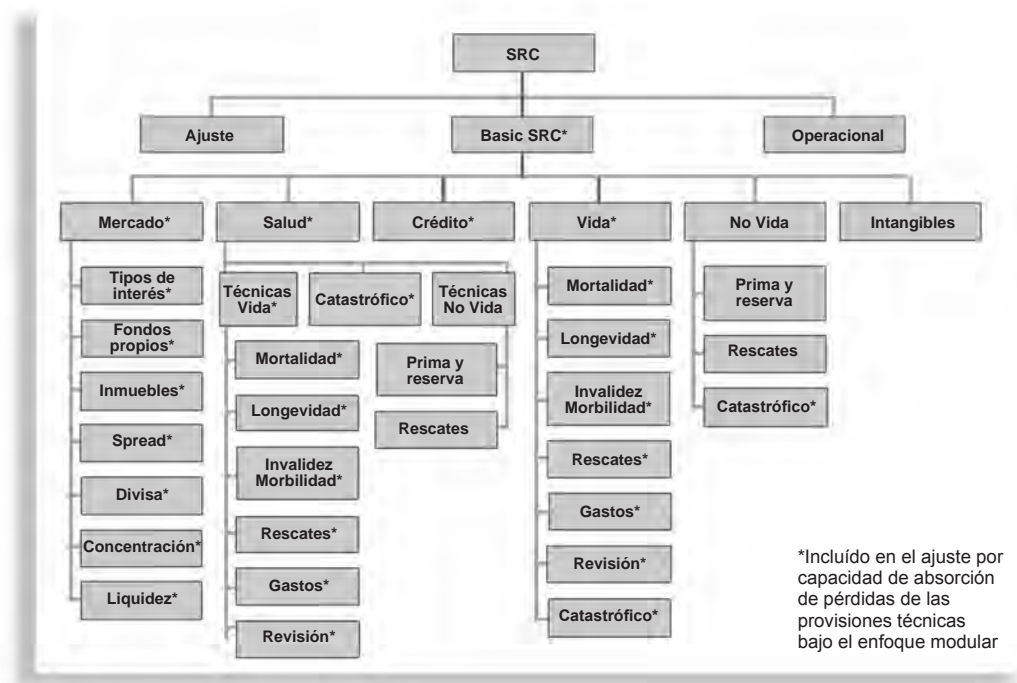
Finalmente, el CEIOPS se inclinó por la aplicación del VaR y su utilización al 99,5% bajo un horizonte temporal de un año.

Se prevé que la determinación de esta cantidad se pueda hacer bien mediante el uso de un *modelo estándar* o mediante el uso de *modelos internos* desarrollados por las propias compañías aseguradoras. Solvencia II permite el uso de modelos propios siempre que estos sean, previamente, aprobados por las autoridades reguladoras.

⁴⁷ **TVaR:** Valor de la cola en situación de riesgo, también conocido como *cola de espera condicional* (en inglés TCE), es una medida de riesgo asociados con el valor más general en situación de riesgo.

Modelo Estándar

Según los últimos trabajos del CEIOPS los riesgos seleccionados, y que deberán ser valuados para poder calcular los requerimientos de capital, son los de mercado, crédito, suscripción en vida, suscripción en no vida, suscripción en salud y riesgo operacional.



Fuente: CEIOPS.

Los cinco primeros riesgos son los que se han definido como el capital básico de solvencia, a dicha cifra se le suma la correspondiente al riesgo operacional, ciertos ajustes, y se obtiene el SCR.

Cabe destacar que el modelo estándar no supone independencia de los riesgos, por lo tanto, la agregación no es de forma lineal sino que se tiene en cuenta la posible correlación entre los riesgos.

A raíz de ello es que el **SCR** se obtiene como:

$$SCR = \sqrt{\sum_{i=1}^N \sum_{j=1}^N C_{ij} SCR_i SCR_j}$$

Dónde:

- **SCR** = es la cifra de capital asociada al riesgo *i/j* - ésimo
- **N** = es el número de riesgos analizados.
- **C** = es el coeficiente de correlación entre los riesgos *i* y *j*

El cálculo del SCR se realiza mediante la elaboración de un mapa de riesgos que diferencia entre módulos y submódulos de riesgos.

Para cada uno de esos elementos básicos se calcula la cantidad de capital correspondiente y, teniendo en cuenta la interrelación dentro de cada módulo de riesgo, se procede a calcular el SCR de ese módulo.

Los subriesgos que se pretenden evaluar son:

- Para el **módulo de mercado**, los riesgos de tipos de interés, renta variable, inmuebles, diferenciales de tipos, concentraciones de riesgos y divisa.
- Para el **módulo de suscripción en vida** encontramos los riesgos por revisión de cláusulas, mortalidad, longevidad, discapacidad, suspensión de pólizas, gastos y catástrofes.
- Para el **módulo de salud**; los riesgos de salud de corto plazo, riesgo de salud de largo y riesgo de compensación de trabajadores.
- Para el **módulo de no vida**, los riesgos de primas y reservas, más el asociado a catástrofes.
- Los módulos de **crédito** y **operacional** no tienen subriesgos.

De esta manera, el SCR total se define como la suma del SCR Básico más el SCR Riesgo Operacional corregido con los ajustes oportunos.

$$SCR = SCR_{BÁSICO} + SCR_{OPERACIONAL} - Ajustes$$

Este trabajo no está enfocado a analizar cada uno de los módulos y submódulos que componen el SCR y su forma de cálculo. Por lo tanto, se define brevemente en qué consiste el SCR básico y los ajustes.

Sin embargo, el aspecto más relevante de este apartado lo ocupa el cálculo del requerimiento de capital por riesgo operacional, *SCR operacional*.

SCR BÁSICO

El SCR Básico se define como la suma ponderada de los distintos módulos de riesgos contemplados para el SCR -SCR No vida, SCR Mercado, SCR Salud, SCR Riesgo de Contraparte y SCR Vida- y minorada en la suma ponderada de los SCR que corresponde a los distintos mecanismos de mitigación de riesgos y al negocio futuro que se haya agregado para la captura de riesgos.

AJUSTES

Solvencia II contempla la realización de ciertos ajustes al BSCR. Estos son los referidos a los requerimientos de capital brutos provenientes de la existencia de impuestos diferidos en el balance de la compañía y los ajustes por la capacidad de absorción de riesgos, efecto de futuras ganancias compartidas por parte de las compañías.

REQUERIMIENTO DE CAPITAL PARA EL RIESGO OPERACIONAL

El artículo 105 de la Directiva de Solvencia II recoge cómo se constituye el requerimiento de capital por riesgo operacional. Así, establece que:

1. *El requerimiento de capital por riesgo operacional abordará los riesgos operacionales en la medida en que no hayan sido incluidos en los módulos (...) que se han enumerado anteriormente.*
2. *El requerimiento de capital por riesgo operacional relativo a contratos de seguros de vida, en los que el riesgo de inversión es asumido por los tomadores, se calcula en función del importe anual de gastos contraídos respecto de esas obligaciones.*
3. *Respecto de todas las demás operaciones de (re)aseguradoras, el requerimiento de capital por riesgo operacional se calculará en función del volumen de estas operaciones, en términos de primas devengadas y provisiones técnicas dotadas en relación con tales obligaciones por (re)aseguradoras.*

En este caso, el requerimiento de capital por riesgo operacional no será superior al 30% del SCR básico correspondiente a las citadas operaciones de (re)aseguradoras.

La fórmula estándar para el cálculo del **SCR operacional** es la siguiente:

$$SCR_{OP} = \min \{0.30 * BSRC; OP_{in\ ul}\} + 0.25 * Exp_{ul}$$

Dónde:

- **BSRC** = SCR básico.
- **OP_{in ul}** = consumo de capital básico de riesgo operacional para todos los negocios, salvo unit-linked.
- **EXP_{ul}** = total de gastos anuales incurridos en el negocio unit-linked (brutos de reaseguro).

A continuación desarrollamos el **OP_{in ul}** como:

$$OP_{in\ ul} = \max \{oppremiums; Opprovisions\}$$

Dónde:

- **Oppremiums** = primas asociadas al riesgo operacional.
- **Opprovisions** = provisiones asociadas al riesgo operacional.

Las **primas asociadas al riesgo operacional** las calculamos como:

$$\begin{aligned} oppremiums = & 0.04 * (Earn_{life} + Earn_{SLT_{healt}} - Earn_{life-ul}) + \\ & 0.03 * (Earn_{nl} + Earn_{NonSLThea}) + \\ & Max(0, 0.04 * (\Delta Earn_{life} - \Delta Earn_{life-ul})) + \\ & Max(0, 0.03 * (\Delta Earn_{non-life})) \end{aligned}$$

Siendo cada uno de los factores que intervienen los siguientes:

- $Earn_{life}$; Primas brutas de vida, incluyendo unit-linked
- $Earn_{SLT_{healt}}$; Primas brutas de salud
- $Earn_{ul-life}$; Primas brutas del negocio unit-linked
- $Earn_{ul}$; Primas bruta de no vida
- $Earn_{NonSLT_{hea}}$; Primas devengadas de las obligaciones del seguro de salud que no se ejercen con bases técnicas similares a las del seguro de vida
- Δ : cambio en las primas devengadas desde el año t-1 a t, incrementos que han superado el 10%. No se permitirá compensar entre vida y no vida.

Las **provisiones asociadas al riesgo operacional** las calculamos como:

$$\begin{aligned}
 Oprovisions = & 0.0045 * (TP_{life} + TPSLT_{healt} - TP_{life-ul}) + \\
 & 0.030 * (TP_{nl} + TP_{NonSLT_{healt}}) + \\
 & Max(0, 0.045 * (\Delta TP_{life} - \Delta TP_{life-ul})) + \\
 & Max(0, 0.03 * \Delta TP_{non-life})
 \end{aligned}$$

Siendo cada uno de los factores que intervienen los siguientes:

- TP_{life} : Provisiones técnicas brutas de vida (sin deducción del reaseguro), incluyendo unit-linked
- $TP_{SLT_{healt}}$: Provisiones técnicas brutas de salud
- $TP_{ul-life}$: Provisiones técnicas brutas del negocio unit-linked
- TP_{nl} : Provisiones técnicas brutas de no vida
- $TP_{NonSLT_{Hea}}$: Provisiones técnicas brutas de las obligaciones del seguro de salud que no se ejercen con bases técnicas similares a las del seguro de vida
- Δ : cambio en las primas devengadas desde el año t-1 a t, incrementos que han superado el 10%. No se permitirá compensar entre vida y no vida

Modelos internos

Solvencia II prevé la posibilidad de emplear modelos internos para la determinación del SCR por parte de las compañías aseguradoras. Estos pueden ser de dos tipos: completos o parciales.

Las finalidades de un modelo interno son varias: analizar la posición global de riesgo de una entidad, cuantificar el mismo y determinar el requerimiento de capital económico en base al perfil específico de la entidad y al nivel de solvencia definido por el regulador.

Los modelos internos **completos** deben evaluar, como mínimo, los mismos riesgos sometidos en el modelo estándar; mientras que los modelos internos **parciales** podrían ser utilizados, por ejemplo, para estimar únicamente el riesgo de vida.

Cuando la entidad gestione y mida sus riesgos conforme a un modelo diferente del subyacente en la fórmula estándar el modelo interno podrá ser reconocido por el supervisor para cuantificar los requerimientos de capital. Solicitada la aplicación de un modelo interno el supervisor dispone de un plazo establecido para la aprobación o no de dicho modelo.

Solvencia II refleja la importancia de la realización de test de uso de calidad estadística, la calibración del modelo interno y su documentación. Además, establece que al menos durante dos años la compañía aseguradora deberá comparar el SCR según el modelo y el SCR estándar.

Cabe la posibilidad de usar otras medidas de riesgo distintas del VaR, al igual que horizontes temporales distintos de un año, siempre y cuando se garantice un nivel de protección mínimo equivalente al 99.5% VaR a un año.

Un aspecto clave en la construcción de un modelo interno son las hipótesis sobre las que se define. En general, deben estar basadas en la propia experiencia de la entidad y han de tener en cuenta aspectos sobre la estructura del modelo, productos y aspectos económicos, entre otros.

Los resultados de auditoría interna deben ser reportados y la documentación tiene que confirmar que el modelo ha cumplido las hipótesis de partida. En general, se aplica el principio de que la documentación aportada debe ser lo suficientemente clara como para que expertos independientes fueran capaces de reproducir los outputs obtenidos por el modelo, si dispusieran de los datos acerca de los parámetros y las exposiciones al riesgo de la entidad.

MODELIZACIÓN ACTUARIAL

En el caso de que se disponga de una base de datos histórica sobre pérdidas provocadas por riesgos de tipo operacional se podrá recurrir a la modelización actuarial ya que, a través de ella, se calcula la distribución de las pérdidas agregadas a partir de los eventos individuales. Dicha distribución se obtiene del número de siniestros y de las pérdidas individuales asociadas a cada siniestro.

La evidencia empírica señala que la frecuencia de eventos de tipo operacional se suele modelizar utilizando distribuciones discretas, tales como la distribución de Poisson, la distribución binomial o la distribución binomial negativa, entre otras, no descartando la mixtura de distribuciones.

La compañía de seguros deberá calcular el VaR Operacional con vistas a desarrollar sus modelos internos en el marco de Solvencia II.

Las metodologías de simulación del VaR son múltiples y deberán recoger las correlaciones entre los diferentes tipos de riesgos así como la estimación de frecuencias y severidades conjuntas.

Para llevar a cabo el cálculo del VaR operacional es necesario conocer la tendencia del número de eventos en un año teniendo en cuenta la estructura y el tamaño de la organización. Este procedimiento implica descubrir la relación entre el tamaño de la organización y la frecuencia de pérdidas históricas y ajustar, posteriormente, dichas pérdidas a la situación actual.

Para el caso de la modelización de la intensidad, severidad o cuantía de las pérdidas operacionales se suelen utilizar las distribuciones continuas lognormal, Weibull, Pareto y Beta. En muchos casos, los datos sobre pérdidas operacionales deben ser recolectados en forma de márgenes o intervalos. El resultado de este tipo de recolección de datos da lugar a muestras que se corresponden con una distribución de la severidad de los siniestros truncada; el ajuste se realiza a través de distribuciones como la Distribución Generalizada de Pareto.

En estos casos, la Teoría del Valor Extremo ofrece una aproximación paramétrico-estadística para valores de pérdidas extremos que permite ajustar las pérdidas derivadas de riesgo operacional a una *GPD* (Distribución de Pareto Generalizada), que, de forma genérica, modeliza la distribución de los valores que exceden de un umbral o prioridad determinado, es decir, la distribución condicionada a que los datos excedan de un determinado nivel.

Las fases que se tienen que desarrollar para aplicar la teoría del valor extremo al riesgo operacional son las siguientes:

- **Recopilación de datos** de pérdidas por encima del límite fijado.
- **Ajuste del exceso** de las cuantía de pérdidas asociadas a datos derivados de riesgos operacionales a una *GDP*, usando máxima verosimilitud u otra técnica de ajuste.
- **Ajuste de los datos** de frecuencia de pérdidas operacionales a una función de distribución de Poisson, usando el método de los momentos u otra técnica de ajuste.
- **Simulación de Montecarlo** para generar la función de distribución de pérdidas para un horizonte temporal determinado.

Por otra parte, para el cálculo del *VaR Operacional* se utilizan tres métodos:

- simulación,
- algoritmo recursivo de Panjer
- o aproximación computacional.

Estos métodos son conocidos por la ciencia actuarial pero, al aplicarlos para la cuantificación de pérdidas operacionales, tienen que ser evaluados y comparados con objeto de tomar las mejores decisiones asociadas a la situación concreta. Dicha técnica se selecciona en función de qué método se aproxime mejor a la realidad en el escenario central.

Por último, dentro de esta fase conviene destacar la teoría Delta-ETV que es una combinación de la teoría de valores extremos y de la metodología Delta. En la metodología Delta se plantea un modelo para la gestión de ORM en el que se asocian las ganancias de la entidad a determinados factores causales; tiene la cualidad de asociar dichos factores causales a diferentes unidades de negocio, con lo que es útil en el ámbito de ORM.

Métodos de cálculo

La crisis ha provocado grandes desafíos para cualquier sector y, particularmente, para el sector financiero. Esta situación supone, para muchas empresas, la revisión de sus modelos atendiendo a aspectos como el capital económico. Sin embargo, no se prevé un cambio fundamental en los marcos metodológicos de los modelos de capital económico de Solvencia II.

Solvencia II, establece una serie de métodos de cálculo, para los requerimientos de capital mínimos por riesgo operacional, sin tener en cuenta la experiencia pasada hasta que se haya generado una base de datos suficiente para poder llevar a cabo la aplicación de técnicas más ajustadas.

Dichos métodos son tres:

- Método del indicador básico.
- Método estándar.
- Métodos de medición avanzada.



Fuente: CEIOPS.

Método del indicador básico

El *método del indicador básico* se fundamenta en la cobertura del riesgo operacional a partir de un capital que equivalga al promedio de los tres últimos años de un porcentaje fijo de los ingresos anuales brutos positivos de la compañía.

Para determinar esta media no pueden considerarse los datos de cualquier año en el que el ingreso bruto anual haya sido negativo o igual a cero.

$$K_{BIA} = \frac{\sum (Gl_{1...n} * \alpha)}{n}$$

Dónde:

- **K**: determina la exigencia del capital en el método del indicador básico.
- **Gl**: son los ingresos anuales medios cuando sean positivos de los tres últimos años.
- **n**: es el número de años (entre los tres últimos) en los que los ingresos brutos han sido positivos.
- **α**: es el parámetro que relaciona el capital exigido al conjunto del sector con el nivel de indicador en el conjunto del sector.

Método estándar

En el *método estándar* la exigencia de capital se establece como la media de tres años de la suma de las exigencias de capital regulador en cada una de las líneas de negocio de la compañía cada año. Para un año determinado, las exigencias de capital negativas, que resultan de ingresos brutos negativos en cualquiera de las líneas de negocio, pueden compensar las exigencias positivas en otras líneas de negocio sin límite alguno.

No obstante, cuando el requisito de capital agregado para todas las líneas de negocio, dentro de un año concreto, sea negativo el argumento del numerador para ese año será cero.

El requerimiento total de capital viene definido como:

$$K_{TSA} = \frac{\sum_{j=1}^3 (\max [Gl_{1-n}^i * \beta_{1-n}; 0])}{3}$$

Dónde:

- **K**: determina la exigencia del capital en el método estándar.
- **Gl**: son los ingresos brutos para cada i y para cada una de las n líneas de negocio de la compañía.
- β_{1-n} : es un porcentaje fijo que relaciona la cantidad de capital requerido con el ingreso bruto de cada una de las líneas de negocio.

Métodos de Medición Avanzada (AMA)

En los *métodos de medición avanzada* –AMA- la exigencia de capital regulador será igual a la medida de riesgo generada por el sistema interno de la compañía para calcular el riesgo operacional, utilizando los criterios cuantitativos y cualitativos aplicables a estos métodos y detallados en el documento *Convergencia internacional de medidas y normas de capital*⁴⁸, desarrollado por el Comité de Supervisión Bancaria de Basilea.

La utilización de los AMA está sujeta a la aprobación del supervisor. En España, se están realizando los trabajos de adaptación para la configuración del Modelo de Cálculo del Capital Requerido por Solvencia II por medio de la constitución de grupos de trabajo conjuntos, que involucran tanto a las entidades (representadas a través de UNESPA) como al supervisor y a los organismos de investigación del sector (ICEA).

En Solvencia II, el cálculo de los requerimientos de capital está integrado en una estructura modular. En el enfoque estándar de cálculo no se incluye el efecto de las correlaciones en los riesgos, quedando abierto para el enfoque avanzado o de modelos internos. Además, en el Pilar II se contempla la realización de análisis de sensibilidad o pruebas de stress en la medición de riesgos.

⁴⁸ En febrero del 2004 el Comité de Supervisión Bancaria de Basilea publicó el documento “*Convergencia internacional de medidas y normas de capital*”.

Evaluación del Riesgo Propio y de Solvencia (O.R.S.A)

No se puede tratar el riesgo operacional en Solvencia II sin mencionar una herramienta menos conocida, pero no por ello menos importante, como es la evaluación del riesgo propio y de solvencia, O.R.S.A (del inglés, *Own Risk and Solvency Assessment*).

La Directiva de Solvencia II habla de ella en dos de sus artículos, el 45 para entidades individuales y el 246 relativo a grupos.

Estos describen una Evaluación del Riesgo Propio y de Solvencia (ORSA) como parte del sistema de gestión de riesgos de los aseguradores y reaseguradores que requiere la determinación de las necesidades de solvencia apropiadas. La información obtenida será reportada a las autoridades de supervisión y utilizada en la revisión del proceso supervisor.

En concreto, el artículo 45 describe el ORSA como una herramienta de la gestión de riesgos en la que las compañías de seguros y reaseguros evalúan sus riesgos en el corto y largo plazo y la cantidad de fondos necesarios para cubrirlos.

Al mismo tiempo, representa una importante fuente de información para la autoridad supervisora y la compañía aseguradora está obligada a describir los procesos que contempla.

Definición y alcance

Se define como el conjunto de procesos y procedimientos empleados para identificar, evaluar, monitorizar, gestionar y reportar los riesgos de corto y largo plazo que afronta o puede afrontar un asegurador y para determinar los Fondos Propios necesarios para asegurar que, en todo momento, se cumplen las necesidades de solvencia, incluyendo activos, provisiones técnicas, requerimientos regulatorios de capital (SCR y MCR), así como las necesidades internas de capital.

Su objetivo consiste en profundizar en el conocimiento de las interrelaciones entre los riesgos y las necesidades internas de capital. Para ello, puede emplear tanto la fórmula estándar como modelos internos para calcular el SCR.

Importancia de ORSA

Solvencia II es un modelo basado en el Riesgo y ORSA representa, fundamentalmente, el conocimiento y la opinión que un asegurador tiene de sus riesgos, necesidades de solvencia y fondos propios.

- La fórmula estándar para calcular el SCR podría no llegar a cubrir todos los riesgos a los que realmente está expuesto un asegurador. Esto no le debería eximir de la evaluación real de sus propios riesgos.

