

177

**El impacto de Solvencia II
en el área de TI**

Estudio realizado por: Javier Portales Pau
Tutor: Montserrat Guillén Estany

**Tesis del Master en Dirección de Entidades
Aseguradoras y Financieras**

Curso 2013/2014

Esta publicación ha sido posible gracias al patrocinio de ARAG SE, Sucursal en España



Esta tesis es propiedad del autor. No está permitida la reproducción total o parcial de este documento sin mencionar su fuente. El contenido de este documento es de exclusiva responsabilidad del autor, quien declara que no ha incurrido en plagio y que la totalidad de referencias a otros autores han sido expresadas en el texto

Agradecimientos

Afortunadamente para mí, no he estado solo en la realización de este trabajo. He recibido mucha ayuda y de índole muy diversa. Mi más sincero agradecimiento a todos.

June, Max y Sandra; Elena y Pere; Helena; Elisa; Montse; Edith; Josep María, María, Gabriela, Alejandro, Raquel, Álex, Xoan, Montse, Albert, Jesús, Anna y Eva.

Con esta compañía, todo es más fácil.

Resumen

La entrada en vigor de la Directiva de Solvencia II va a tener un impacto profundo en las compañías aseguradoras en múltiples aspectos. Con una gestión ya completamente orientada al riesgo, son muchas las empresas que van a tener que, no sólo cambiar sus procesos y estructuras, sino modificar la mentalidad de la organización.

Vivimos en un mundo en que la tecnología y la información son vitales en el éxito o fracaso de la mayoría de negocios y, especialmente, en el mundo financiero. Este trabajo pretende explicar cuál va a ser el impacto que Solvencia II va a tener en las áreas de Tecnologías de la Información de las compañías aseguradoras.

Resum

L'entrada en vigor de la Directiva de Solvència II tindrà un impacte profund en les companyies asseguradores en diversos aspectes. Amb una gestió completament orientada al risc, són moltes les empreses que hauran de, no només canviar els seus processos i estructures, sinó modificar la mentalitat de l'organització.

Vivim en un món on la tecnologia i la informació són vitals per a l'èxit o el fracàs de la majoria de negocis i, especialment, al món financer. Aquest treball pretén explicar quin serà l'impacte que Solvència II tindrà a l'àrea de Tecnologies de la Informació de les companyies asseguradores.

Summary

The entry into force of the Solvency II directive will have a deep impact on insurance companies in multiple aspects. With a risk-based management approach, many companies not only will have to change processes and structures, but also modify the organization's mindset.

We live in a world in which technology and information are paramount to determine the success or failure of the majority of businesses, and that is especially true in the financial world. This work aims to explain which will be the impact of Solvency II in the IT departments of insurance companies.

Índice

1. Sobre este trabajo de investigación.....	9
1.1. Motivación	9
1.2. Intención.....	9
1.3. Limitaciones	10
1.4. Documentación base	10
1.4. Estructura del documento	10
2. La importancia de los Sistemas de Información en las organizaciones	13
2.1. Valor estratégico de las Tecnologías de la Información (TI)	13
2.2. Las TI modifican las estructuras organizativas.....	14
3. Introducción a Solvencia II.....	15
3.1. Fundamentos	15
3.2. Diferencias y similitudes con Basilea.....	16
3.3. Los tres pilares de Solvencia II	16
3.4. La entrada en vigor de la Directiva.....	18
3.5. Algunos aspectos destacables.....	18
4. Impacto en las organizaciones.....	21
4.1. Metodología.....	21
4.2. Procesos.....	22
4.3. Sistemas de Información	22
4.4. Gobierno corporativo	22
5. Solvencia II y las Tecnologías de la Información	25
5.1. Referencias en la Directiva	25
5.2. Referencias en otros documentos relevantes	26
6. La Calidad del Dato.....	29
6.1. Definición.....	29
6.2. Estándares.....	31
6.3. Otros parámetros	32
6.4. Trazabilidad.....	33
6.5. Data Quality Services.....	33
7. Una solución tecnológica para Solvencia II	35

7.1. Pregunta de examen: ¿Qué implica Solvencia II a nivel tecnológico?	35
7.2. Necesidades generales de los Sistemas de Información	35
7.3. Necesidades tecnológicas por Pilar de Solvencia.....	37
7.4. Otras implicaciones	38
7.5. Visión general de la solución	39
7.6. El rompecabezas tecnológico.....	41
7.7. La solución final.....	45
8. Marco de control de la calidad	47
8.1. Descripción de los tipos de controles.....	47
8.2. Documentación de los controles	50
8.3. Evidencias	50
8.4. Roles y responsabilidades.....	51
9. Marco de seguridad	53
9.1. Principios de seguridad.....	53
9.2. Tipos de controles de seguridad	53
9.3. Directrices de seguridad de los Sistemas de Información	55
9.4. Gestión de continuidad del negocio.....	55
9.5. Cumplimiento normativo y legal.....	55
9.6. Seguridad frente a acciones humanas.....	56
9.7. Clasificación e inventariado de activos.....	56
9.8. Adquisición, desarrollo y mantenimiento de sistemas	56
9.9. Seguridad física del entorno	57
9.10. Gestión y operación de sistemas, redes y comunicaciones.....	57
10. La gestión del proyecto	59
10.1. Fases del proyecto.....	59
10.2. Riesgos del proyecto	61
11. Conclusiones.....	63
12. Bibliografía.....	65

El impacto de Solvencia II en el área de TI

1. Sobre este trabajo de investigación

1.1. Motivación

Desde que se aprobara en 2009 la Directiva de Solvencia II, la nueva regulación ha estado envuelta de incertidumbre por muchas razones. Además de la indefinición sobre la fecha definitiva de la entrada en vigor –con la aprobación de la Omnibus II parece factible que la fecha de 1 de enero de 2016 sea definitiva–, la falta de una reglamentación y unas especificaciones técnicas definitivas ha provocado que las compañías se han visto obligadas a trabajar, en ocasiones, a tientas.

Este hecho se ha manifestado especialmente en el área de las Tecnologías de la Información. Si bien la Directiva habla de la información y los datos, no es menos cierto que lo hace de manera vaga y poco clara. Esto, que no sería un inconveniente si desde la publicación de los niveles 2 y 3 de la Directiva a la entrada en vigor hubiera de transcurrir mínimo un año, se convierte en un contratiempo importante al no darse esta circunstancia. Las unidades de tecnología de las compañías aseguradoras se han visto obligadas a interpretar la Directiva e implementar un sistema que cumpla con los requisitos regulatorios sin conocer el desarrollo final de Solvencia II.

En esta tarea, como es habitual en nuestro sector, las aseguradoras han dispuesto de la ayuda de grandes y pequeñas empresas de consultoría que, aprovechando que el texto actual de la Directiva era deliberadamente vago en todo lo que tiene que ver con el impacto tecnológico de los requerimientos que propone, han hecho propuestas de máximos, no se sabe bien si respondiendo a un interés comercial propio o a una interpretación estricta de la normativa.

Por todo ello, y dado que existe muy poca bibliografía respecto al tema, el propósito de este trabajo es hacer un estudio objetivo de la Directiva y los textos adicionales publicados hasta el momento por los reguladores, para establecer el marco de afectación en las áreas de TI de las compañías aseguradoras.

1.2. Intención

La intención de este estudio es la de exponer, de una forma clara y eminentemente práctica, cuáles son las principales consecuencias de la implantación de Solvencia II en el área de TI de las compañías aseguradoras, delimitando los riesgos de dicha implantación y proponiendo una solución tecnológica, con la esperanza de que pueda servir de ayuda a las empresas del sector asegurador, tanto en este proyecto, como en otros de similares características.

1.3. Limitaciones

Este estudio ha sido realizado entre los meses de marzo y junio de 2014. Las hipótesis, el desarrollo y las conclusiones del mismo están condicionadas por la documentación oficial publicada hasta este momento.

El autor asume que desarrollos posteriores de la Directiva puedan modificar el análisis aquí efectuado, si bien considera que los principios generales aquí expuestos seguirán vigentes dado su carácter aceptado y universal.

1.4. Documentación base

Los documentos oficiales que se han utilizado como base para realizar este estudio son los siguientes:

- Directiva de Solvencia II (DIRECTIVA 2009/138/CE)
- Propuesta de modificación (Omnibus II, 2011/0006 (COD))
- Guía para la pre-aplicación de modelos internos (antiguo Consultation Paper 80)
- Directriz para la evaluación interna de los riesgos (EIOP-CP- 13/09)
- Directriz sobre la solicitud previa de modelos internos (EIOPA-CP- 13/011)
- Directriz sobre el sistema de gobierno (EIOPA-CP- 13/08)
- Directriz sobre el suministro de información a las autoridades nacionales competentes (EIOPA-CP- 13/010)

En el resto de documentación oficial existente no se han encontrado aspectos relevantes a los Sistemas de Información.

1.4. Estructura del documento

El presente trabajo ha sido estructurado de la siguiente forma:

- Se inicia con un capítulo a modo de preámbulo sobre la importancia de los datos en las organizaciones empresariales actuales.
- En segundo lugar, sigue un bloque teórico para introducir la Directiva de Solvencia II, sus implicaciones generales en las compañías aseguradoras, así como las menciones que en la norma se hace a las TI. Este bloque termina con algunos aspectos teóricos sobre la calidad de la información.

- Seguidamente se inicia el bloque práctico, que cubre todos los aspectos del proyecto de implantación, desde los riesgos inherentes al mismo, hasta el marco de control y seguridad, pasando por las soluciones tecnológicas propuestas.
- Finalmente, el documento reserva un espacio para hacer balance de todo lo expuesto.

