



El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras

Estudio realizado por: Jorge Sánchez García
Tutor: Marisa Galán Camino

Tesis del Master en Dirección de Entidades
Aseguradoras y Financieras

Curso 2006/2007

Esta tesis es propiedad del autor.

No está permitida la reproducción total o parcial de este documento sin mencionar su fuente.

Presentación

El tema de esta tesis está muy influenciado por dos cosas:

En primer lugar, por mi colaboración en el proyecto QIS -3 (Estudio de Impacto de Solvencia), en el que el CEIOPS (Comité of European Insurance and Occupational Pensions Supervisors) ha pedido a las entidades aseguradoras que participen, de cara a la implantación de un nuevo modelo de cálculo de capitales de Solvencia, y en el que la empresa para la que trabajo, **FIATC, Mutua de Seguros**, ha participado.

Segunda, por la experiencia vivida en el desarrollo del proceso de adquisición del **Grupo Prosperity** por parte de **FIATC, Mutua de Seguros**, la integración de los negocios que se ha llevado a cabo, y las dificultades y, sobretodo, riesgos en los que se podría haber incurrido, y que se salvaron de una manera muy efectiva y controlada.

Quisiera dedicar este estudio a todos mis compañeros de promoción, con los que tantos buenos ratos he compartido a lo largo de este año.

Resumen

Esta tesis se divide en dos grandes bloques.

El primero, dedicado a la definición y desarrollo del concepto de Solvencia, y la transición de un modelo de solvencia estático a un modelo de solvencia dinámico y sus implicaciones a nivel de control de riesgos.

El segundo bloque está orientado a la definición de riesgos, en concreto al riesgo operacional, a su identificación, y a su tratamiento en procesos de fusión y/o adquisición de entidades.

Resum

Aquesta tesi es divideix en dos grans blocs

El primer, dedicat a la definició i desenvolupament del concepte de Solvència, i la transició des d'un model de solvència estàtic a un model de solvència dinàmic, i les seves implicacions a nivell del control de riscos.

El segon bloc està orientat a la definició de riscos, en concret al risc operacional, a la seva identificació, i al seu tractament en processos de fusió i/o adquisició d'entitats.

Summary

This thesis is divided into two big parts.

First one, dedicated to the definition and development of Solvency concept, and the transition from a static solvency model to a dynamic solvency model, and its implications in risks control.

The second one, aimed to the definition of the risks, operational risk specifically, and its processment in companies merger and/or acquisition operations.

Indice

Apartado	Página
Presentación	3
Resumen	4
Índice	5
1. Introducción	6
2. De Solvencia I a Solvencia II	7
2.1 Exigencias de los Mercado Financieros	
2.2 Exigencias Empresariales	
2.3 Exigencias de Supervisión	
2.4 Exigencias de minimización de efectos no deseables	
2.5 Exigencias de los consumidores	
3. Solvencia II	9
3.1 Pilar I: Requisitos Cuantitativos. Exigencia de Fondos Propios.	
3.2 Pilar II: Procesos de Supervisión	
3.3 Pilar III: Disciplina de Mercado	
4. Riesgos	12
4.1 Riesgo de Mercado	
4.1.1.1 Riesgo de tipo de interés	
4.1.1.2 Riesgo de tipo de cambio	
4.2 Riesgo de Crédito	
4.3 Riesgo de Liquidez	
4.4 Riesgo Operacional	
5. El Riesgo Operacional	14
5.1 Tipos de Riesgo Operacional	
5.1.1 El Riesgo Operacional Interno	
5.1.2 El Riesgo Operacional Externo	
6. Detección y Control de Riesgos	20
7. El Comité de Riesgos	26
8. Medición de los Riesgos	30
8.1 Medición nominal	
8.2 Medición ordinal	
8.3 Medición de intervalo	
9. Fusiones y Adquisiciones	35
10. El Riesgo en las Fusiones y Adquisiciones	36
10.1 El Proceso de fusión y/o adquisición	
10.1.1 Inicio de conversaciones	
10.1.2 Due diligence	
10.1.3 Ejecución del acuerdo de fusión	
10.2 Riesgos en las integraciones departamentales	
10.2.1 Tecnologías de la Información y Servicios Informáticos	
10.2.2 Departamento Comercial	
10.2.3 Departamento de Atención al Cliente	
10.2.4 Departamento de Formación	
10.2.5 Departamento de Técnico (Producción y Siniestros)	
10.2.6 Departamento Actuarial	
10.2.7 Otros Departamentos	
10.3 Finalización y Reanálisis	
11. Conclusiones	51
12. Bibliografía	52
Jorge Sánchez García	53

El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras

1. Introducción

El proyecto Solvencia II que se está desarrollando en la UE conlleva una reforma en la regularización de la solvencia basada principalmente en la gestión del riesgo.

Solvencia II es la interpretación para al sector asegurador del proceso revisionista iniciado en el sector bancario bajo la denominación de Basilea II. Es revisionista porque supone un profundo replanteamiento de la filosofía y tendencias hasta ahora imperantes en los ámbitos de gestión aseguradora y de supervisión.

Solvencia II va a suponer un reto común de gran importancia y trascendencia para las aseguradoras y para los supervisores.

2.De Solvencia I a Solvencia II.

Los motivos del cambio del sistema actual puede leerse desde varias perspectivas:

2.1 Exigencias de los Mercado Financieros

El incremento de los procesos de internacionalización, el creciente protagonismo de los conglomerados financieros, el desarrollo de nuevos canales de comercialización, la madurez de los mercados de valores y, sobre todo, la decidida apuesta por crear un mercado financiero único exigen la homogeneización de los criterios por los que se debe medir el nivel de solvencia de las entidades financieras en general y de las aseguradoras en particular.

La aparición de productos, clientes y riesgos financieros con componentes técnicos, operativos y contractuales de seguros aconseja la aplicación de enfoque similares en todos los subsectores del sector financiero.

2.2 Exigencias Empresariales

La evaluación de la solvencia de una aseguradora no debe depender sólo de datos financiero-contables sino que debe ampliar sus enfoques a la calidad de la gestión y de la organización de la empresa.

El actual sistema de exigibilidad del nivel de solvencia mínimo, basado únicamente en las magnitudes de primas y siniestros en no vida, y de provisiones y capital-riesgo en vida, resulta incompleto al no considerar, aparte de otros riesgos, aspectos tan fundamentales como reaseguro, diversificación, tamaño, matching, estrategias, etc.

Las aseguradoras y sus direcciones son cada vez más conscientes de la importancia de desarrollar modelos de control interno de riesgos y de que limitarse a seguir haciendo lo mismo implica ofrecer menor calidad de servicio a sus clientes .

2.3 Exigencias de Supervisión

Los supervisores necesitan poner en marcha nuevos sistemas enfocados a la supervisión preventiva y dinámica que les habilite para poder determinar el nivel de solvencia, no sólo en un momento determinado, sino para evaluar y anticipar su posible evolución a corto y medio plazo.

En realidad, el sistema actual es básicamente retrospectivo y claramente orientado a determinar si existen incumplimientos en el nivel de solvencia exigible al cierre de cada ejercicio y, por lo tanto, no está orientado a facilitar una supervisión prospectiva que posibilite la adopción de medidas administrativas preventivas en aquellas situaciones que puedan dar lugar a incumplimientos futuros.

El ejercicio de una supervisión preventiva sobre solvencia requiere un proceso continuo de análisis sobre aspectos muy diversos de una aseguradora: evolución de su negocio, aspectos legales y contractuales, estrategias, situación económico – financiera y calidad de dirección . Los requerimientos de solvencia que se deriven del sistema que finalmente se adopte deben ser particularizados, caso por caso, a la realidad empresarial de cada aseguradora. El objetivo del supervisor se ampliará a valorar la habilidad o situación de una aseguradora para ser capaz de hacer frente a sus compromisos a corto y medio plazo.

2.4 Exigencias de minimización de efectos no deseables

El sistema actual exige mayores recursos propios y, por lo tanto, penaliza más a aquellas aseguradoras que aplican y mantienen criterios de obtención de provisiones técnicas más prudentes.

Favorece actitudes arriesgadas al no incentivar, mediante la exigencia de menores niveles de recursos propios, a que las aseguradoras mejoren sus sistemas de gestión y control interno, estructuras o procesos, diversificación de negocio, etc.

2.5 Exigencias de los consumidores

La consolidación de los inversores y ahorradores como una nueva “categoría social” aconseja homogeneizar los criterios de solvencia e implementar parámetros de transparencia informativa a fin favorecer los procesos de optimización en sus tomas de decisiones.

Los ciudadanos, cada vez más, demandan nuevas coberturas y productos que exigen una actualización permanente en los sistemas de gerencia de riesgos.

3. Solvencia II

Bajo el nombre de Solvencia II se agrupan todas las iniciativas encaminadas a llevar a cabo una revisión de las normas imperantes sobre valoración de la situación financiera global de las aseguradoras.

Solvencia II no pretende establecer reglas globales o estandarizables que permitan la cuantificación-valoración del nivel de recursos propios necesario para el ejercicio de la actividad aseguradora sino que, por el contrario, parte de un planteamiento diametralmente opuesto y consistente en exigir que cada empresa conozca cuál es su posicionamiento frente a los distintos riesgos que está asumiendo; cuál es su nivel de gestión de los mismos; cuál es la incidencia de sus estrategias y líneas de negocio y, como consecuencia de todo ello, poder determinar la cuantía de recursos propios que necesita.

El objetivo principal de Solvencia II es proteger a los asegurados mediante la valoración de los riesgos que puedan acaecer y con el establecimiento de una medida de la solvencia global del asegurador.

Solvencia II, pues, agrupa las actuaciones y revisiones a llevar a cabo con el fin de implantar en el sector asegurador los siguientes principios orientadores:

- La búsqueda de procedimientos para el cálculo de los requerimientos de capital acordes con el diverso nivel de complejidad de las entidades aseguradoras y cuyos resultados sean mucho más sensibles al riesgo en que incurre cada una de ellas que los hasta ahora vigentes,
- Se intenta potenciar que la actuación supervisora verifique el rigor de los procedimientos utilizados por las entidades en su evaluación interna de los recursos propios totales que precisan para respaldar el conjunto de los riesgos asumidos,
- Se intenta impulsar, mediante una mayor transparencia, la disciplina de mercado, como mecanismo que estimule a las entidades aseguradoras a mantener niveles de recursos propios adecuados.

El nuevo sistema de Solvencia II se estructura en 3 pilares:

- I. PILAR I: Requisitos cuantitativos.
 - a. Elementos esenciales para el cálculo de provisiones técnicas.
 - b. Requerimiento de Capital Mínimo.
 - c. Requerimiento de Capital de Solvencia
 - d. Reglas de Inversión
- II. PILAR II: Requisitos cualitativos.
 - a. Principio de Control Interno y Gestión del Riesgo.
 - b. Principios para el proceso de supervisión.
- III. PILAR III: Disciplina de Mercado..
 - a. Divulgación de Información
 - b. Transparencia.

3.1 Pilar I: Requisitos Cuantitativos. Exigencia de Fondos Propios.

Los recursos propios requeridos para ejercer la actividad aseguradora deben ser considerablemente más sensibles al riesgo que los actualmente vigentes y, por lo tanto, resulta necesario diseñar métodos de cálculo que permitan conseguir que las exigencias de solvencia evolucionen paralelamente a los cambios en los perfiles de riesgo de las aseguradoras.

Con la regulación actual, si el Margen de Solvencia Real es inferior al Margen de Solvencia Requerido, la compañía debe llevar a aprobación un plan de recuperación de una posición financiera correcta.

Si el Margen de Solvencia Real es inferior al Fondo de Garantía, se requiere la aprobación de un plan a corto plazo, el supervisor puede restringir la disposición libre de los activos, y además debe tomar todas las medidas necesarias para proteger al asegurado. También deberá informar al resto de Estados miembros de la Unión, que deberán tomar medidas similares.

En el cálculo del capital objetivo hay que tener en cuenta todos los riesgos importantes y cuantificables a los que está expuesto el asegurador, los cuales se clasifican principalmente en las siguientes categorías:

- Riesgos Operacionales.
- Riesgos de Seguros.
- Riesgo de Crédito.
- Riesgos de Mercado
- Riesgo de Liquidez

3.2 Pilar II: Procesos de Supervisión

A cada tipo de riesgo no puede corresponder siempre la misma necesidad de margen de solvencia, sino que su incidencia dependerá de la efectividad de las estructuras de gestión y control interno de cada aseguradora

El papel de las aseguradoras debe ser el de una Gerencia de riesgos y deben llevar a cabo una auto-evaluación del nivel de recursos necesarios. Para ello las aseguradoras deben desarrollar sus propios sistemas y modelos internos que, previa aprobación por el supervisor, les permita estar en condiciones de determinar por si mismas, de forma permanente y con la suficiente antelación, cual va ser el nivel de recursos propios que necesitan como consecuencia de

los perfiles de riesgo que están asumiendo en ejecución de sus estrategias y planes empresariales.

