

Definición de un modelo dinámico de gestión y cuantificación del riesgo operacional para las entidades aseguradoras



MARÍA VICTORIA RIVAS LÓPEZ
CES Felipe II

MARÍA JOSÉ PÉREZ-FRUCTUOSO
Universidad a Distancia de Madrid (UDIMA)

JAVIER MONTOYA MARTÍN
SAS Spain



en el marco de SOLVENCIA II

La gestión y cuantificación del riesgo operacional en el sector asegurador europeo es un aspecto de vital importancia y envergadura, tanto por su aplicación al ámbito de Solvencia II como a la hora de evaluar la efectividad de los sistemas de control interno en las entidades. La implantación gradual de la problemática de gestión y cuantificación del riesgo operacional requiere una infraestructura que permita recopilar eventos históricos, tanto individuales como sectoriales, en un horizonte temporal prolongado. El objetivo de este artículo es proponer un modelo escalar para abordar la problemática de gestión y cuantificación del riesgo operacional, en el cual se incluyan todos los aspectos teóricos y prácticos que permitan implantar un modelo dinámico de gestión de dicho riesgo en las compañías aseguradoras.

1. INTRODUCCIÓN

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. Desde un punto de vista normativo, la preocupación por garantizar esta protección del asegurado lleva a establecer determinados 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, además, esta investigación debe realizarse dentro de un marco internacional, centrado en el proyecto europeo elaborado por la Asociación Internacional de los Supervisores de Seguros (*International Association of Insurance Supervisors*, IAIS) en colaboración con la Asociación Internacional de Actuarios (*International Actuarial Association*, IAA).

Conocido como Solvencia II, este documento de investigación 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.

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 acuer-

do, ajustados a las características específicas del mercado asegurador, hace referencia a (IAA, 2004):

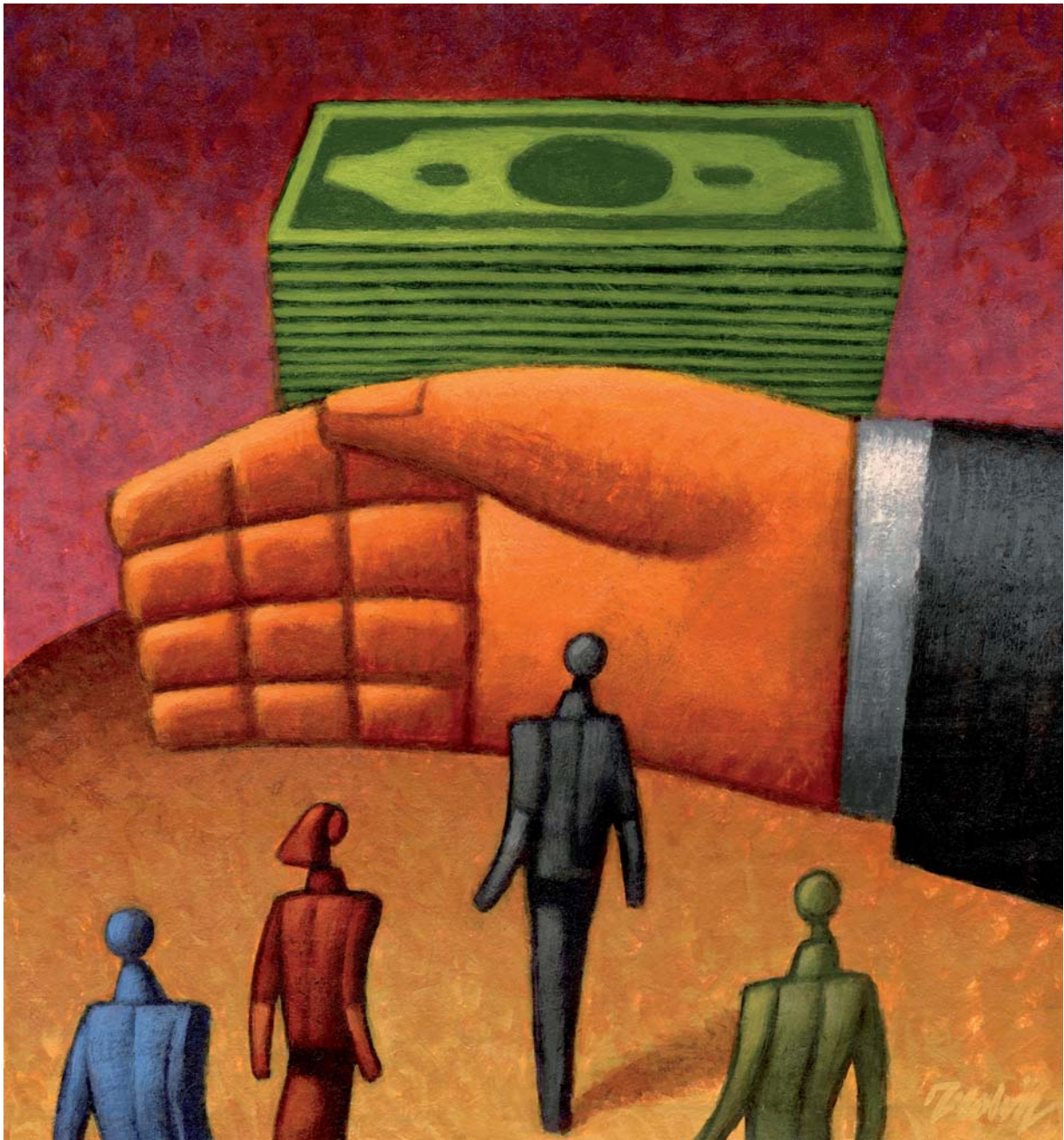
- Pilar I (Necesidades financieras mínimas o requerimientos mínimos de capital). Este pilar es cuantitativo y está centrado en el mantenimiento de unas provisiones técnicas adecuadas, unos activos apropiados que soporten las obligaciones asumidas y una cuantía mínima de capital (definida a partir de un conjunto de elementos de capital disponibles y necesarios) para cada asegurador.
- 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 las lleve a desarrollar y a utilizar técnicas de gestión del riesgo que reflejen el perfil concreto de los riesgos del asegurador, los supervisen y gestionen.