2. La importancia de los Sistemas de Información en las organizaciones

“Estamos ahogándonos de información, pero famélicos de conocimiento”
John Naisbitt

“Lo que hace distinta a esta sociedad no es que el conocimiento sea un recurso, sino que es el recurso”
Peter Drucker

“La verdadera era de la información no llegará a las empresas hasta que éstas no estén en disposición de conocer en tiempo real la verdadera situación de sus cuentas”
Larry Ellison

La información ha sido desde siempre un recurso vital para las organizaciones, y su correcto uso y gestión ha supuesto en muchos casos la diferencia entre el éxito y el fracaso de una compañía. Da la impresión que, entrados en el siglo XXI, hablar de la importancia de la información deba ser algo redundante y accesorio; que su importancia capital se deba dar por descontada. La realidad es que, en un periodo relativamente corto de tiempo, hemos pasado de una situación en que resultaba muy costoso a las empresas recabar y almacenar información (y ese era el reto principal al que se enfrentaban en este ámbito), a un momento en el que los costes de almacenamiento han caído en picado y generamos información a un ritmo vertiginoso. Ser capaces de gestionar la cantidad ingente de información que se genera diariamente en todos los ámbitos de actuación (económicos, financieros, control, clientes, etc.) es el reto al que se enfrentan las compañías actualmente.

Si, tal y como dice Forrester (1968), una de las principales características de gestión de una compañía cualquiera es la de convertir información en acción, es fácil ver cuán importante debe ser este hecho en las empresas que pertenecen al sector financiero. En el caso concreto del sector asegurador, una correcta evaluación de los riesgos o una adecuada caracterización del perfil de los clientes, por poner dos ejemplos muy visibles, son indispensables para poder realizar una correcta tarificación de las pólizas –y eso significa ser competitivos.

2.1. Valor estratégico de las Tecnologías de la Información (TI)

La importancia creciente de la información dentro de las organizaciones es consecuencia de la urgencia con que debe darse respuesta a los problemas que plantea la actual caracterización del entorno en que se desarrolla su actividad, pero también viene motivada por los cambios tecnológicos que se están produciendo en materia de información que son, además, económicamente aplicables en el interior de la empresa.

Los avances tecnológicos, y en concreto los relativos a las TI, así como su rápida difusión, dotan a la información de nuevas características y posibilidades de aplicación, que provocan un cambio en la forma de llevar las empresas (Porter y Millar, 1986).

En este contexto, se puede definir las Tecnologías de la Información, como el conjunto de tecnologías cuya función es la de recoger, almacenar, procesar y distribuir la información necesaria para las actividades operativas, de dirección y control de la empresa; además de emplearse como apoyo en los procesos de toma de decisiones y como soporte a la dirección estratégica.

El papel esencial que pasan a desempeñar las TI se debe básicamente a la constatación de una serie de realidades (Abril y Macau, 1989); un entorno crecientemente competitivo, una reducción de costes de las TI unida a un incremento de las prestaciones y al hecho de que toda actividad en la empresa, ya sea acción o decisión, tiene un componente de información.

2.2. Las TI modifican las estructuras organizativas

La mayoría de las empresas presentan una estructura organizativa que refleja el flujo de información que se produce dentro de ellas. Por ello, a medida que las TI crean nuevas posibilidades de ampliar y compartir el acceso a la información, permiten que surjan nuevas formas de organización.

En la medida en que las TI se hacen cargo de más tareas funcionales y rutinarias, e incluso de análisis, permitiendo a su vez la conexión de dos individuos cualesquiera de la organización, van modificando el contenido del trabajo a todos los niveles y con ello la estructura organizativa. Las nuevas tareas adquieren un carácter más creativo y autónomo, para el que se precisa de un personal más cualificado, capaz de asumir mayores exigencias que progresivamente irán encauzadas a la realización de proyectos diversos en lugar de procedimientos normalizados (OCDE, 1990).

La tecnología de la información está permitiendo obtener estructuras organizativas caracterizadas por la combinación de flexibilidad y capacidad de respuesta rápida, cuestiones típicas de las estructuras descentralizadas, con el alto grado de integración y control que poseen las estructuras centralizadas.

Esto ha llevado a algunos especialistas como Clark (1990), a afirmar que competir en esta tecnología significa competir en formas de organización, no siendo posible explotar las ventajas de las TI sin aspirar a cambios estructurales compatibles con ellos.

3. Introducción a Solvencia II

3.1. Fundamentos

El sistema vigente de solvencia de las entidades aseguradoras (Solvencia I) es un sistema sencillo que, mediante la utilización de unas pocas variables fundamentales (cifra de provisiones y capitales en riesgo para vida, y volumen de primas y siniestralidad para no vida), permite calcular la cuantía mínima del margen de solvencia de una compañía.

Este sistema, sencillo de implementar –sólo precisa de unos cálculos básicos sobre magnitudes que las entidades aseguradoras manejan habitualmente en su día a día– y de fácil supervisión, ha relacionado hasta ahora, de manera directa, el margen de solvencia con el tamaño de la entidad: a mayor volumen de negocio, mayor requisito de capital.

En los últimos tiempos el sector financiero ha empezado a dar cada vez más importancia a una gestión basada en el perfil de riesgos de las compañías. Los avances producidos en este área, sumados a la innegable influencia de la normativa bancaria (Solvencia II podría llegar a considerarse una adaptación de Basilea al sector asegurador), han provocado que la Comisión Europea decidiera iniciar en 2000 un proyecto para modificar la regulación en materia de solvencia y supervisión de las entidades aseguradoras.

El 22 de abril de 2009 el Parlamento Europeo aprobó la Directiva 2009/138/CE sobre Solvencia II. Los principales objetivos de esta Directiva son:

- Armonizar los estándares entre países comunitarios.
- Establecer un marco de solvencia que sea sensible al riesgo.
- Consolidar las principales normas de solvencia entre los grandes grupos empresariales.
- Establecer el cálculo de los requerimientos mínimos que permitan unos niveles de solvencia suficientes para el desarrollo de la actividad aseguradora.

3.2. Diferencias y similitudes con Basilea

El sistema de solvencia contempla evaluar la solvencia de los aseguradores mediante un enfoque basado en tres pilares inspirados en lo sucedido con Basilea II, aunque adaptando los riesgos operativos del sector bancario al mercado asegurador.

Tal como se ha hecho en el sistema bancario con Basilea II, Solvencia II debería incentivar a las empresas de seguros a medir y administrar sus riesgos mediante modelos que reflejen el verdadero perfil de riesgos por encima de una simple fórmula. Sin embargo, Solvencia II no es un calco de Basilea II: contienen elementos similares y otros bastante distintos.

La similitud radica en el ya clásico modelo de los tres pilares que contienen requisitos cuantitativos, cualitativos y de disciplina de mercado. Ambos proyectos también le asignan una importancia radical a la gestión sólida de los riesgos, a la transparencia y a la regulación.

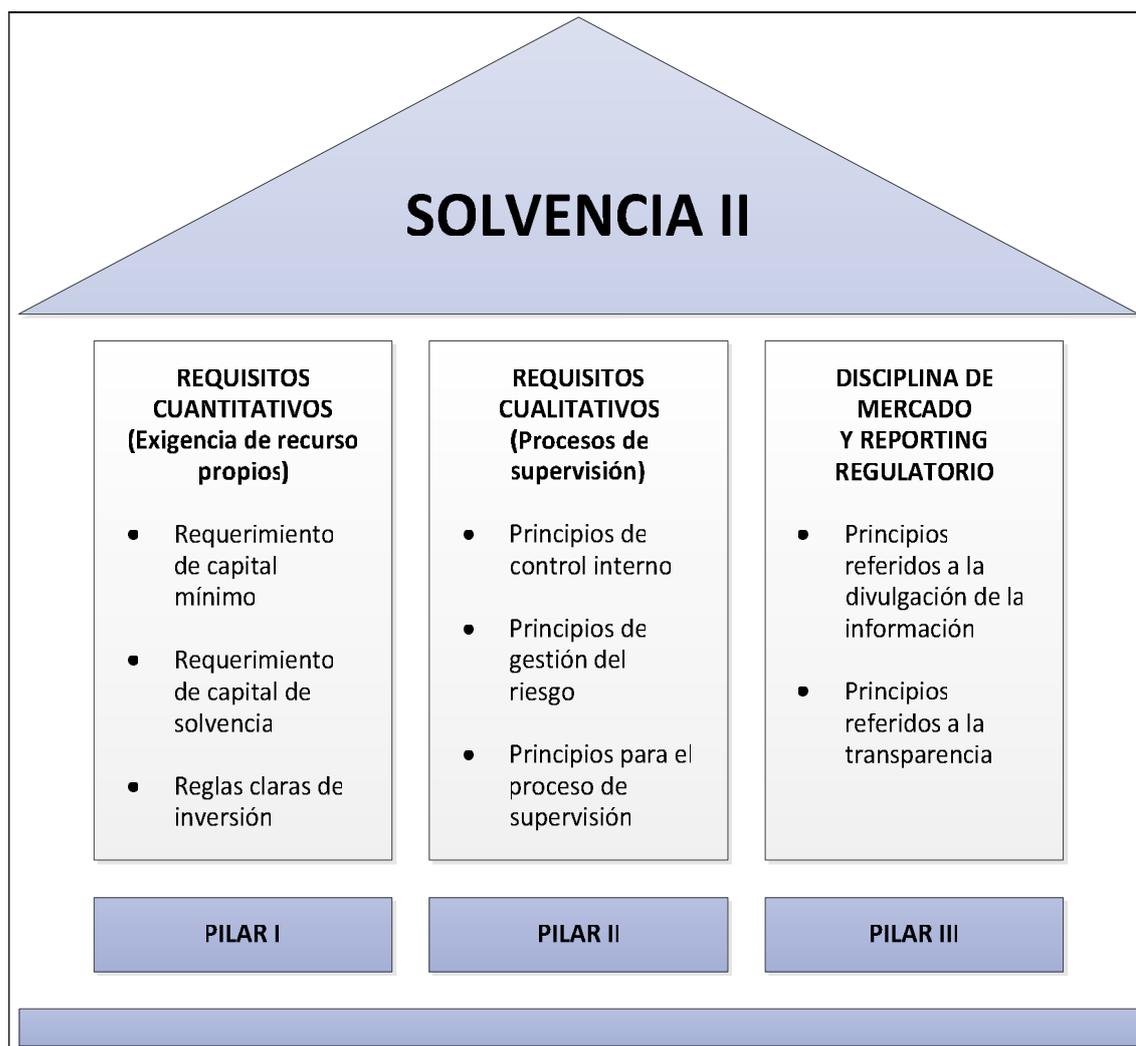
Entre sus diferencias más importantes podemos mencionar que Basilea II tiene por finalidad fortalecer la solidez e integridad del sistema bancario internacional, mientras que Solvencia II apunta a un principio que cada día cobra mayor importancia en el mundo: la defensa del consumidor. Es decir, Basilea II apunta hacia adentro y Solvencia II también lo hace hacia afuera.