Las competencias y mecanismos de actuación de los supervisores deben ser modificados con el fin de que sean capaces de detectar, con la suficiente antelación, situaciones o tendencias que pudieran dar lugar a incumplimientos futuros de los niveles de solvencia exigibles. En consecuencia, los supervisores deben contar con el marco normativo y los medios necesarios para poder ampliar sus funciones y responsabilidades a la evaluación del control de gestión interno de las aseguradoras y la adopción de medidas administrativas desde el mismo momento en que se detecten situaciones que puedan determinar un incremento de los perfiles de riesgo no respaldados con el nivel de solvencia existente en cada momento

3.3 Pilar III: Disciplina de Mercado

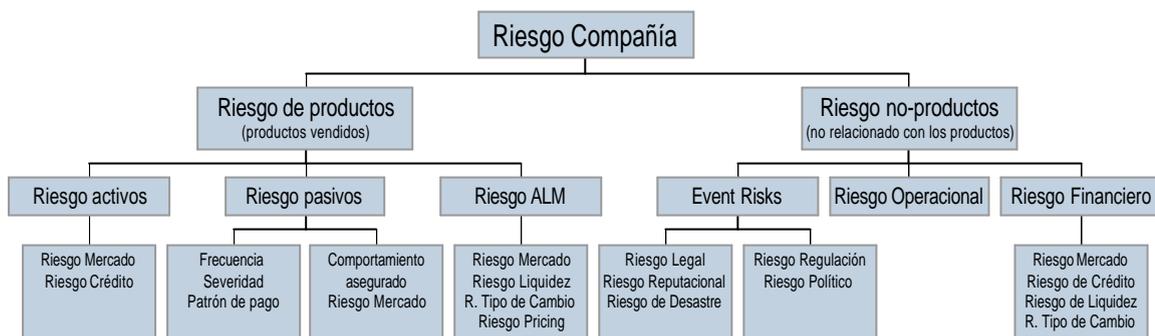
El papel de las aseguradoras debe ser informar al mercado. Las aseguradoras deben incrementar la divulgación de información relativa a su nivel de solvencia, exposición al riesgo y mecanismos de control interno al objeto de hacer posible que, desde un mayor nivel de transparencia, los agentes operadores en los mercados y los ciudadanos puedan evaluar los niveles de riesgo asumidos por cada aseguradora y, en consecuencia, que sus decisiones sirvan de estímulo al mantenimiento de los niveles de solvencia adecuados

La supervisión de las aseguradoras no es una ciencia exacta y, por lo tanto, en el proceso de revisión supervisora, los elementos discrecionales son inevitables. Los supervisores deben cuidar que el desarrollo de sus funciones se lleve a cabo de forma altamente transparente y responsable.

4. Riesgos

La noción de riesgo está ligada a una contingencia o proximidad de un daño al que se está expuesto, con incertidumbre de resultado, y potencial resultado económico adverso en caso de acaecimiento del riesgo.

Gráfico 1: Riesgos de la Compañía de Seguros



Normalmente, en todo negocio existe una cantidad normal de pérdidas que podríamos considerar como esperadas o habituales, que la organización absorberá como un coste más del negocio, son fallos que de forma explícita o implícita están presupuestados y cubiertos o incluidos en los precios de los productos (los que pueden denominarse de bajo impacto). Pero también habrá una serie de fallos o sucesos inesperados para los que será conveniente asignar fondos propios en previsión de que se produjeran.

Los riesgos a los que están expuestas las empresas son básicamente de dos tipos: riesgos de negocio y riesgos financieros.

Los riesgos de negocio son consecuencia de la actividad de la empresa, mientras que los riesgos financieros vienen originados por las fuentes de financiación necesarias para la actividad de la empresa.

Los riesgos de negocio pueden dividirse en varios:

4.1. Riesgo de Mercado

Riesgo en la alteración del valor de activos financieros:

4.1.2 Riesgo de tipo de interés

Producido por las oscilaciones de los tipos de interés en los mercados, y que causan efecto en contratos y obligaciones de la empresa.

4.1.3 Riesgo de tipo de cambio

Puede afectar a las posiciones deudoras y/o acreedoras con respecto a agentes económicos que utilizan diferente moneda de pago en sus operaciones.

4.2 Riesgo de Crédito

Riesgo de incurrir en una eventual insolvencia de la parte deudora de un contrato. Es difícil de mitigar debido a la asimetría en los flujos de información entre las partes del contrato.

4.3 Riesgo de Liquidez

Es el Riesgo producido por el desfase entre el grado de exigibilidad de los pasivos que tiene la empresa y el grado de realización de los activos.

4.4 Riesgo Operacional

Es un riesgo intrínseco a todas las actividades y procesos de cualquier sector. Está muy ligado a errores y fallos humanos, en los sistemas de información, en el control y supervisión..., que surge a partir de los fallos más significativos.

5. El Riesgo Operacional

El Riesgo Operacional adquiere formalidad en el Nuevo Acuerdo de Capital de Basilea, cuyo estudio comenzó en 1999 y que finalmente fue aprobado en Junio de 2004 por los Gobernadores de Bancos Centrales y los Jefes de los Organismos de Supervisión de los países que conforman el Comité de Supervisión Bancaria de Basilea, y en los desarrollos del propio Comité que lo complementa, presentando como aspecto fundamental el requerimiento de un capital mínimo para las entidades financieras.

La definición que se establece en Basilea es la de riesgo de pérdida debido a la inadecuación o fallos en los procesos, el personal y los sistemas internos, o bien a causa de acontecimientos externos.

Factores como la liberalización y la globalización de la actividad financiera, la sofisticación en la tecnología, y los nuevos canales de distribución de los productos y servicios están incidiendo en que dicha actividad financiera sea cada vez más compleja y que el riesgo operacional tenga especial protagonismo por los niveles que han llegado a alcanzar las pérdidas asociadas al mismo. Prueba de ello es que en más del 70% de las entidades aseguradoras del Reino Unido han llegado a reconocer, en un estudio realizado por PriceWaterHouseCoopers de 2002, que el riesgo operacional es tan importante en su actividad como los riesgos de crédito o de mercado.

El mayor uso de tecnología altamente automatizada y la dependencia de los sistemas integrados pueden provocar riesgos en procesos internos, si el sistema incurre en fallos.

El crecimiento del comercio electrónico trae consigo riesgos potenciales, por ejemplo, problemas de fraude externo y de seguridad en los sistemas.

Las fusiones, escisiones y consolidaciones a gran escala ponen a prueba la viabilidad de sistemas nuevos o recientemente integrados.

La aparición de bancos que actúan como distribuidores de seguros de gran volumen crea la necesidad de un continuo mantenimiento de controles internos y de sistemas de seguridad y soportes apropiados.

Este crecimiento en el nivel de riesgo operacional ha propiciado la aplicación y adaptación de técnicas avanzadas de gestión de riesgos.

Existen cuatro principios Marco, que son los siguientes:

- Desarrollo de un ambiente apropiado de gestión de riesgos
- Gestión de Riesgos: Identificación, Medición/Evaluación, Seguimiento y Mitigación/Control.

- El papel de los supervisores
- Divulgación de la información

Al ser un riesgo tan fragmentado (depende de muchos factores), suele ser gestionado de forma individualizada, y hasta ahora no se veía como una parte más, integrada en la gestión de riesgos de las empresas.

Al ser un riesgo presente en todas las actividades de la empresa, nadie se responsabilizaba de él en su totalidad, y la responsabilidad de su control y supervisión recaía de manera particular en las gerencias de las distintas áreas de la empresa. Era un riesgo tratado como imposible de medir. Esta medición, de hecho, es una de las grandes novedades de la nueva regulación de recursos propios de las empresas.

En el **Estudio de Impacto Cuantitativo para Solvencia II – QIS 3**, la fórmula para la cuantificación del riesgo operacional que propone el CEIOPS, Comité of European Insurance and Occupational Pensions Supervisors (Comité de Supervisores de Seguros y Fondos de Pensiones) es la siguiente:

$$\boxed{\text{MIN (30\% BSCR, MAX(A,B))}}$$

Siendo,

BSCR = la cuantificación de los riesgos de Suscripción Vida, Suscripción No Vida, Riesgo de Mercado y Riesgo de Contraparte, ponderados a partir de matrices de correlaciones muy complejas,

A = 2% Primas Brutas *No Vida* + 3% Primas Brutas *Vida*,

B = 2% Mejor Estimación Provisiones Brutas *No Vida* + 0,3% Mejor Estimación Provisiones Brutas *Vida*

Esta fórmula, sencilla en su enunciación, deja claro que ni siquiera el propio CEIOPS (Comité of European Insurance and Occupational Pensions Supervisors) sabe cómo encontrar una fórmula estándar que tenga en cuenta los riesgos y no las magnitudes para cuantificar con propiedad el riesgo operacional.

El mayor reto al que se van a enfrentar las entidades va a ser lograr una verdadera cultura de control de riesgo operacional, que se incentive a la unidades de negocio a comunicar sus propios errores y que fomente la transparencia.

Hoffman, consultor independiente especializado en riesgo operacional, en la primera de sus **20 Buenas Estrategias Prácticas para la Gestión del Riesgo Operacional**, establece que:

“El Riesgo Operacional debe ser definido, y la definición comunicada a toda la organización antes de que éste pueda ser medido y gestionado eficientemente. Es casi imposible que el personal, en su totalidad, se centre y comprometa con un tema si éste no está bien definido y entendido.”

La Alta Dirección, en referencia a la gestión de riesgos en general, y con respecto al Riesgo Operacional en particular, debe aprobar un plan estratégico lo suficientemente amplio que garantice la seguridad y solidez de la entidad. La conexión se consigue con la definición e implantación de un sistema de gestión integral del riesgo, en el que debe figurar el riesgo operacional, que considere los siguientes aspectos:

- Identificación
- Clasificación
- Cuantificación
- Mitigación
- Seguimiento

Las herramientas de gestión más utilizadas son aquellas que, dependiendo de su propia naturaleza, combinan los enfoques cuantitativo y cualitativo desde una perspectiva ex-ante o ex-post. Las técnicas más usuales son las siguientes:

Enfoque cualitativo: evaluación cualitativa basada en autoevaluación (Mapas de Riesgos).

Enfoque cuantitativo: Bases de datos de Pérdidas, cuantificar impacto mediante análisis estadístico (Value at Risk)

Enfoque mixto: cuantitativo y cualitativo: Diseño de indicadores de riesgo, seguimiento y alarmas.

En la fase de diseño de indicadores de riesgos, uno de los objetivos más difíciles de alcanzar es relacionarlos con la estrategia de gestión de riesgos de la entidad, y que además sea capaz de proporcionar información no sólo del grado de consecución de los objetivos prefijados, sino también de reflejar de qué modo se están logrando.

Para poder cumplir este objetivo, resulta imprescindible que la entidad tenga la máxima claridad estratégica de los objetivos que pretende alcanzar con la implantación de un programa de gestión y control del riesgo operacional. La elaboración de un marco de control, aprobado por la Alta Dirección, debe ser el vehículo para concienciar e implicar a toda la organización. Aún teniendo una estrategia de riesgos perfectamente definida, pueden surgir problemas de tipo estructural al diseñar el sistema de indicadores y trata de relacionarlos con la estrategia de la entidad.

Estos problemas se pueden concretar en:

- No reflejar adecuadamente la consecución de objetivos estratégicos por un excesivo énfasis en el corto plazo, no teniendo en cuenta el largo plazo.
- Carecer de una visión de conjunto de la entidad.
- No considerar las perspectivas y exigencias del negocio.
- Poner especial énfasis en indicadores de tipo financiero.
- Realizar un mal uso de los indicadores al utilizarlos como herramientas de motivación o premio, y no como una herramienta de aprendizaje y superación.
- No inducir a la mejora y el perfeccionamiento al ser sistemas concebidos desde una perspectiva más de resultados que de procesos.

Una manera de vincular los principios estratégicos de gestión del riesgo con el diseño de un sistema de indicadores de riesgo es identificar los factores clave del riesgo.

Un factor clave se puede definir como un aspecto, variable o característica que se considera crítica por su influencia, directa o indirecta, con pérdidas de tipo operacional.