- Finalmente, el tercer pilar (medidas para fomentar la disciplina del mercado) complementa a los dos pilares anteriores, fomentando la disciplina de mercado a través del establecimiento de un conjunto de requisitos de divulgación que permi-



PARA LAS COMPAÑÍAS DE SEGUROS EUROPEAS, EL PROYECTO DE SOLVENCIA II SUPONE UN CAMBIO PROFUNDO EN SU SISTEMA DE GESTIÓN, CUANTIFICACIÓN Y CONTROL DEL RIESGO



tan a los agentes del mercado evaluar información esencial referida al ámbito de aplicación, el capital, las exposiciones al riesgo, los procesos de evaluación del riesgo y, con todo ello, a la suficiencia del capital de la institución. Esto es, el Pilar III consolida la disciplina del mercado introduciendo requisitos de acceso con el objetivo de que dichos requisitos mejoren las prácticas de la industria aseguradora.

El proyecto de Solvencia II supone, para las compañías de seguros europeas, un cambio profundo en su sistema de gestión, cuantificación y control efectivo del riesgo, basado en la implementación de un Proceso Integral de Gestión de Riesgos, conocido como ERM, que se adapte a las necesidades regulatoras y de mercado. Uno de los objetivos fundamentales necesarios para alcanzar un ERM adecuado pasa por la elaboración de un apropiado marco de monitorización y

control en el que se desarrollen las fases propias de un ERM, pero centrándose en el riesgo asociado a las operaciones y a los procesos.

La preocupación por la gestión del riesgo operacional por parte de CEIOPS (*Comitee of European Insurance and Occupational Pensions Supervisors*) se puso especialmente de manifiesto cuando dicho organismo incluyó en su cuarto estudio de impacto (*Fourth Quantitative Impact Study for Solvency II*, QIS4) un cuestionario relacionado con la gestión del riesgo operacional por parte de 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». (CEIOPS, 2008)

En lo que hace referencia al caso español, 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».

Este artículo 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.

El documento está organizado como sigue. En la sección 2 se describen las diferentes teorías y metodologías aplicables para la gestión y cuantificación del riesgo operacional. A continuación, y a lo largo de la sección 3, se analizan las fases de un proceso ORM, así como un plan director para la implementación del proceso de gestión del riesgo operacional en el marco de Solvencia II. Finalmente, el último apartado del artículo está dedicado a la exposición de las conclusiones alcanzadas con la realización del trabajo.

2. MARCO GENERAL PARA LA MODELIZACIÓN DEL RIESGO OPERACIONAL (OPERATIONAL RISK MANAGEMENT) EN LAS COMPAÑÍAS DE SEGUROS

El concepto de riesgo operacional surgió dentro del sector bancario e inicialmente se definió como todos aquellos riesgos que no sean riesgos de mercado y de crédito (IAA, 2004). Posteriormente, en el acuerdo de Basilea, se propuso establecer un requisito de capital para la cobertura del riesgo operacional, definiendo dicho riesgo como *«el riesgo de pérdidas resultante de procesos internos, gente, sistemas o eventos externos inapropiados o fallidos»*. Esta definición considera riesgos legales¹ pero excluye riesgos sistemáticos, de reputación y estratégicos. Por tanto, los riesgos operacionales se

¹El riesgo legal es el derivado del incumplimiento de los términos del contrato por parte de la contrapartida. Puede deberse a una falta de claridad en los contratos, por ejemplo, en un contrato *forward* sobre mercancías puede no quedar especificada la calidad de la misma, o bien a que no sea posible hacer cumplir determinados contratos si la otra parte no cumple con sus obligaciones (fallida de la deuda rusa en 1998).



originan por fallos en los sistemas internos de control del riesgo, es decir, fallos en los sistemas de contratación, liquidación y compensación, o en las personas que manejan dichos sistemas.

El Banco de Pagos Internacionales define el riesgo operativo como aquel riesgo que surge por deficiencias en los sistemas de información o en los controles internos que se traducen en pérdidas inesperadas. Este tipo de error está relacionado con errores humanos, fallos de sistemas y procedimientos o mecanismos de control inadecuados. Por ejemplo, en julio de 1998 un operador de deuda tenía que vender 100 contratos de deuda francesa a 10 años con un nominal por contrato de 500.000 francos franceses. El operador no sabía que presionando la tecla F12 de su ordenador ejecutaba la orden de venta automáticamente, de forma que cuando dicho operador apoyó por error su codo

en dicha tecla la orden de venta de los 100 contratos se ejecutó 145 veces. Esto provocó una caída inmediata en el precio de los futuros sobre deuda de un 1,4% (Pérez-Fructuoso, 2005).

El riesgo operacional más común es tener operadores que toman posiciones importantes sin tener en cuenta las directrices de la institución. Los riesgos operacionales pueden dar lugar a situaciones de importancia limitada (como el riesgo de una caída breve del sistema informático) o a situaciones muy graves (como el riesgo de quiebra por fallos en los sistemas de supervisión).

Diariamente, en la industria bancaria se procesan millones de transacciones, por lo que 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 cubrirlas.

Desde el punto de vista asegurador, 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, hay que tener en cuenta que, 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.

Resulta evidente, por tanto, que el riesgo operacional es también un riesgo de importancia relevante en el sector asegurador. El supervisor de la Unión Europea, London Group, en su informe Sharma, hacía constar que los déficit de gestión produjeron muchos



EL ACUERDO DE BASILEA DEFINE EL RIESGO OPERACIONAL COMO «EL RIESGO DE PÉRDIDAS RESULTANTE DE PROCESOS INTERNOS, GENTE, SISTEMAS O EVENTOS EXTERNOS INAPROPIADOS O FALLIDOS»

errores en las aseguradoras de la Unión Europea. Sin embargo, a causa de la falta general de suficientes datos cuantitativos sobre riesgo de operaciones, para las aseguradoras 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 requerimientos cuantitativos de cálculo 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.