- El hecho de que coincidan los Fondos Propios con el perfil de riesgo favorece el fortalecimiento de la cultura de gerencia de riesgos.
- Los aseguradores necesitan establecer medidas apropiadas para monitorizar posibles cambios en la situación de los riesgos y como estos afectan a su nivel de capital y al acceso de fondos adicionales, si fueran necesarios.
- A través de la gestión conjunta de riesgos y capital ayuda a los aseguradores al cumplimiento de los requerimientos regulatorios de capital y de los objetivos de capital interno.
- Si el supervisor descubre cuestiones que hubieran debido ser reflejadas en ORSA y no ha sido así, no sólo debe tomar la acción pertinente sino también valorar la razón por la que dicho elemento no ha sido identificado por el asegurador.

Por otra parte, constituye un poderoso componente del Pilar II; enfatiza la gestión de riesgos como un procedimiento mediante el cual el consejo de administración pueda comprobar si dispone de un proceso de gestión del riesgo asociado a su plan estratégico y si este proceso funciona correctamente.

Así pues, esta autoevaluación desempeñará un rol importante en el sistema de gobierno y en el proceso de toma de decisiones de las compañías aseguradoras y reaseguradoras. Este rol debería reconocer los grandes desafíos existentes para integrar la gestión de riesgos y sus modelos correspondientes en el marco de ORSA.

Esta herramienta afecta a las organizaciones en su conjunto, es decir, a cada uno de los departamentos que la integran y a las diferentes funciones que se realizan. Por lo tanto, es necesario un amplio consenso para identificar qué es lo mínimo requerido para llevarla a cabo.

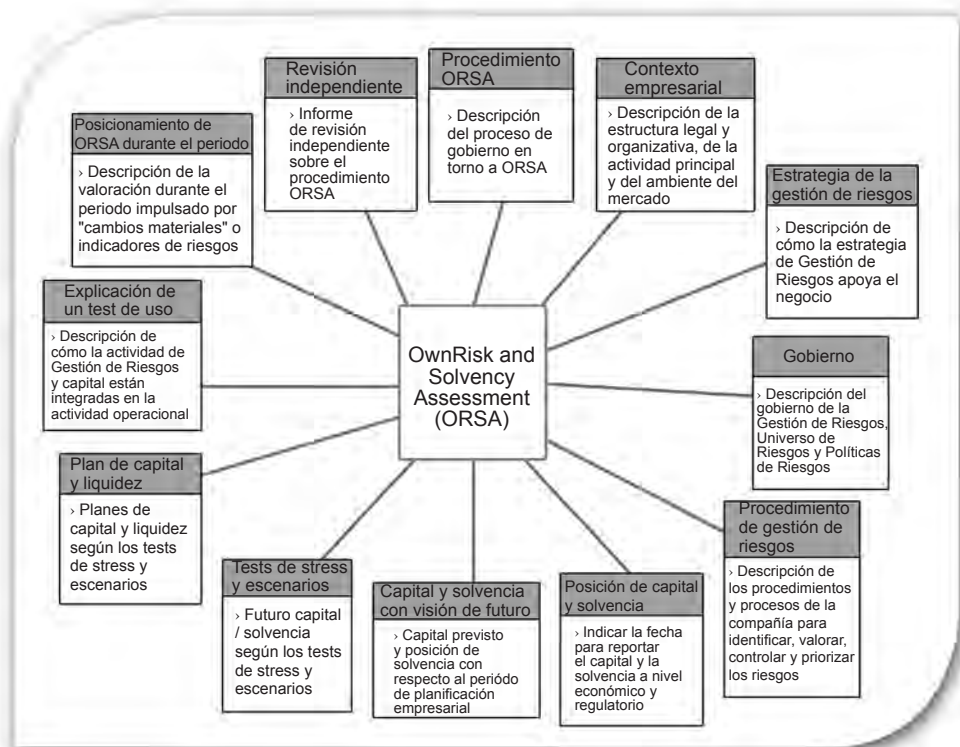
No obstante, con esta evaluación se proporciona una visión del capital económico que se le requiere a la compañía para que su negocio funcione conforme a un nivel de riesgo aceptado previamente.

Complejidad y evaluación del ORSA

En la figura siguiente, obtenida del Issues Paper de CEIOPS de Mayo de 2008 “*Own Risk and Solvency Assessment*”⁴⁹ y del documento elaborado en 2009 por Ernst & Young “*Unlocking the Mystery of the Risk Framework around ORSA*”⁵⁰, se observa la complejidad del ORSA y los grandes desafíos y retos que supondrá para auditoría interna evaluarlo en una compañía.

⁴⁹ Este documento trata la autoevaluación de riesgos y solvencia (ORSA) como el nuevo enfoque de la evaluación interna de riesgos y de capital.

⁵⁰ Este documento versa sobre cómo se estructura en las empresas ORSA alrededor del riesgo y sus implicaciones.



Fuente: Estudio Sector Asegurador en España 2010.

Esta herramienta está presente en todos los ámbitos de la organización y su integración en las diferentes parcelas empresariales está marcada por la evaluación que auditoría interna realice sobre:

- La descripción del proceso de gobierno que haya establecido la compañía.
- La estructura legal y organizativa de la compañía y de su actividad principal, así como el ambiente del mercado o mercados en los que opera la compañía.
- La estrategia de gestión de riesgos como apoyo al negocio.
- La política de riesgos así como el sistema de gobierno.
- Los procedimientos y procesos de la compañía para identificar, valorar, controlar y priorizar los riesgos.
- La posición de capital y de solvencia.

- Capital previsto y posición de solvencia respecto al periodo de planificación empresarial.
- Tests de stress y escenarios y planes de capital y liquidez según los tests de stress y escenarios.
- Explicación de los tests de uso o descripción de cómo la actividad de gestión de riesgos y de capital está integrada en la actividad.

Requerimientos

El *artículo 44* sostiene que la evaluación debe incluir al menos lo siguiente:

- La **necesidad global de solvencia** teniendo en cuenta el perfil de riesgo, límites de tolerancia aprobados y estrategia de negocio del asegurador.
- El **cumplimiento continuo** de los requerimientos de capital y requerimientos de provisiones técnicas.
- La medida en la que el **perfil de riesgo** del asegurador se desvía significativamente de los supuestos incluidos en el Solvency Capital Requirement, como establece el *Artículo 101*.
- El objetivo final es reforzar los procesos de **evaluación y monitorización** de las necesidades de solvencia global, no duplicar, validar o analizar la parametrización del cálculo de SCR.
- La **documentación** de política de gerencia de riesgos debe incluir los procesos ORSA, tal y como menciona el Artículo 41 de la Directiva.

Necesidad de solvencia global

El asegurador no sólo debe evaluar sus riesgos actuales debe realizar proyecciones de negocio como parte integrante de los planes financieros. En este sentido, es conveniente que identifique y tenga en cuenta factores externos que puedan afectar sus necesidades de solvencia global o Fondos Propios.

Es importante contar con perspectiva de mercado y de tendencias apoyándose, si se considera necesario, en expertos externos que mantienen la independencia necesaria.

El supervisor observará las bases de las proyecciones; la entidad tendrá que estar preparada para explicar y demostrar que los métodos y prácticas son apropiados.

Cumplimiento continuo

El asegurador es responsable de tener suficientes fondos propios aptos para cubrir el MCR y el SCR a lo largo del tiempo y, ORSA, debe incluir una evaluación al respecto. Asimismo, debe establecer procedimientos que le permitan estimar los cambios en sus requerimientos de capital y fondos propios aptos de manera recurrente.

Además, debe justificar la frecuencia del cálculo que depende de la volatilidad de las inversiones y del nivel de solvencia, conforme a su perfil de riesgo. En cualquier caso, si el perfil de riesgo cambia significativamente se volverá a calcular el requerimiento de capital y fondos propios.

La evaluación de las necesidades globales de solvencia debe realizarse tanto desde un punto de vista cuantitativo como cualitativo.

Evaluación del Perfil de Riesgo

ORSA incluirá un análisis de las diferencias, si existieran, entre el importe de los fondos propios calculados por el asegurador y los requerimientos del SCR.

La Directiva de Solvencia II permite a los aseguradores usar parámetros específicos para el cálculo de los módulos de Vida, No Vida y Suscripción Especial, sujetos siempre a la aprobación del supervisor.

El informe interno valorará la evaluación para transformar su resultado en la medida y calibración correspondiente al SCR. Se debe justificar la adecuación del modelo en el transcurso del tiempo.

Resultado del ORSA

Si el resultado de ORSA difiere, en cualquier dirección, de las cifras de SCR el asegurador debe poder explicar las razones e identificar el impacto en su cálculo.

El que el resultado sea superior no implica, automáticamente, que el supervisor imponga un aumento de capital para el SCR. Por otra parte, si el resultado es inferior los supervisores tampoco están autorizados a reducir la cifra de SCR aunque el asegurador demuestre que la fórmula estándar sobrevalora sus riesgos.

Integración en la estrategia del negocio

La Directiva, establece que será parte integrante de la estrategia de negocio y que será tenido en cuenta en todo momento en las decisiones del asegurador.

Frecuencia del ORSA

Los aseguradores y reaseguradores llevarán a cabo la evaluación sin ningún retraso consiguiente a cualquier cambio en su perfil de riesgo. Será el propio asegurador quien establezca su frecuencia, teniendo en cuenta su perfil de riesgo y debiendo justificar su adecuación.

Reporte de la información

El *Artículo 45.6 de la Directiva* establece que el asegurador y, en su caso, reasegurador informará a las autoridades de supervisión de los resultados como parte de la información a reportar bajo el *artículo 35*.

En definitiva, el asegurador decide cómo diseña este proceso de forma proporcional a la naturaleza, volumen y complejidad de sus riesgos, pero siempre teniendo en cuenta los requerimientos del *artículo 45 de la Directiva*.

La ejecución del mismo puede ser subcontratada aunque la dirección de la empresa permanece como la responsable del cumplimiento de los requisitos, tal y como ocurre en la actualidad con los requerimientos de Control Interno y de Control de Política de Inversiones que fijan los *artículos 110 y 110 bis del Reglamento de Ordenación y Supervisión de Seguros Privados*.

Principios

Antes de explicar los principios que rigen la aplicación del ORSA, es importante destacar que todos ellos deben ser aplicados de forma proporcional al carácter de los riesgos, su escala y la complejidad de la actividad del asegurador.

El ORSA es responsabilidad del asegurador y debe ser revisado periódicamente y aprobado por el órgano directivo

El órgano directivo debe revisar las premisas, parámetros y acciones estratégicas contenidas en la evaluación y firmar el resultado como último responsable del mismo.

Como el proceso debe formar parte de la estrategia de negocio el órgano directivo debe estar activamente implicado en su revisión. Además, debe tener en cuenta el nivel de apetito al riesgo y de confianza que el asegurador utiliza internamente en relación a la certeza de que sus responsabilidades, con los tomadores de seguro, serán cumplidas.

El ORSA debería finalizar con todos los riesgos materiales que pueden tener impacto en la capacidad del asegurador para cumplir sus obligaciones

Se deben considerar, como mínimo, las siguientes áreas: suscripción, mercado, crédito y **riesgos operacionales**.

Además, es importante tener en cuenta el impacto de las técnicas de mitigación de riesgos (incluido el reaseguro), correlaciones y la capacidad real de absorción de pérdidas de las provisiones técnicas e impuestos diferidos.

El asegurador debe recopilar información sobre los actuales y futuros riesgos a todos los niveles jerárquicos, procesos operacionales y áreas funcionales. Se han de identificar las razones por las que las premisas del ORSA sean diferentes de las del cálculo estándar del SCR, bien por riesgos no considerados o no adecuadamente tratados en éste.

Los riesgos de liquidez, reputacional y estratégico, que no son considerados en la fórmula estándar, aquí si se tienen que incluir si presentan materialidad para el asegurador

El ORSA deberá basarse en procesos de adecuada medida y evaluación y formar parte de la estructura del proceso de gestión y de decisión del asegurador

El ORSA debe:

- Reflejar todos los activos y pasivos, incluidos acuerdos intra-grupo.
- Tener en consideración elementos de fuera del balance. Por ejemplo, fondos propios auxiliares.
- Reflejar las prácticas, sistemas y controles de gestión del asegurador.
- Utilizar una base de valoración que sea consistente a través de todo el proceso de evaluación.

Además, todo asegurador debería ser capaz de explicar y justificar: la metodología usada en la evaluación de cada riesgo, el resultado de la evaluación, la idoneidad del modelo, las fuentes de datos y el enfoque para lidiar con las incertidumbres de los parámetros y fluctuaciones.

Esta herramienta debe incluir una evaluación cuantitativa y cualitativa de los Fondos Propios y de las fluctuaciones que se pueden esperar en situaciones de estrés financiero.

Finalmente, los resultados y el entendimiento obtenido en el proceso deberán ser tenidos en cuenta en la formulación estratégica, cuota de fondos propios, desarrollo de productos, gobierno y proceso de decisión del asegurador.

El ORSA debe mirar hacia delante teniendo en cuenta los planes de negocio y proyecciones del asegurado

El ORSA tiene que demostrar que el asegurador tiene recursos financieros suficientes para realizar las inversiones planeadas y suscribir nuevo negocio en un apropiado plano de tiempo. Debe tener en cuenta, además, cualquier riesgo al que considere que puede estar expuesto en un futuro, tanto por factores internos como externos, manteniendo un grado razonable de beneficio.

El ORSA y el informe correspondiente deben estar debidamente documentados y justificar la independencia en su evaluación

El asegurador debería indicar el alcance de sus procesos estratégicos, operacionales y de gerencia de riesgos. La documentación incluirá como mínimo:

- Descripción de las áreas incluidas, del proceso de realización, de las responsabilidades del personal involucrado, de la evaluación independiente y del resultado del último informe.
- Pruebas de estrés y resultados.
- Importe de solvencia y estado financiero del asegurador firmado por el cuerpo administrativo y directivo.
- Estrategias para aumentar los fondos propios.

El cuerpo directivo se asegurará de que se lleva a cabo una evaluación periódica por personas que no han tenido responsabilidades en la parte revisada siendo, por tanto, independientes en su juicio. Puede ser llevada a cabo por un auditor interno o externo u otra persona o entidad con conocimiento suficiente e independiente. Las conclusiones de este informe independiente se elevarán al cuerpo directivo para que actúen en consecuencia.

Sin lugar a dudas, el papel del ORSA dentro del ámbito de Solvencia II es muy importante para la gestión de los riesgos empresariales y, por ello, debe integrarse en el marco de la entidad.

La función encargada de que la evaluación se cumpla conforme a los requisitos y las pautas establecidas es la auditoría interna. Por este motivo, entre otros, es destacable su papel dentro de las entidades.

En las siguientes páginas, se describe como se implanta un proceso adecuado de auditoría interna que implemente estos objetivos.

3.3 ROLES Y RESPONSABILIDADES EN EL RIESGO OPERACIONAL

El punto de partida de todo proceso de administración y gestión del riesgo operacional es que éste sea responsabilidad de todos y cada uno de los integrantes de la organización. Según sea la posición dentro de la entidad se tienen unas responsabilidades u otras ligadas a funciones concretas y, por lo tanto, es necesario superar determinados retos referentes a la gestión del riesgo operacional en la entidad.

La junta directiva es la máxima responsable del diseño, aprobación, implementación y monitoreo de los procedimientos internos para la administración del riesgo operacional. Por ello, es fundamental que conozca y comprenda sus responsabilidades.

Asimismo, la alta gerencia debe ser consciente de que es co-responsable de que la administración del riesgo operacional se lleve a cabo de forma efectiva.

Por último, aunque anteriormente se ha hecho referencia a la importancia de la auditoría interna y del gobierno corporativo en la gestión y administración del riesgo operacional es ahora cuando se dedica un apartado especial a explicar el papel de ambas funciones en la organización.

Junta Directiva y Alta Gerencia

La junta directiva y la alta gerencia son los órganos más importantes en la administración y gestión del riesgo operacional y, por ello, sus responsabilidades son más significativas. Sin embargo, no son los únicos órganos que influyen en el tratamiento de dicho riesgo.

El Comité de Basilea en el año 2003 elabora un documento de “*Buenas prácticas de riesgo operacional*” donde establece, entre otros aspectos, la importancia de la junta directiva y la alta gerencia y cuáles son sus responsabilidades en la gestión y administración del mismo.

En la entidad de seguros se ha seguido el mismo esquema de responsabilidad adoptado en el marco de Basilea II. En general, las instituciones deben tratar al riesgo operacional no como parte de un riesgo exclusivamente financiero sino como una clase de riesgo distinta que está presente en los varios productos, actividades, procesos y sistemas de todas las líneas de negocio de la institución. En este sentido, debe haber una especialización en la gestión del riesgo operacional; se deben conformar

las estructuras de administración responsables de aprobar y revisar, periódicamente, el marco de tratamiento del este riesgo.

La junta directiva y la alta gerencia son responsables de crear una cultura en la organización que dé alta prioridad a la efectiva administración del riesgo operacional y a la adherencia a controles operativos sólidos. La administración es más efectiva cuando la cultura institucional enfatiza altos estándares de comportamiento y desempeño en todos los niveles.

Junta Directiva

La junta directiva es el órgano de gobierno, ratificado por la asamblea general, cuya función principal es cumplir y hacer cumplir los acuerdos adoptados en ella. Tiene poderes para resolver, acordar y pactar todas las gestiones que estime oportunas, dando cuenta de ellas en la siguiente asamblea general.

Funciones Principales

El Comité de Basilea establece que las principales funciones de la junta directiva, en cuanto al riesgo operacional, serán las siguientes:

- Aprobar un **marco** aplicable a toda la organización para gestionar explícitamente el riesgo operacional, estableciendo principios para identificar, evaluar, monitorear, y controlar o mitigar este tipo de riesgo.
- Establecer una **estructura capaz** de poner en práctica el marco adoptado para la gestión del riesgo operacional en la organización, fijando claras líneas de responsabilidad y asegurando que las políticas y los procedimientos se cumplan.
- Asegurar que el marco definido para la gestión del riesgo operacional en la entidad esté sujeto a un proceso de **auditoría interna** efectivo e integral, llevado a cabo por personal independiente, capacitado y competente, asegurando que el órgano de control no sea responsable de la gestión de dicho riesgo.
- Asegurar que las **políticas y prácticas** son **congruentes** con su cultura empresarial, objetivos y estrategia a largo plazo y con su ambiente de control.
- Proporcionar a la alta gerencia **pautas y orientaciones** inequívocas sobre los principios en los que se basa el marco aplicable a la gestión del riesgo operacional y aprobar las políticas y procedimientos y asegurar que se cumplan.
- Revisar regularmente **información** del riesgo operacional que permita comprender, en todo momento, el perfil de riesgo de la institución así como las implicaciones estratégicas de dicha información.

Por ello, las unidades de control respectivas deberán producir reportes periódicos sobre la exposición al riesgo operacional para la junta directiva y la alta gerencia, sin importar el tamaño de la institución.

Alta Gerencia

La alta gerencia está formada por el conjunto de empleados de alta calificación que se encarga de dirigir y gestionar los asuntos de una empresa.

Funciones Principales

En la misma línea, el Comité de Basilea establece que las principales labores de la alta gerencia en relación al riesgo operacional son las siguientes: _

- **Poner en práctica el marco** adoptado por la junta directiva para la gestión del riesgo operacional; desarrollando políticas, procesos y procedimientos destinados a la gestión de todos los productos, actividades, procesos y controles.
- Establecer **líneas claras de autoridad**, responsabilidad y comunicación para fomentar y mantener la asunción de responsabilidades en la gestión del riesgo operacional.
- Asegurar la **disponibilidad de recursos** suficientes, humanos y financieros, para gestionar el riesgo operacional en forma efectiva.
- Garantizar que el **personal** encargado de la gestión del riesgo operacional esté debidamente **calificado** y que se comuniquen efectivamente con el personal que se ocupa de gestionar los otros riesgos.
- Prestar atención a la **calidad de los controles** sobre la documentación y a las prácticas para realizar operaciones.

Auditoría interna del riesgo operacional

Un gobierno corporativo sólido requiere que el sistema de control interno efectivo esté acompañado por una auditoría, tanto interna como externa, independiente y efectivas.

La experiencia en las instituciones financieras indica que resulta fundamental establecer una relación constructiva y eficiente entre la alta gerencia, los auditores y los supervisores financieros con el fin de garantizar la eficacia de las auditorías y de la supervisión.

El Comité de Basilea señala que la junta directiva de una institución financiera es la responsable de asegurar que la alta gerencia establezca y mantenga un sistema de control interno adecuado y eficaz, así como un marco para asegurar el cumplimiento de leyes, reglamento y políticas. En este sentido, es necesario que la junta directiva revise, al menos una vez al año, los sistemas de control interno.

Por su parte, la alta gerencia es la encargada de desarrollar procesos que identifiquen, calculen, vigilen y controlen los riesgos en los que incurre. Además, debe informar periódicamente a la junta directiva sobre el alcance y el funcionamiento de los sistemas de control interno.

Auditoría Interna en el Marco de Solvencia II

La Directiva de Solvencia II va a introducir cambios significativos en la gestión de las empresas aseguradoras y en la función de auditoría interna.

La *Sección 2 del capítulo IV* de la misma se dedica al Sistema de Gobierno de las entidades Aseguradoras. Entre los requisitos generales de gobierno, en el *artículo 41*, se destacan los siguientes:

- Los Estados Miembros exigirán que todas las empresas, de seguros y de reaseguros, dispongan de un sistema eficaz de gobierno que garantice una gestión prudente de la actividad aseguradora y reaseguradora.
- El sistema de gobierno será proporcional a la naturaleza, la envergadura y la complejidad de las operaciones de la empresa de seguros o de reaseguros.
- Las empresas de seguros y de reaseguros contarán con una política escrita referida, al menos, a la gestión de riesgos, al control interno y a la auditoría interna y, en su caso, a la política de externalización de alguno de estos servicios.

Dada su importancia en la gestión del riesgo operacional resulta fundamental definir claramente la función auditoría interna. Una buena definición puede ser la acuñada por el *Institute of Internal Auditors (IIA)*.

“La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la organización. Ayuda a la organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control interno y gobierno corporativo”.

El documento de CEIOPS *“Advice for Level 2 Implementing Measures on Solvency II: System of Governance”*⁵¹, al igual que el capítulo IV, sección 2 de la Directiva de Solvencia II, establece que las funciones críticas o relevantes en el sistema de gobierno son, al menos, las siguientes:

- Gestión de riesgos.
- Cumplimiento.
- Función actuarial.
- Auditoría interna.