Además, Basilea II, en principio, es más corporativa, pues está dirigida a las entidades bancarias con negocios internacionales, mientras que Solvencia II no efectúa tal distinción y será aplicable a la totalidad de las aseguradoras europeas.

3.3. Los tres pilares de Solvencia II

Solvencia II define los requerimientos de niveles mínimos de capital y establece los procedimientos para identificar, medir y gestionar los niveles asumidos de riesgo. Para conseguir estos objetivos, la Directiva se sustenta sobre 3 pilares fundamentales: requerimientos cuantitativos, requerimientos cualitativos y disciplina de mercado, y reporting regulatorio.

Gráfico 1. Los pilares de Solvencia II



Fuente: Elaboración propia

Pilar I: Requisitos cuantitativos

El pilar I hace referencia al cálculo de capital regulatorio y a la definición de los recursos financieros que una aseguradora debe tener para ser considerada solvente y hacer frente a los riesgos asumidos por la compañía. Es necesaria la valoración de activos y pasivos y los requisitos de capital (capital de solvencia obligatorio –SCR– y requerimiento de capital mínimo –MCR–).

Pilar II: Requisitos cualitativos

Es la parte de Solvencia II que se centra en la gestión del riesgo por parte de la aseguradora, incluyendo la correcta dirección y el cumplimiento de los niveles de gestión del riesgo. Engloba los controles internos, la gestión del riesgo y el FLAOR (Forward Looking Assessment of Own Risks –una autoevaluación de los riesgos–).

Pilar III: Disciplina de mercado y reporting regulatorio

El pilar III hace referencia a los requisitos de información que las entidades aseguradoras estarán obligadas a poner a disposición de los organismos supervisores (FCR), así como la divulgación pública de información de solvencia a inversores y analistas.

3.4. La entrada en vigor de la Directiva

El proceso de entrada en vigor de la Directiva ha estado marcado por las dificultades a la hora de establecer acuerdos entre el Parlamento, el Consejo y la Comisión Europea –referidos habitualmente como el Trío–. Este hecho ha tenido como consecuencia diversos retrasos en la fecha inicial de entrada en vigor, 1 de Noviembre de 2012, cosa que ha condicionado gravemente los desarrollos de las compañías al sembrar de incertidumbre el proyecto. En el gráfico 2, se puede ver la evolución del calendario (ver página siguiente).

3.5. Algunos aspectos destacables

Parece existir un consenso generalizado en cuanto a que bajo la nueva Directiva, las aseguradoras deberán implementar un sistema basado en el riesgo que intente alinear los requisitos de capital con los riesgos subyacentes reales de la compañía. Esta forma de control requerirá un rediseño por parte de las instituciones sobre cómo tratar el riesgo y sobre cómo se adquiere, audita y utiliza la información.

La Directiva persigue un cambio en la manera en que el sector asegurador gestiona su actividad e, idealmente, contempla un futuro en que los equipos directivos vean Solvencia II, no solo como un requisito regulatorio, sino como una nueva herramienta de gestión.

3.5.1. Fórmula Estándar vs Modelo Interno

Solvencia II ofrece a las aseguradoras la opción de utilizar una Fórmula Estándar o un Modelo Interno para calcular el Capital Requerido de Solvencia (SCR).

La Fórmula Estándar es más sencilla y posiblemente menos costosa de implementar pero puede requerir de mayores recursos financieros y podría afectar negativamente a las percepciones del mercado respecto al compromiso de la compañía en relación a la comprensión de sus propios riesgos. Los Modelos Internos son más complejos y requieren de una inversión inicial más elevada dado que deben adaptarse a las particularidades de cada entidad, pero se supone que proveerán de beneficios de capital a largo plazo (la precisa determinación de riesgos debe conducir a una reducción de las necesidades de capital), además de ayudar a implantar una conciencia de sensibilidad al riesgo en la organización.

Gráfico 2. Los retrasos en la entrada en vigor de Solvencia II

25/11/2009
2009/138/EC Solvencia II <ul style="list-style-type: none">• Fecha Aplicación: 1 de Noviembre de 2012.• Fecha Transposición: 31 de Octubre de 2012.
05/07/2011
2011/89/EU (Ficod1) <ul style="list-style-type: none">• Enmienda ciertas directivas, incluyendo Solvencia II, en relación a la supervisión suplementaria de entidades financieras en un conglomerado financiero.
19/01/2011
Propuesta COM (2011) 8 Omnibus II <ul style="list-style-type: none">• Tiene en cuenta la entrada en vigor del Tratado de Lisboa.• Otorga poder a la Comisión para adoptar los actos delegados de acuerdo con el Artículo 290 del Tratado sobre el Funcionamiento de la Unión Europea.
12/09/2012
2012/23/EU Primera "Quick Fix" <ul style="list-style-type: none">• Fecha Aplicación: 1 de Enero de 2014.• Fecha Transposición: 30 de Junio de 2013.• Pospone la revocación de Solvencia I al 1 de Enero de 2014.
02/10/2013
Propuesta COM (2013) 680 Segunda "Quick Fix" <ul style="list-style-type: none">• Fecha Aplicación: 1 de Enero de 2016.• Fecha Transposición: 31 de Enero de 2015.• Pospone la revocación de Solvencia I al 1 de Enero de 2016.
11/03/2014
IP/11/49 Omnibus II <ul style="list-style-type: none">• El Parlamento aprueba la Omnibus II.• Se confirman las fechas de entrada en vigor propuestas en la segunda Quick Fix.

Fuente: Elaboración propia

Una menor necesidad de capital de Solvencia conlleva diversos beneficios, incluyendo un menor coste para la adquisición de capital, la oportunidad de distribuir el capital de manera más efectiva a través de la organización, una ventaja competitiva a través de un establecimiento de precios más preciso y la mejora en la imagen exterior al demostrar transparencia respecto a los inversores, clientes y reguladores.

Una de las posibles barreras para que las compañías contemplen la adopción de un Modelo Interno es, justamente, la tecnológica. Un modelo interno es, esencialmente, un enorme simulador de Monte Carlo que requiere información precisa de gestión y el procesamiento de miles de escenarios. Este enfoque ha sido tradicionalmente caro tanto en recursos económicos como en tiempo de proceso de máquina, además de requerir análisis estadísticos sólidos metodológicamente, para garantizar el establecimiento de hipótesis de comportamiento estocástico que reflejen lo observado en la entidad aseguradora.

En cualquier caso, parece evidente que los reguladores persiguen que, en un futuro, todas las aseguradoras opten progresivamente por modelos internos.

3.5.2. Los test de uso

Bajo Solvencia II, las compañías deberán demostrar a los reguladores que la información que presentan ha sido utilizada y probada de un modo apropiado y consistente, y que los resultados obtenidos en los modelos internos se utilizan de manera activa para la toma de decisiones reales de negocio. Esto es, el uso del modelo interno no puede limitarse a ser un ejercicio teórico que permite reducir las necesidades de capital de la aseguradora.

Es por todo ello que existirá una demanda mayor de información histórica para dar soporte a los cálculos de SCR y las verificaciones del modelo. Mientras que las unidades actuariales tradicionalmente han buscado la información conforme la han ido necesitando, este método dejará de ser el más adecuado a partir de ahora, ya que será necesario demostrar que los datos han sido reconciliados desde las diversas fuentes en un proceso aprobado que, a nivel práctico, supone una auditoría completa de la información de un extremo a otro del proceso (end-to-end).

4. Impacto en las organizaciones

Como ya hemos mencionado anteriormente, Solvencia II es una norma que persigue que las compañías mejoren la gestión de sus riesgos, con el objetivo de proteger al asegurado.

La aplicación de dicha norma conllevará de manera directa una serie de impactos cuantitativos, tales como:

- Posibles variaciones de capital.
- Consideración y gestión de riesgos distintos a los específicamente aseguradores (no actuariales).
- Costes de implantación.
- ...

Pero, además de estos impactos cuantitativos, la implantación de Solvencia II tendrá otros efectos –suponiendo un cambio global en la gestión de la entidad–, afectando a ámbitos como:

- Metodología
- Procesos
- Sistemas de Información
- Gobierno Corporativo

4.1. Metodología

La implantación de Solvencia II supondrá la creación de nuevos sistemas de medición de riesgos, de acuerdo a los requisitos impuestos por la regulación.

Concretamente, las entidades tendrán que centrarse en:

- Creación de nuevos modelos y métodos de cálculo para
 - Riesgo de Mercado
 - Riesgo de Crédito
 - Riesgo Operacional
 - Riesgo de Suscripción (Vida, No Vida, Salud)
- Validación y seguimiento
 - Seguimiento de modelos, integración en gestión y validación
 - Desarrollo de sistemas para su seguimiento
- Cumplimiento de los requisitos regulatorios
 - Corrección metodológica
 - Asunciones prudentes
 - Representatividad de la cartera

- Trazabilidad
- Documentación exhaustiva

4.2. Procesos

Las entidades deberán adaptar sus procesos a los nuevos requisitos, así como aumentar la eficiencia de los mismos poniendo especial énfasis en la gestión del riesgo, dotándose de nuevas herramientas.