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: el método del indicador básico, el método estándar y los métodos de medición avanzada.

El **método del indicador básico** está basado 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.

$$K_{BIA} = \frac{\sum(GI_{1...n} \times \alpha)}{n}$$



SOLVENCIA II ESTABLECE TRES MÉTODOS DE CÁLCULO PARA REQUERIMIENTOS DE CAPITAL MÍNIMOS POR RIESGO OPERACIONAL: MÉTODO DEL INDICADOR BÁSICO, MÉTODO ESTÁNDAR Y MÉTODOS DE MEDICIÓN AVANZADA

donde:

– K_{BIA} : determina la exigencia del capital en el método del indicador básico.

– GI : 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.

En el **método estándar**, la exigencia de capital para el total de la compañía se establece como la media de tres años de la suma simple de las exigencias de capital regulador en cada una de las líneas de negocio de dicha compañía cada año. Para un año determinado, las exigencias de capital negativas (resultantes 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 en concreto sea negativo, el argumento del numerador para ese año será cero.

El requerimiento total de capital viene definido como:

$$K_{TSA} = \frac{\sum_{i=1}^3 (\max[\sum GI_{1-n}^i \times \beta_{1-n}, 0])}{3}$$

donde:

– K_{TSA} : es la exigencia de capital calculada por el método estándar.

– GI_{1-n}^i : son los ingresos brutos para cada i y para cada una de las n líneas de negocio de la compañía.

– B_{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.

Finalmente, 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 operativo utilizando los criterios cuantitativos y cualitativos aplicables a estos métodos detallados en el documento *Convergencia internacional de medidas y normas de capital*, desarrollado por el Comité de Supervisión Bancaria de Basilea. La utilización de los AMA está sujeta a la aprobación del supervisor.

En el caso español se están realizando los trabajos de adaptación para la configuración del «Modelo Español 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).

El cálculo de los requerimientos de capital en el marco de Solvencia II 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 marco del Pilar II se contempla la realización de análisis de sensibilidad o pruebas de *stress* en el ámbito de medición de riesgos.

La gestión y cuantificación del riesgo operacional (*Operational Risk Management*, ORM) puede definirse 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. 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.

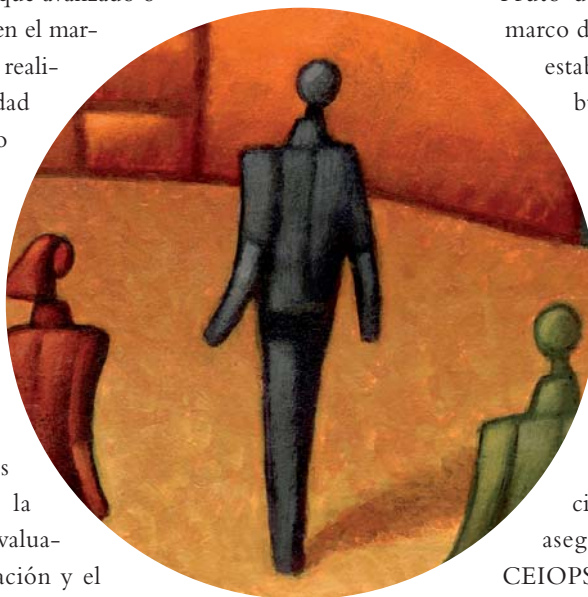
Como consecuencia de esta definición podemos plantearnos las siguientes cuestiones:

- ¿Qué pasos deben seguirse para implantar un proceso ORM?
- ¿Qué recursos, capacitación e información son necesarios para realizarlo?
- ¿Qué metodologías, teorías o técnicas son necesarias para su implantación y desarrollo?
- ¿Cuáles son las responsabilidades de quienes participan en un proceso ORM para que dicho proceso sea efectivo?

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, 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 desgraciadamente en determinadas situaciones pasadas recientes no se le ha prestado suficiente atención.

A la hora de implantar un proceso ORM, atendiendo a los principios del marco de gestión de riesgos operacionales, se deben tener en cuenta los siguientes aspectos desde el punto de vista organizativo y directivo:

- El marco global de la gestión del riesgo se inicia con la definición de la estrategia a seguir, compuesta por los objetivos y políticas en materia de riesgos dentro del modelo de gobierno corporativo. Se deben definir de forma clara tanto la actitud frente al riesgo como la política de retención y de transferencia de riesgos.
- Para la implantación del ORM se debe solicitar la aprobación por parte del consejo de administra-

ción 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 responsable de gestión de riesgos.

- La entidad debe identificar los riesgos operacionales asociados a sus productos, actividades, procesos y sistemas.
- Para la compañía de seguros es fundamental disponer de planes de contingencia y continuidad del negocio que aseguren su capacidad para operar, con lo que se evitará una posible interrupción del negocio.
- Asimismo, también resultará de gran importancia la adaptación de la estructura organizativa a las nuevas circunstancias de gestión del riesgo. El organigrama considerado servirá para marcar los pasos generales de la implantación del ORM. Por otra parte, será necesario conocer aspectos tan importantes como el grado de preparación del equipo líder de las diferentes unidades de negocio y llevar a cabo la designación de los responsables de cada área en materia de riesgo.

Tabla 1: RESUMEN MARCO DE GESTIÓN DE RIESGOS OPERACIONALES

RECURSOS TÉCNICOS	RECURSOS HUMANOS	RECURSOS ORGANIZATIVOS
<ul style="list-style-type: none"> - Bases de datos - <i>Software</i> adecuado 	<ul style="list-style-type: none"> - Formación - Contratación 	<ul style="list-style-type: none"> - Integración de procesos de riesgos en los procesos de negocio - Cambios estructura organizativa - Nuevo departamento de riesgos - Asignación de responsabilidades de riesgos



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

● 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.