⁵¹ **Advice for Level 2 Implementing Measures on Solvency II: System of Governance:** documento publicado por CEIOPS en octubre del año 2009 que señala una serie de consejos sobre el sistema de gobierno de las aseguradoras en el marco de Solvencia II.

Todas las personas que sean responsables de las anteriores funciones han de actuar conforme los requisitos de notificación al órgano supervisor.

Se ha tratado, ampliamente, los temas relativos a la gestión de riesgos y al cumplimiento normativo y, en menor medida, a la cuantificación o función actuarial del mismo. Por lo tanto, este apartado se dedica exclusivamente a la auditoría interna.

El mencionado documento de CEIOPS establece lo siguiente con respecto a la función de auditoría interna:

“Es una función independiente en la organización que examina y evalúa el funcionamiento de los controles internos y de todos los demás elementos del sistema de gobierno, así como la adecuación de las actividades a las estrategias, políticas, procesos y procedimientos de reporting.

Necesita ser independiente de las actividades auditadas y llevar a cabo su trabajo con imparcialidad. La auditoría interna debe ser supervisada, únicamente, por el consejo de administración o el comité de auditoría como órgano delegado del mismo.

Debe contar con los suficientes recursos para que pueda ser efectiva. Debe tener comunicación directa con todos los miembros de la organización.

Su posición y estatus en la organización deben establecerse en un documento formal que debe ser aprobado por el consejo de administración (estatuto de auditoría interna).

Necesita disponer de un completo e ilimitado acceso a la información necesaria para realizar su trabajo, incluidas actas de los órganos de gobierno. Ello supone que se le proporcione, de forma oportuna, toda la información necesaria y que pueda revisar todas las actividades y procesos de la compañía que sean relevantes para el ejercicio de sus responsabilidades.

Todas las unidades de negocio tendrán la obligación de informar a auditoría interna cuando conozcan deficiencias en los controles internos, se produzcan pérdidas o existan sospechas fundadas relacionadas con irregularidades.

Debe preparar un plan anual de auditoría basado en un análisis de riesgos, teniendo en cuenta todas las actividades y el sistema de gobierno completo, así como los desarrollos previstos de actividades e innovaciones.

Las actividades de auditoría deben ser complementadas por un adecuado seguimiento de las recomendaciones propuestas al objeto de mantener un registro de las acciones adoptadas por la dirección para subsanar las deficiencias observadas.

Las Buenas Prácticas sugieren que la función de auditoría interna debería emitir informes escritos y transmitirlos oportunamente a los responsables de las áreas auditadas con independencia de si se han encontrado deficiencias materiales.

Debe elaborar, al menos anualmente, un informe escrito con los principales hechos observados y remitirlo al consejo/comité de auditoría.

Debe informar al consejo/comité de auditoría sobre el cumplimiento de los objetivos de su función, en particular del cumplimiento del plan de auditoría”.

La Directiva de Solvencia II realza el rol del auditor interno en la organización y, al mismo tiempo, aumenta de forma considerable las responsabilidades que auditoría interna tendrá que asumir.

En España, el *Código Unificado de Buen Gobierno de las entidades cotizadas*, publicado por la Comisión Nacional del Mercado de Valores (CNMV) en mayo de 2006, refuerza el valor de auditoría interna al incluir al auditor interno -responsable de la función- entre los miembros de la alta dirección y sitúa a la misma en una posición muy clara e importante en la entidad.

”Alta Dirección: Aquellos directivos que tengan dependencia directa del consejo de administración o del primer ejecutivo de la compañía y, en todo caso, el auditor interno”

Implantar un proceso de Auditoría Interna

Para implantar una función eficaz de auditoría interna es necesario cumplir con los aspectos formales y legales que las normas imponen a las compañías aseguradoras pero, en muchos casos, esto no es suficiente.

La implantación de una auditoría interna eficaz y de alto rendimiento, como textualmente dice la Directiva Marco de Solvencia II, *requiere que la organización en su totalidad, no solo el consejo de administración, el comité de auditoría o la alta dirección, comprenda y valore la función de auditoría interna, la cual estará eficazmente implantada si la organización percibe que agrega valor.*

Para implantar una eficaz función de auditoría interna es necesario definir y disponer de:

- Estatuto de auditoría interna.
- Políticas adecuadas.
- Plan anual con los objetivos y metas.
- Plan estratégico de desarrollo de la auditoría.

Estatuto de Auditoría Interna

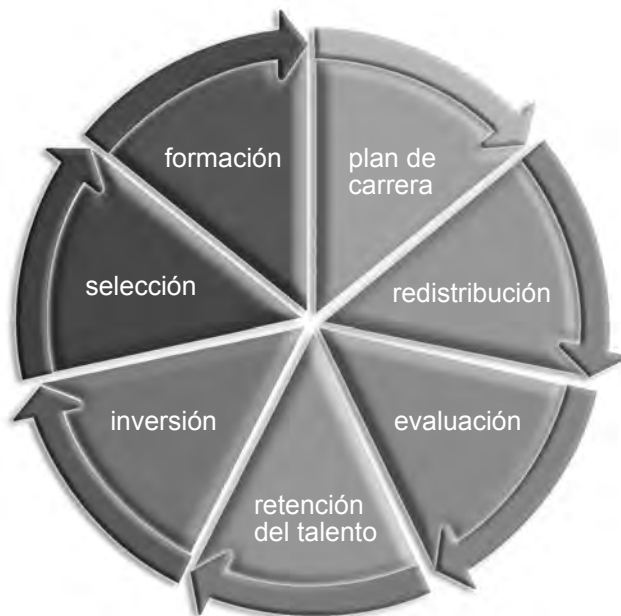
Este importante documento debe ser conocido por todos los directivos y empleados de la organización y es obligación del máximo responsable de auditoría interna garantizar su adecuada difusión.

Debe ser aprobado por el consejo de administración y por el comité de auditoría y en él, al menos, se tiene que establecer:

- La misión, funciones y atribuciones del área de auditoría interna.
- La estructura organizativa de auditoría interna.
- El marco de relaciones entre el área de auditoría interna, el comité de auditoría, la alta dirección, la dirección y el auditor externo.
- Las referencias clave en las que se fundamenta la actuación de auditoría interna.
- El alcance, definiendo con precisión, el ámbito de aplicación del estatuto de auditoría interna.
- Los derechos y obligaciones del área de auditoría interna.

Políticas de Auditoría Interna

Es aconsejable que la auditoría interna defina políticas aprobadas por el consejo de administración y el comité de auditoría, en su caso. Estas políticas hacen hincapié en el activo más relevante de auditoría interna: sus recursos humanos, y serían las siguientes:



Fuente: elaboración propia.

- *Política de selección*

Debe quedar por escrito qué requisitos se tienen que cumplir para poder ser auditor interno con la finalidad de definir claramente las necesidades del área.

- *Plan de formación*

Para que los informes de auditoría interna sean solventes y de calidad es imprescindible que el área de auditoría disponga de una política de formación a corto y largo plazo. Esta política debe incluir un plan de formación adecuado a la categoría profesional de los auditores internos y contemplar formación interna y externa.

- *Política sobre plan de carrera*

Los auditores internos deben ser clasificados por categorías las cuales deben estar muy vinculadas a sus conocimientos y responsabilidades. Para que los auditores internos tengan “certeza en su carrera” deben conocer cuáles son los criterios que auditoría interna tiene establecidos para que un auditor promocione.

- *Política de retribución*

Esta política es consecuencia de la distribución de los auditores internos en diferentes categorías profesionales. Debe quedar documentado cual es la retribución del auditor en sus diferentes categorías. Implantar esta política requiere de las habilidades de liderazgo del director de auditoría interna.

- *Política de evaluación*

La función de auditoría interna evalúa, entre otros aspectos, actividades, procedimientos, procesos, controles y sistemas de gobierno pero también se debe someter a la evaluación de los demás. En este sentido, es recomendable que se disponga de una política de evaluación que abarque a la actividad de auditoría interna en su conjunto.

- *Política de retención del talento*

Auditoría interna es un área a la que se suele demandar internamente profesionales para desempeñar responsabilidades en áreas de gestión. Pero para no descapitalizar la función se debe tener una política de retención del talento, de tal forma que no haya desequilibrios en el periodo de rotación de los auditores internos.

- *Política de inversiones*

El área de auditoría interna debe tener una política de inversiones para estar a la vanguardia en tecnología, software especializado y en herramientas para acercar la función de auditoría interna al auditado. Asimismo, la política de inversiones además de

las adquisiciones tecnológicas, debe llevar asociada la formación de los auditores en estas nuevas herramientas informáticas, así como en todas las novedades normativas y financieras que afecten a la entidad y al mercado en el que se mueve.

Plan Anual de Auditoría Interna

El plan anual de auditoría tiene que ser realista y detallar los recursos necesarios, tanto económicos como humanos. Para cumplir los objetivos de auditoría interna debe remitirse para su aprobación al consejo de administración y al comité de auditoría. Además, este plan debe estar basado en un análisis de riesgos de la entidad.

Este es otro de los documentos importantes de auditoría interna y del que, al menos, se debe hacer un seguimiento trimestral e informar al comité de auditoría, si existiese, y al consejo de administración.

Plan Estratégico de Auditoría Interna

El plan estratégico debe tener un horizonte temporal de, al menos, tres años para el que se marcarán los objetivos de auditoría interna y las medidas necesarias para alcanzarlos. La extensión de este plan dependerá del tamaño y complejidad de la organización pero tiene que abarcar aspectos estratégicos para auditoría interna.

El papel del Gobierno Corporativo

La Directiva de Solvencia II dedica los *artículos 40-56* a las cuestiones relacionadas con el gobierno corporativo de las entidades aseguradoras.

El principio esencial es que el órgano de administración de la entidad asumirá la responsabilidad última de cumplimiento de la normativa de Solvencia II.

De la misma manera, destacan los documentos del CEIOPS para el desarrollo de medidas de nivel 2 de octubre de 2009: *System of Governance*⁵² así como el relativo a *tests y standards for internal model approval*⁵³.

Es importante definir claramente qué es el gobierno corporativo y cuáles son sus objetivos principales para entender cómo se involucra en la gestión y administración del

⁵² **System of Governance**: es un documento del CEIOPS dedicado al sistema de gobierno de las entidades aseguradoras. Proporciona asesoramiento final sobre las medidas de ejecución de nivel 2 por y recomienda fomentar la convergencia de la supervisión.

⁵³ **Tests y standards for internal model approval**, documento de CEIOPS que proporciona más detalles sobre las disposiciones generales de los requisitos para la aprobación de modelos internos para la cuantificación del riesgo operacional.

riesgo operacional. Así, el gobierno corporativo es el *conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa*. Como parte integrante y fundamental del gobierno corporativo destacan los accionistas, la dirección y la alta administración.

Un buen gobierno corporativo provee los incentivos para proteger los intereses de la compañía y los accionistas, monitorizar la creación de valor y uso eficiente de los recursos brindando una transparencia de información.

Sin embargo, para conocer ampliamente que abarca el gobierno corporativo y porqué representa un papel tan importante en el sistema de gestión de riesgos de las entidades aseguradoras, es necesario analizar una serie de elementos que conforman el mismo, desde su origen hasta la actualidad.

Estos elementos son: sus antecedentes-imprescindibles si se quiere conocer el origen del gobierno corporativo y su evolución-, el impacto del gobierno corporativo en el control de la actividad aseguradora, las guías de *Buenas Prácticas* en el sector y el papel del gobierno corporativo en el control de riesgos.



Fuente: elaboración propia.

Antecedentes

La crisis de 1929

Resulta tarea complicada delimitar las primeras apariciones del denominado “gobierno corporativo”. Sin embargo, un acontecimiento que marcó una primera aproximación a

dicho concepto, aunque este ha ido evolucionando con el paso del tiempo y conforme las necesidades de cada etapa, fue el *Great Crash*⁵⁴ de 1929 y la Gran Depresión posterior.

El *Crash* de 1929 puso de manifiesto una primera gran oleada de interés por llevar la democracia a las corporaciones; con medidas destinadas a acentuar los deberes de transparencia de las sociedades y la información que proporcionan a sus accionistas, produciendo las grandes regulaciones de 1933. Estas regulaciones se asientan sobre el descubrimiento de que el crédito bancario a los inversores se había fundado sobre intereses confusos, con los bancos cada vez más implicados en banca no comercial sino de inversión, y las primeras reglas coordinadas sobre información financiera obligatoria a proporcionar por las grandes empresas.

Distintas aproximaciones: Modelos y Códigos

Si la actual crisis ha demostrado algo es que si muchas son las diferencias entre las corporaciones del siglo XXI y las de principio del siglo XX, no hay tanta distancia entre las deficiencias detectables en los mecanismos de control disponibles en cuanto a la solvencia financiera y gobierno corporativo de estas entidades.

Se puede pensar que el avance experimentado respecto de esta época anterior ha sido importante pero, realmente, se han producido pequeños pasos que hacen que muchos de los males predicados en 1929 parezcan actuales.

Para observar este paralelismo conviene destacar dos enseñanzas aprendidas a consecuencia de la Gran Crisis que, sin embargo, reflejan situaciones que la sociedad atraviesa actualmente:

- *Fallo de los sistemas*

La empresa global del siglo XXI no queda perfectamente cubierta por ninguna regulación. Las brechas existentes entre Europa y EEUU, o las que se perciben en el horizonte más próximo, hacen que por mucho que grupos empresariales hayan quedado más o menos abrigados frente a la Gran Crisis Financiera esta situación no les blinde totalmente de consecuencias indeseadas.

Ni Basilea II ni ningún esfuerzo local dentro de la Unión Europea han salvado al sector financiero de quedar afectado por esta crisis.

⁵⁴ **Great Crash:** término inglés que hace referencia al **Crac del 29**, también conocido como la **Crisis de 1929** y fue la más devastadora caída del mercado de valores en la historia de la Bolsa en Estados Unidos, tomando en consideración el alcance total y la larga duración de sus secuelas.

- *Necesidad de refundar el gobierno corporativo*

Existe una necesidad de refundar el gobierno corporativo en torno a esfuerzos de autorregulación que permitan recuperar la credibilidad perdida en agencias de rating y otros calificadores externos; todo ello en combinación con regulaciones flexibles, adaptables y adecuadas a la evolución de la actividad empresarial.

Curiosamente, si en el sector asegurador todo eran dudas, ahora se apuesta definitivamente por Solvencia II y por un incremento en el control y la regulación corporativa, pero también por un esfuerzo sectorial por un mayor autocontrol.

Primeros pasos en España

- *Código Olivencia*

Los primeros esfuerzos por introducir una cultura del gobierno corporativo surgen en febrero de 1997 de la decisión del Consejo de Ministros de crear una *Comisión Especial para el Estudio Ético de los Consejos de Administración de las Sociedades*.

Esta Comisión, presidida por Manuel Olivencia, emite en febrero de 1998 un informe centrado en la problemática de los consejos de administración de las sociedades que acceden a los mercados financieros junto con un código de asunción voluntaria por dichas sociedades, centrado en el buen gobierno y compuesto por 23 recomendaciones. De estas recomendaciones destacan:

- La necesidad de separar gestión y propiedad de la empresa, proponiendo incorporar al consejo de administración una mayoría de consejeros independientes de la dirección de la empresa.
- La misión de los consejeros se basa en defender los intereses de la sociedad, fomentando la toma de decisiones que mejoren la gestión de la empresa y arbitran mecanismos para la defensa de los intereses del pequeño y mediano inversor.
- La creación de las llamadas comisiones delegadas de control⁵⁵, que deberán garantizar la función de supervisión del órgano de administración.
- La recomendación de que los administradores tengan un único mandato de cuatro o cinco años.

Sin que deba restarse importancia a este precedente en materia de buen gobierno corporativo, hay que recordar que fue ampliamente criticado. Por un lado, la concepción

⁵⁵ Estas comisiones están compuestas por consejeros externos y serían básicamente: de auditoría, encargada de la verificación de la contabilidad de la sociedad, de nombramientos, cuya misión es la selección de los consejeros, y de retribuciones, que deberá supervisar la política de remuneración.

que se tenía del gobierno corporativo era propia de su época, es decir, limitada a las relaciones administradores-accionistas y, por el otro, sus aportaciones cifraban prácticamente todas sus virtudes en las ventajas de los consejeros independientes.

- *Comisión Aldama y Conthe*

La *Comisión Especial para el Fomento, Transparencia y Seguridad de Mercados Financieros y Sociedades Cotizadas*, creada en 2002, dio un paso más en la materia huyendo del carácter voluntario y sin control de las propuestas del informe anterior, y abogando para que se exija a las empresas publicar un “*Informe anual de Gobierno Corporativo*” con la obligación de mantener actualizada su política sobre gobierno corporativo a través de sus webs.

El gran mérito del Informe Aldama es influir en algunos aspectos de la reforma llevada a cabo por la Ley 26/2003, de 17 de julio, por la que se modifican la Ley 24/1988, de 28 de julio, del Mercado de Valores, y el Texto Refundido de la Ley de Sociedades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre, con el fin de reforzar la transparencia de las sociedades anónimas cotizadas (más conocida como Ley de Transparencia), y de modo más importante la Ley del Mercado de Valores, con órdenes de desarrollo como la ECO/3722/2003, de 26 de diciembre, sobre el informe anual de gobierno corporativo y otros instrumentos de información de las sociedades anónimas cotizadas y otras entidades.

Todo esto se tradujo en un nuevo esfuerzo conocido como el *Informe Conthe* y su *Código Unificado de Buen Gobierno*, aprobados por la Comisión Nacional del Mercado de Valores (CNMV) en 2006, que supone un avance respecto a la visión limitada a aspectos relacionados a lo que se ha conocido como gobernanza de las sociedades, es decir, su mera administración.

El Código Conthe o Código Unificado supuso una obligación para las sociedades cotizadas a partir del ejercicio 2007. Sin embargo, muchos comentarios negativos sobre este código lo han hecho fracasar ya que no ha sido aceptado dentro del colectivo de empresas destinatarias del mismo.

- *Consecuencias de la gran crisis financiera*

El rechazo suscitado por el Código Unificado unido al escenario actual a raíz de la Gran Crisis Financiera de 2007, permiten aventurar que el modelo Conthe será superado en el medio plazo por nuevas propuestas que combinen en materia de gobierno corporativo dos elementos:

- códigos de autorregulación y
- obligaciones derivadas del ordenamiento jurídico.

En medio del análisis sobre las causas de la crisis actual, no han faltado numerosas voces apuntando a una relación directa entre la misma y un mal gobierno corporativo.

Ninguno de los precedentes, internacionales o nacionales, preveían respuestas a muchas de las cuestiones planteadas en la Gran Crisis.

En el último año ha aparecido lo que puede ser la última revolución en gobierno corporativo de mano de la Ley estadounidense *Dodd-Frank sobre Reforma de Wall Street y Protección de los Consumidores*, de 21 de julio de 2010.

Esta norma introduce la necesidad de que se aprueben por los accionistas, al menos cada tres años, tanto la remuneración de los directivos como las previsiones de blindajes en caso de fusiones y adquisiciones y, como algo muy cercano a nuestro sector, la creación de la FIO (*"Federal Insurance Office"*), como parte del Departamento del Tesoro, oficina que actuará en representación de Estados Unidos en reuniones internacionales de reguladores de seguros.

El control de la Actividad Aseguradora y su impacto en el Gobierno Corporativo

Históricamente, la actividad aseguradora ha gozado de un tratamiento diferenciado en nuestro país con un regulador específico la *Dirección General de Seguros y Fondos de Pensiones (DGSFP)* y con notaciones únicas incluso en referencia al mercado europeo.

El gobierno corporativo y la gobernanza aparecen ya como elementos regulados en el Texto Refundido de la Ley de Ordenación y Supervisión de los Seguros Privados, aprobado por Real Decreto Legislativo 6/2004, de 29 de octubre (TRLOSSP), y en su Reglamento, aprobado por Real Decreto 2.486/1998, de 20 de noviembre (ROSSP).

Por lo tanto, en el sector asegurador no sólo se conoce quiénes son los socios de las entidades y se regula su idoneidad, sino que se regulan las entradas y salidas de socios con influencia significativa en el capital, así como la aptitud para desempeñar cargos tanto de administración como de dirección.

Todo ello resta protagonismo a la autorregulación. Sin embargo, aunque es fácil detectar de una lectura detenida del TRLOSSP y el ROSSP que queda mucho espacio para ese esfuerzo.

Las Guías de Buenas Prácticas en el Sector Asegurador Español

El origen de las Guías de Buenas Prácticas en el Sector Asegurador Español se sitúa en el año 2005, cuando la DGSFP requirió a UNESPA⁵⁶ -patronal que agrupa a las entidades aseguradoras en España- que implementase en el sector prácticas de buen gobierno y control interno similares a las de otros sectores financieros.

⁵⁶ **Unespa:** Unión Española de Entidades Aseguradoras y Reaseguradoras.

UNESPA ha realizado un importante esfuerzo en crear guías completas, trascendiendo a la Responsabilidad Social Corporativa y el Buen Gobierno para centrarse en cuestiones tales como las relaciones del sector con personas discapacitadas o las características de productos de seguros específicos.

Sin embargo, existen dos críticas a estas Guías de Buenas Prácticas; la primera reprochar que no se desarrollen más de las mismas y la segunda que no sean lo suficientemente conocidas por el público.

Por otra parte, una guía de cumplimiento voluntario únicamente puede resultar efectiva de la conjunción de dos elementos:

- el que sus principios originen efectos beneficiosos para los consumidores y
- que quién ha de aplicarla encuentre un beneficio de su aplicación, en la medida de conseguir una mayor confianza de sus clientes y accionistas.

Una última observación es la falta de definición de un sistema de control del cumplimiento por las entidades de lo dispuesto en estas guías. Resulta difícil dar credibilidad a las guías si no se establecen parámetros y controles de cumplimiento de lo dispuesto en las mismas.

La Guía de Buen Gobierno

UNESPA define *“La guía de Buen Gobierno”* como aquella que *“recoge los principios emanados desde organismos internacionales, comunitarios y nacionales, y dirigidos esencialmente a las sociedades anónimas cotizadas que deben servir para orientar el gobierno de las entidades aseguradoras.”*

Por ello, para la elaboración de la Guía se ha seguido un esquema descriptivo de materias como son, especialmente, las que afectan a los órganos de gobierno que deberán ser analizadas y desarrolladas por cada entidad, adaptándolas a su forma jurídica, a su propia estructura organizativa, de gestión y, muy especialmente, de propiedad.