Los principales puntos a abordar serían:

- Creación de cuadros de mando ejecutivos
 - Reporting interno con indicadores
 - Reporting focalizado por área
- Herramientas de gestión de modelos y políticas de riesgo
 - Documentación exhaustiva de metodologías y procesos
 - Test de Uso y calibración
 - Test de estrés, pruebas de regresión, etc.
 - Herramientas paramétricas de administración de Modelos y Políticas
- Transformación de Procesos
 - Análisis de los procesos existentes
 - Identificación de puntos de mejora
 - Identificación de nuevas necesidades
 - Certificación de la calidad del dato
 - Trazabilidad informacional
 - Implantación nuevas herramientas

4.3. Sistemas de Información

En los capítulos siguientes veremos las implicaciones que la norma tiene en los Sistemas de Información.

4.4. Gobierno corporativo

Las entidades se verán impactadas también a nivel organizativo y de la estructura de gobierno corporativo, afectando a la toma de decisiones por parte de la Alta Dirección y de los mandos medios, ya que es necesaria la gestión de la rentabilidad y el riesgo teniendo en cuenta el impacto del capital.

En este caso, las cuestiones a tratar serían:

- Organización
 - Mayor implicación de la Alta Dirección

- Rediseño de funciones de Riesgos
 - Creación o refuerzo de: control del riesgo, áreas técnicas, auditoría de modelos
 - Separación de funciones
 - Cambio cultural: formación para Solvencia II
- Normativos
 - Nuevas exigencias de reporting regulatorio
 - Supervisión de Modelos Internos por el regulador
 - Evaluación de la suficiencia y planificación de capital
- Toma de decisiones
 - Creación de nuevos productos en base al capital que requieren
 - Gestión mediante rentabilidad ajustada al riesgo
 - Fijación progresiva de precios ajustados al riesgo

5. Solvencia II y las Tecnologías de la Información

En una primera fase del estudio, hemos revisado la documentación oficial existente para buscar todas aquellas referencias que tuvieran implicaciones en los Sistemas de Información.

A continuación se detalla lo observado.

5.1. Referencias en la Directiva

Como ya hemos comentado anteriormente, la Directiva de Solvencia II es imprecisa al respecto de las TI. En líneas generales, podemos decir que si bien no hay una mención específica a los aspectos tecnológicos, sí existen diversas referencias concernientes a las necesidades de información.

En la primera parte de la Directiva, las consideraciones previas, vemos reflejada la necesidad que van a tener las compañías de poner a disposición del público información financiera de manera periódica (DO L 335 de 17.12.2009, p. 4), ya sea en formato físico o en formato digital.

Pese a que esta primera consideración no establece obligatoriedad en cuanto al formato de la información pública, la Directiva es más precisa cuando se refiere a la información que deberá facilitarse a efectos de supervisión. En el artículo 35 (DO L 335 de 17.12.2009, p. 30), podemos encontrar lo siguiente:

- Las empresas deberán presentar a las autoridades supervisoras la información necesaria para que éstas puedan evaluar el sistema de gobernanza de la compañía y puedan tomar decisiones respecto a sus obligaciones de supervisión.
- La información comprenderá datos cualitativos y/o cuantitativos, datos históricos, actuales y/o prospectivos, y datos de fuentes internas y/o externas.

Para ello, la Directiva determina que será exigible “que dispongan de sistemas y estructuras apropiados para cumplir los requisitos establecidos” en términos de información (DO L 335 de 17.12.2009, p. 30).

Profundizando en esta idea, y al referirse a los requisitos generales de gobernanza, la Directiva vuelve a referirse a la necesidad de disponer de “un sistema eficaz para garantizar la transmisión de la información” (DO L 335 de 17.12.2009, p. 33).

La necesidad de un “sistema eficaz” vuelve a quedar de manifiesto cuando la Directiva se refiere a la gestión de los riesgos. Específicamente, se exige a las empresas que dispongan “de un sistema eficaz de gestión de riesgos, que comprenderá las estrategias, los procesos y los procedimientos de información necesarios para identificar, medir, vigilar, gestionar y notificar de forma continua

los riesgos a los que, a nivel individual y agregado, estén o puedan estar expuestas, y sus interdependencias” (DO L 335 de 17.12.2009, p. 34). Parece razonable pensar que un sistema de esas características deberá, por necesidad, estar conectado con el resto de sistemas de gestión existentes en la compañía siendo por tanto su naturaleza fundamentalmente tecnológica.

Finalmente, y expresado en relación a la información relevante para el cálculo de modelos internos, pero aceptado como de aplicación a toda la información relevante para Solvencia II, la Directiva se refiere a los datos y exige que sean “exactos, completos y adecuados” (DO L 335 de 17.12.2009, p. 58). Uno de los requisitos que serán imprescindibles para validar cualquier modelo será la existencia de un “examen de la exactitud, integridad y adecuación de los datos utilizados” (DO L 335 de 17.12.2009, p. 59).

Como podremos ver más adelante, estas características de la información no son casuales y para garantizar que sus datos las cumplen, las compañías deberán implementar sistemas de cierta complejidad.

5.2. Referencias en otros documentos relevantes

La Directiva se ha ido complementando por el momento, con una serie de documentos auxiliares (directrices y consultation papers) que deben servir de ayuda para la interpretación práctica de los artículos, hasta que se produzca la aprobación oficial de las medidas de implementación / actos delegados (nivel 2), las especificaciones técnicas (nivel 2.5) y las guías de implementación de EIOPA.

En la documentación publicada hasta ahora, se pueden encontrar algunas referencias a la información que insisten sobre aspectos ya mencionados en la Directiva y, en ocasiones, amplían un poco el alcance de las recomendaciones.

En el ámbito de la gestión del gobierno, por ejemplo, la Directriz relacionada (EIOPA-CP- 13/08) vuelve a insistir sobre la necesidad de establecer “líneas de información dentro del grupo y sistemas eficaces para garantizar que la información fluya en el grupo en sentido ascendente y descendente”. También identifica a la función actuarial como la responsable “que valore la coherencia de los datos internos y externos utilizados en el cálculo de las provisiones técnicas en relación con las normas de calidad de datos según se indica en la Directiva Solvencia II”, instándola a “proporcionar recomendaciones sobre los procedimientos internos para mejorar la calidad de los datos de modo que se garantice que la empresa esté en posición de cumplir estos requisitos cuando se aplique” la Directiva.

Una de las directrices publicadas, se refiere específicamente al suministro de información a las autoridades nacionales competentes (EIOPA-CP- 13/010). En este documento se insta a las autoridades nacionales a que velen porque las empresas:

- Creen “sistemas y estructuras para suministrar información de alta calidad con fines de supervisión”.

- Presenten “la información cualitativa y cuantitativa establecida en estas directrices que permita a dichas autoridades revisarla y evaluarla”.

Adicionalmente, se dice de manera expresa que la información cuantitativa se debe facilitar “por medios electrónicos y la información cualitativa [...] se facilite en un formato legible electrónicamente”. Parece imposible, ya, obviar el impacto tecnológico de todo lo visto hasta ahora, por mucho que no haya detalles específicos al respecto.

6. La Calidad del Dato

6.1. Definición

La calidad del dato es un proceso de evaluación de los datos pertenecientes al conjunto de información de una compañía o entidad con el objetivo de asegurar la precisión, completitud y adecuación de éstos, que son los tres estándares que la definen, y a su vez procurar el ajuste de otros parámetros relacionados cualitativos y cuantitativos como pueden ser la validez, accesibilidad y disponibilidad de los datos.

Es un elemento clave que sienta las bases para el éxito o el fracaso de cualquier proyecto de Business Intelligence, porque abarca aspectos tan importantes como la recolección automática de datos procedentes de sistemas diversos, el control de la gestión de los datos basados en reglas parametrizables, la limpieza de datos (data cleansing), detección de duplicados, enriquecimiento con datos adicionales, matching, estandarización de valores y formatos, corrección de datos, consolidación, migración de modelos y sistemas, sincronización o compliance.

Un dato incorrecto puede tener diferentes causas o motivos, por ejemplo la entrada errónea de un usuario, la corrupción de la información durante su transmisión o almacenamiento, entradas coincidentes en el diccionario de datos, etc. Además, recoger datos de diferentes fuentes de información que usan diferentes estándares o formatos puede resultar en una inconsistencia que derive en la aplicación de una regla incorrecta o en la eliminación de algún dato anterior. En consecuencia, los datos erróneos afectan la habilidad de una compañía para realizar sus funciones y le pueden producir una pérdida de credibilidad, la insatisfacción de los clientes, etc. Los datos incorrectos obstaculizan el funcionamiento tanto de los sistemas automáticos como los procesos manuales. Además, pueden causar estragos en el análisis de datos, la presentación de informes, la minería de datos y el almacenamiento.

En cambio, una correcta evaluación de la calidad de los datos es siempre importante para asegurar resultados fiables y para garantizar una óptima toma de decisiones. Además, está demostrado que un mal análisis de la calidad de los datos puede afectar de manera negativa en la eficiencia operacional de las compañías de seguros, en concreto:

- Una baja calidad del dato provoca que los procesos de negocio requieran una constante revisión y repetición del trabajo, incrementando así los costes y el volumen de trabajo del personal.
- Personal altamente cualificado se ve forzado a realizar tareas de extracción de datos a bajo nivel y la validación de éstos.
- La creación defectuosa de orígenes de datos y reglas de negocio crea una arquitectura de datos compleja que dificultan y encarecen las tareas de desarrollo, extracción de datos y reporting.

- Los datos inexactos pueden afectar a las habilidades de una empresa para reportar sus resultados financieros, provocando errores regulatorios, pérdida de reputación e incremento de auditoría y costes de reparación.