5.1. Tipos de Riesgo Operacional

Los factores clave del riesgo operacional que se puedan definir o identificar pueden ser de carácter interno o externo de acuerdo con el grado de control o influencia que la entidad pueda ejercer sobre ellos. Y dentro de esa división, aún podemos subdividirlos en:

5.1.1 El Riesgo Operacional Interno

Comprende todos aquellos riesgos que se originan dentro de la propia entidad, y dependen directamente del control realizado por la dirección. Se pueden concretar en tres factores clave:

- Procesos
- Sistemas
- Recursos Humanos

5.1.2 El Riesgo Operacional Externo

Es el riesgo asociado, por una parte, a cambios en cuestiones como sistemas políticos, necesidades sociales, regímenes fiscales y políticas legales, y, por

otra, a cualquier acontecimiento de naturaleza catastrófica como terremotos, incendios, inundaciones, etc.

Son todos ellos riesgos ajenos a la empresa y que de algún modo afectan a las relaciones con los clientes, las autoridades, los proveedores, los competidores, etc.

En principio, aunque únicamente se pueden gestionar los internos, se debe tener presente que en ocasiones, los riesgos externos trasladan sus efectos al interior, produciendo en última instancia un riesgo operacional interno.

Así, por ejemplo, un cambio en la política fiscal, que nos viene impuesta, puede hacer que un operador realice una transacción indebida, una operación no autorizada o que supere algunos de los límites establecidos por la dirección, con lo que finalmente se habrá producido una pérdida fruto de un riesgo operacional interno.

Gráfico 2: Tipo de Riesgo Operacional según sea el origen de su causa.

RIESGO OPERACIONAL INTERNO	RIESGO OPERACIONAL EXTERNO
* Procesos * Sistemas * Personal	* Acontecimientos externos

Cuando se produce un evento que pueda producir una pérdida potencial, es necesario determinar si:

A) Se trata de un evento con pérdida operacional, es decir, si el evento ha tenido algún impacto negativo sobre la cuenta de resultados o la situación patrimonial de la entidad.

B) Si supera el “margen” establecido para su registro y consideración.

Y el primer paso para determinar si una pérdida es susceptible de que sea calificado como pérdida operacional consistirá en verificar que el evento que lo ha ocasionado ha sido provocado por alguna de las circunstancias contempladas en la definición de Riesgo Operacional, es decir:

1. ¿Ha sido causado por algún error humano en la ejecución de las tareas asignadas a una determinada función?

2. ¿Es consecuencia de deficiencias en el diseño de los procedimientos establecidos o de los controles existentes?
3. ¿Se debe a fallos en el soporte tecnológico y en la red de comunicaciones utilizadas, o en el equipamiento necesario para el buen funcionamiento de los procesos?
4. ¿Ha sido ocasionado por algún hecho externo no controlable por la entidad?
5. No corresponde a ninguno de los riesgos excluidos. Es decir, no es consecuencia de un riesgo estratégico ni de negocio.

Las características que debe reunir un factor para tener la consideración de clave, se pueden concretar en:

- Capacidad para identificar el éxito y el fracaso de la gestión.
- Nivel de significación ante la exposición y severidad al riesgo.
- Representativo ante cambios en la evolución del riesgo.
- Debe ser medible, de forma directa o indirecta.
- Debe provocar acciones inmediatas ante cambios relevantes en el factor de riesgo.

Cada uno de los factores de riesgo identificados como clave se pueden escindir a su vez en otros factores de riesgo más específicos y claramente relacionados con la causa o el origen del riesgo. Para que la gestión del riesgo sea eficaz, los factores de riesgo se deben medir utilizando indicadores que actuarán a su vez como señales de alerta o indicadores para fijar objetivos

La identificación de factores clave de riesgo operacional afecta a todos los niveles de la organización, lo que conlleva importantes ventajas en la gestión y es el punto de partida para definir el sistema de indicadores de riesgo. Para la entidad, tener identificados un conjunto de factores de riesgo clave presenta las siguientes ventajas:

- El perfil de riesgo se define con mayor claridad.
- Vincula la estrategia de gestión global del riesgo con factores concretos que es necesario identificar y medir.
- Facilita la identificación de los indicadores de riesgo asociados a cada factor de riesgo.
- Contribuye a orientar y centrar la atención de la organización en la gestión del riesgo.
- Centra la atención en lo que es esencial y no en lo que es fácil medir.
- Mejora el proceso de planificación al poder vincular los objetivos estratégicos de gestión del riesgo con los factores clave respectivos.

6. Detección y Control de Riesgos

La implantación de sistemas integrales de gestión del riesgo en el ámbito empresarial trata de invertir situaciones de pérdida de confianza en las compañías por parte de los asegurados ya que pone a disposición de la alta Dirección sistemas de control y supervisión de para verificar que la empresa identifica, evalúa y controla y mitiga eficaz y eficientemente los riesgos claves del negocio¹.

Gráfico 3 : Identificación de Riesgos Clave



Para lograr un control de riesgos efectivo es imprescindible la implicación integral de las entidades en los distintos niveles. Junto con la participación de los órganos de dirección, esta forma de gestión afecta a los distintos departamentos que se reparten las responsabilidades relacionadas con los riesgos. Además, como parte de este sistema de control y en consonancia con la diversidad y complejidad de la actividad de la entidad, debería existir una auditoría interna amplia y eficaz realizada por personal operativamente independiente, adecuadamente formado y competente.

Esta función de auditoría interna debe informar directamente a la dirección ejecutiva y ha de tener acceso a la junta directiva de modo que las deficiencias apreciadas y las recomendaciones que pudiera formular sean adecuadamente transmitidas y tratadas.

La Dirección General de Seguros y Fondo de Pensiones está comprometida con esta visión de la gestión de riesgos, tanto en su faceta de supervisor como en la de regulador, por ello, la reforma del ROSSP desarrolla las obligaciones

¹ Gráfico Mitigación del Riesgo Operacional, KPMG Consulting.

en materia de control interno. Dicha reforma contiene deberes generales para las entidades que deben establecer e incluso documentar procedimientos de control interno adecuados, tanto a nivel individual como de grupo.

La modificación del ROSSP, aprobada el 27 de diciembre de 2006, en su artículo 110 sobre el **Control Interno de las entidades aseguradoras**, establece lo siguiente:

3. Los procedimientos de control interno comprenderán, en todo caso, el desarrollo de una adecuada función de revisión y el establecimiento de sistemas de gestión de riesgos.

4. La función de revisión será ejercida por personal con suficiente conocimiento y experiencia que garantice, en el ejercicio de sus funciones, plena independencia respecto a las distintas áreas de la entidad, correspondiendo al Consejo de Administración de la misma garantizar los recursos precisos para el adecuado cumplimiento de las funciones que tienen encomendadas.

5. Las entidades aseguradoras establecerán sistemas de gestión de riesgos adecuados a su organización que les permitan identificar y evaluar, con regularidad, los riesgos internos y externos a los que están expuestas. Para ello establecerán estrategias respecto a los mismos, adecuadas a la naturaleza e incidencia de tales riesgos, incorporando procesos que permitan una medición de los riesgos identificados, incluyendo su 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.

6. Los procedimientos de control interno se extenderán, en aquellas entidades que externalicen cualesquiera de sus funciones o actuaciones, a las actividades externalizadas. En ningún supuesto la externalización de funciones implicará que la entidad transfiera o deje de asumir las responsabilidades derivadas de tales funciones.

7. Anualmente la entidad elaborará un informe sobre la efectividad de sus procedimientos de control interno, incidiendo en las deficiencias significativas detectadas, sus implicaciones, y proponiendo, en su caso, las medidas que se consideren adecuadas para su subsanación. El referido será suscrito y remitido por el consejo de administración de la entidad a la Dirección General de Seguros y Fondos de Pensiones junto con la documentación estadístico-contable anual en los plazos a los que se refiere el artículo 66.

8. Las entidades aseguradoras establecerán, atendiendo a sus características particulares, una adecuada segregación de tareas y funciones tanto entre su personal como entre las actividades que se llevan a cabo en la misma.

9. Los requerimientos establecidos en este artículo, de aplicación a todas las entidades aseguradoras, podrán implementarse por las mismas de acuerdo con

el principio de proporcionalidad, de manera que, exigiéndose los mismos principios y elementos de control, su ejecución podrá llevarse a cabo atendiendo a la dimensión de la entidad y a su nivel de riesgos. En ningún caso la aplicación de este apartado podrá suponer una menor protección para el asegurado.

10. *Corresponde al Consejo de Administración de la entidad obligada a presentar la documentación estadístico-contable consolidada establecer los procedimientos de control interno que resulten necesarios a fin de asegurar el cumplimiento de lo dispuesto en los apartados anteriores con referencia al grupo consolidable de entidades aseguradoras*

El grupo consolidable de entidades aseguradoras, a través de las entidades que lo componen, establecerá los procedimientos de control interno necesarios para asegurar la plena disponibilidad y adecuada presentación de cuantos datos e información general se precise para la elaboración y cumplimentación de las cuentas consolidadas, incluidos los estados de cobertura de provisiones técnicas y de margen de solvencia consolidados.

Esta modificación del ROSSP está en la línea del ya mencionado **Estudio de Impacto Cuantitativo para Solvencia II – QIS 3**, en el que, a parte de las valoraciones cuantitativas de capitales de solvencia, el CEIOPS ha facilitado también a los participantes en el estudio un cuestionario cualitativo a rellenar, y que valoran varios aspectos relacionados sobretodo con los órganos de dirección de cada entidad aseguradora.

Alguna de las preguntas del citado cuestionario son:

-¿Su entidad aseguradora tiene aprobada por el Consejo de Administración (u órgano equivalente) una estrategia para el riesgo operacional?

-¿Tiene su Consejo de Administración (u órgano equivalente) definidos niveles de tolerancia sobre el riesgo operacional como parte de su estrategia?

-¿Existe una política de riesgo operacional en su entidad aseguradora?

-¿Hay políticas / guías que expliquen y apoyen la política de riesgo operacional?

-¿Tiene su entidad aseguradora una estructura u organización de gestión de riesgo operacional con funciones y responsabilidades bien definidas?

-¿Estas funciones y responsabilidades están registradas en políticas / guías?

-¿Existe un control o gestión independiente del riesgo operacional en su entidad aseguradora?

-En el caso de que no haya un control o gestión independiente del riesgo operacional en su entidad aseguradora, ¿es el departamento de auditoría interna quien gestiona o controla el riesgo operacional?

-¿Existe algún comité (por ejemplo, el Comité de Riesgo Operacional) implicado en la gerencia del riesgo operacional en su entidad aseguradora?

-¿El Consejo de Administración (u órgano equivalente) está implicado en tales comités?

-¿Existe una estructura de reporting claramente definida sobre el riesgo operacional en su entidad aseguradora (por ejemplo, hay una persona de contacto – una central de riesgo operacional – Comités – Consejo de Administración - ...)?

-¿El Consejo de Administración (u órgano equivalente) ha recibido algún informe estándar sobre riesgo operacional?

-¿Existen medios (jornadas de formación, workshops, boletines de noticias...) para aumentar el conocimiento de sus empleados sobre el riesgo operacional de su entidad aseguradora?

-¿Su entidad aseguradora utiliza el mapa de riesgos como herramienta de gestión del riesgo operacional?

-¿Su entidad aseguradora realiza auto-evaluaciones sobre el riesgo como herramienta de gestión para el riesgo operacional?

-¿Su entidad aseguradora utiliza indicadores de riesgo (indicadores clave sobre riesgo) como herramienta para la gestión del riesgo operacional?

-¿Su entidad aseguradora almacena datos históricos sobre pérdidas e incidencias ocasionadas por el riesgo operacional?

-¿Están las herramientas de gestión de riesgo operacional (por ejemplo indicadores de riesgo, auto-evaluaciones sobre el riesgo) sujetas a un análisis de correlación basado en datos de pérdidas reales?

-¿Tiene su entidad aseguradora (o su entidad matriz) cualquier información sobre la pérdida operacional compartida con el Consorcio (por ejemplo el Consorcio de Seguros de Riesgo Operacional – ORIC)?

-¿Su entidad aseguradora utiliza el análisis de escenarios como parte de la gestión del riesgo operacional?

-¿Su entidad aseguradora utiliza métodos cuantitativos (modelos internos) encaminados a la gestión del riesgo operacional?

-¿Qué método cuantitativo (modelo interno) es utilizado o está planificado para ser utilizado?

-¿Su entidad aseguradora realiza algún proceso de validación para todos los métodos y herramientas aplicados al riesgo operacional?