El objetivo principal es reforzar los procedimientos de transparencia interna de las entidades y de sus órganos de gobierno”.

Esta Guía enfatiza una serie de elementos claves para reforzar los deberes legales en materia de información sobre buen gobierno y gobernanza de las entidades aseguradoras. Así, y tanto dentro de sus webs corporativas como mediante la introducción de un específico *Informe Anual de Gobierno Corporativo*, se recomienda en que se facilite la suficiente información no sólo para poder tener mediciones eficaces sino para progresar en los esfuerzos y pasos emprendidos.

Por otra parte, resultaría recomendable que UNESPA condujera controles de cumplimiento periódicos y diagnósticos sobre la efectividad de las medidas tomadas en cada caso.

Otras guías

La Guía del Buen Gobierno es sólo una pieza más dentro de los esfuerzos de UNESPA por proporcionar nuevos patrones de conducta al sector que propicien una mayor transparencia y mejores prácticas de mercado.

Las últimas estadísticas de UNESPA del año 2009 respecto a la adhesión a las guías aportan los siguientes resultados:

- 87 entidades a la Guía de Buenas Prácticas en materia de Gobierno Corporativo.
- 104 entidades a la Guía de Buenas Prácticas en materia de Control Interno.
- 104 entidades a la Guía de Buenas Prácticas en materia de Transparencia.
- 84 entidades a la Guía de Buenas Prácticas en materia de Publicidad.
- 33 entidades a la Guía de Discapacidad.
- 28 entidades a la Guía de Internet.
- 23 entidades a la Guía relativa a unit-linked.
- 15 entidades a la Guía relativa a salud.
- 17 entidades a la Guía relativa a automóviles.
- 12 entidades a la Guía relativa a multirriesgos.

Estos resultados manifiestan como, a pesar de que el esfuerzo que se está realizando es importante, es necesaria una mayor concienciación por parte de las entidades sobre la relevancia de adherirse a estas guías. Con ello se pretende conseguir un mercado más transparente y, por lo tanto, que genere mayor confianza.

El Control de Riesgos y el Gobierno Corporativo: elementos clave del nuevo sistema

Como ya se conoce, Solvencia II nace del modelo de Basilea II dirigido a mejorar la seguridad en el sistema financiero, poniendo mayor énfasis en los controles internos de los bancos y procesos de administración de riesgos.

Para ello, se utilizan modelos estadísticos elaborados con bases de datos históricas de las entidades de tal forma que cada entidad cubra sus pérdidas en base a la calidad histórica de su cartera.

Básicamente, Solvencia II persigue tres grandes objetivos:

- El desarrollo y establecimiento de un sistema que permita determinar los recursos propios mínimos a requerir a cada aseguradora en función de los riesgos asumidos y la gestión que se realice de cada uno de ellos.

- El establecimiento de nuevas competencias y mecanismos de actuación de los supervisores.
- El establecimiento de la información que las entidades deberían proporcionar en relación, fundamentalmente, a su política de gestión de riesgos con el objeto de potenciar la disciplina de mercado.

Esos objetivos se conocen como los “pilares” del sistema de Solvencia II y afectan claramente al gobierno corporativo, tanto por la posición en la que queda la supervisión del sector como por la revolución en materia de transparencia que se impone a las entidades aseguradoras.

- *La Importancia del segundo pilar*

El segundo pilar de Solvencia II implicaría una migración del actual sistema de ordenación y supervisión a un sistema de regulación por autosupervisión.

La Comisión Europea indica que este debe buscar ante todo la protección de los tomadores y ello supone, en relación con el gobierno corporativo, el que sea necesario *“preservar la coherencia entre las exigencias impuestas en los sectores de la banca, los valores mobiliarios, los seguros y los reaseguros.*

Dichas exigencias comprenden, entre otras, la gestión del riesgo y la solvencia, y el control y la auditoría internos. La responsabilidad última por el cumplimiento de los requisitos cualitativos y de control recae en el órgano de administración o dirección de la empresa”.

La Directiva en su *artículo 41* establece, por primera vez, una regulación uniforme sobre gobierno corporativo que exige un *“sistema eficaz”* que *“garantice una gestión sana y prudente de la actividad”*, en proporción al tamaño de la entidad y sujeto a revisiones periódicas.

Como señala el punto 1 de dicho artículo, *“el citado sistema comprenderá, como mínimo, una estructura organizativa transparente y apropiada, con una clara distribución y una adecuada separación de funciones, y un sistema eficaz para garantizar la transmisión de la información”.*

Concretamente, tales requisitos afectan a:

- Condiciones de aptitud y honorabilidad de los administradores y directores efectivos de la empresa.
- Establecimiento de un *“ sistema eficaz de gestión de riesgos, que comprenderá las estrategias, los procesos y los procedimientos de información necesarios para vigilar, gestionar y notificar de forma continua los riesgos a los que estén o puedan estar expuestas, y sus interdependencias”.*
- Ese sistema de gestión de riesgos incluirá *“una autoevaluación de riesgos y solvencia”.*

- Establecimiento de un sistema de control interno, que conste “*de procedimientos administrativos y contables, de un marco de control interno, de mecanismos adecuados de información a todos los niveles de la empresa, y de una función permanente de comprobación de la conformidad*”.
- Establecimiento de una “*función efectiva y permanente de auditoría interna*” y de una “*función actuarial efectiva*”.

Lo cierto es que como la propia DGSFP recuerda, “*la Directiva Solvencia II es el escalón normativo comunitario de mayor rango en un proceso en etapas, al que sucederán las medidas de implementación de nivel 2 y las guías de supervisión de nivel 3.*”

Parte de las medidas de implementación tendrán forma de Reglamento de la Comisión Europea y serán, por tanto, de aplicación directa sin necesidad de transposición, otras tendrán forma de Directivas de la Comisión Europea y tendrán que ser debidamente transpuestas”, por lo que resulta difícil predecir el grado de impacto hasta que no se implementen estas medidas en las entidades y transcurran los suficientes años como para que se puedan extraer conclusiones claras.

4. Conclusiones

En los últimos años la preocupación por el riesgo operacional, que hasta hace poco tiempo era considerado un riesgo secundario, ha aumentado progresivamente.

Por una parte, las entidades y los supervisores perciben que la exposición a este riesgo se ha intensificado a medida que el sector financiero ha evolucionado. Los factores decisivos de esta tendencia han sido: la mejora de las tecnologías, el desarrollo de nuevas técnicas de mitigación de riesgos y la creciente globalización y complejidad del sistema financiero.

Por otra parte, la industria bancaria en primer lugar y , posteriormente otras como la aseguradora, se han visto cada vez más interesadas en la medición de este riesgo motivada por la necesidad de mejorar sus ratios de eficiencia y racionalizar la asignación de capital entre las diferentes unidades de negocio.

Finalmente, como el riesgo operacional se ha tratado desde diversas ópticas es conveniente que las conclusiones que se extraen se refieran específicamente a cada uno de los temas estudiados, sin olvidar aquellos aspectos generales del tratamiento del mismo en las entidades aseguradoras.

Entorno del riesgo operacional

La preocupación por el control del riesgo operacional adquiere cada vez mayor importancia y esto se manifiesta en los cambios normativos que se están produciendo en el panorama económico-financiero. Por este motivo es importante que, antes de analizar

las conclusiones particulares para los diferentes aspectos que se han tratado en este trabajo, se destaquen los puntos claves del riesgo operacional.

Resulta fundamental que las regulaciones de todos los países converjan hacia una **definición única** de riesgo operacional; lo que facilita la homogeneización de conceptos y mejora el intercambio de información y colaboración entre los distintos supervisores. Los supervisores deberán profundizar la revisión de los estándares de gestión del riesgo operacional que han desarrollado sus respectivos países, promoviendo la creación de unidades especializadas que sean capaces de enfrentarse a la creciente complejidad de este riesgo.

Para las entidades que usan diferentes métricas en distintos mercados y países, se debe potenciar la colaboración y coordinación de los supervisores para asegurar una supervisión efectiva del riesgo operacional.

Las instituciones han de tratar al riesgo operacional no como parte de un riesgo netamente financiero sino como una clase de riesgo distinta que está presente en los diversos productos, actividades, procesos y sistemas de todas las líneas de negocio de la institución. En este sentido, debe haber una **especialización en la gestión** del riesgo operacional, por lo que tienen que conformar adecuadamente las estructuras de administración responsables de aprobar y revisar periódicamente el marco de tratamiento del riesgo operacional.

Responsabilidades en el riesgo operacional

Para una adecuada implementación del proceso de gestión, administración y cuantificación del riesgo operacional el papel de la junta directiva y de la alta gerencia se convierte en relevante.

La junta directiva es responsable, fundamentalmente, del diseño e implementación de un marco de prevención del riesgo operacional y del establecimiento de líneas de responsabilidad y reportes. Asimismo, debe revisar la información del riesgo operacional para una mayor comprensión del perfil del mismo. Por ello, las unidades de control respectivas deberán producir reportes periódicos.

La junta directiva y la alta gerencia son los responsables de que se cree una cultura en la organización que dé prioridad a la efectiva administración del riesgo operacional y a controles operativos sólidos.

Además, otros órganos de la entidad como el gobierno corporativo y la auditoría interna representan una importancia clave para el tratamiento de este riesgo.

- *Auditoría interna*

Este departamento constituye un importante generador de valor para las empresas a través de la gestión y el control de riesgos.

Por lo tanto, involucrar a la auditoría interna con los demás departamentos de la empresa resulta imprescindible; no solo para una adecuada gestión de los riesgos sino para la creación de valor, que es el fin que busca cualquier actividad económica.

- *Gobierno corporativo*

El entorno de aplicación de gobierno corporativo reside, esencialmente, en el control interno de las juntas directivas y en los comités de auditoría; los cuales tienen la responsabilidad de dar seguridad en la contabilidad de los reportes financieros.

El marco normativo del gobierno corporativo ha experimentado un desarrollo relativamente lento y está llamado a ser revisado tras la crisis financiera actual. Esta revisión es necesaria para prevenir las situaciones que desembocaron precisamente en esta gran crisis.

En el sector asegurador dicho fenómeno coincide en el tiempo, además, con la promulgación de la Directiva de Solvencia II y su absorción en los derechos de los Estados miembros de la Unión.

En definitiva, hablar de gobierno corporativo es hablar no sólo de marcos normativos de obligado cumplimiento sino de prácticas empresariales desarrolladas más allá del entorno regulatorio. En ese sentido, destaca el importantísimo esfuerzo realizado a nivel sectorial en el mercado asegurador español en los últimos tiempos.

Tratamiento del riesgo operacional

El tratamiento del riesgo operacional engloba la gestión, administración y cuantificación del mismo y, además, la evaluación del riesgo propio y de solvencia.

- *Gestión del riesgo operacional*

El objetivo principal de la gestión del riesgo operacional (*ORM*) es la minimización de las pérdidas operacionales y la mejora en los controles. Para ello, es necesario crear una unidad de riesgo específica que defina el marco de gestión e informe a la alta dirección de los resultados obtenidos.

Los resultados conducen a decisiones estratégicas en las que es básico un adecuado proceso de retroalimentación y, para ello, se necesita una infraestructura informática óptima. Por lo tanto, habrá que aunar esfuerzos para el desarrollo de la misma.

Una adecuada implantación de un proceso ORM depende de varios aspectos, que se desarrollan tanto desde el punto de vista organizativo como directivo. Las entidades deberían desarrollar su propio enfoque y metodología para la gestión de riesgos de acuerdo con su objeto social, tamaño, naturaleza y complejidad de operaciones, aparte de otras características que consideren oportunas. Además, las entidades financieras deben contar con una estrategia aprobada por la dirección estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operacional.

- *Administración del riesgo operacional*

Para un proceso de administración del riesgo operacional eficaz, es necesario que los líderes de las entidades y los encargados de las unidades de negocio entiendan los beneficios que este proceso puede aportar.

Cada institución tiene que implementar la combinación de herramientas que ayuden a mejorar su gerencia de riesgo operacional, teniendo en cuenta su tamaño, complejidad y perfil de riesgo. Estas herramientas deberán ser capaces de reconocer las áreas más vulnerables y evaluar los controles con los que cuenta la institución para reducir la probabilidad o impacto de las pérdidas.

- *Cuantificación del riesgo operacional*

Este es un aspecto de vital importancia para evaluar la efectividad de los sistemas de control interno. El tratamiento del riesgo operacional en Solvencia II implica requerimientos cuantitativos de capital, a través del SCR, y requerimientos cualitativos relativos al proceso de revisión supervisora enmarcados en el Pilar II.

Un aspecto destacable de esta directiva es la flexibilidad que otorga en cuanto a la utilización de un modelo estándar o interno para el cálculo de los requerimientos de capital. La elección de un modelo interno supone un cambio en la filosofía del control del riesgo. Sin embargo, el sector va a encontrar una falta de registros históricos que reflejen este tipo de pérdidas, lo que dificulta el cálculo de los requerimientos mediante modelos internos.

Independientemente del método seleccionado, para desarrollar el método interno de cuantificación del riesgo operacional es importante que éste incorpore: datos internos, datos externos, escenarios e indicadores de control de riesgos.

Finalmente, se proponen tres métodos de medición de creciente complejidad y sensibilidad al riesgo: básico, estándar y modelos internos; a su vez pretenden servir de estímulo para que las entidades desarrollen sistemas más avanzados de gestión y medición del riesgo operacional.

- *Evaluación del riesgo propio y de solvencia (ORSA)*

ORSA es un modelo basado en el riesgo y representa el conocimiento y la opinión que un asegurador tiene de sus riesgos, necesidades de solvencia y fondos propios. Por lo tanto, el consejo de administración puede comprobar si dispone de un proceso de gestión del riesgo asociado a su plan estratégico y si este proceso funciona correctamente.

Además, desempeña un rol importante en el sistema de gobierno y en el proceso de toma de decisiones de las compañías, y tiene que estar presente en todos los ámbitos de la organización. Su integración en las distintas áreas empresariales va a estar marcada por la evaluación que auditoría interna realice.

La aplicación del ORSA en las entidades aseguradoras se rige conforme unos principios que, en general, deben ser aplicados de forma proporcional al carácter de los riesgos, su escala y la complejidad de la actividad del asegurador.

III

REFLEXIONES FINALES

En las entidades aseguradoras, al igual que en cualquier otro tipo de negocio, la preocupación principal es la obtención de resultados positivos al finalizar cada ejercicio y que estos se incrementen de un año para otro.

Siempre ha existido interés por el control de los riesgos ya que estos pueden provocar pérdidas financieras que supongan un coste añadido y que repercutan, de forma negativa, en los beneficios de la entidad. Sin embargo, a medida que los servicios financieros se van haciendo cada vez más complejos, como consecuencia de la globalización, y las tecnologías experimentan un avance, aumentan los perfiles de riesgo de las entidades. Así, establecer una adecuada administración y supervisión de los riesgos se convierte en uno de los retos empresariales más importantes.

La concepción del riesgo ha experimentado un gran desarrollo y, en la medida en la que este ha evolucionado, lo ha hecho también la forma de entender su gestión y administración.

La gestión de los riesgos se concibe como parte de la estrategia empresarial; la capacidad de un negocio de prosperar al afrontar sus riesgos es un indicador de su aptitud para competir y su administración está ligada a la creación de valor. Por lo tanto, interesa clasificar los distintos riesgos a los que la entidad está expuesta ya que el tratamiento de cada uno de ellos ha de ser diferente y, además, influyen en el futuro empresarial de distinta forma.

Referente al tratamiento del riesgo operacional

La primera acción que las entidades tienen que llevar a cabo es identificar cada uno de los riesgos a los que están expuestas. Estos afectan de distinta forma al desarrollo de las actividades y, por lo tanto, a pesar de que exista un marco de gestión de riesgos global, es necesario tratarlos de forma diferenciada.

Como consecuencia, la definición consensuada de riesgo operacional es vital; homogeneizar los términos resulta clave para el adecuado tratamiento de este tipo de riesgo. Solvencia II recoge, por primera vez, la importancia del riesgo operacional y desarrolla una serie de métodos y herramientas para su tratamiento.

En dicha normativa se pone de manifiesto que la consecución del mercado único está dentro de las prioridades de la UE. Para ello es necesario fortalecer la función de las aseguradoras como inversores institucionales, lograr un adecuado nivel de protección para los asegurados y fomentar la estabilidad del sistema financiero en su conjunto.

Para la supervivencia de cualquier compañía de seguros es imprescindible contar con una adecuada gestión del riesgo operacional ya que, de no ser así, el impacto en

términos de coste asociado a la falta de gestión para las compañías aseguradoras puede ser enorme.

En general, en el pasado no se ha prestado la suficiente atención a este aspecto. Sin embargo, situaciones como la gran crisis actual ponen de manifiesto la importancia de un control interno eficaz que proporcione una respuesta adecuada ante la aparición del riesgo operacional, y que controle y mitigue los impactos que tienen lugar como consecuencia de la manifestación de dicho riesgo.

No basta con tener claro que es necesario un proceso de ORM, hay que implantarlo en la organización de forma adecuada. Para ello, se tiene que definir una estrategia apropiada y establecer los límites de tolerancia que la entidad pueda soportar.

Muchas entidades establecen un proceso de gestión del riesgo operacional porque conocen la importancia que el mismo tiene pero, cuando determinan los límites de tolerancia, no lo hacen de forma consecuente con la propia organización, sus recursos y su capacidad de absorción de pérdidas. Esta situación puede constituir un grave problema si se implanta un proceso de gestión asentado en bases que no reflejan la realidad de la organización. La consecuencia inmediata será que la entidad no tenga un sistema diseñado específicamente para la propia institución y, por lo tanto, lo más probable es que se produzcan una serie de consecuencias negativas que van a reducir los resultados, e incluso pueden provocar grandes pérdidas.

Otro aspecto muy importante es el referente a los datos de pérdidas operacionales que provienen de fuentes tanto internas como externas.

En España, uno de los problemas es que el sector asegurador carece de una base de datos privada externa. Por lo tanto, si las compañías contarán, además de con su base de datos interna, con datos históricos de pérdidas operacionales, sería posible crear escenarios futuros más acordes con la realidad. Esto supondría un gran paso adelante en el tratamiento del riesgo operacional

De hecho, Inglaterra desarrolló una base de datos de pérdidas operacionales externas con el objetivo de reducir las pérdidas de este tipo y los resultados manifestados hasta la fecha demuestran el éxito de la misma.

La implementación del sistema de gestión de riesgo operacional debería considerar la identificación, evaluación, medición, monitoreo y control ya que en cada etapa se llevan a cabo procesos concretos que, actuando en conjunto, propician la eficacia del proceso.

En cuanto a las herramientas empleadas

El uso de herramientas específicas permite que cada entidad pueda llevar a cabo el tratamiento del riesgo operacional con aquellas técnicas que más se adapten a su entorno. Por lo tanto, la gestión del riesgo operacional se debe realizar “a medida” para cada tipo de entidad.

Sería erróneo pensar que este riesgo se puede gestionar de igual forma para todas las entidades; en función de la situación de cada una se tienen que considerar unas necesidades u otras. Así, las organizaciones deben implementar aquella combinación de herramientas que ayuden a mejorar su gerencia de riesgo operacional teniendo en cuenta su tamaño, complejidad y perfil de riesgo.

Existen dos tipos de herramientas de administración del riesgo operacional: herramientas cuantitativas y herramientas cualitativas. Sin embargo, con independencia del tamaño de las instituciones, estas deben ser capaces de reconocer las áreas en las que son más vulnerables y evaluar los controles con los que cuenta la institución para reducir la probabilidad o impacto de las posibles pérdidas.

Una adecuada divulgación sobre la exposición al riesgo operacional y la evaluación pertinente es también importante para determinar las herramientas óptimas para cada entidad.

Cuantificación del riesgo operacional

Una de las dificultades que entraña la cuantificación del riesgo operaciones es que, como no hay una base de datos sólida para las aseguradoras, resulta complejo identificar ese tipo de riesgo dentro de los datos de pérdidas que las propias entidades recogen.

La importancia del riesgo operacional en Solvencia II se manifiesta en el cálculo del SCR; una de las partidas del mismo está destinada exclusivamente a recoger el requerimiento de capital por riesgo operacional. Dicho requerimiento de capital representa una de las diferencias fundamentales respecto a Solvencia I; antes no se especificaba la necesidad de un capital específico para riesgo operacional. Actualmente, la nueva directiva manifiesta la importancia de recoger este riesgo y su influencia en la solvencia de las entidades y en su actividad.

Para determinar el SCR se prevé la utilización de modelos internos, aunque deberá prestarse especial atención a la insuficiencia de datos y a la falta de experiencia histórica.

Evaluación del riesgo propio y solvencia

La evaluación del riesgo propio y de solvencia es un aspecto más desconocido de la directiva y, aunque no forma parte del riesgo operacional como tal, su mala gestión sí puede dar lugar a pérdidas importantes de este tipo.

Es importante que sean las propias entidades las que realicen una evaluación de sus riesgos y de la solvencia. Así, se fomenta el conocimiento de la propia estructura de la organización y, por lo tanto, la opinión que un asegurador tiene de sus riesgos, necesidades de solvencia y fondos propios.

Este conocimiento resulta muy interesante para la propia entidad ya que no será posible una adecuada gestión de los riesgos en general, y del riesgo operacional en particular, si no se conocen los límites de tolerancia al riesgo o si la misma no se realiza teniendo en cuenta dichos límites.

En la mayoría de las entidades, ante la falta de bases de datos se emplean modelos estándar para el cálculo del requerimiento de capital (SCR). La fórmula estándar para calcular el SCR podría no llegar a cubrir todos los riesgos a los que realmente está expuesto un asegurador, sin embargo, esta situación no le exime de la evaluación real de sus propios riesgos.

Una vez más, el análisis de la documentación y un correcto reporte de la información entre los distintos niveles de la organización van a ser la clave de una adecuada evaluación del riesgo propio y de la solvencia.

Sobre los roles y las responsabilidades

La junta directiva es la máxima responsable del diseño, aprobación, implementación y monitoreo de los procedimientos internos para la administración del riesgo operacional. Por ello, es imprescindible que conozca y comprenda sus responsabilidades. Asimismo, la alta gerencia es co-responsable de asegurar que la administración del riesgo operacional se lleve a cabo de forma adecuada.