● Otro aspecto a destacar a la hora del establecimiento de un proceso ORM es la problemática de obtención 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 de operaciones partirán de la información de la compañía y de un estudio de sus procesos y procedimientos. También 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 *ad hoc* para dicha función y que disponen de mecanismos de validación de la información. Los datos privados de carácter externo son obtenidos generalmente cooperando con instituciones que estén de acuerdo en compartir sus datos internos.

En España, en lo que se refiere a este punto, el sector carece de una base de datos privada externa. En este sentido, queda todavía mucho por hacer, ya que no sólo es necesario que las compañías tengan su base de datos de pérdidas operacionales interna, sino que además deben disponer de datos históricos sobre las mismas



de al menos cinco años para que dicha base de datos proporcione datos significativos 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, en Inglaterra se creó la base de datos de pérdidas operacionales externas privada de las compañías que operan en ese mercado, y que es conocida como *Operational Risk Insurance Consortium* (ORIC). En dicho consorcio participan las principales compañías de seguros inglesas. ORIC fue promovida por la *Association British Insurance* (ABI) y *SAS Business Intelligence*. En 2004, a raíz de que las organizaciones registraron pérdidas de más de 20 billones de dólares, se constituyó ORIC con objeto de reducir pérdidas potenciales futuras en la industria aseguradora. En este sentido, España y el resto de Europa tendrán que tomar ejemplo de dicho organismo con vistas a crear una base de datos de riesgo operacional que permita modelizar de una forma óptima sus pérdidas operacionales. 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



ESPAÑA Y EL RESTO DE EUROPA DEBERÁN TOMAR EJEMPLO DEL CONSORCIO BRITÁNICO ORIC CON VISTAS A CREAR UNA BASE DE DATOS DE RIESGO OPERACIONAL QUE PERMITA MODELIZAR DE UNA FORMA ÓPTIMA SUS PÉRDIDAS OPERACIONALES

riesgo con vistas a la optimización de su control. Para agrupar los datos se pueden considerar 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.

La categorización de las pérdidas se puede llevar a cabo en función de la causa, el efecto y el evento, desagregando posteriormente a nivel de proceso de negocio o actividad:

a) Categorización por causa. Se atribuye a la relación entre ciertos factores causales y las pérdidas operacionales. Por ejemplo, un error en la suscripción puede estar asociado a la falta de formación de un empleado, mientras que otro puede estar ocasionado por una sobrecarga de trabajo.

b) Categorización por efecto. Se basa en la forma en que se manifiestan las pérdidas. El primer problema de este criterio está asociado a que el mismo tipo de eventos operacionales puede provocar pérdidas de diversa índole. El segundo problema deriva de la dificultad de establecer un método de control adecuado por parte del gerente de riesgos, al estar asociado dicho control a los efectos que provocan las pérdidas operacionales.

c) Categorización por evento. Se basa en los mismos principios que la categorización por causa pero definiendo la pérdida a partir de la naturaleza del evento. Por ejemplo, una pérdida asociada al fraude por parte de la red comercial de la compañía puede ser agrupada en la categoría de fraude interno y una pér-

didada debida a discriminación puede ser agrupada en la categoría de prácticas de empleados.

Este método mejora la categorización de las pérdidas y permite que los eventos con similares tipologías sean agrupados de forma conjunta. Lo más importante de la categorización por evento es que permite una mejora en la gestión relativa a la asignación de responsabilidad, roles y controles, así como la comparación con el resto del sector en los mismos términos.

3. PROCESO DE GESTIÓN Y CUANTIFICACIÓN DEL RIESGO OPERACIONAL (*OPERATIONAL RISK MANAGEMENT*) EN LAS COMPAÑÍAS DE SEGUROS

El proceso ORM es un marco metodológico que permite la identificación del riesgo, el marco de control, el análisis, la evaluación, la medición, la retroalimentación y el *reporting*. La gestión de riesgos es un proceso que debe expandirse por toda la organización, para lo cual resulta necesario crear una unidad de riesgo específica que defina el marco de gestión e informe a la alta dirección de los resultados derivados del proceso de gestión del riesgo. Para llevar a cabo esta función también es fundamental la existencia de una auditoría en el proceso 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, sino que los resultados conducen a decisiones estratégicas y diarias que inciden sobre la operativa del negocio, en el que es básico un adecuado proceso de retroalimentación

Las fases del proceso de gestión (ORM) son, por tanto, identificación, análisis y valoración, medición, control y *reporting*. Los puntos clave del mismo



LA GESTIÓN DE RIESGOS DEBE EXPANDIRSE POR TODA LA ORGANIZACIÓN; PARA ELLO SE DEBE CREAR UNA UNIDAD DE RIESGO ESPECÍFICA QUE DEFINA EL MARCO DE GESTIÓN E INFORME A LA ALTA DIRECCIÓN DE LOS RESULTADOS DEL PROCESO DE GESTIÓN DEL RIESGO

son las causas, las consecuencias (pérdidas monetarias, incidencias en el negocio, daños en la reputación de la entidad), 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.

ORIC lleva a cabo una clasificación de los diferentes tipos de riesgos operacionales que existen en los siguientes grupos: fraude interno, fraude externo, clientes, productos y prácticas de negocio, daños a los activos físicos, interrupción del negocio o caída del sistema y riesgos en los procesos de negocio.

Esta clasificación, sin embargo, simplemente debe servir de guía para que las entidades de seguros operen bajo un mismo criterio a la hora de llevar a cabo una determinación de cuáles son sus riesgos y de establecer una clasificación propia, detallada y acoplada a sus procesos.

Tabla 2: CATEGORÍAS DE RIESGO OPERACIONAL
ORIC (*Operational Risk Insurance Consortium*)

Fraude interno (ej: malversación de fondos).