Así pues, para preservar la calidad de la información será necesaria, entre otras medidas, la corrección de datos duplicados, datos erróneos, valores nulos, así como la completitud de la información para ofrecer un modelado y tratamiento consistente de la misma.

Para asegurar la calidad del dato se requiere un programa continuo de mejoras en todos los aspectos de la empresa a nivel de información, que van desde las normas de entrada de datos y rutinas de validación de datos técnicos, a cómo se implementan las organizaciones empresariales y los cambios de estructura.

El análisis sistemático de los datos, o de su rendimiento, reúne información práctica y medible sobre su calidad. La información obtenida del análisis de los datos se usa para evaluar la salud general de éstos y determinar la orientación de las iniciativas de calidad del dato. El data cleansing, es decir, el descubrimiento, corrección o eliminación de datos erróneos de las Bases de Datos, es un proceso continuo que requiere de acciones correctivas en todo el ciclo de vida de los datos. Las actividades de data cleansing deben contar con suficientes recursos dedicados, tanto de las organizaciones de apoyo técnico como comercial, hecho fundamental para proporcionar un contexto y una visión de las anomalías potenciales de los datos.

Los procesos automatizados y/o manuales se utilizan para evaluar continuamente el estado de los datos de una empresa. La información obtenida de estas actividades de monitorización de datos sirve para orientar el plan y el enfoque de las iniciativas de mejora de datos. Es necesario, también, garantizar el cumplimiento de las normas de calidad de los datos garantizadas en las reglas de negocio de la empresa y en los requisitos legales. Hay que focalizar la atención en tres aspectos: controles de auditorías, cumplimiento normativo y cumplimiento legal.

Se debe planificar y llevar a cabo todos los procesos de administración de calidad de datos bajo condiciones controladas. Estas condiciones deben incluir las siguientes validaciones del Modelo Interno:

- La disposición de información que describe el origen de los datos.
- La disposición de instrucciones de trabajo.
- El uso del equipamiento adecuado.
- La disposición y uso de procesos y aparatos de monitorización y medición de la calidad de los datos.

- La implementación de la monitorización y la medición de la calidad de los datos.

Además, se recomienda hacer un inventario de todos los datos que serán tratados durante el proceso y que formarán parte del Modelo de Datos. En concreto, se debería especificar su fuente y su uso.

6.2. Estándares

Para los tres estándares de la calidad del dato se definen los siguientes criterios de evaluación:

6.2.1. Precisión

Que los datos sean precisos indica que no deben contener errores u omisiones. Tienen que ser guardados de manera consistente, ser temporalmente coherentes, ser vigentes y estar actualizados. La empresa necesita ser confidente en cuanto a éstos, es decir, tiene que revisarse a menudo la robustez del sistema de almacenamiento y la calidad de los datos.

El término precisión se puede dividir en dos tipos principales. La precisión estadística es la cercanía con la que las observaciones repetidas se ajustan a la media. Esto no tiene por qué tener una relación directa con el valor real, y aunque suele tener una precisión muy alta, la desviación de algunos valores puede ser elevada. La precisión numérica es el número de dígitos significativos que se registra de una observación. Es importante que coincida con los requeridos por los datos que se almacenan y no perder información.

6.2.2. Adecuación

Los datos tienen que ser adecuados para cumplir sus propósitos concretos y adaptarse a su riesgo asociado. Tienen que estar presentados de manera clara y con el nivel de detalle apropiado para poder cumplir con dicho riesgo. Por ejemplo, los datos para el cálculo del riesgo de Vida seguramente no serán los mismos que para el de No Vida, y hay que procurar que sean diferenciados correctamente. También deben tener el formato adecuado para ser tratados, y probablemente existir un formato común para todos los ficheros que se tengan que analizar conjuntamente.

6.2.3. Completitud / Integridad

Los datos tienen que estar disponibles al completo, es decir, debe mostrarse toda la información disponible. Además, tiene que estar suficientemente detallada y debe incluir tanto información actual como los históricos necesarios para permitir el correcto análisis de ésta. Los procedimientos deben estar correctamente implementados con tal de asegurar la captura de datos completa. Una medida de la incompletitud de conocimiento o información puede ser pensada como incertidumbre. Siempre hay incertidumbre en los datos, la dificultad está en la grabación, la comprensión y la visualización de la incertidumbre, para que

otros también puedan entenderlo. La incertidumbre es un término clave en la comprensión y evaluación de riesgos.

Se debe procurar que los datos sean íntegros y que todos los registros elegibles puedan ser usados como fuente de generación de datos. Es mejor tener datos completos para una unidad discreta y que, así, estén disponibles que no tener un gran volumen de datos incompletos que no serán comprendidos por el sistema.

6.3. Otros parámetros

6.3.1. Disponibilidad

Los datos deben estar disponibles cuando sea necesario consultarlos, es decir, es preciso asegurar que los sistemas de almacenamiento están habilitados para la consulta en los intervalos de tiempo definidos. También deben poder capturarse y almacenarse de manera rápida y eficiente, para no provocar retrasos ni desfases temporales que podrían provocar ciertos errores de precisión o de cálculo.

6.3.2. Accesibilidad

Los datos deben ser accesibles a todos los colectivos que tienen permiso para tratarlos en cuanto estén disponibles. Eso significa que la información permanece intacta y apta para ser consultada y/o modificada a pesar de las adversidades que puedan surgir (físicas, naturales, producto de errores humanos, etc.). Además, tienen que ser fácilmente entendibles.

Las copias de seguridad prevén una falta de accesibilidad y permiten recuperar los datos en caso de cualquier error, por tanto ayudan a aumentar la accesibilidad de la información.

6.3.3. Validez

Los datos tienen que ser válidos, es decir, tienen que cumplir con los estándares correspondientes. Algunos datos pueden necesitar ser registrados mediante un conjunto de requisitos (como reglas de cálculo) para asegurar su coherencia en el momento de ser comparados con otros datos. También es importante que se pueda recuperar el origen de la información para demostrar, si es necesario, que proviene de una fuente fiable. Los Sistemas de Información tendrán que tener filtros para aceptar sólo aquellos datos que cumplan con el grado de aceptación correspondiente.

Por tanto, la validación es un proceso utilizado para determinar si los datos son inexactos, incompletos o no razonables. El proceso puede incluir el control de formato, chequeo de la integridad, verificaciones de razonabilidad, la revisión de los datos para identificar valores atípicos u otros errores. Estos procesos suelen dar lugar a documentación y a la posterior comprobación de los registros sospechosos y al cumplimiento de las normas, reglas y convenciones. Una etapa clave en la validación de datos y en el data cleansing es identificar las

causas de los errores detectados y centrarse en la prevención de los errores se vuelvan a presentar.

6.4. Trazabilidad

El término trazabilidad es definido por la ISO en su International Vocabulary of Basic and General Terms in Metrology como: “La propiedad del resultado de una medida o del valor de un estándar donde éste pueda estar relacionado con referencias especificadas, usualmente estándares nacionales o internacionales, a través de una cadena continua de comparaciones todas con incertidumbres especificadas.”

En el contexto de la calidad del Modelo de Datos, la trazabilidad se define como la posibilidad de recuperar el camino que ha seguido la información desde su origen hasta el punto actual y así asegurar su completa corrección y validez. Esto permite conocer los orígenes de ciertos datos, que pueden haberse descontextualizado durante el proceso de translación, y también tomar muestras en diferentes puntos de la cadena para poder verificar su valor o estado en dicho punto o para conocer la información acumulada por el proceso. El concepto de trazabilidad está asociado, sin duda, a procesos productivos modernos y productos de mayor calidad y valor para el cliente final.

La trazabilidad del Modelo de Datos sigue el ciclo de vida de los datos para hacer un seguimiento de todos los accesos y cambios en los datos. Ayuda a una empresa demostrar la transparencia y el cumplimiento del reglamento. El propio concepto de trazabilidad puede considerarse como parte de un proceso de auditoría de datos.

Para evaluar la capacidad para reconstruir la historia, recorrido o aplicación de un determinado producto, se deben identificar:

- Origen de sus componentes.
- Historia de los procesos aplicados al producto.
- Distribución y localización después de su entrega.

En análisis de la trazabilidad del Modelo de Datos por parte de TI es importante para auditar las mediciones de riesgos. Por eso la gestión de riesgos incluye gran parte de análisis de la calidad del dato, y en concreto, de su trazabilidad. Cierta información que contenga carencias cualitativas puede resultar en errores o incoherencias que deben ser previstas como posibles riesgos y ser tratados en consecuencia.

6.5. Data Quality Services

La información es un aspecto crítico para la eficiencia de las empresas y las instituciones. Por lo tanto habrá que procurar que el modelo de información sea suficientemente completo como para cumplir todas las propiedades de la Cali-

dad del Dato y que existan sistemas que permitan la ejecución de operaciones que aseguren esta calidad, también llamados Data Quality Services (DQS).

Una compañía puede usar un DQS para mejorar el valor del contenido de sus datos, haciéndolos más apropiados para su propósito. Estos sistemas permiten a los usuarios, trabajadores o profesiones de las IT que no son expertos en Bases de Datos ni en programación, poder crear, mantener y ejecutar operaciones de la Calidad del Dato con el mínimo tiempo de preparación. Los DQS permiten construir una base de conocimiento y ejecutar tareas de calidad de los datos como corrección, enriquecimiento, estandarización y eliminación de datos duplicados. Además deberían poder reconocer y marcar anomalías como números fuera de rango y similitudes entre diferentes entradas de datos, similar al reconocimiento de patrones que podría tener un cerebro humano. Una vez introducidas las reglas de reconocimiento que debe seguir el sistema, éstas no sólo deberían procurar solventar los errores futuros sino que, además, tendrían que fijar los datos ya existentes con tal de no repetir el mismo proceso más veces. Finalmente debería permitir la entrada de información de varias fuentes y aplicar las reglas una vez combinada y uniformizada la información, de modo que no se tengan que aplicar métodos diferentes para cada fuente de datos.