El riesgo operacional es una variable que no resulta fácil de analizar debido a la heterogeneidad de factores que lo componen. Por ello, para una mejor identificación de su comportamiento, se puede estudiar realizando una división de los factores de riesgo en otros tipos de riesgo que, siendo de la misma base conceptual, las causas que lo originan difieren significativamente.

La vinculación de los factores clave y los indicadores de riesgo se puede sintetizar definiendo el factor clave como lo que es necesario medir, y el indicador de riesgo como la manera de medir el factor de riesgo.

La utilidad de los indicadores es la posibilidad de establecer un valor óptimo para cada uno de ellos, y a partir de éste, fijar intervalos de variación aceptables. Los valores óptimos se determinan en función del grado de tolerancia establecido por la entidad, los objetivos estratégicos o los planes de negocio. En función del intervalo de variación establecido, la entidad puede definir planes de acción o medidas correctoras.

Un indicador de riesgo es un elemento empírico de naturaleza generalmente cuantitativa, aunque también puede ser de tipo cualitativa, cuyos valores son por lo general calculados en base a datos históricos, que permiten representar la dimensión teórica o específica de un factor de riesgo considerado clave.

El uso de indicadores de riesgo permite implantar un sistema de gestión que proporcione pistas sobre el nivel de riesgo de la entidad y proporcionar una visión multidimensional de su perfil de riesgo.

La cuestión principal es determinar qué tipo de indicadores son los que mejor definen el perfil de riesgo de la entidad y en qué medida actúan como señales de alerta que anticipan pérdidas.

Una manera de vincular los principios estratégicos de gestión del riesgo con el diseño de un sistema de indicadores es identificar los factores claves de riesgo,

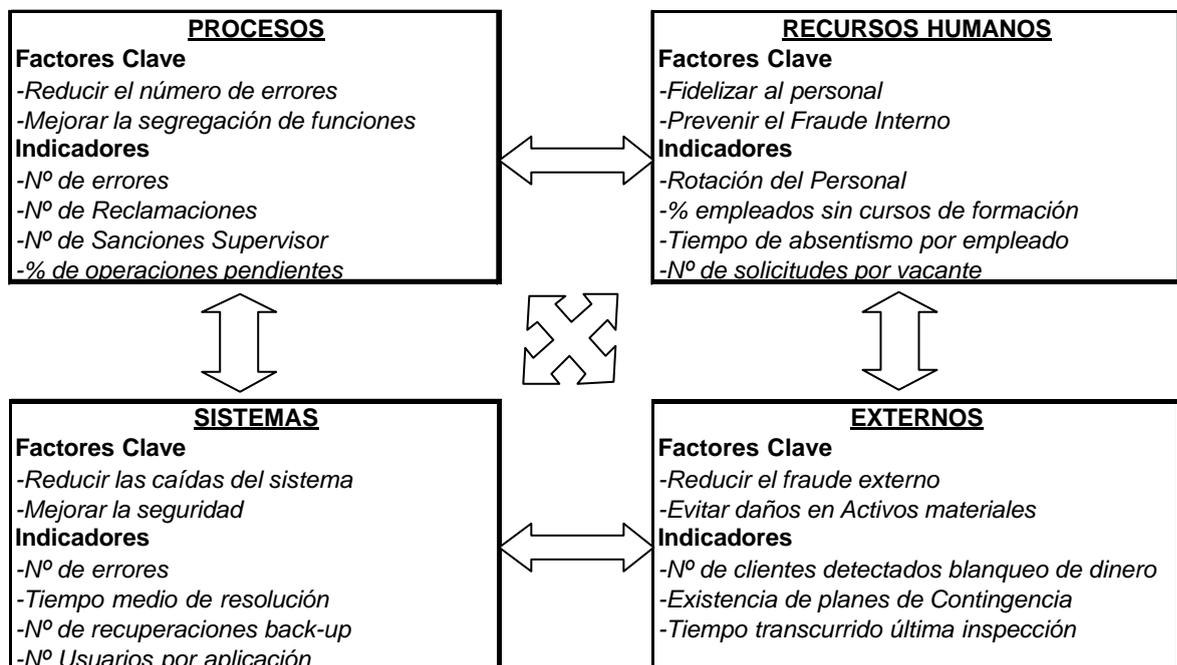
que en relación con el riesgo operacional se pueden asociar por tipos de riesgo por su propia naturaleza.

El desarrollo de la metodología deberá contemplar el siguiente proceso:

- Identificar las causas del riesgo asociadas a cada factor clave, mediante auto-evaluaciones, análisis de eventos de pérdidas o simulación de escenarios desfavorables.
- Definir los indicadores de riesgo, valorar la obtención y recogida de datos, y seguimiento.
- Almacenar eventos de pérdida por riesgo operacional, para contrastar resultados.
- Utilizar la información para la gestión efectiva del riesgo operacional, tendente a mitigar el riesgo.
- Calcular y distribuir capital económico por áreas de negocio.

CUADRO DE RIESGO OPERACIONAL

Categorías de Riesgo, Objetivos e Indicadores Asociados



7. El Comité de Riesgos

El sistema ideal de gestión del riesgo mitiga la probabilidad de ocurrencia e impacto de las amenazas, e identifica y aprovecha las oportunidades de negocio.

La gestión de los riesgos se centra en los siguientes aspectos:

a) Alinea el riesgo aceptado y la estrategia

En su evaluación de alternativas estratégicas, la Dirección considera el riesgo aceptado por la entidad, estableciendo los objetivos correspondientes y desarrollando mecanismos para gestionar riesgos asociados.

b) Mejora las decisiones de respuesta a los riesgos

La gestión de riesgos proporciona rigor para identificar los riesgos y seleccionar entre posibles alternativas como respuesta: evitar, reducir, compartir o aceptar.

c) Reduce las sorpresas y pérdidas operativas

Las entidades consiguen mejorar su capacidad para identificar los riesgos potenciales y establecer respuestas contra ellos, reduciendo las “sorpresas” y los costes o pérdidas asociados.

d) Identifica y gestiona la diversidad de riesgos para toda la entidad

Cada entidad se enfrenta a múltiples riesgos que afectan a distintas partes de la organización, y la gestión de riesgos facilita respuestas eficaces a los impactos y las consecuencias de la ocurrencia de dichos riesgos.

e) Mejora de la dotación de capital

La obtención de información consistente sobre el riesgo permite a la dirección evaluar las necesidades globales de capital, y mejorar su asignación con una mejora del control de los riesgos.

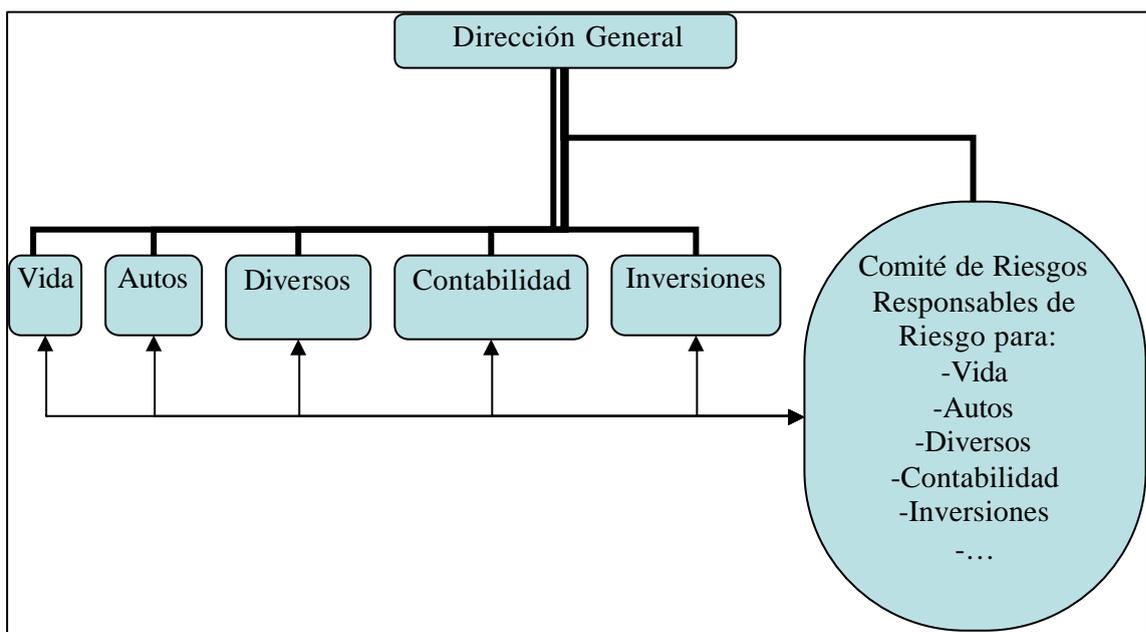
Asimismo, un buen sistema integral de gestión del riesgo incide de forma positiva en la creación de valor al accionista, al permitir el reparto eficiente del capital de la compañía entre las distintas líneas de negocio, y optimizar las ganancias según los distintos niveles de riesgo asumido.

Todas las personas que integran una entidad tienen alguna responsabilidad en la gestión de los riesgos. El Consejero Delegado es el responsable último. El resto de la cúpula directiva debe apoyar la gestión de riesgos de la entidad, promover el cumplimiento del riesgo aceptado, y gestionar los riesgos dentro de sus áreas de responsabilidad.

Para la efectividad del sistema, la existencia de un Comité de Riesgos se perfila como una figura imprescindible para la correcta gestión de éste, ya que define las políticas y metodologías, asesora, analiza e informa a las distintas áreas de negocio sobre la mejor forma de controlar el riesgo. El director financiero, administrativo, auditor interno u otros han de desempeñar funciones clave de apoyo, mientras que el restante personal de la entidad es responsable de ejecutar el plan de gestión de riesgos de acuerdo con las directrices y protocolos establecidos.

Las compañías pueden optar por integrar a este Comité en sus organizaciones de maneras diversas. Un ejemplo podría ser:

Gráfico 4: Organigrama



El Comité de Riesgos lo formaría un responsable de Riesgos de cada departamento. Esto puede llevar aparejado un vicio de origen, como puede ser que, por ejemplo, personal del departamento de Vida controle los riesgos del departamento de Vida. No tiene mucho sentido que una persona que, por su trabajo, ya ha de controlar posibles riesgos, supervise esos mismos riesgos como miembro del Comité.

Sería mucho más práctico que los miembros del Comité no tuvieran vinculación laboral con el departamento que han de supervisar, para no estar influenciados sobre los posibles riesgos que puedan detectar. Su función es detectarlos,

definirlos y comunicarlos al responsable de cada departamento o unidad de negocio, que será el responsable de intentar controlar y, si es posible, mitigar el riesgo detectado.

La composición del Comité de Riesgos debería ser personal cualificado y especializado, y con amplia experiencia en el mundo de los seguros para poder llevar a cabo una buena labor, debido la importancia de la misma.

También es evidente que la creación de un Comité de Riesgos en el que se integrara personal únicamente para desempeñar esta función no está al alcance de todas las empresas. Por ello, una posibilidad podría ser el cruce de supervisión, es decir, que una persona del departamento de Vida supervisara los riesgos del departamento de Autos, que una persona del departamento de Salud supervisara los riesgos de Decesos... Esto daría una visión "limpia" de los riesgos, ya que los supervisores no estarían influenciados por su día a día.

Vistos los riesgos a los que se puede enfrentar una compañía en su día a día es muy importante nombrar un Comité de Control que vele por el correcto funcionamiento de los circuitos y procesos planificados, ya que el control de los riesgos y posee el potencia de disminuir o aumentar el valor de la empresa.

Se minimizan los riesgos cuando la Dirección establece una estrategia y unos objetivos encaminados a encontrar el óptimo equilibrio entre la finalidad de la empresa, que es el crecimiento sostenible y la rentabilidad, y los riesgos asociados.

La gestión de riesgos debe ser un proceso continuo que debe fluir por toda la entidad, realizado por su personal en todos y cada uno de los niveles de la organización, y debe recoger la perspectiva del riesgo a nivel conjunto de la entidad. Debe estar diseñado para identificar los acontecimientos potenciales que, de ocurrir, afectarían a la entidad, y para gestionar los riesgos dentro del nivel aceptado.

Este análisis debe ser capaz de proporcionar una seguridad razonable al consejo de Administración y a la dirección de la entidad.