Fraude externo (ej: fraude en la contratación, no veracidad de los datos declarados en la solicitud de seguro de vida).

Cientes, productos y prácticas de negocio (ej: Inclusión de coberturas no contrastadas: incorporación de coberturas poco contrastadas, por presiones comerciales debido a demandas del mercado sin una base estadística suficiente ni experiencia práctica de siniestros. También puede dar lugar a la existencia de «lagunas» en las coberturas, producidas por la ambigüedad en los textos comerciales).

Daños a activos físicos (ej: incendio, terremoto, inundación, terrorismo).

Interrupción de negocio y caída de sistema (ej: establecimiento de un nuevo sistema informático).

Riesgos en los procesos de negocio (ej: errores en la elaboración de tarifas o cálculo de primas).

Fuente: ORIC

El proceso de gestión del riesgo operacional (ORM) está integrado por las siguientes fases:

Identificación del riesgo. Consiste en determinar cuáles son los tipos de riesgo existentes y cuál es su influencia en las actividades de la entidad. Resulta obvio que sin una identificación de riesgos apropiada es muy difícil alcanzar una gestión exitosa. Para ello será clave el conocimiento de las fuentes de riesgo, realizar un inventario de riesgos y analizar las causas de los eventos que los generan.

Desde el punto de vista metodológico para el estudio de las relaciones causales, en el marco ORM se destaca la dinámica de sistemas que nos permite pasar de un enfoque cualitativo a un enfoque más cuantitativo y establecer un sistema integral basado en realidad que facilita el control de los procesos y la minimización de las pérdidas operacionales.

La dinámica de sistemas (Sternan, 2000) es un nombre propio que designa un determinado método de construcción de modelos de sistemas sociales suscepi-

bles de ser simulados por ordenador. El origen de esta técnica se remonta a finales de los años cincuenta y su implantación definitiva se produce durante la década de los sesenta. El desarrollo de este método se debe al trabajo de J. W. Forrester, del Instituto Tecnológico de Massachussets, quien utilizó por primera vez técnicas pertenecientes a las disciplinas de ingeniería automática para el estudio de procesos sociales y económicos.

La dinámica de sistemas es una metodología que trata la aproximación a la modelización de sistemas complejos, como poblaciones biológicas o los sistemas económicos, en los que las partes demuestran propiedades interactivas entre los objetos, dando como resultado una comunicación gracias a las transacciones que se derivan de las relaciones mutuas.

Uno de los fundamentos básicos en la dinámica de sistemas es el diseño de los denominados bucles de realimentación. Estos bucles de realimentación hacen referencia a que si la situación X afecta a la situación Y y viceversa, quizás se deba a una cadena de causas y efectos. Crear un mapa causa-efecto basado en dinámica de sistemas, asociado a los riesgos operacionales de la entidad, puede facilitar la explicación y la simulación de posibles escenarios futuros (Shah, 2001).

Un aspecto notable del método es su enorme capacidad descriptiva. Los modelos se representan mediante unos diagramas conocidos como diagramas de flujo. Un diagrama de flujo es una descripción gráfica del sistema en estudio construida de acuerdo a unas determinadas reglas.

Análisis y evaluación del riesgo. En la fase de análisis y evaluación del riesgo, la entidad, a partir de datos históricos y de la opinión de expertos, construi-

rá un mapa de riesgos inherente o puro. Para la construcción de dicho mapa de riesgos se fijarán dos ejes de forma bidimensional: uno asociado a la frecuencia y otro a la intensidad de ocurrencia de los riesgos. La determinación de ambas variables se realizará a partir de la opinión de expertos o de datos históricos, y se calculará para cada riesgo un par ordenado de frecuencia en intensidad. Con ello se obtendrá el mapa de puntos que constituirá el mapa de riesgos.

Una vez construido el mapa de riesgos puro o inherente, se analizan los posibles controles efectivos asociados que puedan minimizar esa frecuencia o intensidad. El objetivo de dichos controles es obtener un mapa de riesgos residual.

La problemática asociada a dichos controles está centrada en la necesidad de disponer de unos adecuados programas informáticos que permitan ese control efectivo en tiempo real. Para ello, dicho proceso se verá apoyado por los *Key Risk Indicators* (KRI), que serán tratados con posterioridad.

Una vez obtenido el mapa de riesgos residual se aplicará la política que en materia de riesgos tenga la entidad para su tratamiento y que pertenece al apartado de planes de acción.

Cuantificación del riesgo. En el caso de disponer 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, podremos calcular la distribución de las pérdidas agregadas a partir de los eventos individuales. Dicha distribución se obtiene a partir del número de siniestros y de las pérdidas individuales asociadas a cada siniestro, es:

$$\text{Agg}L = \sum_{i=1}^N X_i$$



LA DINÁMICA DE SISTEMAS, MÉTODO DE CONSTRUCCIÓN DE MODELOS DE SISTEMAS SOCIALES SUSCEPTIBLES DE SER SIMULADOS POR ORDENADOR, SE REMONTA A FINALES DE LOS AÑOS 50 Y SE IMPLANTÓ DEFINITIVAMENTE UNA DÉCADA DESPUÉS

siendo X_i y N variables aleatorias y donde cada X_i representa un pérdida o cuantía individual del siniestro y N es el número de siniestros.

La evidencia empírica sugiere 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, pero deberán recoger las correlaciones entre los diferentes tipos de riesgos, así como la estimación de frecuencias y severidades conjuntas. Por dicho motivo se recomienda la utilización de cópulas.

El VaR es una medida de la máxima pérdida esperada (o peor pérdida) que puede tener una entidad durante un horizonte temporal específico y para un intervalo de confianza determinado.