Un DQS tiene dos partes diferenciadas, la de almacenamiento y la de tratamiento de los datos. La primera, que acostumbra a ser un servidor, se ejecuta en el background, mientras que la segunda es la interfaz con la que los usuarios pueden interactuar ya sea gestionando los datos o fijando las reglas de reconocimiento. Hay tres aspectos básicos en una interfaz DQS: la gestión de la base de conocimiento, que permite introducir reglas y asegurar que el sistema es consistente, la gestión de los proyectos de calidad del dato y la administración.

7. Una solución tecnológica para Solvencia II

Como ha quedado dicho, la adopción de la Directiva de Solvencia II por parte de las compañías lleva acompañada la necesidad de cambiar metodologías, procesos, estructuras y demás. En un mundo empresarial que se sustenta fundamentalmente en los sistemas tecnológicos de información, estos cambios deben traducirse necesariamente en la adaptación de las tecnologías existentes o bien en la adquisición de nuevas.

Es necesario destacar, aunque pueda parecer una obviedad, que el impacto que la transformación que exige Solvencia II tendrá, tecnológicamente hablando, en cada compañía dependerá de su situación concreta de partida: aquellas empresas que tienen un alto nivel de desarrollo tecnológico; que ya están gestionando sus riesgos y midiéndolos mediante una aplicación; o que ya disponen de un repositorio unificado de información, no precisarán un esfuerzo tan grande en recursos invertidos, como aquellas que ya hubieran hecho avances en esos aspectos.

El objetivo de este capítulo es, pues, entrar en detalle de dichos cambios, intentando cubrir aquellos aspectos comunes a cualquier entidad.

7.1. Pregunta de examen: ¿Qué implica Solvencia II a nivel tecnológico?

Si en un examen nos preguntaran sobre las implicaciones de Solvencia II en los Sistemas de Información, y nos pidieran una respuesta breve, deberíamos decir algo parecido a lo siguiente.

Fundamentalmente, la Directiva requiere dos cosas:

1. Una gestión adecuada de la información relativa a Solvencia (y por gestión, entendemos tanto la localización, normalización, almacenamiento y reporting tanto interno como regulatorio), y
2. La creación de unos motores de cálculo que permitan ejecutar los modelos de capital, ya sea para la fórmula estándar, ya para los Modelos Internos.

7.2. Necesidades generales de los Sistemas de Información

Para implantar con éxito la Directiva en los Sistemas de Información de la compañía, el área de TI va a tener que enfrentarse a algunos retos al respecto de la información relativa a Solvencia II. Entre ellos, podríamos destacar los siguientes:

- Unificación de fuentes de información. Será necesario unificar la información financiera y de negocio, distribuida actualmente en los diferentes sistemas de la compañía (no siempre estructurada) y necesaria para el

reporting regulatorio, minimizando los riesgos de dependencias en sistemas heredados o las diferencias en formatos de datos.

- Integridad y trazabilidad del dato. Se debe asegurar la integridad, coherencia y consistencia del dato, a través de validaciones técnicas y funcionales, como punto crítico para permitir la aprobación de las auditorías ejecutadas sobre las bases de datos. Del mismo modo, se debe implementar la trazabilidad de la información desde su origen hasta el dato mostrado, con el objetivo de poder identificar todo el flujo de información hasta el reporting. Esta traza deberá estar adecuadamente estructurada y documentada para poder facilitar cualquier tipo de análisis de impacto (e.g. identificar todos los datos necesarios para realizar un cálculo determinado o realizar un report concreto).
- Reconstrucción del histórico. Se debe asegurar que todos los datos generados para el reporting regulatorio sean replicables. En este sentido, el sistema informacional desde el que se ha de generar el reporting regulatorio ha de mantener las series históricas de datos empleadas para justificar las cifras de cálculo facilitadas al regulador. Una modelización adecuada y el uso de tablas de control de cambios se hacen necesarios para equilibrar adecuadamente este requerimiento con la optimización del espacio. Todo esto cobra especial importancia en caso de optar por Modelos Internos, ya que entonces se plantean escenarios de diez años de histórico y calidad de la información.
- Documentación de los procesos. Se deben respaldar con documentación todos los elementos intervinientes en el proceso de cálculo de capitales de Solvencia II (SCR), de un modo que permita su comprensión total y con absoluta transparencia para el auditor (sea éste el propio regulador directamente o un tercero). La documentación del proyecto de Solvencia deberá ser integrada dentro del sistema de documentación de la entidad, constituyendo un área documental propia.
- Automatización de procesos. Se debe asegurar la consistencia de la información contable y de gestión como requisito básico para utilizarla dentro del ámbito de Solvencia II. Asimismo, será necesaria la identificación de todas las fuentes de información y procesos asociados a la generación de esa información, con el objeto de sistematizar todo en la medida de lo posible. La implantación de la normativa de Solvencia requiere, por lo tanto, eliminar todos aquellos procesos y tratamientos de información manuales o no automatizados y sistematizarlos, con el fin de mejorar la calidad de la información.
- Gestión de metadatos. Será preciso disponer y documentar toda la información vinculada al dato (metadato técnico y funcional) que permite el uso óptimo y la interpretación adecuada de la información disponible en los Sistemas de Información. La integración de este metadato en el propio sistema permite su inclusión en el reporting.
- Infraestructuras robustas. La infraestructura de hardware debe ser capaz de soportar toda la información adicional que se va a generar a raíz de la

entrada en vigor de la Directiva, manteniendo la fiabilidad, estabilidad, flexibilidad y rapidez de respuesta que tenía anteriormente.

7.3. Necesidades tecnológicas por Pilar de Solvencia

Cada uno de los pilares de Solvencia tiene implicaciones directas sobre los Sistemas de Información. A continuación pasamos a detallarlas.

7.3.1. Pilar I

Desde el punto de vista del área de sistemas de la información, la implicación principal del pilar I tiene que ver con la necesidad de registrar la información financiera y de riesgos en un repositorio central de datos, para ser aprovechado por las herramientas de modelización y reporting. Dicho repositorio debe cumplir con las exigencias de todo sistema informacional de Inteligencia de Negocio (Business Intelligence): agrupación, consistencia, uniformidad, historicidad, replicabilidad, trazabilidad y accesibilidad. Paralelamente, se deberán utilizar herramientas y metodologías para la medición de riesgos y la certificación de resultados.

Dentro del pilar I intervienen, asimismo, los motores de cálculo de Provisiones Técnicas, Requerimientos de Capital Mínimo (MCR), Requerimientos de Capital de Solvencia (SCR), cálculos para la mejor estimación del pasivo (BEL) y balance económico ajustado a Solvencia (EBS), todo ello bajo dos posibles modelos de integración: modelo Estándar (utilizando la fórmula común propuesta por la Directiva) o modelo Interno (personalizado para cada entidad y aprobado previamente por el Supervisor). Existe la posibilidad de realizar un enfoque mixto, por el que algunos riesgos se acogen al modelo estándar y otros al modelo interno. En cualquier caso, es necesario que las áreas de sistemas dispongan de la información de entrada para esos motores de cálculo y que registren la información de salida de los mismos.

Otro requisito inherente a la normativa es la replicabilidad de los cálculos realizados en el ámbito de Solvencia II, es decir, cualquier cálculo de requisitos de capital y ajustes de Solvencia ha de ser replicable con posterioridad. Esto conlleva que el modelo de datos almacene las distintas versiones de cálculo de BEL, SCR, MCR, EBS, etc. tanto la información que se utilizó como entrada para realizar dichos cálculos, como la información de salida de los mismos, esto se soluciona con el versionado del modelo de input y output de los motores de cálculo.

Resaltar que es imprescindible atender en el Pilar I, de manera especial, la principal problemática detectada para el cumplimiento de la normativa: la relacionada con la calidad de la información y el perfilado de datos. Es necesario, por tanto, la corrección de datos duplicados, erróneos y valores nulos así como la completitud de la información para ofrecer un modelado y tratamiento consistente de la misma. En términos generales, por lo tanto, habrá que mejorar y completar o implantar si no existiese, el modelo de información de la entidad aseguradora, para poder trabajar de manera más eficiente con los datos.

7.3.2. Pilar II

Para el cumplimiento de este pilar, podría ser necesaria la adopción de herramientas específicas para el control interno y administración de los riesgos y pruebas de estrés de los mismos.

Además de disponer de las herramientas necesarias para el cumplimiento de los requisitos cualitativos de este pilar, se debe ser consciente de la necesidad de respaldar con documentación suficiente todos los elementos intervinientes en los procesos de Solvencia II, de modo que permita su comprensión total y transparencia para los auditores (sea éste el regulador directamente u otro). Toma especial relevancia dentro de este ámbito, la definición del diccionario de conceptos de la compañía, de cara a facilitar el entendimiento de la gestión de riesgos de manera unificada.

7.3.3. Pilar III

Una problemática común que deberán resolver las áreas de sistemas es la ausencia de procesos de seguimiento y monitorización en la calidad de datos de negocio de las organizaciones. Es necesario, por lo tanto, garantizar la integridad lógica, calidad y completitud de la información aprovisionada a través de procesos de validación técnica y asegurar la conciliación de la operativa de negocio y finanzas, mediante validaciones funcionales.

Para el cumplimiento de la disciplina del mercado que exige la normativa, las empresas aseguradoras deberán disponer de las herramientas de reporting adecuadas, que garanticen la divulgación segura de la información (tanto al supervisor como a otras empresas), así como la trazabilidad de la información, desde el dato mostrado en el informe hasta el proceso de cálculo y obtención del mismo, llegando incluso al origen de la información (aplicativo fuente) que proporciona dicho dato.