Veamos algunos ejemplos:

Tabla de ejemplos de procesos y Riesgos Asociados a los mismos

PROCESOS	RIESGOS
-Contratación de póliza	-Criterio equivocado en la selección de riesgos (salud, profesión, deportes...) -Inclusión de garantías o riesgos no asegurables -Superación de capitales máximos asegurables -Descontrol de cúmulos.
-Cesión al Reaseguro	-Superación de la capacidad máxima del contrato. -No cesión a Facultativo
-Tramitación del siniestro	-Darle curso habiendo carencia de documentación para realizarlo.
-Pago del Siniestro	-Realización de pagos incorrectos -Aplicación incorrecta de la fiscalidad en el pago (IRPF en lugar de ISD)

8. Medición de los riesgos

Aunque el objeto principal de esta tesis no es tanto tratar los posibles modelos de cuantificación de los riesgos como identificarlos y ver sus pautas de control, veamos cómo podrían medirse estos riesgos operacionales.

Veíamos en el Capítulo 5 (El Riesgo Operacional) que ni siquiera el **CEIOPS** (Comité de Supervisores de Seguros y Fondos de Pensiones) tiene claro cómo cuantificarlo en su **Estudio de Impacto Cuantitativo para Solvencia II – QIS 3** y se limita a proponer, de momento, una fórmula estándar que pondera las Primas y las Provisiones de Vida y de No Vida.

A modo de ejemplo, se pueden establecer tres tipos generales de medida, que si bien no quedarán reflejados directamente en la cuenta de resultados, puede ayudar en la medición de los riesgos operacionales:

8.1 Medición nominal

Es la forma más sencilla de medición e implica el agrupamiento de los riesgos por categorías, tales como la económica, tecnológica, etc., sin situar un acontecimiento encima de otro. Los números asignados en la medición nominal sólo tienen una función de identificación y los riesgos no pueden ser ordenados, clasificados ni agregados.

8.2 Medición ordinal

En este tipo de medición, los riesgos se describen en orden de importancia, posiblemente con etiquetas del tipo **Alta, Media o Baja**; o bien clasificados por medio de una escala. La Dirección determina si el riesgo con el número uno es más importante que el riesgo con el número dos. Por ejemplo, la Dirección puede estimar que la probabilidad de pérdidas de Datos confidenciales de los clientes por parte de personal que cesa en la empresa es más importante que la probabilidad de que un nuevo virus informático afecte a sus sistemas.

Si bien algunas evaluaciones cualitativas de riesgos se establecen en términos subjetivos y otras en términos objetivos, la calidad de estas evaluaciones depende principalmente de los conocimientos y criterios de las personas implicadas en su identificación y control, su comprensión de los acontecimientos posibles y su contexto.

También es útil valorar, en términos de Riesgo Operacional, tanto el impacto que esas pérdidas pueden ocasionar a la entidad, como la frecuencia con que se pueden llegar a dar, porque de la combinación de ambos dependerá el nivel de Riesgo Operacional (como queda reflejado en el **gráfico 5**), y en función de ello se decidirá la mejor forma de enfrentarse a dichas pérdidas (**gráfico 6**)

Gráfico 5: Niveles de Riesgo

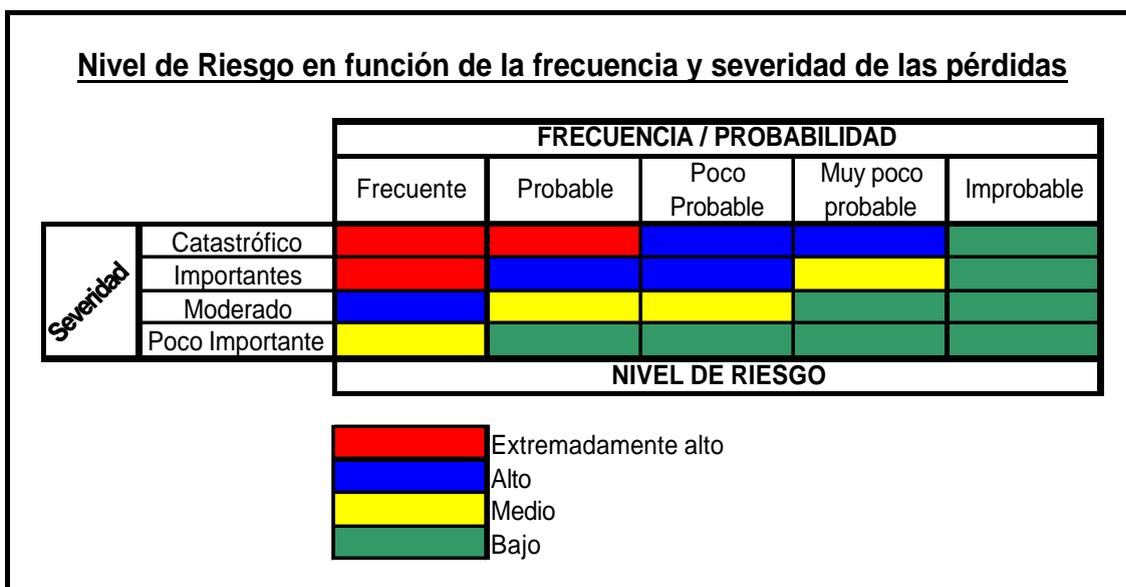
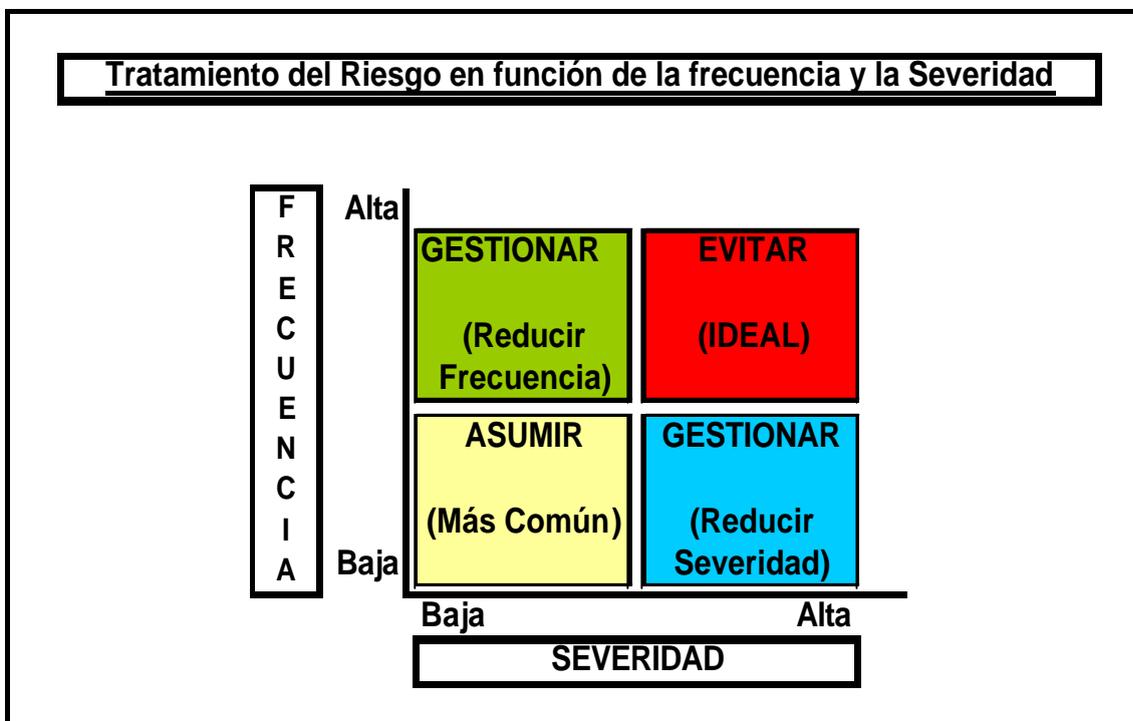


Gráfico 6: Tratamiento del Riesgo



De este modo, las pérdidas mas relevantes derivadas del riesgo operacional se pueden clasificar en dos categorías:

A)Alta Frecuencia – Bajo Impacto

Sucesos de pequeña cuantía que, del alguna manera, son esperados y que parece lógico considerarlos como un coste general, a la vez que se trata de minimizarlos mediante los convenientes planes respectivos.

Las pérdidas derivadas del riesgo operacional se pueden dividir en pérdidas esperadas y pérdidas inesperadas.

En las compañías aseguradoras, normalmente existe una cantidad de pérdidas que podrían considerarse como esperadas o habituales, que la organización absorberá como un coste más del negocio. Son fallos que, de forma explícita o implícita, están presupuestados y cubiertos o incluidos en las primas.

Existen también una serie de fallos inesperados para los que sería conveniente asignar Fondos Propios en previsión de que se produjeran. Éstas últimas pueden clasificarse en dos categorías:

A.1) Las pérdidas severas pero no catastróficas

Deberían ser cubiertas mediante la adecuada asignación de capital, y que determinan el cálculo del capital regulatorio.

A.2) Las pérdidas catastróficas

Son aquellas que representan las formas más extremas del riesgo operacional pero que por su impacto podrían acabar completamente con la entidad. Para éstas, la entidad tratará de encontrar formas alternativas para cubrirse ya que el capital no protege de tales riesgos.

B)Baja Frecuencia – Elevado Impacto

Sucesos aislados de muy variada naturaleza, imposibles de prevenir. La mejor forma de gestionarlos es a través de procedimientos de prevención de pérdidas, diversificación del riesgo, outsourcing y otras medidas y acciones para prevenir el riesgo.

A continuación, un ejemplo de una evaluación de riesgos cualitativa mediante una escala de medición ordinal:

Nivel	Descripción	Probabilidad	Riesgo
1	Muy Improbable	Muy baja	Sistemas informáticos no operativos durante largo tiempo por acciones terroristas
2	Improbable	Baja	Sistemas informáticos no operativos durante largo tiempo por bajadas de tensión
3	Posible	Moderada	Piratas informáticos se introducen en nuestro sistema de seguridad informática
4	Probable	Alta	La plantilla utiliza recursos de la empresa para contenidos inadecuados en internet
5	Casi seguro	Muy alta	La plantilla utiliza recursos de la empresa para mensajería personal

8.3 Medición de intervalo

Utiliza una escala de distancias numéricamente iguales. Si, por ejemplo, el impacto de la pérdida de la emisión de una póliza por fallo de un ordenador se mide como “tres”, el impacto de una caída de tensión de una hora como “seis” y el efecto de un puesto de trabajo clave que queda vacante de forma imprevista como “nueve”, la dirección puede determinar que la diferencia en impacto entre un “tres” y un “seis”, en la misma que entre un “seis” y un “nueve”. Eso no significa que el impacto del riesgo medido con un “seis” sea el doble de importante que el riesgo medido con un “tres”.

También se puede intentar llevar a cabo una medición cuantitativa:

Las técnicas cuantitativas pueden utilizarse cuando existe suficiente información para estimar la probabilidad de ocurrencia de un riesgo. Para ello es necesario disponer de una información precisa y con datos válidos. Las técnicas probabilísticas incluyen modelos de evaluación de riesgos con pérdidas asociadas, establecidas en unidades que podamos medir y cuantificar de alguna manera.

Un ejemplo de este tipo de medición cuantitativa puede ser la siguiente:

Objetivo: Emisión de Pólizas de Vida Individual		
Riesgo		Unidades de Medida
Errores en la emisión		Tiempo de Administrativo Pólizas a emitir paralizadas Tiempo de Informáticos Tiempo de Responsables Coste de espera de resolución
Nivel	Impacto Relativo	Mediciones
1	Despreciable	Ninguna incidencia reseñable Pérdida mínima de tiempo
2	Leve	1 Incidencia Tiempo de Administrativo pérdida de 15 minutos 2 pólizas paralizadas
3	Moderado	2 Incidencias Tiempo de Administrativo Pérdida de 30 minutos 4 pólizas paralizadas
4	Grave	3 Incidencias Tiempo de Administrativo Tiempo de Informáticos Pérdida de 60 minutos 8 pólizas paralizadas
5	Muy Grave	5 Incidencias Tiempo de Administrativo Tiempo de Informáticos Pérdida de 120 minutos 16 pólizas paralizadas Tiempo de Responsables

9. Fusiones y Adquisiciones

La comercialización de servicios, como los aseguradores, cumple una función esencial en el desarrollo económico y la creación de empleo. El tamaño de las empresas de todo el mundo ha aumentado considerablemente a raíz de las fusiones y adquisiciones. La globalización, la modificación de la legislación y la liberalización de los mercados han propiciado una competencia intensa, lo que ha añadido más importancia aún al tamaño de la empresa.

La concentración del sector fomenta estrategias basadas en el aumento de los servicios y su calidad, y en los precios: los menores costes se utilizan para disminuir los precios. Tales estrategias exigen una mayor base de ventas, y las fusiones y adquisiciones constituyen un medio para responder a esa necesidad de expansión.