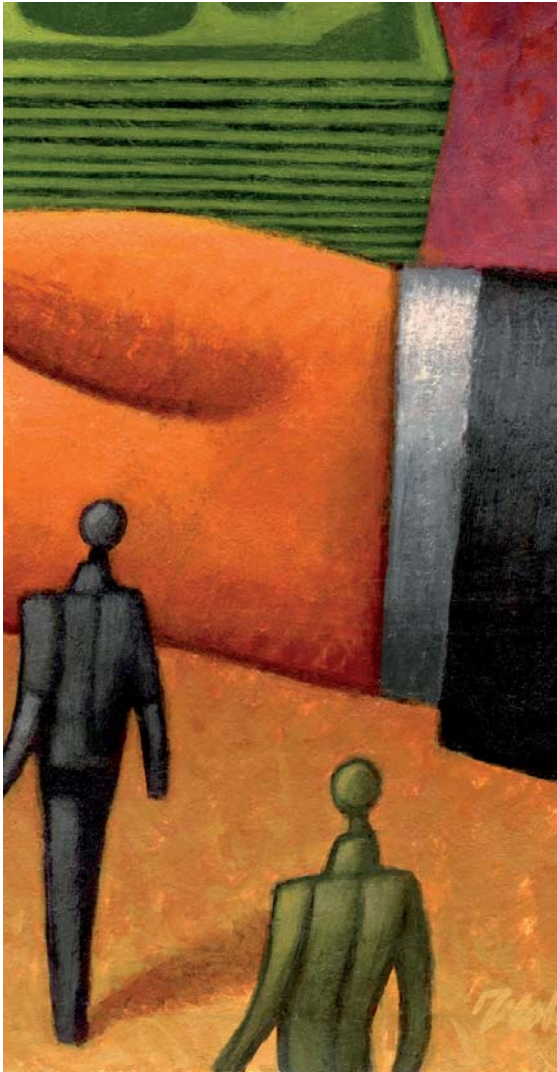
Para llevar a cabo este cálculo del VaR operacional, será necesario conocer la tendencia del número de eventos en un año teniendo en cuenta la estructura y el tamaño de la organización. Este procedimiento implica descubrir la relación entre el tamaño de la organización y la frecuencia de pérdidas históricas, 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, en cuyo caso el ajuste se realiza a través de distribuciones como la distribución generalizada de Pareto (*Generalized Pareto Distribution*, GPD). (Fabozzi, 2007)



En estos casos, la teoría del valor extremo (*Extreme Value Theory*, ETV) 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 un umbral o prioridad determinado, es decir, la distribución condicionada a que los datos excedan de un determinado nivel. (Pérez-Fructuoso, et al. 2007).

El teorema de Pickands-Balkema-de Haan (Balke-ma y de Haan, 1974; Pickands, 1975) muestra que, bajo condiciones de máximos dominios de atracción, la distribución generalizada de Pareto es la distribución límite para los excesos sobre un límite cuando este umbral es lo suficientemente elevado. La distribución GPD permite ajustar bien los valores absolutos de las pérdidas que exceden un determinado umbral o bien los valores



representativos de excesos sobre el límite, y es una distribución condicionada, ya que está sujeta a que el siniestro exceda el valor marcado como límite. Esto conduce a la función de distribución de los excesos por encima del valor, cuya forma de cálculo es:

$$F^u(x) = F^u(y+u) = P(X-u \leq y / X > u) = \frac{F(x) - F(u)}{1 - F(u)} \quad \text{para } 0 \leq y \leq x_0 - u$$

donde x representa la pérdida operacional total asociada a un determinado siniestro e y el exceso por encima del umbral u , de modo que y puede expresarse como $y=x-u$. Al ajustarse los excesos sobre el umbral, el extremo inferior de la distribución, esto es, el punto final izquierdo, es cero.

En este caso de ajuste de una GPD, la dificultad se encuentra en la elección del límite, ya que la teoría no propone dicho aspecto. La elección de este umbral está sujeta al problema de elección entre la varianza y sesgo, esto es, si se disminuye el umbral, se incrementa el número de observaciones que forma la serie presenta un mayor sesgo entre los distintos valores que la integran. Por otra parte, si se reduce el sesgo se hace que la estimación del índice sea más volátil, al realizarse sobre un menor número de observaciones.

Los pasos para aplicar la teoría del valor extremo al riesgo operacional son los 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.

Para el cálculo del VaR Operacional se utilizan tres métodos: simulación, algoritmo recursivo de Panjer o aproximación computacional. Estos métodos son bien conocidos por la ciencia actuarial, pero a la hora de 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 (Fabozzi, 2007). Dicha técnica se seleccionará 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. Esta metodología tiene la cualidad de asociar dichos factores causales a diferentes unidades de negocio, con lo que es útil en el ámbito de ORM. La clasificación de pérdidas se realiza a partir de la fijación de un límite de pérdidas máximo, de forma que las pérdidas por debajo del límite serán tratadas siguiendo la metodología Delta, mientras que las consideradas grandes pérdidas serán tratadas según la teoría de valores extremos. (King, 2001).

Determinación de los indicadores de riesgo, KRI (Key Risk Indicators). Los KRI son parámetros o indicadores que permiten predecir los cambios en el perfil de riesgos de la compañía de seguros. Como consecuencia de ello, propician la realización de las correcciones que sean necesarias, favoreciendo de esa forma el proceso de realimentación y control.

Los componentes de un KRI pueden estar 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 pueden clasificarse 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 puede partir 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 semafóricos o de alerta de un KRI, los baremos pueden recalibrarse de manera periódica hasta que se garantice su efectividad. Si, por ejemplo, un KRI que representa un número de incidencias informáticas está en rojo cuando se producen más de 5 en un mes –lo que sólo ha ocurrido en un 1% de las ocasiones y que, al cabo de dos años, pasa en más del 10% de las ocasiones–, se necesita reevaluar tanto el KRI como la naturaleza del riesgo.

Planes de acción. Un plan de acción 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. Para ello la entidad podrá optar por la reducción de la frecuencia de la pérdida o/y intensidad de la misma.