Es necesaria una cooperación efectiva entre todos los niveles de la entidad para que fluya convenientemente la información y, así, cada uno de los órganos pueda desarrollar de forma eficaz sus funciones.

Por último, la auditoría interna y el gobierno corporativo tienen una importancia especial en el tratamiento del riesgo operacional en las entidades aseguradoras. Esto se debe a que la eficacia del control interno se basa en una auditoría, tanto interna como externa, efectiva para conseguir que el gobierno corporativo sea eficaz en sus funciones.

Un buen gobierno corporativo proporciona los incentivos necesarios para proteger los intereses de la compañía y a los accionistas, monitorizar la creación de valor y el uso eficiente de los recursos brindando una transparencia de información.

Las funciones que realiza cobran una especial relevancia en el contexto económico-financiero actual. En el análisis de la presente crisis se ha apuntado en numerosas ocasiones a una relación directa entre la misma y el mal gobierno corporativo. Por lo tanto, el que en las entidades haya un mal gobierno corporativo puede derivar en consecuencias negativas para la propia empresa y para la sociedad en su conjunto.

El gobierno corporativo se apoya en criterios de autorregulación y transparencia. Como consecuencia, tener una mala política de gobiernocorporativo supone no contar con la transparencia informativa adecuada y, por lo tanto, la gestión de los propios riesgos se asienta en bases que no se corresponden con la realidad.

En este ambiente de incertidumbre marcado por una profunda inestabilidad económica y financiera, la correcta asunción de los riesgos y la determinación de límites de tolerancia apropiados se convierten en labores muy complicadas y, por lo tanto, establecer un proceso adecuado de gestión del riesgo operacional resulta especialmente complejo.

Todo aquello que propicie el establecimiento de buenas prácticas en materia de riesgo operacional, como por ejemplo guías, recomendaciones, etc., es bienvenido; una gestión apropiada repercute directamente en el resultado financiero de la entidad. Tanto es así que el único inconveniente que existe en materia de guías y recomendaciones es, precisamente, la falta de más de estos documentos y que los que hay no sean lo suficientemente conocidos por el público general.

A pesar de que están definidas las prácticas que hay que implementar para la adecuada gestión del riesgo operacional todavía hay mucho camino por recorrer. Aunque este riesgo es intrínseco a la propia naturaleza de cualquier actividad empresarial, la preocupación por su tratamiento es relativamente nueva y las organizaciones tienen que adecuar sus procesos internos para una gestión eficaz del mismo.

En general

Elaborar el trabajo de fin de carrera sobre el tratamiento del riesgo operacional me ha resultado mucho más gratificante de lo que a priori podía suponer. Los riesgos a los que están expuestas las empresas y la forma en la que se enfrentan a ellos resultan aspectos clave en la estrategia empresarial y, evidentemente, decisivos para la actividad presente y futura de la misma.

Antes de profundizar en este tema conocía la clasificación de los diferentes riesgos corporativos, pero para mí -al igual que, durante tantos años, para el sector financiero- la importancia fundamental recaía sobre los riesgos típicos, es decir, riesgo de mercado y de crédito. Sin embargo, el riesgo operacional era un tipo de riesgo más que, evidentemente, había que controlar pero no de una forma específica ni con recursos y herramientas concretas.

Sin embargo, en estos meses de trabajo he descubierto la creciente importancia que adquiere del riesgo operacional en la realidad empresarial y las adversidades que se pueden presentar en la organización como resultado de un inadecuado proceso de gestión del mismo. Ha sido el "gran desconocido" de los riesgos pero, a su vez, el que siempre ha existido en todas las actividades económicas y financieras que se desarrollan en cualquier entidad.

De hecho tal es su importancia que constituye, entre otros aspectos, la base de Solvencia II y representa la diferencia fundamental respecto de Solvencia I.

Como suele ocurrir siempre, el desconocimiento se aprecia después de sufrir las consecuencias de una gran crisis o de situaciones desfavorables y es entonces cuando se observa la importancia de tener en cuenta determinadas cuestiones, como es el caso de la relevancia del riesgo operacional.

Si en el pasado se hubieran tenido en cuenta estas cuestiones en el diseño de las estrategias empresariales o en el tratamiento de los riesgos, las consecuencias podían haber sido mucho menores y quiebras tan sonadas como la del Banco Barings (1995) o pérdidas como las de Daiwa (1984-1995) se hubieran, si no evitado, si mitigado o controlado en cierta manera.

Sin embargo, siempre se pueden extraer conclusiones positivas unidas a estas situaciones tan dramáticas por las que han pasado algunas empresas. Actualmente, y gracias al acaecimiento de estos sucesos, se tiene en cuenta el riesgo operacional en las estrategias empresariales. La preocupación por su control ha propiciado que se realice una definición homogénea del mismo categorizando los diferentes eventos que pueden dar lugar a pérdidas operacionales, y como consecuencia la posibilidad de sufrir grandes pérdidas de este tipo se ha reducido notablemente.

Según el Comité de Basilea, *“riesgo operacional es el riesgo de sufrir pérdidas debido a la inadecuación o a fallos en los procesos, personal y sistemas internos o bien por causa de eventos externos”*. La primera conclusión que se extrae es que puede surgir como consecuencia de eventos tanto internos como externos. Puede parecer que esto no aporta gran información, pero no es así. Afirmar que los riesgos no sólo son externos es entender que todas las personas que forman parte de la entidad tienen responsabilidad en la gestión del riesgo operacional. Por lo tanto, esta afirmación representa la importancia del papel de la cultura empresarial; estrechamente relacionada con el gobierno corporativo, el sistema de control interno y la auditoría interna.

A nivel europeo se han desarrollado una serie de pautas, establecidas en múltiples guías y recomendaciones, que aportan información sobre la forma de llevar a cabo una adecuada gestión del riesgo y sobre las buenas prácticas que deben realizar en numerosos ámbitos empresariales. Sin embargo, es necesaria la publicación de más documentos orientativos y de una publicidad suficiente de las mismas para que las empresas las puedan aplicar en la realización de sus acciones y actividades.

Por lo tanto, aunque los esfuerzos europeos por homogeneizar los criterios para la gestión de este riesgo son notables, no serán suficientes si las entidades no trabajan para que la cultura del riesgo operacional forme parte importante de las mismas.

El progreso de las entidades en materia de gestión del riesgo operacional se observa cuando son capaces de establecer límites de tolerancia adecuados a sus propios riesgos e involucran a todo el personal en el tratamiento de los mismos.

Aunque queda trabajo por hacer, en un futuro Solvencia II debe asegurar dos puntos fundamentales: la calidad suficiente de capital para la absorción de pérdidas, especialmente bajo escenarios de crisis, y la adecuada formación del personal en función de la labor que realice.

Finalmente, para asegurar la eficacia de esta directiva es imprescindible un profundo cambio en la concepción de la cultura empresarial. Hay que tener consciencia de la dificultad añadida que determinados aspectos de Solvencia II tienen y, por lo tanto, es necesaria la existencia de recursos técnicos y humanos adecuados y suficientes. Sin

embargo, uno de los objetivos principales es que los desarrollos tengan un grado de sofisticación razonable y unos costes soportables.

En definitiva, tanto el conocimiento de los propios riesgos como una adecuada autoevaluación de los mismos resultan imprescindibles en su tratamiento; si se es crítico con la gestión de la propia entidad se conocen y comprenden mejor aquellos aspectos que hay que cambiar para que el límite de tolerancia al riesgo se adapte a las necesidades de cada entidad y se empleen las herramientas apropiadas para su control y seguimiento.

REFERENCIAS BIBLIOGRÁFICAS

Álvaro Camacho. *Solvencia II: supervisión basada en riesgo de entidades aseguradoras en el marco de la Unión Europea*. Año 2009.

Ana Belén Herrero Brañas. *El Gobierno Corporativo: Prácticas de Responsabilidad Social de la Empresa*. Trabajo fin de carrera Año 2010.

Área XXI. *Modelos Internos y Solvencia II*. Año 2009.

ÁREA XXI. *Own Risk and Solvency Assessment (ORSA), orientación a la Gerencia de Riesgos en la empresa aseguradora*. Julio 2009.

ASM Consultores de Riesgo. *Riesgo Operativo*. Año 2010.

Banco de España. *Guía para la aplicación del Método Estándar en la determinación de los recursos propios por riesgo operacional*. Año 2008.

CEIOPS. *Advice for Level 2 Implementing Measures on Solvency II: Articles 120 to 126 Tests and Standards for Internal Model Approval*. Octubre 2009.

CEIOPS. *Advice for Level 2 Implementing Measures on Solvency II: SCR standard formula - Article 111 (f) Operational Risk*. Año 2009.

CEIOPS. *Advice for Level 2 Implementing Measures on Solvency II: Article 109 1 (f) SCR standard formula - Operational Risk*. Octubre 2009.

CEIOPS. *Lecciones aprendidas de la crisis: Solvencia II y después*. Año 2009.

Comité de supervisión bancario de Basilea. *Buenas prácticas para la gestión y supervisión del riesgo operacional*. Febrero 2003.

COSO. *Enterprise Risk Management – Integrated Framework*. AÑO 2004.

COSO. *Gestión de Riesgos Corporativos - Marco Integrado Técnicas de Aplicación*. Septiembre 2004.

COSO. *Internal Control – Integrated Framework (IC-IF)*. Año 1992.

Cristina Gutiérrez López, Alicia Rodríguez Pérez y José María Fernández Fernández. *Métodos para la Gestión de Riesgos Operacionales en Entidades Financieras*.

Deloitte. *Management of Operational risks in Insurance*. Año 2007.

DIRECTIVA 2009/138/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II).

EIOPA. *EIOPA Report on the fifth Quantitative Impact Study (QIS5) for Solvency II*. Marzo 2011.

Emilio Gómez Déniz y José María Sarabia Alegría. *Teoría de la credibilidad: Desarrollo y aplicaciones en primas de seguros y riesgos operacionales*. Fundación Mapfre. Año 2008.

Ernst & Young. *Solvencia II: implicaciones prácticas*. Año 2007.

Ernst & Young. *Solvencia II: visión general*. Año 2007.

European Commission. *Anexo a las especificaciones técnicas del QIS 5*. Año 2010.

European Commission. *QIS4 Technical Specifications*. Año 2008.

Everis. *Estudio de la Gestión de Riesgos en el Sector Asegurador*. Año 2009.

FERMA. *Estándares de Gerencia de Riesgos*. Año 2003.

Harry H. Panjer. *Operational Risk Modeling Analytics*. Año 2006.

José Antonio Núñez Mora y José Juan Chávez Gudiño. *“Riesgo operativo: esquema de gestión y modelado del riesgo”*. Año 2010.

José Moreno Codina. *Enterprise risk management y Solvencia II. De una buena práctica a una necesidad*. Boletín informativo semanal de seguros, julio, 2009.

KPMG. *Entendiendo la Administración del Riesgo Operacional*. Año 2006.

KPMG. *Metodologías de valoración de la posición financiera global de una entidad aseguradora desde la perspectiva de una supervisión prudencial*. Mayo 2002.

Ley 50/1980, de 8 de octubre, de Contrato de Seguro.

Laura Pilar Duque Santamaría, DGSFP. *Solvencia II. El QIS 3: una gran oportunidad*. Año 2007.

Luis Bautista, DGSFP. *El Nuevo régimen de solvencia en Europa*. Año 2011.

M^a Ángeles Nieto Giménez-Montesinos. Dirección General de Supervisión del Banco de España. *El tratamiento del Riesgo Operacional en Basilea II*.

María Victoria Rivas López, María José Pérez- Fructuoso y Javier Montoya Martín. *Definición de un modelo dinámico de gestión y cuantificación del riesgo operacional para las entidades aseguradoras*. Gerencia de riesgos y seguros nº105. Año 2009.

Mauricio Castro G. *El Nuevo estándar ISO para la Gestión del Riesgo*. Año 2010.

Mazars Auditores S. L. P. *Solvencia II: Notas sobre QIS 5*. Año 2011.

Miguel Delfiner y Cristina Pailhé. *Técnicas cualitativas para la gestión del riesgo operacional*. Octubre 2008.

Miguel Delfiner, Ana Mangialavori y Cristina Pailhé. *Buenas prácticas para la administración del riesgo operacional en entidades financieras*. Enero 2007.

NAS AUDIT. *COSO II: Enterprise Risk Management*. Año 2009.

Pablo Alonso González (Universidad Carlos III de Madrid). *Solvencia II: ejes del proyecto y diferencias con Basilea II*. Año 2007.

Pablo Alonso González e Irene Albarrán Lozano. *Análisis del riesgo en seguros en el marco de Solvencia II: Técnicas estadísticas avanzadas Monte Carlo y Bootstrapping*. Fundación Mapfre. Año 2009.

Pilar Blanco-Morales Limones, Montserrat Guillén Estany e Inmaculada Domínguez Fabián, FUNDACIÓN DE ESTUDIOS FINANCIEROS. *Estudio sobre el sector asegurador en España 2010: Los aspectos cualitativos de Solvencia II*. Año 2011.

PricewaterhouseCoopers. *COSO II – ERM y el Papel del Auditor Interno*. Año 2009.

PriceWaterhouseCoopers. *Gestión del riesgo operacional en las Instituciones Financieras*. Año 2000.

PriceWaterhouseCoopers. *Solvencia II: Principios incluidos en la propuesta de Directiva*. Año 2007.

Santiago Romera (Socio Director de AREA XXI Madrid – España). *Solvencia II, una oportunidad única que conviene aprovechar*. Año 2011.

XIX Congreso Español de Gerencia de Riesgos y Seguros. *La Gerencia de Riesgos en tiempos de turbulencias Financieras*. Mayo 2008.

Páginas webs

Las diferentes páginas webs consultadas, en orden alfabético, son las siguientes:

Blog de Riesgo Operacional. <http://www.riesgooperacional.com/>

Comisión Europea (European Commission). http://ec.europa.eu/index_es.htm

COSO (The Committee of Sponsoring Organizations of the Treadway Commission). <http://www.coso.org/>

DGSFP (Dirección General de Seguros y Fondos de Pensiones). <http://www.dgsfp.meh.es/>

Diccionario de la Lengua Española. Real Academia Española. <http://www.rae.es/>

Diccionario Mapfre de Seguros. www.diccionariomapfredeseguros.es/

EIOPA (European Insurance and Occupational Pensions Authority). <https://eiopa.europa.eu/>

IAA (International Actuarial Association). <http://www.actuaries.org>

IASB (International Accounting Standards Board). <http://www.iasb.org>

ANEXOS

Este apartado está dedicado al desarrollo de ciertos temas a los que se ha hecho referencia a lo largo del trabajo, sin embargo, por su importancia en el tratamiento del riesgo operacional o por las consecuencias que conllevan deben ser desarrollados de forma más extensa.

Dichos temas, en concreto, son tres y cada uno de ellos se corresponde con un anexo.

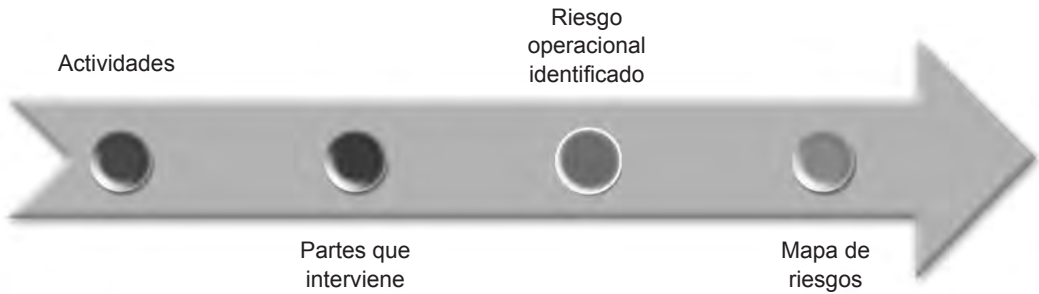
- **Mapas de riesgo operacional.** Los mapas de riesgos son una de las herramientas cualitativas más difundidas y empleadas en la administración del riesgo operacional y, por ello, resulta conveniente analizar en profundidad en qué consisten a través de un ejemplo práctico que se pueda desarrollar en cualquier entidad aseguradora.
- **Comparativa Europa-Latinoamérica en la gestión del riesgo operacional.** El objetivo de este anexo es proporcionar una visión más amplia del contexto del riesgo operacional a través del análisis no sólo del entorno europeo sino también del latinoamericano.
- **El riesgo operacional en prensa.** Después del completo análisis que se ha realizado la teoría del riesgo operacional se conoce perfectamente. Sin embargo, es importante observar algunos casos publicados en prensa de quiebras importantes en empresas. Con esto se pretende poner de manifiesto la magnitud que puede alcanzar una mala gestión del riesgo operacional.

Mapa de riesgo operacional

El objetivo de esta herramienta consiste en identificar las distintas circunstancias que pueden dar lugar a situaciones de riesgo operacional y explicar cómo las compañías de seguros suelen catalogar estos eventos para tratarlos, posteriormente, de forma adecuada.

En particular, se observa esta situación a través de un ejemplo típico que refleja el procedimiento de emisión de pólizas en el que intervienen tanto mediadores de seguros como tramitadores de la compañía en cuestión. Se detectan los distintos riesgos operacionales que pueden surgir en la actividad y los controles que se llevan a cabo para paliar tales riesgos.

El análisis del procedimiento se plasma en un mapa de riesgos que representa una foto de los riesgos operacionales a los que está expuesta la entidad y su intensidad.



Procedimiento de emisión de póliza

El mapa de riesgos será más eficaz si la actividad sobre la que se centra está especificada. Se pueden realizar mapas de riesgos sobre la actividad aseguradora en general, sin embargo, si la actividad está delimitada convenientemente esta herramienta va a reflejar de forma más exacta los riesgos y los mecanismos que se emplean para paliar o mitigar las consecuencias de los mismos; incluso, con las medidas adecuadas y dependiendo del riesgo, estos efectos se pueden llegar a evitar.

Una vez que se centra el mapa de riesgos en un aspecto concreto de la actividad, en este caso en la emisión de pólizas, el proceso de elaboración es muy sencillo. En primer lugar, se exponen en una tabla las actividades que se llevan a cabo en la emisión de pólizas; para ello, es necesario tener en cuenta quiénes intervienen en dicho proceso y cuáles son los diferentes eventos que pueden generar un riesgo operacional en la actividad.

Solo se pueden recoger los eventos que sean susceptibles de generar problemas de tipo operacional si se detallan las fases del procedimiento de emisión de póliza. Por lo tanto, el siguiente paso es identificar todas las etapas de este procedimiento y observar en cuáles de ellas pueden surgir problemas o fallos de este tipo.

FASES DEL PROCEDIMIENTO DE EMISIÓN DE PÓLIZAS

1. El mediador entrega la solicitud de seguro al tomador (o asegurado)

En esta primera etapa se identifica un riesgo operacional y es el que surge como consecuencia de que no se rellene, convenientemente, la solicitud.

2. El mediador recibe la solicitud y valida o no la documentación aportada por el tomador del seguro

Es posible que se reciba la solicitud sin toda la documentación que se requiere para la emisión de la póliza. En este caso, se produce un fallo importante asociado a la falta de información que puede acarrear consecuencias negativas para la compañía; acepta un asegurado sin conocer todas las circunstancias necesarias que lo rodean.

Si, por el contrario, se determina que la documentación aportada no es suficiente o que la solicitud es incompleta el mediador tendrá que reiniciar el proceso. En este caso, el error se ha subsanado a tiempo.

3. El sistema captura la información de la póliza

Si se comprueba que la solicitud y la documentación están completas el sistema va a proceder a capturar la información de la póliza.

Puede ocurrir que se apruebe la solicitud sin toda la documentación necesaria o que, una vez capturada la información en el sistema, esta sea errónea o se produzca cualquier otro fallo tecnológico.

4. Comprobación de la suma asegurada

Una vez que el sistema haya capturado, convenientemente, la información se comprueba que la suma asegurada está dentro de los límites de suscripción autorizados; puede ocurrir que se haya suscrito una póliza cuya suma asegurada exceda los límites establecidos.

Si la suma asegurada está dentro de los límites de suscripción el proceso finaliza con la etapa siguiente.

Si la suma asegurada no está dentro de los límites establecidos el tramitador tendrá que derivar la póliza al departamento técnico, que recibe la solicitud y determina si requiere información adicional para realizar la suscripción.

Si requiere información adicional se la tendrá que solicitar al mediador o al tramitador, dependiendo del tipo de información que necesite, y comenzar el proceso de nuevo.

Si, por el contrario, no requiere información adicional entregará la póliza al tramitador y el procedimiento de emisión de póliza finalizará con la siguiente fase.

5. Formalización de la póliza

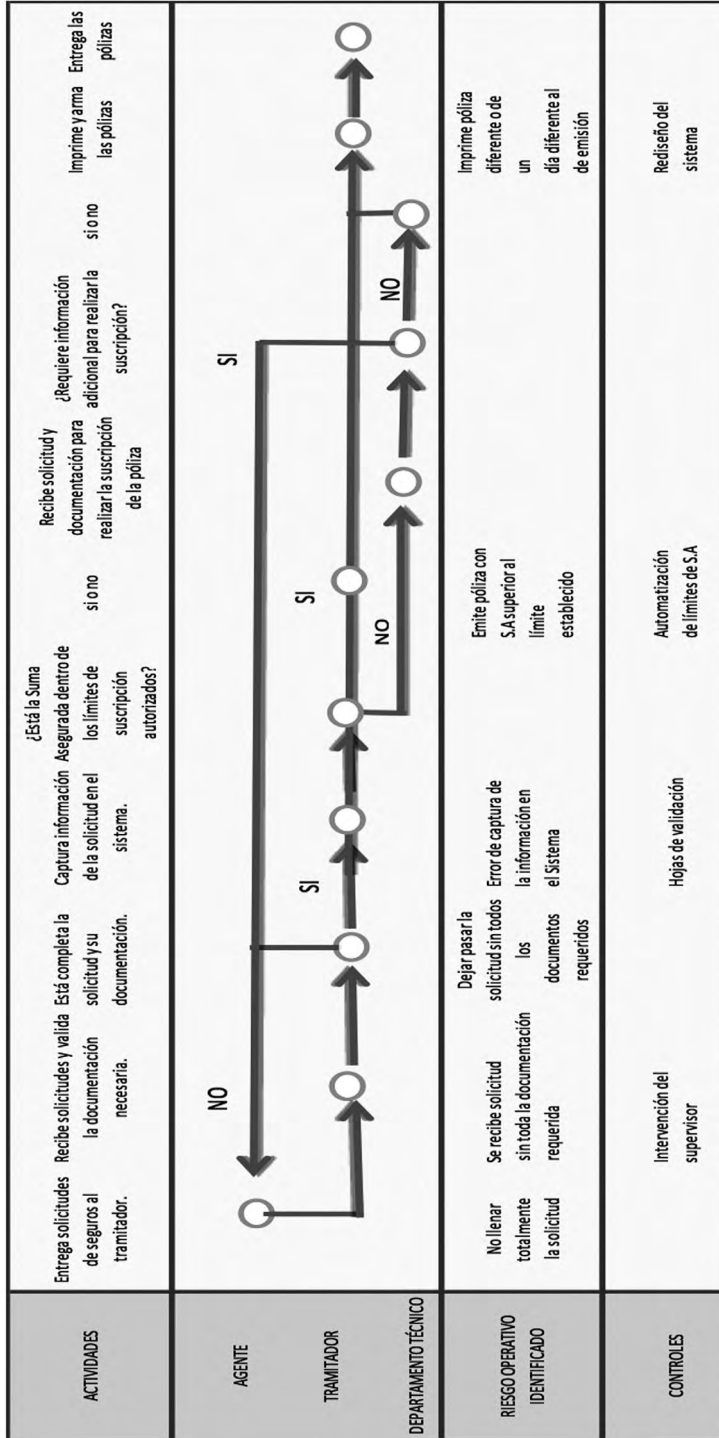
El procedimiento de emisión de póliza finaliza cuando se imprime y arma la misma, es decir, cuando se disponen todos los documentos que la conforman y se entregan al tomador (o asegurado).