Las economías de escala pueden surtir efectos beneficiosos y las empresas que no amplían sus actividades pueden encontrarse en desventaja en una economía cada vez más competitiva, de ahí que la tendencia a la fusión y a la adquisición vaya creciendo, si bien es necesario que exista complementariedad entre los negocios a fusionar, ya que de este modo será más probable obtener sinergias y ventajas competitivas, manteniendo las fortalezas que tenían ambas empresas por separado.

El aspecto práctico de las fusiones y adquisiciones conlleva lógicas dificultades en la integración de los negocios y las estructuras debido a las diferentes culturas corporativas, diferentes sistemas de información, implica el reposicionamiento de directivos, pasando por la combinación de las instalaciones, reubicación del personal y armonización de las condiciones laborales. La manera en que se afronten estas cuestiones puede tener una influencia decisiva en el éxito de una fusión o adquisición.

Toda integración debe ser rápida, ya que deja a la empresa en situación de debilidad operativa y comercial de la que se aprovechan los competidores. También debe ser operativamente eficiente, la calidad del servicio y la resolución de los problemas del día a día no puede abandonarse. Y es importante hacerlo en un entorno informático único. La plataforma informática sintetiza el modelo de empresa, por lo que es urgente decidirse por un modelo e implantarlo.

10. El Riesgo en las Fusiones y Adquisiciones

Como hemos podido ver hasta ahora, el control de los riesgos en situación de normal funcionamiento de cualquier empresa en general, y de una entidad aseguradora en particular, es muy importante, así como su cuantificación, para poder analizar en qué manera una buena gestión de los mismos se refleja en la cuenta de resultados de la compañía.

Los procesos de fusión crean incertidumbre, y esta incertidumbre implica riesgos y oportunidades que poseen el potencial de disminuir o aumentar el valor de la empresa.

Lógicamente, en un proceso de fusión / adquisición podemos encontrarnos muchos más riesgos, y sobre todo operacionales, que deberían ser detectados, controlados y mitigados en la medida de lo posible.

Los procesos de integración de negocios son largos y complicados. La descripción de los circuitos de funcionamiento y procedimiento debe hacerse al detalle para no dejar cabos sueltos que puedan dar lugar a pérdidas inesperadas por fallos en el control. Su cuantificación global es muy complicada ya que aparecen en momentos en que nada es habitual, y la prioridad no es tanto ver cómo nos han afectado, sino tratar de solucionar los problemas para que no se vuelvan a repetir.

Debido a ello es importante la creación de grupos de trabajo o comités de riesgos de para la integración que serán los encargados de supervisar el proceso.

Veamos primero un proceso de fusión muy simplificado, pero que nos dará una idea de lo que podemos encontrarnos, y cómo podrían funcionar los comités.

10.1 El Proceso de fusión y/o adquisición

Las etapas básicas de un proceso de fusión / adquisición, una vez se ha tomado la decisión de intentar realizarla, resumiendo mucho, pueden agruparse en las siguientes:

1. Inicio de conversaciones
2. Due diligence, para fijar el precio.
3. Firma del acuerdo.
4. Ejecución del acuerdo
5. Integración de compañías
6. Seguimiento de la integración
7. Finalización
8. Re-análisis.

10.1.1 Inicio de conversaciones

Durante el proceso de conversaciones es muy importante que la empresa compradora analice el tipo de negocio de la entidad que se propone comprar, porque será muy importante y necesario que exista complementariedad entre los negocios a fusionar, ya que de este modo será más probable obtener sinergias y ventajas competitivas, manteniendo las fortalezas que tenían ambas empresas por separado.

10.1.2 Due diligence

En el momento en que una empresa decide fusionarse / adquirir otra, la parte compradora necesita conocer al detalle el estado de situación de la compañía que pretende adquirir. La función básica de la “due diligence” es valorar la compañía objetivo, investigando los aspectos significativos de su pasado, presente y futuro predecible.

El proceso de due diligence permite evaluar a la empresa en funcionamiento, valorar sus activos y pasivos, conocer tanto sus aspectos legales como los contratos y estatutos, cumplimiento de la legislación vigente, marcas registradas, activos intangibles, determinar los riesgos contingentes del negocio, juicios actuales y potenciales y determinar la existencia de pasivos ocultos, reales o potenciales, así como el análisis de circuitos y procesos para determinar riesgos operacionales latentes.

Producto de la realización de este trabajo, se realiza un informe con comentarios y observaciones que servirá como base para la negociación del acuerdo final en temas como potenciales riesgos contingentes, cláusulas de garantías, etc.

En esta etapa aparece un primer riesgo muy importante: la fiabilidad de los datos que se faciliten a quien realice la auditoría.

Es muy probable que las conversaciones se lleven en secreto entre las direcciones de las empresas implicadas, pero es inevitable que cuando se empiezan a pedir datos contables, ficheros con bases de datos, programas de cálculos de provisiones, etc, comiencen a difundirse noticias y rumores acerca de una posible venta de la empresa, con la afectación que ello implica para los trabajadores.

Dependerá mucho de la manera cómo se comunique a los trabajadores que se van a dedicar a generar datos y ficheros para qué son. Es evidente que no trabaja igual y con la misma dedicación, exigencia y detalle un personal que no teme por su futuro, que un personal que puede ver su peligrar su estabilidad laboral por un futuro proceso de fusión y/o adquisición. La tendencia natural de los trabajadores es a pensar en negativo cuando de lo que se trata es de

conservar un puesto de trabajo. Y si una persona sospecha que la empresa puede estar en venta, y que su continuidad puede ser más que dudosa, su trabajo se resentirá y los datos que elabore quizá no sean tan exactos y correctos como los que elaboraría sin esa intranquilidad. Y ello redundaría en un riesgo para la empresa compradora, ya que debe fiarse de los datos que le facilitan, con el riesgo de que éstos no sean exactos al 100%.

Y debe fiarse porque el tiempo es un factor muy importante, siempre apremia en este tipo de operaciones, y un retraso de días en la valoración de unas provisiones matemáticas, o en la estimación de unas provisiones de IBNR puede implicar mucho dinero en el precio final de la operación, lo cual supone que, en ocasiones, es mejor dar por buenos los datos que se facilitan para la auditoría, y descontar un margen de error razonable, que esperar a que todo cuadre al céntimo, sin saber cuánto tiempo se debe esperar para ello.

Este margen de error aceptado irá aflorando poco a poco, conforme comiencen a integrarse las compañías, si finalmente se llega a un acuerdo.

10.1.3 Ejecución del acuerdo de fusión

Una vez se ha concretado la fusión / adquisición, y se ejecuta el acuerdo, se lleva a cabo el proceso de modelización y diseño de la nueva compañía, unión de las anteriores y su integración. Los procesos de integración llevan aparejados golpes de timón en la dirección, y decisiones que afectan a muchas personas y departamentos.

Los departamentos de Recursos Humanos y de Organización deben ser los primeros en entrar en contacto con los colaboradores de la empresa absorbida. Su primera tarea debe ser analizar el organigrama de la entidad e intentar tener no sólo el esquema sino también las funciones que realizan todos y cada uno de los colaboradores.

Es evidente que los procesos de fusión conllevan movimientos de ajuste de plantilla debido a la redundancia de cargos y puestos en las organizaciones. Debe evitarse la falta de valentía a la hora de reducir personal sobrante, ya que puede convertirse en una rémora más adelante y afectar mucho a la cuenta de resultados.

Debe llevarse a cabo una selección de personal lo más rigurosa posible, ya que de ella saldrá la plantilla que formará parte de la empresa en el futuro, y además, estos colaboradores son los que van a tener un papel más importante en la integración. Conocen “su” parte de la empresa y tienen contacto con las personas que les van a traspasar su trabajo.

Esta tarea también ha de llevarse a cabo con grandes dosis de diplomacia y mano izquierda, ya no sólo por la selección de personal que se deberá hacer,

sino por la muy difícil tarea de “cuidar”, hasta que se produzca el proceso real de integración, a las personas que deberán abandonar la empresa, y la tarea de conciliar condiciones laborales de una y otra empresa de los trabajadores que permanecerán.

Los trabajadores con los que no se contará para el nuevo proyecto llevan incorporado un “know-how” de su puesto de trabajo, problemáticas, soluciones..., su día a día, en fin. Ese capital humano ha de transmitir su conocimiento a las personas que asumen sus funciones, pero con varias particularidades:

1) La motivación del transmisor de la información no será óptima debido a su situación de transitoriedad e inestabilidad, por tanto, es muy probable que no deposite todo su conocimiento en el receptor.

2) Es muy probable que la calidad de la transmisión no sea todo lo buena que sería deseable, debido al estado de ánimo de los colaboradores que cesarán en sus funciones.

3) El tiempo de transmisión es, en la mayoría de los casos, insuficiente para el volumen de información que seguramente se debe traspasar con todas las particularidades.

4) Se crean vacíos de información de los que nadie dispone una vez se ha reducido e integrado la plantilla, ya que, desgraciadamente, en la mayoría de las ocasiones no todo consta, aunque debería para evitar riesgos operacionales importantes, en los manuales de procedimientos de las compañías.

Para intentar paliar estas deficiencias, y seguro que no podrá hacerse al 100%, serán vitales dos cosas: intentar compensar de alguna manera esa falta de motivación con incentivos económicos o de otro tipo; y en segundo lugar, será necesario nombrar un Comité de Análisis de Riesgos, que pueda discernir entre temas realmente importantes desde el punto de vista del riesgo, y otros que lo sean menos, y un Comité Coordinador de los traspasos de tareas, que los controlen.

Aún así, será inevitable encontrarse con actitudes que, si bien podrían ser humanamente entendibles, profesionalmente no lo son. Son todas aquellas personas que intenten desvincularse del día a día, y de los traspasos, amparándose en que se van a ir de la empresa, y en que no van a facilitar la tarea a aquellos que le han despedido. Tampoco será posible evitar el aumento de absentismo laboral y las “depresiones” repentinas, por ejemplo.

Intentar controlar al máximo estos comportamientos será muy importante para que se haga un buen traspaso de tareas y un buen control del riesgo operacional.

De la misma forma, se han de marcar de forma clara las atribuciones y responsabilidades de las personas que se integran, para evitar duplicidades y solapamientos en las funciones, y tratar de solventar rápidamente aspectos sociales y sindicales: la paz social es muy importante para poder llevar a cabo la integración con rapidez.

Previamente al nombramiento de los mencionados comités, la Dirección debe plantearse cómo desplegarlos en la organización y su funcionamiento: el tamaño, complejidad, cultura, estilo de gestión y otras características de la entidad absorbida afectarán al diseño de los comités para hacerlos lo más eficientes posible.

Principales aspectos a tener en cuenta:

1. Grado de preparación y cualificación de los miembros de los comités

El equipo debe tener representación de todas las unidades de negocio y de los departamentos clave. Este equipo se familiarizará a fondo con la estructura de la compañía a controlar, y diseñará los circuitos y procesos que sean necesarios para una buena integración, ateniéndose a su propia experiencia en el día a día de la empresa.

2. Apoyo de la Alta Dirección

Es positivo que el Consejo de Administración y la Alta dirección de la empresa se impliquen de manera directa y visible, y que apoyen y supervisen la labor de los comités.

3. Diagnóstico previo

Análisis de la situación de los departamentos y unidades de negocio a integrar en cuestiones de riesgo operacional, fundamental para un buen diseño del circuito.