Evitar. Estableciendo las medidas necesarias para evitar la ocurrencia del riesgo, llevando a cabo una óptima prevención y reduciendo su frecuencia a cero.



LOS INDICADORES DE RIESGO (KRI) SON PARÁMETROS QUE PERMITEN PREDECIR LOS CAMBIOS EN EL PERFIL DE RIESGOS DE LA COMPAÑÍA DE SEGUROS, POSIBILITANDO LA REALIZACIÓN DE LAS CORRECCIONES QUE SEAN NECESARIAS

Retener. Respecto a los tipos de retenciones, destacamos la total o la parcial. La retención 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, a provisión contable, estableciendo una o varias líneas de crédito y/o un fondo interno o externo a la empresa. Respecto a la retención parcial o transferencia, puede acudir directamente al reaseguro con las diferentes modalidades que éste ofrece.

Una vez implementado un plan de acción, la organización deberá monitorizar si los controles son efectivos y si al cabo del tiempo la frecuencia y severidad del riesgo se reducen. Para ello se implementarán 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.

Stress testing y escenarios test. Este tipo de pruebas permiten a la organización comprender mejor sus riesgos y poder actuar en 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, por ejemplo, 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 (Pérez-Fruitoso, 2008). A través de ellas, las compañías de seguros pueden mejorar la gestión de sus riesgos para, de esa forma, mantener los recursos financieros adecuados para cubrirlos mediante la identificación y la cuantificación de diferentes escenarios complejos sobre posiciones financieras futuras esperadas. Dichas pruebas estiman el impacto cuantitativo 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.

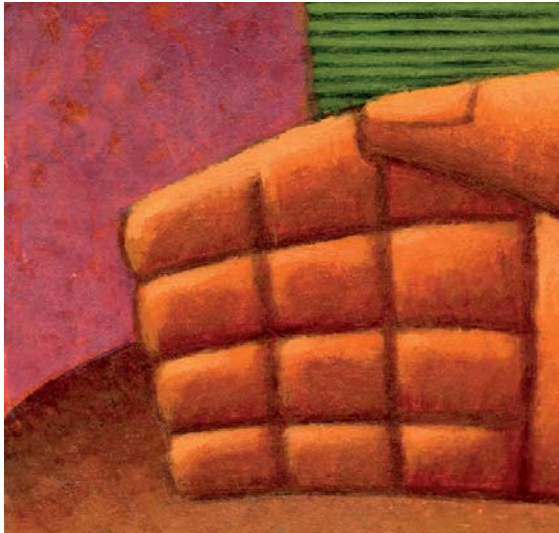
Las pruebas de estrés comprenden dos tipos de análisis, uno de sensibilidad y otro de escenarios, cuyo objetivo es que los aseguradores dispongan de un mayor número de datos que les permitan entender las vulnerabilidades a las que han de hacer frente en situaciones atípicas, con baja probabilidad de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

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.

El análisis de escenarios, por su parte, 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, lo que se conoce con el nombre de escenarios históricos, o en la estima-



LAS PRUEBAS DE ESTRÉS SON HERRAMIENTAS APLICADAS EN INSTITUCIONES FINANCIERAS Y DE SEGUROS CON OBJETO DE VALORAR SU NIVEL POTENCIAL DE VULNERABILIDAD ECONÓMICA Y FINANCIERA ANTE EVENTOS EXCEPCIONALES



ción de las consecuencias de un evento que aún no hayan ocurrido, encontrándonos entonces antes un análisis de escenario hipotético (KPMG, 2002). 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 (días o meses) 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, midiendo o cuantificando el efecto y las consecuencias, tanto en la entidad individualmente como en la totalidad del mercado asegurador analizado. Los escenarios hipotéticos, en cambio, están basados en un conjunto de *shocks* que se sabe que pueden producirse, pero que todavía no han ocurrido.

En cualquier caso, a la hora de diseñar las pruebas de estrés, el asegurador debe demostrar, como mínimo, que los riesgos incluidos en el riesgo operativo han sido considerados y que existen planes y procedimientos apropiados para un manejo adecuado de los mismos en una situación adversa.

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. Ayudan a determinar el perfil de riesgo global de toda la organización facilitando la determinación del apetito de la entidad respecto al riesgo. Es un *input* adicional para el cálculo de los requerimientos de capital económico.

Finalmente, y para terminar la sección, vamos a comentar las líneas generales que debe contener un plan director para la implantación del proceso ORM en el marco de Solvencia II. El plan director se divide en tres fases: una primera introductoria, centrada en los modelos estándar en la construcción del marco general; una segunda centrada en la implementación y el desarrollo de modelos internos, y una última orientada a un enfoque avanzado y dinámico. El proceso ORM va a estar localizado principalmente en el Pilar II, aunque será necesario que la información obtenida a raíz del mismo sea utilizada en los modelos internos y en el cálculo del capital económico. En la primera fase del Pilar II, haciendo referencia al ORM, se establecerán los objetivos, estrategias, asignación de responsabilidades, estudio de las relaciones causa-efecto y el lugar donde la dinámica de sistemas tendrá una especial relevancia. Para todo ello, la entidad, de forma detallada, analizará los procesos y procedimientos de las posibles fuentes de riesgo. Se construirá el mapa de riesgos inherente o puro y, una vez fijados o analizados los controles existentes, se procederá a la obtención del mapa de riesgos residual. En esta primera fase se habrá determinado la política de retención y transferencia de la entidad frente al riesgo. Respecto a la fase segunda correspondiente al Pilar II, se finalizará el diseño del proceso ORM y se comenzarán a aplicar modelos avanzados para la gestión y cuantificación del riesgo operacional, *stress testing*, planes de continuidad de negocio y gobierno corporativo. 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.