En esta última fase se puede producir un error en la impresión y causar pérdidas de tipo operacional.

En cada una de las actividades anteriores, susceptibles de generar un riesgo operacional para la entidad, se pueden llevar a cabo distintos controles que permitan reducir o mitigar dicho riesgo -tal y como se recogen en la siguiente tabla-. Por supuesto esto es un ejemplo; se pueden dar otras actividades dentro de este mismo procedimiento que generen diversas situaciones o eventos potencialmente peligrosos.

Del análisis de las actividades, los riesgos operacionales generados, la intensidad de los mismos y los diferentes controles que se pueden llevar a cabo se desarrolla el mapa de riesgo operacional.

Procedimiento de emisión de póliza



Fuente: elaboración propia.

Identificación de eventos

Después del análisis de las actividades se identifican los diferentes riesgos que se han localizado, su origen, el tipo de riesgo operacional de que se trata y la fuente generadora del mismo.

| Número de Riesgo | Descripción | Origen | Tipo | Fuente |
|------------------|--|----------|---------------------|-----------------------|
| R.O 1 | Recibe solicitud sin tener todos los datos rellenos | Interno. | Riesgo Humano. | Errores, Experiencia. |
| R.O 2 | Error en la captura de información al Sistema | Interno. | Riesgo Humano. | Errores. |
| R.O 3 | Autorizar emisión con Suma Asegurada fuera de los límites de suscripción | Interno. | Riesgo Humano. | Experiencia, Abuso. |
| R.O 4 | Imprimir póliza con error en la impresión | Interno. | Riesgo Tecnológico. | Fallo. |

A continuación, se analiza cuál es su frecuencia, severidad y peso. Con esto se busca posicionar estos datos en el mapa de riesgo operacional.

| Número de Riesgo | Descripción | Frecuencia | Severidad | Peso |
|------------------|--|------------|---------------|------|
| R.O 1 | Recibe solicitud sin tener todos los datos rellenos | Casi Nula. | Moderado. | 2 |
| R.O 2 | Error en la captura de información al Sistema | Raro. | Fuerte. | 6 |
| R.O 3 | Autorizar emisión con Suma Asegurada fuera de los límites de suscripción | Casi Nula. | Fuerte. | 3 |
| R.O 4 | Imprimir póliza con error en la impresión | Probable. | Significante. | 12 |

Elaboración del mapa de riesgo operacional

Una vez que se analiza la frecuencia e intensidad de los riesgos operacionales que se han localizado se procede a posicionar los mismos en un mapa.

La cualidad más importante de esta herramienta es que expresa gráficamente la información. Así, basta con observar el mapa para tener una representación del grado de importancia, en términos de intensidad y frecuencia, de todos los riesgos operacionales a los que se expone la entidad.

Por lo tanto, determina qué riesgos precisan de una mayor atención y hay que tratar de forma urgente, implementando acciones inmediatas, y cuáles no son tan urgentes pero que, también, hay que tener muy presentes.

Retomando el proceso de emisión de pólizas el mapa de riesgo resultante es el siguiente:

| | | | | | |
|-------------------|------------------------|---------------------------|---------------------|-------------------|-------------------------|
| FRECUENCIA | CASI SEGURO (4) | 4 | 8 | 12 | 16 |
| | PROBABLE (3) | 3 | 6 | 9 | R.04 12 |
| | RARO (2) | 2 | 4 | R.02 6 | 8 |
| | CASI NULA (1) | 1 | R.01 2 | R.03 3 | 4 |
| | | INSIGNIFICANTE (1) | MODERADO (2) | FUERTE (3) | SIGNIFICANTE (4) |
| | | SEVERIDAD | | | |

En función de los riesgos identificados se llevan a cabo unas medidas u otras. Independientemente, son necesarios controles generales durante todo el proceso cuya función es prevenir cualquier situación de pérdida por riesgo operacional.

Los riesgos que aparecen en la zona roja son los que deben atenderse con mayor rapidez puesto que su situación es la más crítica. Indudablemente, aquellos que no están en esta zona también se tienen que tener en cuenta ya que si se menosprecian son susceptibles de convertirse en riesgos importantes. Sin embargo, su tratamiento puede realizarse a continuación de los anteriores.

Para cada uno de los riesgos se deben identificar una o varias actividades de control a realizar, algunas de las cuales son modificar el sistema de captación de información, formación del personal, redefinir funciones, etc.

Para los riesgos operacionales identificados en el proceso de emisión de pólizas, son susceptibles de llevarse a cabo los siguientes controles:

| Número de Riesgo | Descripción | Control |
|------------------|--|---|
| R.O 1 | Recibe solicitud sin tener todos los datos rellenos | Supervisión |
| R.O 2 | Error en la captura de información al Sistema | Hojas de validación |
| R.O 3 | Autorizar emisión con Suma Asegurada fuera de los límites de suscripción | Automatización de control de límites de sumas aseguradas por usuarios del sistema |
| R.O 4 | Imprimir póliza con error en la impresión | Solicitar que el sistema permita marcar pólizas que ya se imprimieron |

Periódicamente, se deben revisar los procesos para validar si el riesgo identificado ha disminuido en su calificación en términos de frecuencia-severidad.

Los mapas de riesgos se emplean para cualquier tipo de riesgo y se deben, completar con otras técnicas para aumentar la eficacia del sistema de gestión.

Comparativa: Europa – Latinoamérica

En Europa, los organismos supervisores en coordinación con la Comisión de la Unión Europea, siguiendo las directrices acordadas en el seno de la Conferencia de Autoridades de Control, han participado en los distintos grupos de trabajo constituidos con la finalidad de definir Solvencia II.

En Latinoamérica, no existe una directriz global para la gestión de riesgos pero los supervisores de varios países han anunciado que tomarán Solvencia II como marco de trabajo para sus exigencias regulatorias.

Este anexo se apoya en su desarrollo en el estudio publicado por Everis⁵⁷ en año 2009 y denominado “*Estudio de Gestión de Riesgos en el Sector Asegurador*”.

En primer lugar, se observan cuáles son las principales diferencias entre Europa y Latinoamérica y, a continuación, se analiza la gestión del riesgo en cada uno de los ámbitos geográficos para establecer así una comparativa.

Diferencia entre Europa y Latinoamérica

Para que la comparativa entre dos zonas geográficas refleje la realidad de las mismas es preciso analizar detalladamente las diferencias identificadas. Se tiene en cuenta el entorno político, económico, social y tecnológico de cada una de ellas. En función de estas disparidades, se extraen las conclusiones finales que ponen de manifiesto la situación actual de cada uno de los países.

La Unión Europea, a diferencia de Latinoamérica, permite el sistema de libre prestación de servicios transfronterizos, entre los que se incluyen el seguro. Por lo tanto, todas las entidades ubicadas en el espacio comunitario deberán ajustarse a las mismas normas. Puesto que en Latinoamérica no existe un espacio común, y mucho menos la libertad de prestación de servicios, la legislación de cada uno de los países debería acoger las normas aplicables respecto de las cuestiones de Solvencia II.

Desde el año 1990 hasta la fecha, en muchos países y legislaciones de Latinoamérica, se vienen sustituyendo los conceptos de capital mínimo como concepto estático por normas vinculadas a solvencia.

A nivel mundial existe una organización rectora de los organismos supervisores de seguro, la *Asociación Internacional de Supervisores de Seguros* (IAIS, en inglés). Sin embargo, no está previsto que las normas de Solvencia II entren en vigencia en América de modo común, sino en las adaptaciones que se formulan en las respectivas legislaciones de cada uno de los países que conforman dicha región.

Con estas premisas, lo realmente importante es analizar las disparidades existentes, observar a qué se deben estos contrastes y cómo se pueden homogeneizar ambas regiones de manera que las necesidades de solvencia estén cubiertas.

Conocimiento de los riesgos

Para analizar la gestión de riesgos en regiones tan diferentes como Europa y Latinoamérica resulta conveniente prestar atención al grado de conocimiento de los distintos tipos de riesgos y de Solvencia II, que tiene un entorno respecto del otro. Además, si se analizan las partidas presupuestarias que se dedican a la gestión del riesgo y la

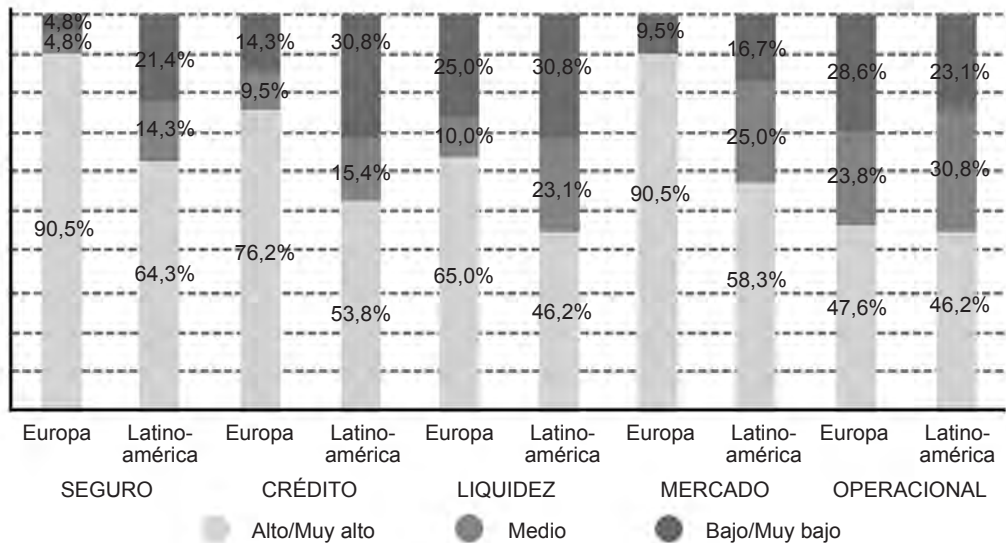
⁵⁷ **Everis** es una consultora multinacional de origen español que ofrece soluciones de negocio, estrategia y desarrollo, mantenimiento de aplicaciones tecnológicas y outsourcing. Fue fundada en Madrid en 1996.

existencia o no de un plan directo se puede tener una idea bastante aproximada del esfuerzo que se realiza en el tratamiento de los riesgos.

- *Grado de Conocimiento de los Distintos Tipos de Riesgos y de Solvencia II*

Las mayores discrepancias entre Europa y Latinoamérica surgen en los riesgos de gestión tradicional, es decir, el riesgo de seguro y el riesgo de mercado.

En general, un importante porcentaje de las compañías latinoamericanas reconocen no tener un gran conocimiento de estos riesgos, frente el 90% de las europeas que afirma tener un alto conocimiento de los mismos. Sin embargo, en los riesgos menos tradicionales, como el riesgo operacional, las diferencias son mínimas, lo que pone de manifiesto que es un riesgo que ha sido ignorado por la industria aseguradora.



Fuente: Everis.

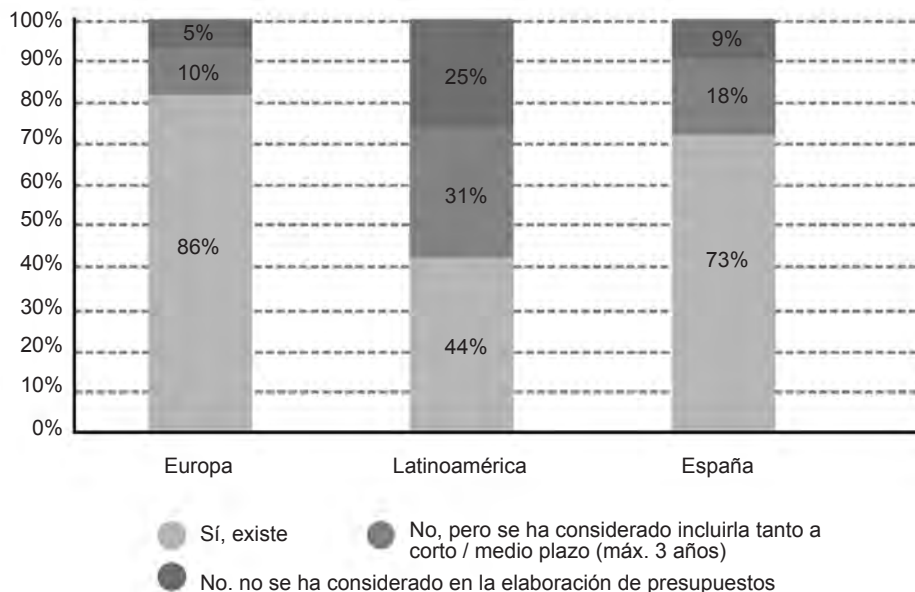
A pesar del dato anterior, el 84,7% de las compañías latinoamericanas participantes aseguran tener algún tipo de conocimiento de Solvencia II.

Se observa que, en el sector asegurador latinoamericano, las entidades van por detrás en la implantación de la gestión del riesgo respecto de Europa. Sin bien es cierto, estas entidades no se impulsan de igual manera en el avance en esta materia por Solvencia II.

- *Partida presupuestaria y plan director*

Respecto de la magnitud de las partidas presupuestarias, en Latinoamérica, el presupuesto asignado es menor. Esto se debe a dos motivos: el coste de desarrollo de los proyectos en esta zona es inferior y la menor concienciación sobre riesgos.

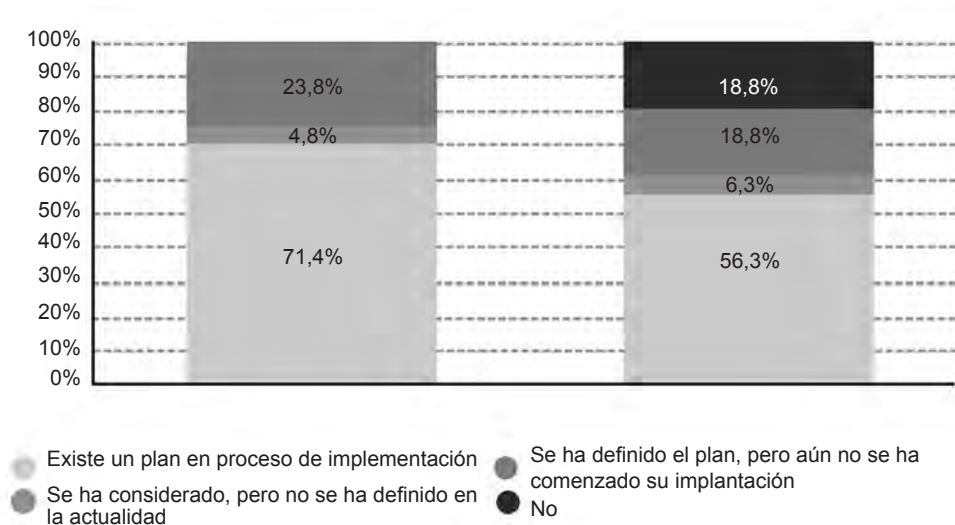
Los valores obtenidos en España se sitúan entorno a los valores europeos, por lo tanto, efectivamente hay una coherencia geográfica.



Fuente: Everis.

La existencia de un plan director demuestra las buenas prácticas adquiridas en cultura de riesgos y supone la obtención de ventajas competitivas. Además, representa un elemento clave en el análisis de las diferencias entre ambas regiones.

En cuanto a su existencia, el 75% de las entidades Europeas declaran que existe un plan director mientras que este porcentaje se reduce a un 62% en el caso de las entidades latinoamericanas. Es destacable que casi un 19% de las entidades latinoamericanas declaran que no existe un plan director en la compañía ni la iniciativa de crearlo, frente al 100% de las entidades europeas que declaran que disponen del plan o, al menos, existe la iniciativa.



Fuente: Everis.

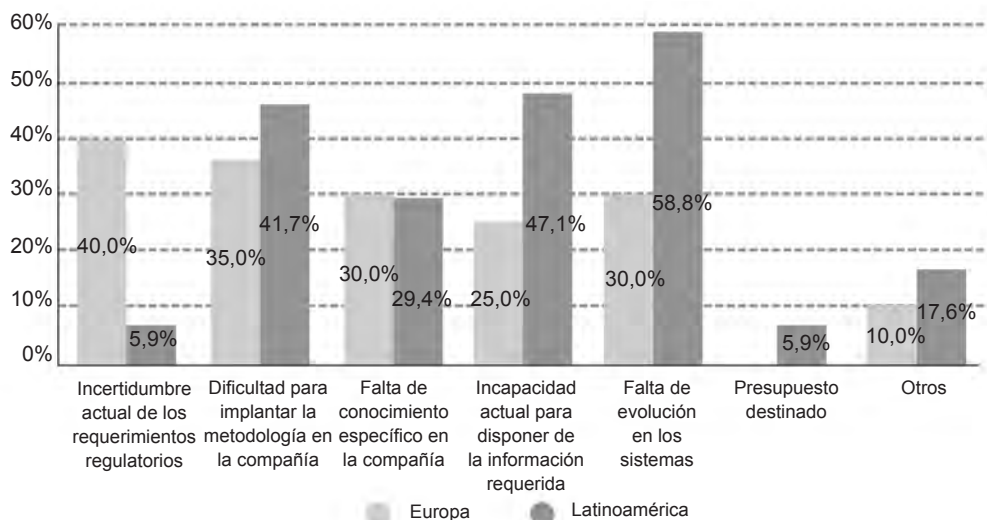
Tras considerar varios aspectos de la gestión de riesgos tales como: el conocimiento que las propias compañías tienen de sus riesgos, el presupuesto que dedican las entidades aseguradoras y la existencia o no de un plan director que marque las directrices, se pueden explicar las principales diferencias en materia de gestión de riesgos entre Europa y Latinoamérica.

Diferencias en la gestión de riesgos

Una vez identificadas las diferencias en materia normativa entre ambas zonas geográficas y los conceptos previos a la propia gestión que muestran la situación de partida, se procede a la comparación de la gestión de riesgos entre Europa y Latinoamérica.

- *Principales Dificultades para un Control Eficiente*

Resulta interesante conocer cuáles son las características que dificultan un adecuado sistema de control y gestión de los riesgos; si se identifican y confrontan las principales adversidades que presentan cada una de las regiones es más fácil observar ambos modelos de control y diferenciarlos que es, precisamente, el objetivo que se persigue.



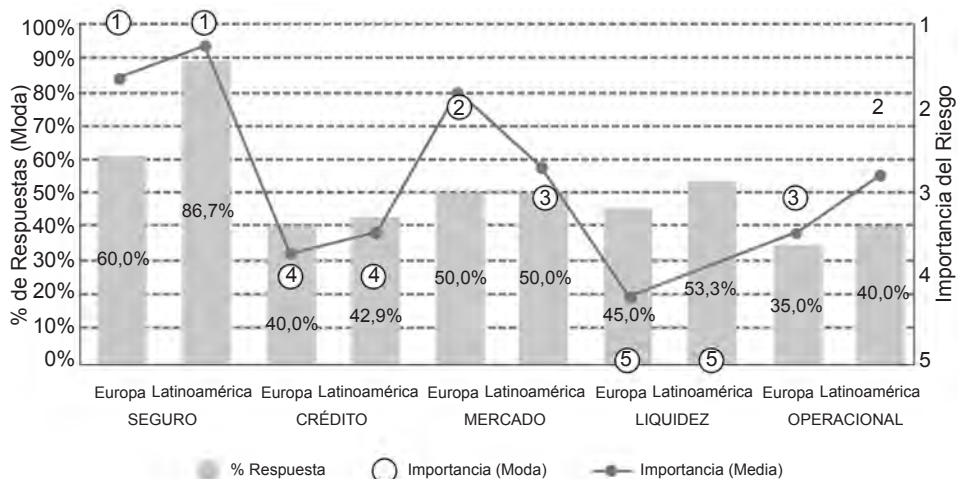
Fuente: Everis.

En cuanto a las circunstancias que impiden o dificultan un control eficiente de los riesgos se aprecian importantes contrastes; se explican, fundamentalmente, por el momento normativo actual. La dificultad principal para las entidades europeas es la incertidumbre actual de los requerimientos. Esto se debe a que las entidades europeas están más avanzadas en el desarrollo de los sistemas de información en comparación con las entidades latinoamericanas.

- *Importancia asignada a cada tipo de riesgo*

En función del ámbito geográfico se observan discrepancias en cuanto a la clasificación del Riesgo de Mercado (importancia 2 y 3 respectivamente) y del Riesgo Operacional (3 para Europa, 2 para Latinoamérica).

Además, el porcentaje de entidades que consideran el Riesgo de Seguro como el más importante es significativamente superior en Latinoamérica que en Europa, con un 86,7% y 60% de las entidades respectivamente.