4. Diseño del plan de integración

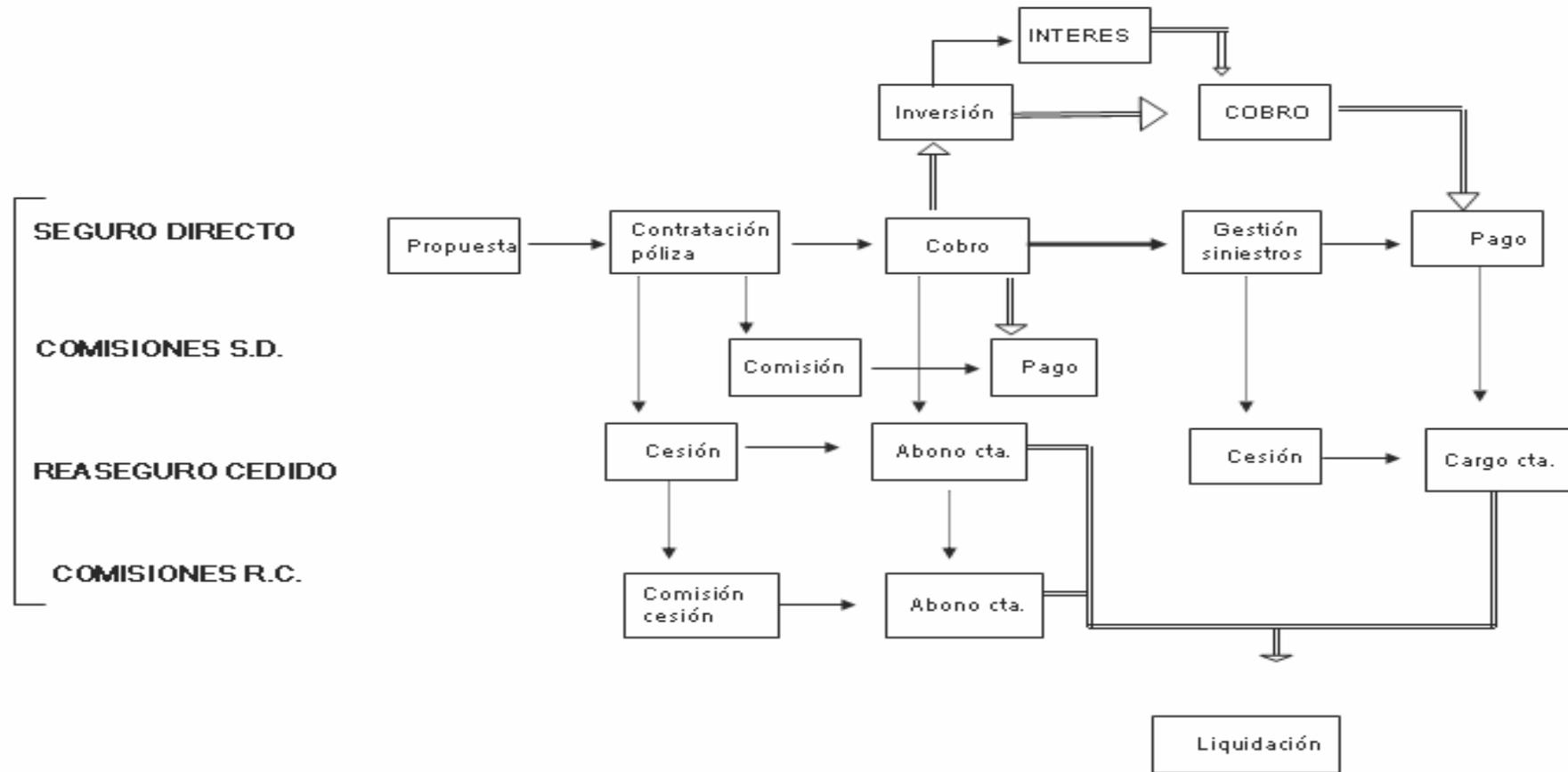
Conjuntamente, los departamentos de Recursos Humanos y de Organización deben identificar los puestos de trabajo clave, y conservarlos, con el fin de no prescindir de elementos fundamentales, y quedarse con otros prescindibles.

5. Realizar un análisis del flujo de procesos

Un posible diagrama de los procesos, aunque muy simplificado y sólo a modo de ejemplo, de una entidad aseguradora podría ser el siguiente:

Gráfico 7 : Circuito de Procesos simplificado

Circuito de procesos de una entidad aseguradora



Una vez estén nombrados los comités, clarificadas las funciones y responsabilidades de cada miembro, y teniendo el circuito, será el momento de que los comités se pongan a trabajar y a analizar el proceso de integración.

Para cada punto del circuito diseñado se han de tratar de identificar los posibles riesgos que se pueden encontrar. Se trata de realizar un mapa de riesgos lo más completo posible, con el fin de poder priorizarlos por orden de importancia.

Una vez definido el circuito de procesos, y detectados los posibles riesgos, y sobretodo los que afectarán en el proceso de integración, los comités se encargarán de gestionar los trasposos que generan **riesgos-clave** del negocio.

En las organizaciones es imprescindible que los comités de supervisión estén coordinados y liderados por un órgano creado en la empresa para este cometido, que debe estar formado por pocas personas, y que deben formar parte de la Alta Dirección, que finalmente tomarán decisiones y priorizarán, en su caso, ante varias acciones a realizar a la vez.

La compañía debe realizar periódicamente auditorías internas de procesos con personal independiente que no participe en la gestión activa del riesgo a auditar, para asegurar su control efectivo y eficiente. La dirección debe asegurar que el alcance y la frecuencia del programa de auditorías es apropiado para los riesgos en que puede verse inmersa la compañía.

10.2 Riesgos en las integraciones departamentales

10.2.1 Tecnologías de la Información y Servicios Informáticos

Los factores externos (cambios en cuestiones como sistemas políticos, necesidades sociales, regímenes fiscales y políticas legales, y, por otra parte, cualquier acontecimiento de naturaleza catastrófica como terremotos, incendios, inundaciones, etc) pueden ser causa de aumento de nuestro riesgo operacional. De la misma forma, a veces, decisiones estratégicas de la empresa, pueden llevarnos al mismo resultado.

Uno de los primeros problemas con los que se puede encontrar un departamento de Tecnologías de la Información (TI) es la diversidad de plataformas y arquitectura informática que puedan tener las empresas absorbente y absorbida.

Aún siendo ésta una decisión estratégica, que puede generar riesgos estratégicos, las consecuencias pueden convertirse en riesgos de tipo operacional.

Por ejemplo, que una empresa que tiene una arquitectura Host se fusione con una que tiene Cliente-Servidor. Y es una de las primeras decisiones que se debe tomar:

a) Mantener ambos sistemas

Esta opción tiene la ventaja de no necesitar un proceso de migración de datos de un sistema al otro, y por tanto, no hay riesgo de pérdida de información por el camino, con la importancia que tiene este factor.

Será una decisión muy cara y la menos práctica. Necesita personal especializado en ambos sistemas dedicados a los mantenimientos, implementaciones e incidencias, con el coste que ello conlleva.

Ejemplos recientes de modificaciones legislativas que han dado trabajo a los departamentos de Tecnologías de la Información han sido la modificación del recargo para el Consorcio de Compensación de Seguros, o la creación del Registro de Contratos de Seguros de cobertura de fallecimiento. Ha dado mucho trabajo en términos de horas y de pruebas que, en caso de mantener dos sistemas paralelos, tienen un coste altísimo.

Mención aparte de que el mantenimiento de los dos sistemas no permitirá nunca la integración real de negocios, ni a nivel contable, ni a nivel de gestión de siniestros, cálculo de provisiones matemáticas, etc. Siempre deberían sacarse resultados y estadísticas por separado, y unificarlas en otro entorno. Y los mediadores deberían tener también instalados ambos sistemas para poder operar con lo que ya es una única compañía.

En el caso de las campañas de marketing, que requieran un envío de información a todos los clientes, que deberá ser homogéneo hasta en el formato de la carta, y en ocasiones, no será posible debido a las diferentes configuraciones y flexibilidad de los sistemas.

b) Integrar uno en otro

Puede ser una buena solución, siempre que el sistema integrador sea completo, dinámico y flexible. Se pasa a operar con un solo sistema, lo cual es muy útil para los trabajadores, mediadores y usuarios en general.

Se requiere, una vez finalizada la integración, menos personal para su mantenimiento que con la opción anterior. El proceso de migración de datos de

un sistema a otro debería permitir la absorción de toda la información necesaria para la gestión diaria: emisión de ofertas y cotizaciones, producción, emisión de recibos, suplementos, gestión de siniestros, cálculo de provisiones matemáticas..., pero se corre el riesgo de pérdidas de información en el proceso, teniendo en cuenta, además, que el sistema receptor ha de ser capaz de almacenar toda la información que se quiera traspasar: un sistema integrador debe poder almacenar toda la información propia, más la que se migre del otro sistema, ser capaz de integrar, por ejemplo, todos los recibos de la BBDD, con todos los campos, y toda la información que éstos contengan.

Además, es necesario crear aplicativos “puente” que absorban información que llegue al aplicativo receptor y que haya sido enviada desde el aplicativo migrado, por ejemplo, recibos emitidos que se devuelven desde las entidades bancarias. Estos aplicativos “puente” tienen una vida limitada, pero su fiabilidad ha de ser máxima debido a la importancia de esta información para la gestión diaria.

Debe ser posible trasladar la programación informática de un sistema a otro, quizá en lenguajes distintos, etc

c) Crear un nuevo aplicativo que integre los de las dos compañías.

Suele ser la mejor solución, pero también la más cara de las tres, y también la más lenta ya que implica empezar desde cero. Puede integrar las mejores soluciones de cada uno de los sistemas y permite ver también las deficiencias de ambos, sirviendo esto, tras un profundo análisis, para poder hacer un diseño que, si bien puede ser costoso al principio, puede resultar una inversión muy útil en un futuro en caso de nuevas integraciones en la compañía.

Los manuales de Política de Empresa siempre apuestan por un único entorno informático, un único sistema que debe prevalecer cuanto antes. Según los teóricos, la plataforma informática sintetiza el modelo de empresa.

Otros problemas pueden ser la integración de los servicios de correo electrónico, la intranet, el soporte web para los mediadores (que los de la antigua empresa no conozcan los tarificadores de la nueva, etc)

Problemas de compatibilidad de entornos informáticos, migraciones de datos a aplicaciones comunes de gestión, compatibilidad de la programación, capacidad suficiente para albergar las nuevas BBDD, conocimiento de los productos para poder adaptarlos o traducirlos a nuevos lenguajes de programación, costes de los trasvases de información y buena medición de tiempos para hacerlo. Las migraciones, además, se han de hacer cuando se tienen todos los programas de gestión implementados: no tiene mucho sentido migrar una Base de Datos sin tener preparados entornos de producción, de

cartera, de suplementos, de siniestros y de cálculos de provisiones, por mencionar sólo algunos.

10.2.2 Departamento Comercial

La integración del departamento comercial es básica y prioritaria para no perder oportunidades de negocio.

Dar una buena formación a los empleados comerciales, para que todos conozcan todos los productos, y no haya ningún gap que impida vender o dar información y soporte a clientes. Si un cliente de la entidad absorbida es atendido por un trabajador de la absorbente, éste debe ser capaz de dar cualquier tipo de información que se le solicite, so pena de perderlo si no le responde de forma satisfactoria.

Se ha de evitar que haya personal comercial que deba dar la cara ante clientes sobre productos vendidos por otros comerciales y que desconozcan los productos que éstos vendían.

Habrá que tener mucho cuidado con las posibles ventas que pueda realizar personal que no va a continuar en la empresa, ya que pueden ser ventas ficticias cuyo único fin es el cobro de comisiones, y que será difícil su detección antes de la desvinculación contractual.

Y es importante la protección de los datos de los asegurados, ya no sólo por lo regulado vía L.O.P.D. sino por posibles apropiaciones de BBDD de la compañía. Poseer una buena BBDD de clientes en una herramienta fundamental para una compañía de seguros. Si el acceso a ella no está blindado (o al menos en parte, no a la totalidad) a personas clave de la entidad, se corre el riesgo de que los clientes vuelen junto con el personal que no continuará, causando un grave perjuicio al negocio vigente.

Se debe informar muy bien a los mediadores, para que no se vean desatendidos y que no tengan inseguridad por desconocimiento de los nuevos productos que van a vender, o de los que se tienen que hacer cargo por cese de antiguos mediadores.

A la hora de definir los objetivos al Departamento Comercial se debe ser muy cuidadoso en el sentido de dar más peso a la venta de los productos que ya conocen y que llevan tiempo vendiendo, y menos a los nuevos productos que están conociendo. La finalidad es que las ventas sean de calidad, y que no se vean forzados a vender mal algo que no conocen, o al menos no en profundidad, porque han de llegar a los objetivos marcados.

Con el tiempo, y sobretodo a través de la formación que se les dará, se irán compensando los pesos de las ventas hasta que sean totalmente polivalentes y vendan cualquiera de los productos de la empresa fruto de la integración.

10.2.3 Departamento de Atención al Cliente

La buena gestión del Departamento de Atención al Cliente es base del éxito de una compañía. Una buena atención, rápida, profesional y diligente da una buena impresión, y una sensación de seguridad a los asegurados que puede ser clave a la hora de mantener un cliente o de perderlo.