4. CONCLUSIONES Y VISIÓN GENERAL DE LA GESTIÓN DEL RIESGO OPERACIONAL FRENTE A SOLVENCIA II

En el presente artículo se ha desarrollado un marco ampliado y dinámico para la gestión y cuantificación del riesgo operacional de las entidades aseguradoras dentro del marco regulador que supone la implantación de Solvencia II.

Una de las principales aportaciones es la inclusión de la dinámica de sistemas y de la metodología Delta-EVT para desarrollar un ORM efectivo. La aplicación de la dinámica de sistemas incrementará la transparencia del proceso de negocio, detectando nuevos aspectos o puntos de vista sobre el mismo, y permitirá inte-

grar el riesgo operacional junto a otros riesgos ampliamente tratados hasta la fecha, como son el riesgo de crédito y el riesgo de mercado. Por su parte, la metodología Delta-ETV permitirá desarrollar un proceso claro de relación entre las ganancias y los factores de causales (teniendo en cuenta los riesgos) que minoran dichas ganancias provocando pérdidas.

El artículo dedica especial atención a la recogida de datos de pérdidas operacionales, destacando la importancia de una adecuada categorización basada en el criterio causa-evento de los datos sobre pérdidas derivadas de riesgo operacional.

Asimismo, se han descrito e incorporado al proceso de forma clara los componentes y pasos para la creación de KRIs efectivos que, insertados dentro del

BIBLIOGRAFÍA

CEA, Solvency Assessment Models Compared, Essential Groundwork for the Solvency II, 2005.

CEIOPS, Lesson learned from the crisis, Solvency II and beyond, 2009.

CEIOPS, Processing Quantitative Impact Study 4 groups resultant an EU level, Operational Risk Questionnaire, 2008.

Comité de Supervisión Bancaria de Basilea. Convergencia internacional de medidas y normas de capital. Banco de Pagos Internacionales. Press & Communications. Basilea. Suiza. 2004.

Fabozzi Chernobai, Svetlozar, Operational Risk. A guide to Basel II Capital Requirements, Models and Analysis. New Jersey: Wiley Finance, 2007.

International Association of Insurance Supervisors (IAIS), (2005), A new framework for insurance supervision: Towards a common structure and common standards for the assessment of insurer solvency. www.iais.org.

International Association of Insurance Supervisors (IAIS), (2005), Insurance principles, standards and guidance papers. www.iais.org.

International Actuarial Association. A global framework for insurance solvency assessment. Research Report of the Insurance solvency assessment working party. International Actuarial Association. 2004.

International Association of Insurance Supervisors (2003), Insurance core principles and methodology. http://www.iaisweb.org/133_ENU_HTML.asp.

King, Jack. L., Operational Risk. West Sussex: Wiley & Sons, 2001.

Klugman, S. A. Panjer H. A. Willmot, G. E., Loss Models – From Data To Decisions, New York: Wiley & Sons, 1998.

Lozano, R. «Las implicaciones de Solvencia II en el sector asegurador español». Estabilidad Financiera, n° 9, pp.61-70, 2005.

sistema, puedan establecer las diferentes alertas y favorecer el establecimiento de las medidas correspondientes a dicho proceso ORM.

Por otra parte, los riesgos operacionales abarcan una tremenda diversidad de tipos de riesgo cuya cuantificación no resulta fácil. La escasez de datos es una característica fundamental. La confección de una base de datos de mantenimiento permanente es un requisito ineludible del subsistema de información. En ella habrá datos de captación interna, como se ha comentado, pero también, por su escasez, habrá que recurrir a datos externos, como ORIC (sectoriales, por ejemplo, los fraudes, los robos, etc.).

Ligado a este problema, las compañías están teniendo dificultades a la hora de extraer la información

asociada al riesgo operacional ya que no tienen un dataMart único, sino diferentes extracciones del operacional para distintas aplicaciones de nicho (siniestros, actuarial, comercial, etc.). Por lo que uno de los ejes en los que hay que enfatizar es la integración y la construcción de un repositorio único de información. Las compañías tienen muy definidos mapas de riesgos y procesos de auditoría, pero a algunas les falta un circuito efectivo, con lo que la aplicación del enfoque sistémico ayudará en dicho proceso.

Para terminar, se concluye que existe una clara necesidad de un sistema de tecnologías de información que permita un gestión integral de riesgos que propicie el establecimiento de controles efectivos que van a ser imprescindibles para el cumplimiento del Pilar II. ■

Pérez-Fructuoso, M. J. «Análisis de los riesgos de las aseguradoras bajo Solvencia II». Revista Española de Seguros N° 122, pp. 245-263, 2005

Pérez-Fructuoso, M. J. «Desarrollo de pruebas de estrés en entidades aseguradoras bajo Solvencia II». Gerencia de Riesgos y Seguros, n° 101, pp. 23-47. Madrid, 2005.

Pérez-Fructuoso, M. J., A. García, A. Berlanga y J. M. Molina, «Adjusting the Generalized Pareto Distribution with Evolution Strategies. An application to a Spanish motor liability insurance database». Lecture Notes in Computer Science, 4881, pp. 1010-1019. Springer Berlin / Heidelberg, 2007.

Real Decreto 1318/2008, de 24 julio, de modificación del ROSSP.

Shah, S. Operational Risk Management. Casualty Actuarial Society, Tillinghast-Towers Perrin, San Francisco, 2001.

Shimpi, P, Integrating Corporate Risk Management, New York: Texere, London, 2001.

Sterman, John, Business Dynamics, Cambridge: Irvin- Mc Graw-Hill, 2000.

PÁGINAS WEB:

http://ec.europa.eu/internal_market/insurance/solvency/index_en.htm

<http://www.ceiops.org/>

<http://www.actuaries.org/index.cfm?DSP=MENU&ACT=HOME&LANG=EN>

<http://www.sas.com/offices/europe/uk/solutions/riskmgmt/pdf/oric.pdf>

<http://www.iasb.org/Home.htm>

<http://www.sas.com>