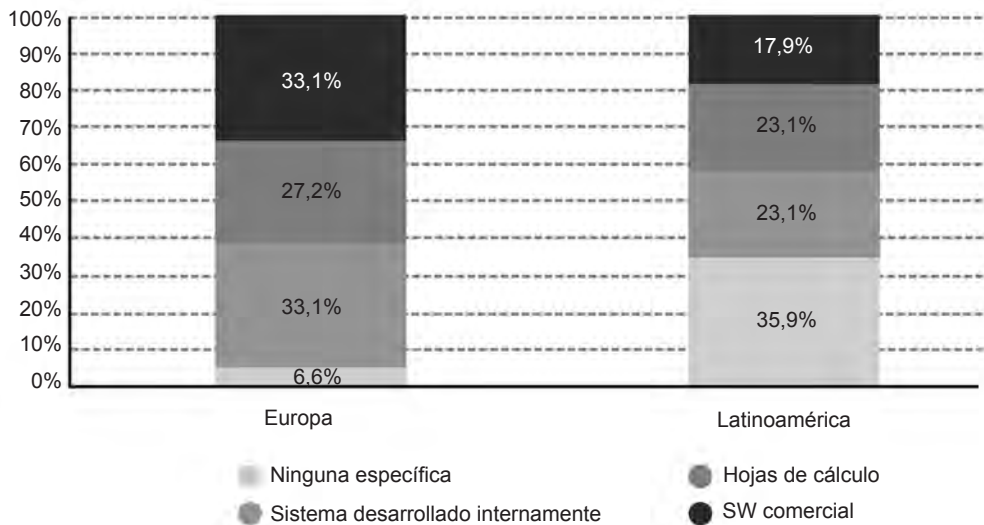
Fuente: Everis.

- Herramientas empleadas en el cálculo de los requisitos de capital*

Mientras en Europa casi un 60% de las entidades utiliza los métodos más sofisticados para el cálculo de los requisitos del capital (simulación, método paramétrico y stress testing), en Latinoamérica este porcentaje se reduce a un 44% de las entidades.

Los métodos menos sofisticados (determinista y benchmarking) se utilizan más en Latinoamérica que en Europa. Las razones se deben, principalmente, a las distintas velocidades en la implementación de la gestión de riesgos y la falta de evolución de los sistemas de las entidades latinoamericanas, tradicionalmente menos avanzadas que las europeas.

Estas mismas razones explican las diferencias observadas en cuanto a los tipos de herramientas que se manejan. Es importante destacar que las entidades aseguradoras europeas cuentan con algún tipo de herramienta para la medición del riesgo, en especial en los riesgos tradicionales, a diferencia de las entidades latinoamericanas que han manifestado no contar con las herramientas adecuadas. Llama la atención que el 36% de las entidades latinoamericanas no utilicen herramientas cuando la inmensa mayoría de las europeas sí que las utilizan.

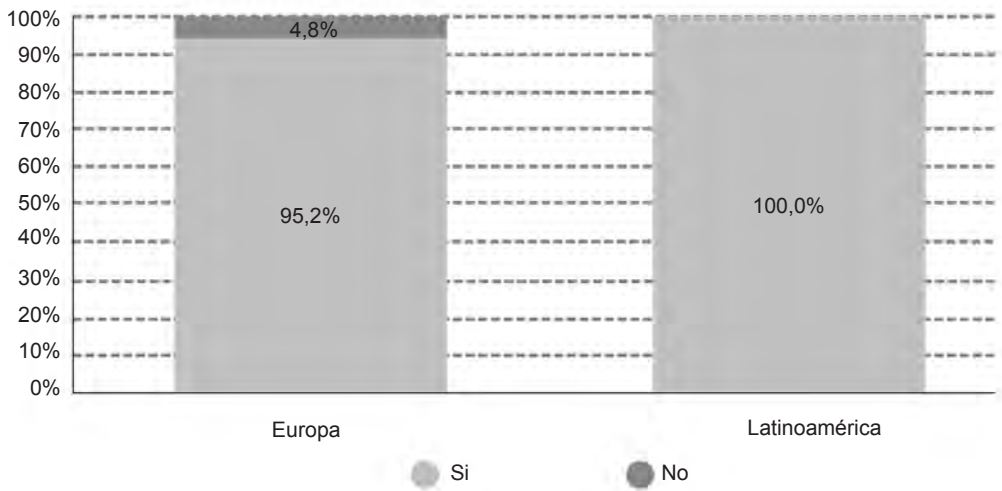


Fuente: Everis.

- *El control de riesgos como objetivo estratégico*

La mayoría de las entidades encuestadas consideran el control de riesgo como un elemento muy importante en el negocio; más del 97% manifiestan que éste forma parte de los objetivos estratégicos del sector asegurador.

Sin embargo, en Europa existe un pequeño porcentaje de empresas que no consideran el control de riesgos como un objetivo estratégico del sector. Con más detalle, se observa que la totalidad de estas entidades son portuguesas.

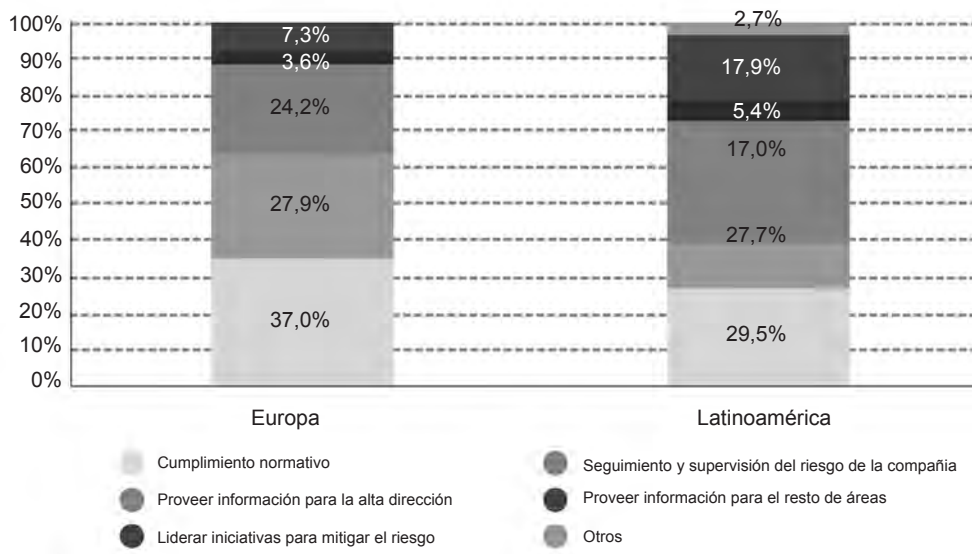


Fuente: Everis.

- *Objetivos del sector para la gestión de riesgos*

En general, el 34% de las entidades considera que el principal objetivo del sector asegurador es el cumplimiento normativo. Esto es así para el 37% de las entidades europeas y para el 29% de las entidades latinoamericanas.

Sin embargo, estos datos resultan sorprendentes ya que, aunque para el 82% de las entidades latinoamericanas el personal tiene como función principal el cumplimiento normativo, para el 85% de las entidades europeas la función más importante es la que engloba la identificación, medición, monitorización y control de cada tipo de riesgo.



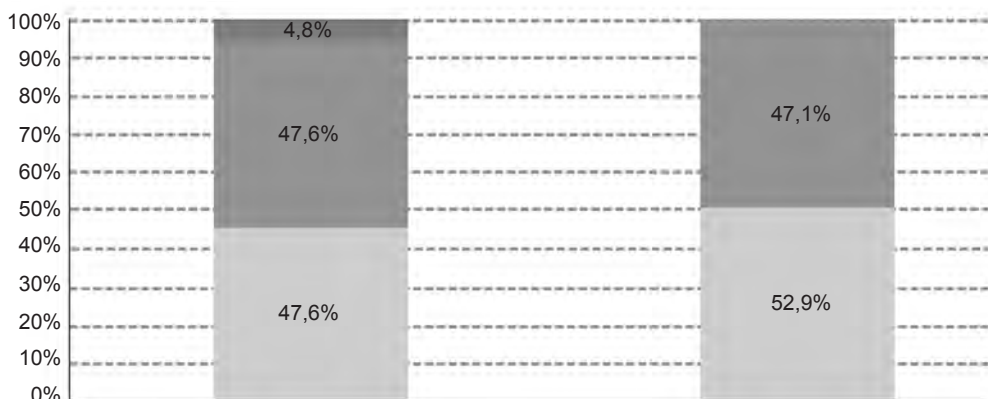
Fuente: Everis.

- *Estrategia más empleada para la gestión de los riesgos*

El 50% de las entidades considera que el sector afronta, mayoritariamente, el control de riesgos en el ámbito organizativo mediante la existencia de un área independiente dentro de las compañías.

Por otra parte, un 47 % de las entidades entienden que la estrategia principal consiste en disponer de personal específico integrado en distintas áreas. Por último, el 3% restante opina que en general el sector no dispone de personal específico dedicado al control de riesgos.

Resulta sorprendente que el 4,8% de las entidades europeas entienden que no hay personal específico dedicado al control de riesgos y que, precisamente, el 9% de las entidades españolas tengan dicha apreciación.



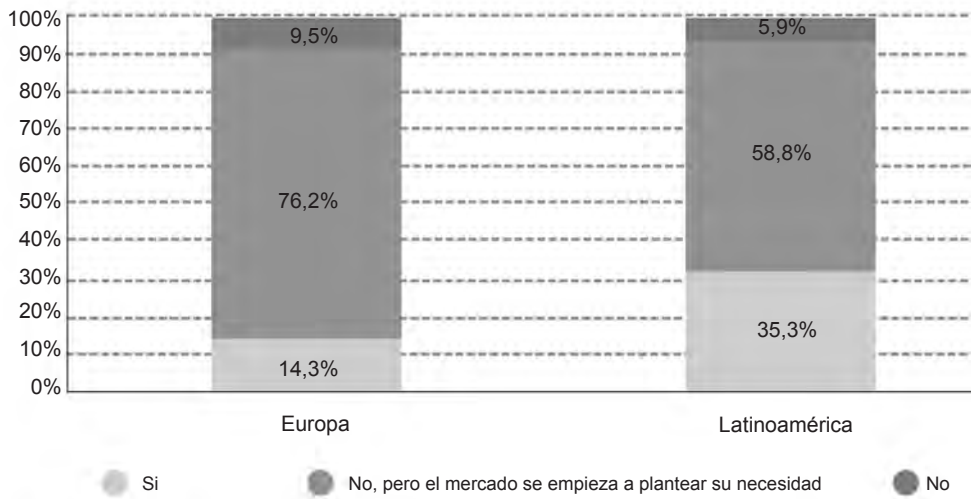
- Existe un área independiente dentro de la compañía
- Hay personal específico, que se encuentra integrado dentro de distintas áreas de la compañía
- No hay personal específico dedicado al control de riesgos

Fuente: Everis.

- *Reporte de la información en la gestión del riesgo*

Ante la pregunta de si las entidades consideran que dentro de sus herramientas de reporting actuales disponen de información de control de riesgos, el 68% de las mismas opina que el sector no dispone de tal información pero que el mercado comienza a plantearse su necesidad. En el caso de las entidades europeas este porcentaje se eleva hasta el 76%.

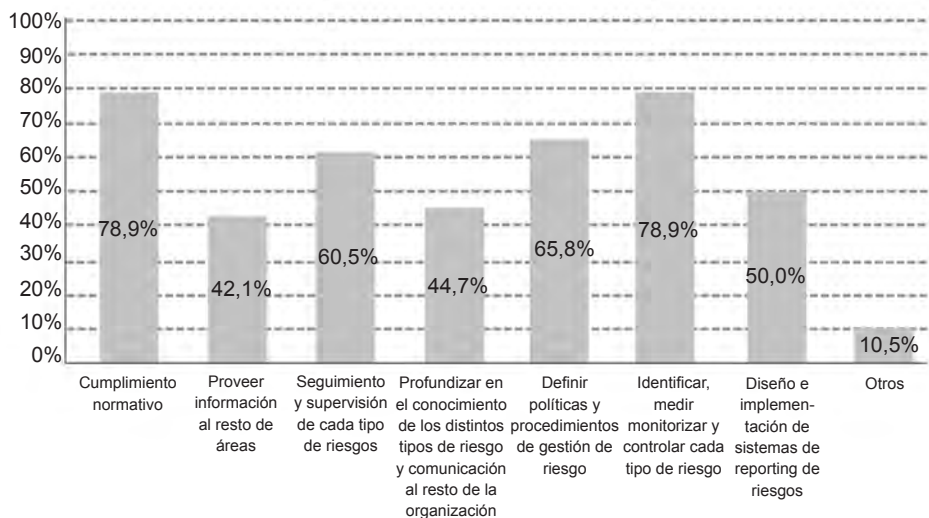
En cuanto a las entidades latinoamericanas, el 35,3% considera que el sector dispone de dicha información, lo que contrasta con el 14,3% de las entidades europeas.



Fuente: Everis.

- *Principales funciones del personal encargado del control de riesgos*

Como refleja el grafico siguiente, las principales funciones del personal asignado al control de riesgos son: el cumplimiento normativo y la identificación, monitorización y control de cada tipo de riesgo, ambas con un 78,9% de las respuestas.



Fuente: Everis.

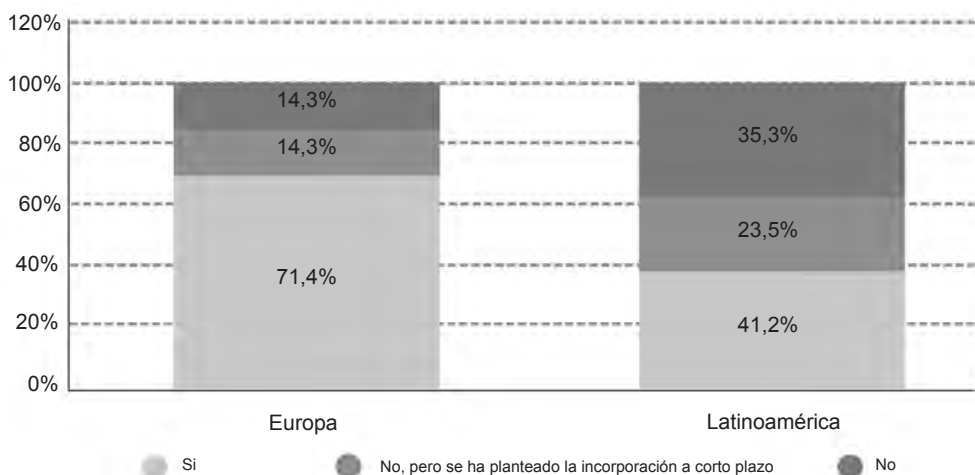
En Europa existe una mayor sensibilización en cuanto al control de riesgos. Esta situación se debe, probablemente, a la implantación de Solvencia II. Además, la principal función del personal responsable es la identificación, monitorización y control de cada tipo de riesgo.

| EUROPA | | LATINOAMÉRICA | |
|--|-------|--|-------|
| 1 Identificar, medir, monitorizar y controlar cada tipo de riesgo | 85,7% | 1 Cumplimiento normativo | 82,4% |
| 2 Cumplimiento normativo | 76,2% | 2 Definir políticas y procedimientos de gestión de riesgo | 76,5% |
| 3 Diseño e implementación de sistemas de <i>reporting</i> de riesgos | 61,9% | 3 Seguimiento y supervisión de cada tipo de riesgos | 70,6% |
| 4 Definir políticas y procedimientos de gestión de riesgo | 57,1% | 4 Identificar, medir, monitorizar y controlar cada tipo de riesgos | 70,6% |
| 5 Seguimiento y supervisión de cada tipo de riesgos | 52,4% | 5 Promover información al resto de áreas | 64,7% |
| 6 Profundizar en el conocimiento de los distintos tipos de riesgo y comunicación al resto de la organización | 42,9% | 6 Profundizar en el conocimiento de los distintos tipos de riesgo y comunicación al resto de la organización | 47,1% |
| 7 Proveer información al resto de áreas | 23,8% | 7 Diseño e implementación de los sistemas de <i>reporting</i> de riesgos | 35,3% |
| 8 Otros | 4,8% | 8 Otros | 17,6% |

Fuente: Everis.

- *Gestión de riesgos como un proceso Independiente*

Si se considera la integración del control de riesgos dentro del mapa corporativo de procesos se observa que, aunque se aprecian algunas diferencias, en la mayoría de las organizaciones el control de riesgos es un proceso independiente.



Fuente: Everis.

A la vista de los resultados observados, resulta esencial contar con una metodología eficaz para la ejecución de proyectos de implantación de modelos de riesgo operativo.

Cuando se lleva a cabo tanto un análisis de la situación actual como la definición de un modelo para la gestión de riesgos, es fundamental considerar absolutamente todos los procesos operativos dentro de la entidad y no sólo aquellos que se consideren críticos. De la misma forma, deberán considerarse aquellos procesos operativos incluidos en el Plan de Continuidad de Negocio y el Plan de Recuperación de Desastres.

Por otra parte, la definición del modelo de gestión de riesgos, así como su medición y seguimiento, deberá estar alineada con los procesos. De tal forma que, cuando se lleve a cabo una modificación o reestructuración en los procesos, el modelo sea revisado y actualizado para que se adecue a la nueva situación.

Conviene involucrar a toda la organización para que la implementación del modelo de gestión de riesgos sea eficaz y se asegure, en todo momento, una adecuada gestión del cambio. Para que esto sea posible, es necesario que todo aquello que parta de los niveles más altos de la compañía se transmita, convenientemente, al resto de la entidad.

Finalmente, los sistemas y herramientas de medición no lo son todo para asegurar el éxito de una iniciativa de esta magnitud; la gestión del riesgo es una cultura que debe ser adoptada por la organización en su conjunto, y como tal, debe asumirse tanto su definición, como su implementación y seguimiento.

Por lo tanto, y a pesar de las diferencias observadas, en Latinoamérica el 84,7% de las compañías manifiestan tener algún tipo de conocimiento de Solvencia II y de las

directrices establecidas para una adecuada gestión de los riesgos. Sin embargo, hay tres razones fundamentales que reflejan, y justifican, la importancia de estas disparidades:

- Solvencia II nace en el seno de la UE
- El coste de desarrollo de los proyectos es inferior
- Se tiene menor concienciación sobre riesgos

Una vez más, es importante recalcar que **una cultura de riesgos apropiada que involucre a toda la entidad, y a todos los niveles, resulta clave para el éxito del proceso de gestión de riesgos.**

El riesgo operacional en prensa

La necesidad de poner en práctica un adecuado proceso de gestión del riesgo operacional en todas las áreas de actividad, ha quedado más que demostrada a lo largo de los últimos años.

Se ha constatado que las entidades que tienen configurado un adecuado sistema de control de sus riesgos, son capaces de afrontar no sólo los peligros o las amenazas propias de cualquier actividad sino, también, los cambios en el entorno. De la misma forma, el tratamiento que se realiza de los riesgos influye tanto en el resultado final de la entidad como en su solvencia.

Este anexo pretende trasladar la teoría aprendida a casos prácticos concretos, la mayoría de ellos conocidos y publicados en prensa. El objetivo, por lo tanto, es demostrar como una gestión inadecuada del riesgo operacional puede acarrear una serie de consecuencias, en muchos casos irreversibles, para las entidades que no han prestado la atención o el cuidado suficiente al mismo.

Los ejemplos que se analizan a continuación son, fundamentalmente, de entidades financieras ya que la normativa en materia de solvencia y gestión de riesgos para las entidades aseguradoras está basada en la normativa bancaria, Basilea II.

Pérdidas por riesgo operacional publicadas en prensa

Los casos seleccionados sirven de ejemplo para analizar la importancia del riesgo operacional, sin embargo, son sólo algunos los que existen en la realidad; éste riesgo es inherente a la actividad financiera y, por lo tanto, forma parte de la misma desde siempre.

Se ha comprobado que las pérdidas derivadas de los procesos operacionales han sido superiores, en cuantía, a las



más importantes de las provocadas por el riesgo de mercado o de crédito. Por otra parte, según una encuesta elaborada por la *Asociación de Bancos Británicos*, el 24% de los bancos han experimentado pérdidas por motivos operacionales superiores a 1,5 millones de euros en los últimos 3 años.

Debido a estos motivos, entre otros, es conveniente analizar como surgen algunas de las pérdidas financieras derivadas de eventos de tipo operacional más importantes acaecidas en los últimos años.

BANCO BARINGS (1995)

El Barings Bank (fundado en 1762) fue la compañía bancaria comercial más antigua de Londres hasta su colapso en 1995, después de que uno de los empleados, Nick Leeson, perdiera 827 millones de libras especulando en contratos de futuros.

Las actividades del banco en Singapur entre 1992 y 1995 permitieron a Nick Leeson operar sin supervisión en Londres. Debido a esto, fue capaz de hacer “aparentemente” pequeñas apuestas en el mercado de futuros y cubrir sus pérdidas al reportar pérdidas como ganancias al *Barings* en Londres.

A través de una cuenta oculta, Leeson comenzó a comerciar agresivamente en futuros y opciones en el SIMEX⁵⁸. Sus decisiones provocaban pérdidas de grandes sumas, pero él empleaba dinero confiado al banco para utilizarlo en sus propias cuentas. Falsificó registros de comercio en los sistemas informáticos del banco y usó dinero destinado al pago de márgenes y otras actividades.

Cuando ocurrió el terremoto de Kobe, Leeson apostó a una recuperación rápida del *Nikkei Stock Average*⁵⁹ que no se materializó. En ese momento, auditores del *Barings Bank* descubrieron el fraude pero las pérdidas que se habían generado eran del doble del capital disponible del banco.

Barings fue declarado insolvente el 26 de febrero de 1995. El colapso fue dramático al haber sido repentinamente retenidos los bonos de sus empleados en el mundo.

Conclusiones

La conclusión principal es que de haberse llevado a cabo una adecuada gestión del riesgo operacional la quiebra del Banco Baring se podría haber evitado.

Una gestión óptima del riesgo operacional, para este caso concreto, se hubiera manifestado con las siguientes prácticas:

⁵⁸ **SIMEX:** Intercambio Monetario Internacional de Singapur.

⁵⁹ **Nikkei Stock Average:** Nombre del índice más representativo de la bolsa de Tokio. Es la suma de las cotizaciones de los 225 valores más importantes de la bolsa.

- Establecimiento de distintos niveles para la autorización de operaciones.
- Segregación de funciones entre front office y back office.
- Grabación de transacciones y autorización de clientes.
- Supervisión periódica.
- Realización de una auditoría interna suficiente.

Con la puesta en marcha de estas prácticas, probablemente, situaciones como la anterior se pueden si no evitar del todo si mitigar algunas de sus consecuencias.