7.4. Otras implicaciones

Todos estos requisitos influirán directamente en los Sistemas de Información de la siguiente forma:

- **Aplicativos:** Se deberán mejorar, transformar o crear aplicativos específicos para la medición y la gestión del riesgo.
- **Modelos de Información:** Se deberán organizar de forma coherente, estructurada y explotable. Además, deberán dar soporte a Modelos estándar y/o internos, capital regulatorio y económico y a la gestión mediante rentabilidad ajustada al riesgo (RAROC).
- **Sistemas de almacenamiento de datos:** Deberán soportar un mayor volumen de información, permitir mayor profundidad histórica, garantizar la calidad del dato y asegurar la trazabilidad y replicabilidad de la información.

Las grandes diferencias que introduce Solvencia II en los Sistemas de Información y en el tratamiento de los datos recaen en requisitos no funcionales – y no

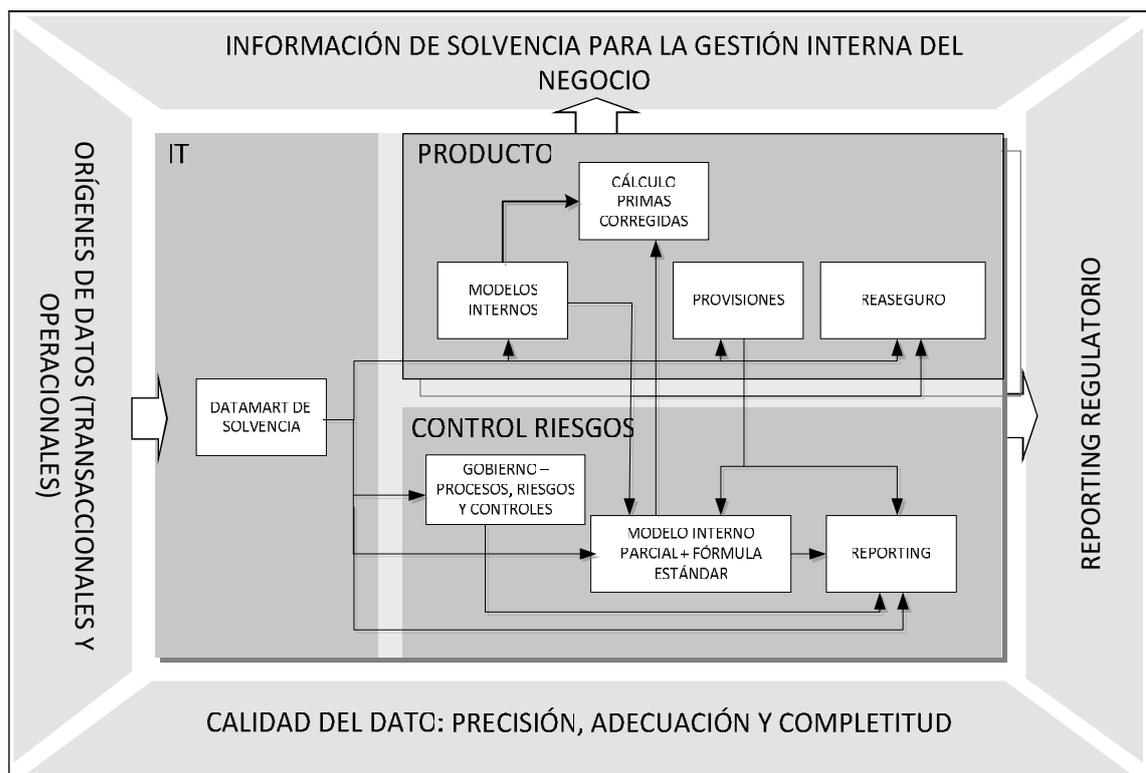
en los funcionales, como suele ser el caso – como pueden ser controles cualitativos y gestión del riesgo. Entre ellos, y marcando uno de los retos más difíciles, se encuentra el control de la calidad de los datos, puesto que nunca antes había estado sujeto a una auditoría tan rigurosa. Ahora será necesario asegurar que los datos son exactos, completos y apropiados, especialmente dentro del nuevo IMAP (Internal Model Application Process).

Por eso es importante definir una política de calidad del dato que englobe todos los procesos y decisiones necesarios para cumplir con las medidas descritas en Solvencia II y también, en general, para asegurar la buena salud de los datos y una óptima explotación de éstos.

7.5. Visión general de la solución

Más allá del hecho de que cada problema puede tener múltiples soluciones, y que los criterios de reparto de las responsabilidades pueden variar de una compañía a otra, podríamos decir que la solución tecnológica para Solvencia II tendría una estructura similar a esta:

Gráfico 3. Visión general de la solución para Solvencia II

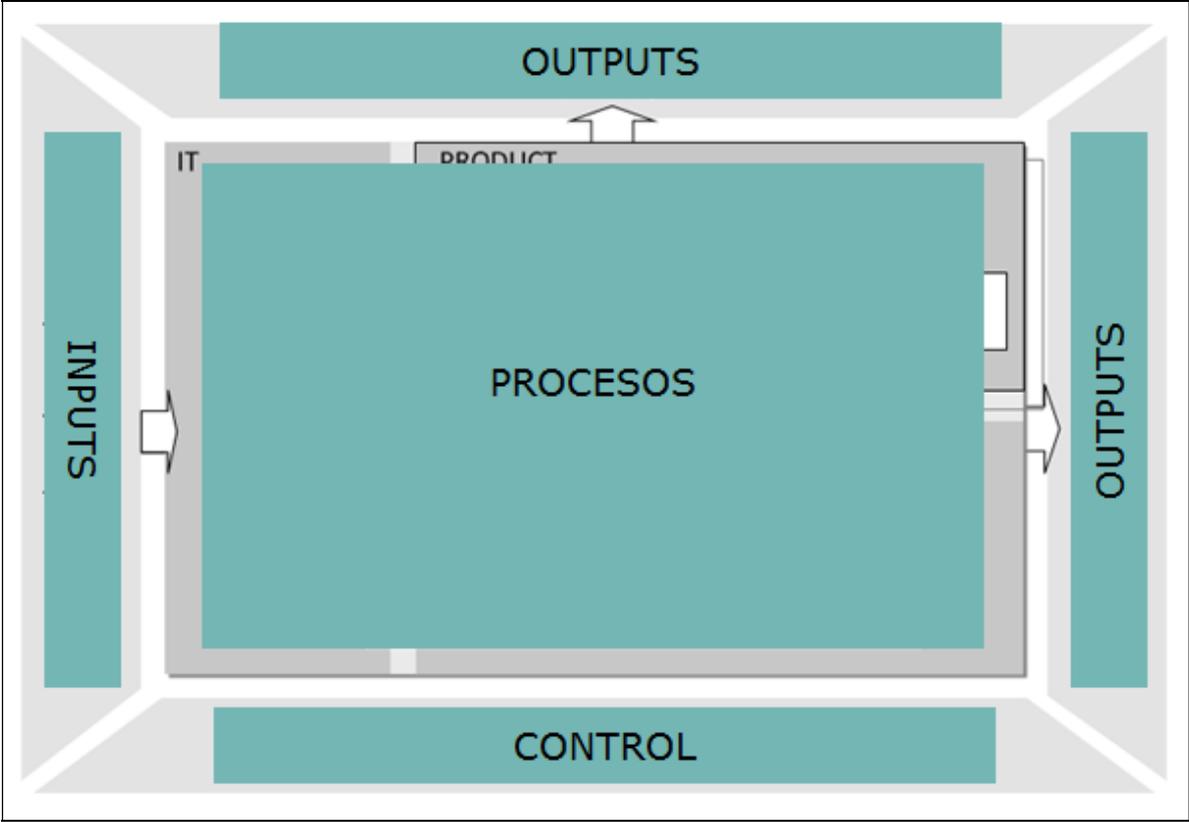


Fuente: Elaboración propia

Fundamentalmente, la solución comprende una entrada de información que, después de ser procesada, debe generar unos informes tanto internos como externos, y todo el proceso se debe realizar bajo un marco de control que garantice en todo momento la precisión, adecuación y completitud de los datos involucrados, es decir, la calidad de la información del proceso.

De manera casi anecdótica, parece interesante destacar que un esquema como este, responde perfectamente a la idea de sistema abierto expuesto en la teoría general de sistemas, no en vano, disponemos de una serie de entradas (inputs) que, tras la aplicación de una serie de procesos, se convierten en salidas (outputs), todo ello bajo la supervisión de un marco de control.

Gráfico 4. La solución de Solvencia como sistema



Fuente: Elaboración propia

7.6. El rompecabezas tecnológico

La Directiva de Solvencia II abarca un abanico tan amplio de aspectos del negocio de una compañía aseguradora, que es imposible poder cubrirlo con una única aplicación de software. La plataforma tecnológica que dé solución al sistema necesario será un rompecabezas formado por diferentes “piezas” de software que tendrán que intercambiar información de manera eficiente, para poder cumplir con todos los objetivos propuestos.