En los procesos de fusión / adquisición, éste es un factor más importante, si cabe. En cuanto la noticia se conoce, se hace pública o aparece en medios de comunicación, y a pesar de que a todos los asegurados se les remita una carta informativa del proceso, y asegurándoles que sus pólizas continúan en vigor con las mismas características, los clientes de la compañía absorbida pueden ponerse nerviosos y tener una sensación de inestabilidad y de que su dinero no está seguro en esa compañía. Y su primera reacción suele ser llamar a la compañía. Si la información que se le da es vaga, imprecisa o nota desconocimiento en las explicaciones, éste cliente tiene muchas posibilidades de marcharse de la compañía, y será un cliente no recuperable.

Por ello es muy importante mantener al equipo de atención al público el mayor tiempo posible, ya que tienen o pueden tener un profundo conocimiento de los productos, o de las personas con las que poner en contacto a los clientes para que reciban la información solicitada. Pero casi más importante es mantenerlo motivado. El cliente nota el interés que se toma en la consulta la persona que responde al teléfono. Y si además de llamar preocupados por su dinero, notan desinterés en la respuesta o en la atención que se les da, malo. Cliente perdido. Es imprescindible que las personas que contestan al teléfono puedan disponer de un argumentario confeccionado expresamente para cuestiones de clientes preocupados por la fusión.

10.2.4 Departamento de Formación

Es muy importante conservar en su totalidad, o al menos en su mayoría, el departamento de Formación. Al fusionar el de la empresa absorbente con el de la empresa absorbida, podrán formar en todos los productos a los comerciales, agentes y mediadores de una manera profunda, detallada y eficiente, ya que no se pierde conocimiento en el proceso de integración, en lo que a producto se refiere.

Han de elaborar un buen plan de formación, y que pueda impartirse de forma rápida y dinámica, ya que el tiempo es un factor importante, se mejorará la Calidad del servicio percibido por el cliente, y mejorará la confianza del equipo comercial en sí mismo, porque no tendrá dudas ni vacíos de conocimiento.

Y para ello también es necesaria una evaluación previa de los conocimientos que posee cada uno de los nuevos colaboradores. La empresa absorbente ya sabe qué tipo de formación han recibido sus trabajadores, pero no tiene por qué saber qué conocimientos tienen los que absorbe. Homogeneizar el nivel de conocimientos es muy positivo, no sólo a nivel de conocimiento de los productos, sino también a otros niveles, como puedan ser temas tan dispares como aplicaciones informáticas propias, fiscalidad, tarificadores, procedimientos internos, etc.

10.2.5 Departamentos Técnicos (Producción y Siniestros)

Aunque en un principio, las compañías tendrán criterios de suscripción diferentes, estos deberán tender a converger, para evitar que los productos a la venta de una compañía, sin son de la misma tipología que los de la otra, tengan distintas normas, que puedan dar lugar a errores a la hora de contratar, con la correspondiente posible pérdida asociada.

Se han de definir dichas normas, y verificar rigurosamente su cumplimiento durante los primeros meses desde su implantación.

Y no sólo a la hora de emitir pólizas, sino también en el momento de las emisiones de suplementos, regularizaciones de capitales y garantías. Mucha importancia, en las compañías de vida, tiene la buena gestión de recibos y pólizas en productos que garanticen capitales. Si una póliza tiene recibos devueltos sistemáticamente, se ha de proceder rápidamente a su paralización / reducción, ya que podemos estar sobredotando provisiones matemáticas cuando los recibos de los que deberían partir están devueltos.

De la misma forma, se han de definir cuidadosamente los procedimientos de tramitación, aceptación y pago de los siniestros, y controlar el posible fraude derivado de los resquicios que pueda haber entre las normas de las compañías.

Además, durante los primeros meses de integración, deberían verificarse por varios sistemas los importes de los siniestros que se vayan a abonar, tanto por si la cantidad es inferior a la que correspondería y perjudica al asegurado, como en el caso contrario. En procesos de integración nunca hay que dar un nivel de confianza total a los datos que puedan salir de aplicaciones informáticas que calculen valores de siniestro, debido a los gaps que hubieran podido generarse en ello.

10.2.6 Departamento Actuarial

En principio, durante el proceso de Due Diligence, el departamento actuarial debe haber tenido una importancia capital a la hora de tener el primer contacto con los productos de la compañía absorbida. Debe estudiar sus notas técnicas,

hacer una valoración y contraste de los cálculos de primas y provisiones matemáticas en el caso de Vida, estudiar la adecuación de las bases técnicas a la realidad siniestral de la cartera de clientes de la compañía; y provisiones de Siniestros, en el caso de No Vida, que son las que pueden obedecer a criterios menos objetivos y discutibles en principio.

Comprobar que no haya infradotaciones o sobredotaciones que puedan afectar al pasivo del balance y variar sustancialmente la valoración que se haga de la compañía.

Aunque a priori, cualquier actuario que disponga de las notas técnicas podría ser capaz de conocer el producto y su gestión técnica básica, dominar el producto y su gestión profundamente no es tan sencillo. Nunca, o casi nunca, por no ser tan rotundo y absoluto, un producto es “redondo” y no tiene casuísticas o peculiaridades que sólo quién trabaja con él día a día domina y conoce.

El desconocimiento de estas peculiaridades provoca que, tras discusiones y conversaciones acerca de los cálculos y criterios para realizarlos se recurra a ciertos márgenes de seguridad que, aunque no garantizan la exactitud en las valoraciones, dan un margen de confianza suficiente como para aceptarlas.

Cabe destacar que, habitualmente, el tiempo para realizar una due diligence no es el suficiente y necesario para bucear en las profundidades de la compañía..., y cuanto más corto es el tiempo empleado, mayor riesgo de errores, y por tanto mayor cuantía de dinero, entra en juego.

Durante la integración, la intervención de los actuarios en el proceso de migración de datos y de programas informáticos de cálculo y de gestión a la nueva plataforma informática, si es esa la decisión que se ha tomado, resultará de mucha ayuda a la hora de poder implementar, si es necesario, las posibles deficiencias que pudieran tener los mencionados programas. En la mayoría de compañías se hacen cálculos fuera de la informática por fallos o deficiencias de diseño, que no se llegan a solucionar nunca, porque la vorágine del día a día no lo permite, y son una fuente de riesgo muy importante.

10.2.7 Otros Departamentos

Inversiones, Asesoría Jurídica, Reaseguro...

En el Departamento de Inversiones deberán vigilar de una manera especial las carteras de inversiones afectas a provisiones, y, como asume nuevas carteras de la compañía absorbida, deberá estar alerta en cuanto a utilización de bienes aptos para cobertura, límites de diversificación y dispersión, valoración de las inversiones, centralizar la custodia de los títulos en un número limitado de entidades de depósito. Todo ha de estar en línea con la política de inversiones

que se adopte en cuanto a la mayor o menor aversión al riesgo, ratings de las compañías en las que se invierte, etc.

En el Departamento de Asesoría jurídica pueden existir en proceso de trámite reclamaciones de asegurados, del Defensor del Asegurado, etc., que no pueden quedar en el aire mientras se traspasa al nuevo equipo jurídico, deben vigilarse los plazos de prescripción, de reclamación, etc.

La redefinición de políticas de reaseguro también es muy importante, ya que ha de tener coherencia, a la hora de la integración, que los riesgos de cada ramo, si son homogéneos, tengan el mismo tipo de contrato.

Habrà que tener cuidado también con las fechas de cancelación o vencimiento de los contratos que ser quieran dar de baja. Y valorar en qué momento de lleva a cabo el cut-off de los contratos que se mantengan en vigor, con vistas a no tener una mayor siniestralidad de la esperada que nos afecte a la cuenta de resultados.

10.3 Finalización y Reanálisis

Una vez se dé por finalizado el proceso de integración, o, al menos, de la que se considere parte más importante, será necesario volver a hacer un análisis profundo de toda la compañía, pero en este caso, de la compañía resultante de la integración.

Se deberán verificar los circuitos y procesos resultantes, analizar y verificar la adaptación de la plantilla a sus nuevos puestos de trabajo y a sus nuevas funciones, valorar si existen redundancias en los puestos de trabajo o en las responsabilidades y competencias, y de existir, proceder a la recolocación de los redundantes, en caso de que sean lo suficientemente polivalentes como para incorporarse a otro departamento o unidad de negocio.

11. Conclusiones

El riesgo operacional, en un marco de normal funcionamiento de la empresa, es difícil de gestionar debido a la carencia de modelos normalizados. Más aún en procesos de integración de negocios debidos a fusiones y adquisiciones.

El Objeto de esta tesis no era tanto tratar los posibles modelos de cuantificación de los riesgos operacionales en estos tipos de procesos, como su identificación y pautas de control.

La implantación del sistema de gestión de este riesgo en procesos de integración debe ser resultado de un profundo y riguroso análisis de los circuitos y traspasos de tareas, detección de riesgos-clave de cada uno de ellos, y control exhaustivo vía comités o grupos de trabajo creados a tal efecto, con un grado de conocimiento de la empresa y sus procesos muy profundo, y con un nivel de implicación altísimo en el proyecto hasta su finalización.

Emplearse a fondo en la gestión de Recursos Humanos durante el proceso de integración es una de las claves, ya que la mayoría de errores o fallos en los circuitos pueden venir de la mano de la desmotivación y nerviosismo de las personas que temen por su futuro y que consciente o inconscientemente cometen errores que afectan al normal funcionamiento de la empresa y al normal desarrollo del proceso de integración.

La tarea de análisis tras la finalización del proceso de integración permitirá ver qué se ha hecho bien, pero sobretodo qué se ha hecho mal o se ha controlado poco o nada, de cara a mejorarlo en previsión de futuras fusiones y/o adquisiciones que puedan necesitar de procesos similares. Las entidades deberían anticiparse y empezar a diseñar y planificar cómo gestionar el riesgo sin esperar a encontrarse con la primera pérdida que venga por esta causa.

Para que la una entidad esté preparada para los procesos de fusión y/o adquisición, la importancia de la gestión del Riesgo Operacional debe quedar plasmada en la estructura organizativa de la compañía y en la fijación de los objetivos estratégicos.

12. Bibliografía

Committee of Sponsoring Organizations of the Treadway Comisión (COSO) (Septiembre de 2004) *Gestión de Riesgos Corporativos – Marco Integrado: TÉCNICA DE APLICACIÓN.*

Tripp, Bradley, Devitt, Orros, Overton, Pryor and Shaw; (Marzo de 2004): *Quantifying Operational Risk in General Insurance Companies.* Institute of Actuaries and Faculty of Actuaries

Cea, José Manuel (Noviembre de 2002): *Mitigación del Riesgo Operacional (2ª Jornada de Riesgos Financieros).* Bearing Point

UNESPA (2006): *La Gestión de Riesgos de la Industria Aseguradora bajo Solvencia II*

Tripp, Bradley, Devitt, Orros, Overton, Pryor and Shaw; (Marzo de 2004): *Quantifying Operational Risk in General Insurance Companies.* Watson Wyatt.

REPSOL YPF (2006): *Sistemas de Control de Riesgos*

Celma Sanz, Jordi (2003): *La Solvencia Financiera del Asegurador de Vida y su relación con el Coste de Capital.* Universitat Autònoma de Barcelona.

Comisión Europea, DG Mercado Interior, Entidades Financieras, Seguros (Marzo de 2003): *Concepción de un Futuro sistema de Control Cautelar en la UE – Recomendaciones de los Servicios de la Comisión (MARKT/2509/03)*

Comisión Europea, DG Mercado Interior, Entidades Financieras, Seguros (Marzo de 2005): *Policy issues for Solvency II – Possible amendments to the Framework for Consultation (MARKT/2505/05)*

Comisión Europea, DG Mercado Interior, Entidades Financieras, Seguros (Marzo de 2005): *Considerations concerning the Outline for a Framework Directive on Solvency-II (MARKT/2507/05)*

Cunill Salgado, Montserrat (2004): *Los Riesgos Operacionales en las Entidades Aseguradoras (Cómo Gestionarlos).* Universidad de Barcelona

UNESPA (2007): *Introducción a la Metodología propuesta en el QIS-3 para calcular el Margen de Riesgo.*

UNESPA (2007): *QIS-3 Riesgo de Mercado.*

Koch, Julio (2007): *Cumplimentación de QIS-3: Un enfoque práctico (Riesgo de Suscripción de Vida).* Watson Wyatt

Jorge Sánchez García

Master en Dirección de Entidades Aseguradoras y Financieras.

Licenciado en Ciencias Actuariales y Financieras.

Diplomado en Ciencias Empresariales (Especializado en Finanzas).

Experiencia laboral en departamentos técnicos y en el área de Consultoría de Previsión Social en empresas como Deutsche Seguros y Pensiones; Mutua de Terrassa, M.P.S.; VidaCaixa, S.A; Prosperity Vida y Pensiones, S.A.; y FIATC, Mutua de Seguros.