DAIWA BANK (1995)

El escándalo del Daiwa Bank tiene como protagonista al trader⁶⁰ Toshihide Iguchi, quien se encargaba del back-office de una sucursal de Daiwa en Nueva York y, cuando fue promovido a trader, no delegó sus tareas de back-office.

La función principal de la sucursal era la salvaguarda de los bonos del tesoro de los Estados Unidos. Así, para pagar las pérdidas derivadas de sus decisiones equivocadas vendió bonos y falsificó los estados contables para que no se indicase que éstos habían sido vendidos.

Cuando Daiwa decidió separar las actividades de back-office del front-office salió a la luz el fraude. El monto total de pérdida fue de 1.1 billones de dólares y de 340 millones de dólares de multa.

Conclusiones

Como consecuencia de la mala gestión de uno de sus empleados se produjeron pérdidas muy importantes. Estos problemas surgen por no contar con adecuados mecanismos de tratamiento del riesgo operacional, tales como:

- Segregación de funciones donde existe el potencial de conflictos de interés.
- Vigilancia en el cumplimiento de controles existentes.
- Ausencia de una supervisión efectiva por parte de los auditores internos.
- Falta de conciliación de transacciones por terceros.
- Un comportamiento cíclico.

⁶⁰ **Trader:** Persona física que en una sociedad bursátil, o de intermediación bursátil, se dedica a gestionar una clientela institucional.

CASO ENRON (2001)

Enron Corporation fue una empresa de energía con sede en Houston (Texas) que empleaba cerca de 21.000 personas hacia mediados de 2001, antes de su quiebra.

Una serie de técnicas contables fraudulentas, apoyadas por su empresa auditora el entonces prestigioso despacho Arthur Andersen⁶¹, permitieron que esta empresa fuera considerada como la séptima corporación de los Estados Unidos y se esperaba que siguiera siendo empresa dominante en sus áreas de negocio. En lugar de ello, se convirtió en el más grande fraude empresarial de la historia.

Después de varios escándalos sobre el uso de prácticas irregulares de contabilidad, Enron INC llegó al borde de la bancarrota hacia mediados de noviembre de 2001. Las acciones de la empresa en Wall Street cayeron cuando se hizo público que la mayoría de sus ganancias eran el resultado de negocios con una de sus subsidiarias; práctica que les permitía “maquillar” en los balances financieros las gigantescas pérdidas que había sufrido.

Las implicaciones a largo plazo de la caída de Enron aún continúan y, desde el año 2002, se lleva a cabo la investigación sobre el enorme desfaldo cometido a sus accionistas y empleados.

La importancia del caso reside en que fue el principal detonante en la elaboración de la Ley Sarbanes Oxley. Con esta ley se establecieron medidas de control interno más rígidas y eficientes para evitar que las empresas que cotizan en bolsa realicen fraudes como el que sucedió con Enron.

Conclusiones

En respuesta al importante fraude cometido se elaboró la Ley Sarbanes Oxley que sienta las bases del control interno al que deben estar sometidas las entidades en la actualidad.

En el caso Enron se aprecia una falta de tres elementos fundamentales y necesarios para un adecuado tratamiento de los riesgos. Éstos son:

- Evaluación de principales criterios contables por tercero independiente.
- Revisión, conciliación y documentación clara de pasivos.
- Suficiencia en la auditoría interna.

⁶¹ **Arthur Andersen LLP** fue hasta el año 2002 una de las cinco grandes compañías auditoras del mundo. Además de la auditoría, ofrecía servicios de asesoramiento fiscal y jurídico. En 2002, Arthur Andersen se vio involucrado en el escándalo financiero Enron, lo que motivó el cese de sus actividades.

Estos casos que se han expuesto resaltan la importancia de un marco general y adecuado para la gestión y el tratamiento del riesgo operacional. Sin embargo, existen otros muchos ejemplos que ponen de manifiesto esta necesidad; son numerosos los casos de pérdidas importantes e incluso quiebras que han tenido lugar como consecuencia del acaecimiento de diferentes eventos de tipo operacional.

Para tener constancia de algunos casos importantes, se adjunta en la página siguiente una tabla dónde se explican brevemente otros ejemplos de pérdidas de este tipo que surgen como consecuencia directa de una falta de gestión del riesgo operacional o de un tratamiento inadecuado del mismo.

Otros ejemplos de pérdidas por riesgo operacional

Fuente: elaboración propia

| AÑO | INSTITUCIÓN | PÉRDIDA OCACIONADA | DESCRIPCIÓN |
|------|---|-------------------------------|---|
| 1991 | Metalgesellschaft (industria del petróleo) — subsidiaria de Deutsche Bank | US \$ 1.4 billones | Error de modelo resultante de incorrectos supuestos sobre el precio de futuros. |
| 1994 | Procter & Gamble (P&G) y Bankers Trust | US \$ 20 y US \$ 1.4 millones | Transacciones con derivados de propiedad de P&G y administrados por Bankers Trust que no fueron bien valorados ni segregados. |
| 1997 | NatWest Capital Markets | 90 millones de libras | Errores en los supuestos y modelos de pricing de opciones y swaps. |

Continúa

| AÑO | INSTITUCIÓN | PÉRDIDA OCASIONADA | DESCRIPCIÓN |
|------|----------------------|--|---|
| 2001 | Lehman Brothers Bank | 40 millones de libras (temporales) | Un broker al ejecutar una orden de venta añadió un cero más a la derecha y realizó una operación de 300 millones de libras esterlinas, en lugar de los 30 millones perseguidos. El índice FTSE 100 cayó 120 puntos. |
| 2001 | USB Warburg Bank | US \$ 50 millones | Un trader erró al transar acciones a un precio equivalente al número de acciones y a una cantidad equivalente al precio. |
| 2002 | Worldcom | US \$ 180 billones para accionistas y más de US \$ 8 billones de costos para la industria. | El presidente de la compañía efectuó fraudes contables. |
| 2002 | Allied Irish Banks | US \$ 691 millones | Transacciones fraudulentas llevadas a cabo por un trader desde 1997. |
| 2007 | Crisis Sub-Prime | US \$ 195 billones para la industria financiera | Fallos en los procesos de otorgamiento de créditos, burbuja hipotecaria, disminución de requerimientos, complejos instrumentos de crédito estructurados y baja comprensión de la exposición, entre otros. |

COLECCIÓN “CUADERNOS DE LA FUNDACIÓN”

Instituto de Ciencias del Seguro

*Para cualquier información o para adquirir nuestras publicaciones
puede encontrarnos en:*

FUNDACIÓN MAPFRE

Publicaciones

Paseo de Recoletos 23 – 28004 Madrid – (España)

Telf.: + 34 915 818 768 Fax: +34 915 818 409

www.fundacionmapfre.com/cienciasdelseguro

- 177. Riesgo operacional en el marco de Solvencia II. 2012
- 176. Un siglo de seguros marítimos barceloneses en el comercio con América. 2012
- 175. El seguro de Caución. 2012
- 174. La Contabilidad de los corredores de seguros y los planes y fondos de pensiones. 2012
- 173. El seguro de Vida en América Latina. 2011
- 172. Gerencia de riesgos sostenibles y Responsabilidad Social Empresarial en la entidad aseguradora. 2011
- 171. Investigaciones en Seguros y Gerencia de Riesgos. 2011
- 170. Introdução ao Resseguro. 2011
- 169. La salud y su aseguramiento en Argentina, Chile, Colombia y España. 2011
- 168. Diferencias de sexo en conductas de riesgo y tasa de mortalidad diferencial entre hombres y mujeres. 2011
- 167. Movilización y rescate de los compromisos por pensiones garantizados mediante contrato de seguros. 2011

166. Embedded Value aplicado al ramo No Vida. 2011
165. Las sociedades cautivas de Reaseguro. 2011
164. Daños del amianto: litigación, aseguramiento de riesgos,y fondos de compensación.. 2011
163. El riesgo de tipo de interés: experiencia española y Solvencia II. 2011
162. I Congreso sobre las Nuevas Tecnologías y sus repercusiones en el Seguro: Internet, Biotecnología y Nanotecnología. 2011
161. La incertidumbre bioactuarial en el riesgo de la longevidad. Reflexiones bioéticas. 2011
160. Actividad aseguradora y defensa de la competencia. La exención antitrust del sector asegurador. 2011
159. Estudio empírico sobre la tributación de los seguros de vida. 2010
158. Métodos estocásticos de estimación de las provisiones técnicas en el marco de Solvencia II. 2010
157. Introducción al Reaseguro. 2010
156. Encuentro Internacional sobre la Historia del Seguro. 2010
155. Los sistemas de salud en Latinoamérica y el papel del seguro privado. 2010
154. El Seguro de Crédito en Chile. 2010
153. El análisis financiero dinámico como herramienta para el desarrollo de modelos internos en el marco de Solvencia II. 2010
152. Características sociodemográficas de las personas con doble cobertura sanitaria. Un estudio empírico. 2010
151. Solidaridad impropia y seguro de Responsabilidad Civil. 2010
150. La prevención del blanqueo de capitales en las entidades aseguradoras, las gestoras y los corredores de seguros 2010

149. Fondos de aseguramiento agropecuario y rural: la experiencia mexicana en el mutualismo agropecuario y sus organizaciones superiores. 2010
148. Avaliação das Provisões de Sinistro sob o Enfoque das Novas Regras de Solvência do Brasil. 2010
147. El principio de igualdad sexual en el Seguro de Salud: análisis actuarial de su impacto y alcance. 2010
146. Investigaciones históricas sobre el Seguro español. 2010
145. Perspectivas y análisis económico de la futura reforma del sistema español de valoración del daño corporal. 2009
144. Contabilidad y Análisis de Cuentas Anuales de Entidades Aseguradoras (Plan contable 24 de julio de 2008). 2009
143. Mudanças Climáticas e Análise de Risco da Indústria de Petróleo no Litoral Brasileiro. 2009
142. Bases técnicas dinámicas del Seguro de Dependencia en España. Una aproximación en campo discreto. 2009
141. Transferencia Alternativa de Riesgos en el Seguro de Vida: Titulización de Riesgos Aseguradores. 2009
140. Riesgo de negocio ante asegurados con múltiples contratos. 2009
139. Optimización económica del Reaseguro cedido: modelos de decisión. 2009
138. Inversiones en el Seguro de Vida en la actualidad y perspectivas de futuro. 2009
137. El Seguro de Vida en España. Factores que influyen en su progreso. 2009
136. Investigaciones en Seguros y Gestión de Riesgos. RIESGO 2009.
135. Análisis e interpretación de la gestión del fondo de maniobra en entidades aseguradoras de incendio y lucro cesante en grandes riesgos industriales. 2009

134. Gestión integral de Riesgos Corporativos como fuente de ventaja competitiva: cultura positiva del riesgo y reorganización estructural. 2009
133. La designación de la pareja de hecho como beneficiaria en los seguros de vida. 2009
132. Aproximación a la Responsabilidad Social de la empresa: reflexiones y propuesta de un modelo. 2009
131. La cobertura pública en el seguro de crédito a la exportación en España: cuestiones prácticas-jurídicas. 2009
130. La mediación en seguros privados: análisis de un complejo proceso de cambio legislativo. 2009
129. Temas relevantes del Derecho de Seguros contemporáneo. 2009
128. Cuestiones sobre la cláusula cut through. Transferencia y reconstrucción. 2008
127. La responsabilidad derivada de la utilización de organismos genéticamente modificados y la redistribución del riesgo a través del seguro. 2008
126. Ponencias de las Jornadas Internacionales sobre Catástrofes Naturales. 2008
125. La seguridad jurídica de las tecnologías de la información en el sector asegurador. 2008
124. Predicción de tablas de mortalidad dinámicas mediante un procedimiento bootstrap. 2008
123. Las compañías aseguradoras en los procesos penal y contencioso-administrativo. 2008
122. Factores de riesgo y cálculo de primas mediante técnicas de aprendizaje. 2008
121. La solicitud de seguro en la Ley 50/1980, de 8 de octubre, de Contrato de Seguro. 2008

120. Propuestas para un sistema de cobertura de enfermedades catastróficas en Argentina. 2008
119. Análisis del riesgo en seguros en el marco de Solvencia II: Técnicas estadísticas avanzadas Monte Carlo y Bootstrapping. 2008
118. Los planes de pensiones y los planes de previsión asegurados: su inclusión en el caudal hereditario. 2007
117. Evolução de resultados técnicos e financeiros no mercado segurador iberoamericano. 2007
116. Análisis de la Ley 26/2006 de Mediación de Seguros y Reaseguros Privados. 2007
115. Sistemas de cofinanciación de la dependencia: seguro privado frente a hipoteca inversa. 2007
114. El sector asegurador ante el cambio climático: riesgos y oportunidades. 2007
113. Responsabilidade social empresarial no mercado de seguros brasileiro influências culturais e implicações relacionais. 2007
112. Contabilidad y análisis de cuentas anuales de entidades aseguradoras. 2007
111. Fundamentos actuariales de primas y reservas de fianzas. 2007
110. El Fair Value de las provisiones técnicas de los seguros de Vida. 2007
109. El Seguro como instrumento de gestión de los M.E.R. (Materiales Especificados de Riesgo). 2006
108. Mercados de absorción de riesgos. 2006
107. La exteriorización de los compromisos por pensiones en la negociación colectiva. 2006
106. La utilización de datos médicos y genéticos en el ámbito de las compañías aseguradoras. 2006

105. Los seguros contra incendios forestales y su aplicación en Galicia. 2006
104. Fiscalidad del seguro en América Latina. 2006
103. Las NIC y su relación con el Plan Contable de Entidades Aseguradoras. 2006
102. Naturaleza jurídica del Seguro de Asistencia en Viaje. 2006
101. El Seguro de Automóviles en Iberoamérica. 2006
100. El nuevo perfil productivo y los seguros agropecuarios en Argentina. 2006
99. Modelos alternativos de transferencia y financiación de riesgos "ART": situación actual y perspectivas futuras. 2005
98. Disciplina de mercado en la industria de seguros en América Latina. 2005
97. Aplicación de métodos de inteligencia artificial para el análisis de la solvencia en entidades aseguradoras. 2005
96. El Sistema ABC-ABM: su aplicación en las entidades aseguradoras. 2005
95. Papel del docente universitario: ¿enseñar o ayudar a aprender?. 2005
94. La renovación del Pacto de Toledo y la reforma del sistema de pensiones: ¿es suficiente el pacto político?. 2005
92. Medición de la esperanza de vida residual según niveles de dependencia en España y costes de cuidados de larga duración. 2005
91. Problemática de la reforma de la Ley de Contrato de Seguro. 2005
90. Centros de atención telefónica del sector asegurador. 2005
89. Mercados aseguradores en el área mediterránea y cooperación para su desarrollo. 2005

88. Análisis multivariante aplicado a la selección de factores de riesgo en la tarificación. 2004
87. Dependencia en el modelo individual, aplicación al riesgo de crédito. 2004
86. El margen de solvencia de las entidades aseguradoras en Iberoamérica. 2004
85. La matriz valor-fidelidad en el análisis de los asegurados en el ramo del automóvil. 2004
84. Estudio de la estructura de una cartera de pólizas y de la eficacia de un Bonus-Malus. 2004
83. La teoría del valor extremo: fundamentos y aplicación al seguro, ramo de responsabilidad civil autos. 2004
81. El Seguro de Dependencia: una visión general. 2004
80. Los planes y fondos de pensiones en el contexto europeo: la necesidad de una armonización. 2004
79. La actividad de las compañías aseguradoras de vida en el marco de la gestión integral de activos y pasivos. 2003
78. Nuevas perspectivas de la educación universitaria a distancia. 2003
77. El coste de los riesgos en la empresa española: 2001.
76. La incorporación de los sistemas privados de pensiones en las pequeñas y medianas empresas. 2003
75. Incidencia de la nueva Ley de Enjuiciamiento Civil en los procesos de responsabilidad civil derivada del uso de vehículos a motor . 2002
74. Estructuras de propiedad, organización y canales de distribución de las empresas aseguradoras en el mercado español. 2002
73. Financiación del capital-riesgo mediante el seguro. 2002

72. Análisis del proceso de exteriorización de los compromisos por pensiones. 2002
71. Gestión de activos y pasivos en la cartera de un fondo de pensiones. 2002
70. El cuadro de mando integral para las entidades aseguradoras. 2002
69. Provisiones para prestaciones a la luz del Reglamento de Ordenación y Supervisión de los Seguros Privados; métodos estadísticos de cálculo. 2002
68. Los seguros de crédito y de caución en Iberoamérica. 2001
67. Gestión directiva en la internacionalización de la empresa. 2001
65. Ética empresarial y globalización. 2001
64. Fundamentos técnicos de la regulación del margen de solvencia. 2001
63. Análisis de la repercusión fiscal del seguro de vida y los planes de pensiones. Instrumentos de previsión social individual y empresarial. 2001
62. Seguridad Social: temas generales y régimen de clases pasivas del Estado. 2001
61. Sistemas Bonus-Malus generalizados con inclusión de los costes de los siniestros. 2001
60. Análisis técnico y económico del conjunto de las empresas aseguradoras de la Unión Europea. 2001
59. Estudio sobre el euro y el seguro. 2000
58. Problemática contable de las operaciones de reaseguro. 2000
56. Análisis económico y estadístico de los factores determinantes de la demanda de los seguros privados en España. 2000
54. El corredor de reaseguros y su legislación específica en América y Europa. 2000

53. Habilidades directivas: estudio de sesgo de género en instrumentos de evaluación. 2000
52. La estructura financiera de las entidades de seguros, S.A. 2000
51. Seguridades y riesgos del joven en los grupos de edad. 2000
50. Mixturas de distribuciones: aplicación a las variables más relevantes que modelan la siniestralidad en la empresa aseguradora. 1999
49. Solvencia y estabilidad financiera en la empresa de seguros: metodología y evaluación empírica mediante análisis multivariante. 1999
48. Matemática Actuarial no vida con MapleV. 1999
47. El fraude en el Seguro de Automóvil: cómo detectarlo. 1999
46. Evolución y predicción de las tablas de mortalidad dinámicas para la población española. 1999
45. Los Impuestos en una economía global. 1999
42. La Responsabilidad Civil por contaminación del entorno y su aseguramiento. 1998
41. De Maastricht a Amsterdam: un paso más en la integración europea. 1998
39. Perspectiva histórica de los documentos estadístico-contables del órgano de control: aspectos jurídicos, formalización y explotación. 1997
38. Legislación y estadísticas del mercado de seguros en la comunidad iberoamericana. 1997
37. La responsabilidad civil por accidente de circulación. Puntual comparación de los derechos francés y español. 1997
36. Cláusulas limitativas de los derechos de los asegurados y cláusulas delimitadoras del riesgo cubierto: las cláusulas de limitación temporal de la cobertura en el Seguro de Responsabilidad Civil. 1997

35. El control de riesgos en fraudes informáticos. 1997
34. El coste de los riesgos en la empresa española: 1995
33. La función del derecho en la economía. 1997
32. Decisiones racionales en reaseguro. 1996
31. Tipos estratégicos, orientación al mercado y resultados económicos: análisis empírico del sector asegurador español. 1996
30. El tiempo del directivo. 1996
29. Ruina y Seguro de Responsabilidad Civil Decenal. 1996
28. La naturaleza jurídica del Seguro de Responsabilidad Civil. 1995
27. La calidad total como factor para elevar la cuota de mercado en empresas de seguros. 1995
26. El coste de los riesgos en la empresa española: 1993
25. El reaseguro financiero. 1995
24. El seguro: expresión de solidaridad desde la perspectiva del derecho. 1995
23. Análisis de la demanda del seguro sanitario privado. 1993
22. Rentabilidad y productividad de entidades aseguradoras. 1994
21. La nueva regulación de las provisiones técnicas en la Directiva de Cuentas de la C.E.E. 1994
20. El Reaseguro en los procesos de integración económica. 1994
19. Una teoría de la educación. 1994
18. El Seguro de Crédito a la exportación en los países de la OCDE (evaluación de los resultados de los aseguradores públicos). 1994
16. La legislación española de seguros y su adaptación a la normativa comunitaria. 1993

15. El coste de los riesgos en la empresa española: 1991
14. El Reaseguro de exceso de pérdidas 1993
12. Los seguros de salud y la sanidad privada. 1993
10. Desarrollo directivo: una inversión estratégica. 1992
9. Técnicas de trabajo intelectual. 1992
8. La implantación de un sistema de controlling estratégico en la empresa. 1992
7. Los seguros de responsabilidad civil y su obligatoriedad de aseguramiento. 1992
6. Elementos de dirección estratégica de la empresa. 1992
5. La distribución comercial del seguro: sus estrategias y riesgos. 1991
4. Los seguros en una Europa cambiante: 1990-95. 1991
2. Resultados de la encuesta sobre la formación superior para los profesionales de entidades aseguradoras (A.P.S.). 1991
1. Filosofía empresarial: selección de artículos y ejemplos prácticos. 1991

ÚLTIMOS LIBROS PUBLICADOS

Historia del seguro en Chile, 1810-2010. 2011

Modelo de proyección de carteras de seguros para el ramo de decesos. 2011

Desarrollo comercial del seguro colectivo de dependencia en España. 2010

La mediación de seguros en España: análisis de la Ley 26/2006, de Mediación de Seguros y Reaseguros Privados. 2010

Museo del Seguro. Catálogo. 2010

Diccionario MAPFRE de Seguros. 2008

Teoría de la credibilidad: desarrollo y aplicaciones en primas de seguros y riesgos operacionales. 2008

El seguro de caución: una aproximación práctica. 2007

El seguro de pensiones. 2007

Las cargas del acreedor en el seguro de responsabilidad civil. 2006

Diccionario bilingüe de expresiones y términos de seguros: inglés-español, español-inglés. 2006

El seguro de riesgos catastróficos: reaseguro tradicional y transferencia alternativa de riesgos. 2005

La liquidación administrativa de entidades aseguradoras. 2005

INFORMES Y RANKINGS

Desde 1994 se publican anualmente estudios que presentan una panorámica concreta de los mercados aseguradores europeos, de España e Iberoamérica y que pueden consultarse en formato electrónico desde la página Web: www.fundacionmapfre.com/cienicasdelseguro

Mercado español de seguros

Mercado asegurador de Iberoamérica

Ranking de grupos aseguradores europeos

Ranking de grupos aseguradores iberoamericanos