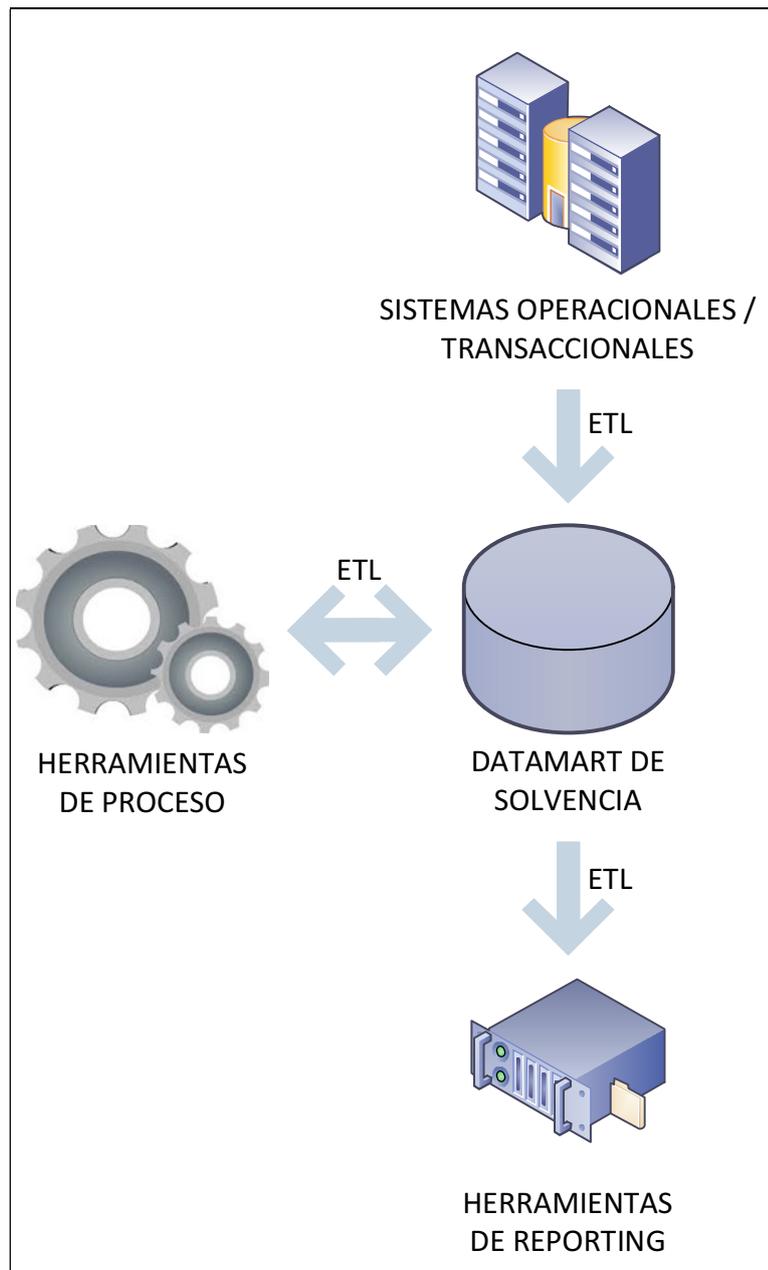
En esencia, Solvencia II nos obligará a disponer de cuatro grupos principales de aplicaciones:

- Sistemas operacionales y/o transaccionales. Son los sistemas donde residen los datos principales de la compañía, origen de la gran mayoría de la información que aprovisionará el repositorio de información de Solvencia. Ejemplos de estos sistemas son: la aplicación de suscripción de pólizas, la de gestión de clientes, la de emisión de recibos, etc.
- Repositorio de información (Datamart de Solvencia). Sistema informacional que almacenará toda la información relativa a Solvencia, tanto la información de entrada (inputs) como la que se genera a partir de ella (outputs).
- Herramientas y motores de proceso. Este bloque de aplicaciones incluye tanto las aplicaciones actuariales para el cálculo de provisiones, etc., como las específicas para el cálculo de los capitales de Solvencia (SCR) y la gestión de los riesgos (GRC).
- Herramientas de reporting. Sistema encargado de generar tanto los informes internos (cuyo objetivo es dar soporte a la gestión del día a día de la compañía) como externos (informes destinados a los reguladores).

A los aplicativos mencionados, y en función de la arquitectura tecnológica de cada compañía, podría ser necesario añadir un quinto grupo de aplicaciones:

- Herramientas de extracción, transformación y carga de la información (ETL). Estas herramientas serán las encargadas de mover la información entre los diferentes grupos de aplicaciones, garantizando tanto su calidad como la trazabilidad de todo el proceso.

Gráfico 5. El rompecabezas tecnológico



Fuente: Elaboración propia

Como se ha mencionado anteriormente, la situación de partida de cada compañía en cada uno de estos grupos de aplicaciones condicionará el esfuerzo que habrá que hacer para cumplir con Solvencia. Pese a estas posibles diferencias, vale la pena dibujar un escenario general que puede ser común a un buen número de compañías.

- Sistemas operacionales y/o transaccionales. Parece lógico suponer que la mayoría de las compañías disponen ya de sistemas operacionales para la gestión de su negocio. Las diferencias aquí pueden residir en el nivel de detalle de la información con la que trabajan (Solvencia exige datos que podría ser que hubiera aseguradoras que hasta ahora no utiliza-

ban) o en la automatización de algunos procesos. Esto implica que, a priori, no parece necesaria la adquisición de nuevo software, pero es posible que sea necesario invertir horas en la adecuación de los aplicativos.

- Repositorio de información (Datamart de Solvencia). Al igual que en el caso anterior, es muy probable que las compañías dispongan ya de un sistema informacional. Las tareas a realizar aquí se ciñen a la creación de un repositorio (y, por tanto, de un modelo de datos) que esté preparado para albergar toda la información relevante para Solvencia. Hay que prever que la cantidad de información a almacenar puede ser muy grande (sobre todo teniendo en cuenta los requerimientos a nivel de conservación de históricos).
- Herramientas y motores de proceso. Aquí la situación puede ser muy diversa y es uno de las áreas donde es más probable la necesidad de adquirir nuevo software (bien sea mediante la compra de productos de terceros, bien con desarrollos a medida). Esto será necesariamente así en lo referente a los motores de cálculo de capital regulatorio (fórmula estándar y/o Modelos Internos), ya que es una novedad de la Directiva. Aquellas compañías que todavía no habían avanzado en la gestión de los riesgos, podrían necesitar algún software de gestión de riesgos y gobierno (GRC –Governance, Risk, Compliance–).
- Herramientas de reporting. De modo similar a los repositorios de información, es previsible que las compañías dispongan de herramientas de reporting. Aquí la decisión a tomar tiene que ver más con la posibilidad de adquirir paquetes que automaticen la generación del reporting regulatorio, como alternativa a tener que desarrollar esos informes internamente.
- Herramientas de extracción, transformación y carga de la información (ETL). Existen diversas maneras de transportar información entre sistemas y garantizar la trazabilidad de las operaciones. El mercado dispone de multitud de herramientas comerciales específicas para ese cometido, pero no es infrecuente encontrar compañías que consiguen los mismos objetivos mediante desarrollos propios y almacenamiento de información en sus bases de datos.

7.6.1. Una reflexión necesaria: desarrollos a medida vs soluciones comerciales

Comprar o construir es una decisión crítica que las compañías deben afrontar actualmente, en un mundo en que la tecnología forma parte del corazón del negocio. Tanto los desarrollos a medida, como las soluciones comerciales tienen ventajas e inconvenientes que se deben evaluar antes de escoger el enfoque adecuado para una compañía. Mientras que las soluciones comerciales pueden ofrecer ventajas en términos de ahorro de costes inicial y disponibilidad inmediata, el enfoque genérico que necesariamente deben tener, puede no ser el más adecuado para una organización concreta.

A continuación mostramos una tabla que compara ambas opciones.

Tabla 1. Solución Comercial vs Desarrollo a Medida

Categoría	Solución Comercial	Desarrollo a Medida
Riesgo	Ha sido comprobado y testeado	Cada nuevo desarrollo conlleva un incremento del riesgo
Cualificación del Equipo	El nivel de conocimiento experto en tareas de análisis, diseño y desarrollo es bajo.	Requiere un nivel de conocimiento experto elevado.
Tiempo	Requiere un menor tiempo de implementación	El tiempo necesario para realizar las tareas de análisis, diseño y desarrollo es considerablemente superior
Coste	El coste inicial es más bajo	El coste inicial es más alto
Coste operativo	Puede ser innecesariamente alto si no se utilizan todas las funcionalidades de la solución	Corresponde a la naturaleza del sistema
Requerimientos	No cumplirá exactamente con todos los requerimientos	Diseñado para cumplir todos los requerimientos
Soporte	Depende del soporte de la empresa comercializadora y de la formación disponible.	El soporte y la formación dependen del equipo de desarrollo
Documentación	Se espera un nivel elevado de documentación	La calidad de la documentación dependerá de la habilidad del equipo de desarrollo
Flexibilidad	Generalmente, se pueden obtener otras aplicaciones comerciales complementarias	Cualquier otra aplicación complementaria debe ser desarrollada a medida.
Obsolescencia	Las mejoras/cambios en la aplicación son realizados por el proveedor	Las mejoras/cambios en la aplicación deben ser desarrolladas a medida

Fuente: Elaboración propia

Actualmente, el Mercado no ofrece soluciones comerciales para Solvencia que cubran los tres Pilares de la Directiva (una solución end-to-end), si bien es cierto que existen algunos proveedores (SAS es uno de los principales) que han apostado por intentar cubrir el mayor espectro posible en plataformas que incluyen la parte cuantitativa de la norma (Pilares I y III). Existen, por otro lado, soluciones GRC para la parte de Pilar II, que es un mercado bastante más maduro, ya que la gestión de riesgos y la gobernanza son aspectos en los que las empresas llevan más tiempo trabajando.

La realidad de las compañías es que, para cada uno de los aspectos tecnológicos del proyecto de Solvencia, tienen que hacer un análisis particular sobre la conveniencia de optar por una solución comercial o un desarrollo a medida, con lo que la Plataforma Tecnológica final viene a ser una solución mixta compuesta por aplicativos de ambos tipos.

En nuestra opinión parece una buena opción optar por los desarrollos a medida tanto para los sistemas informacionales como para los Motores de Cálculo de Capitales (si bien es cierto que las compañías que opten por la fórmula estándar podrían decantarse por una solución comercial), y buscar en proveedores

de software aplicaciones específicas para la gestión de los Riesgos (GRC) o la generación del reporting regulatorio (que promete ser cambiante y, de este modo, traspasamos los costes de los cambios futuros al proveedor tecnológico).

7.7. La solución final

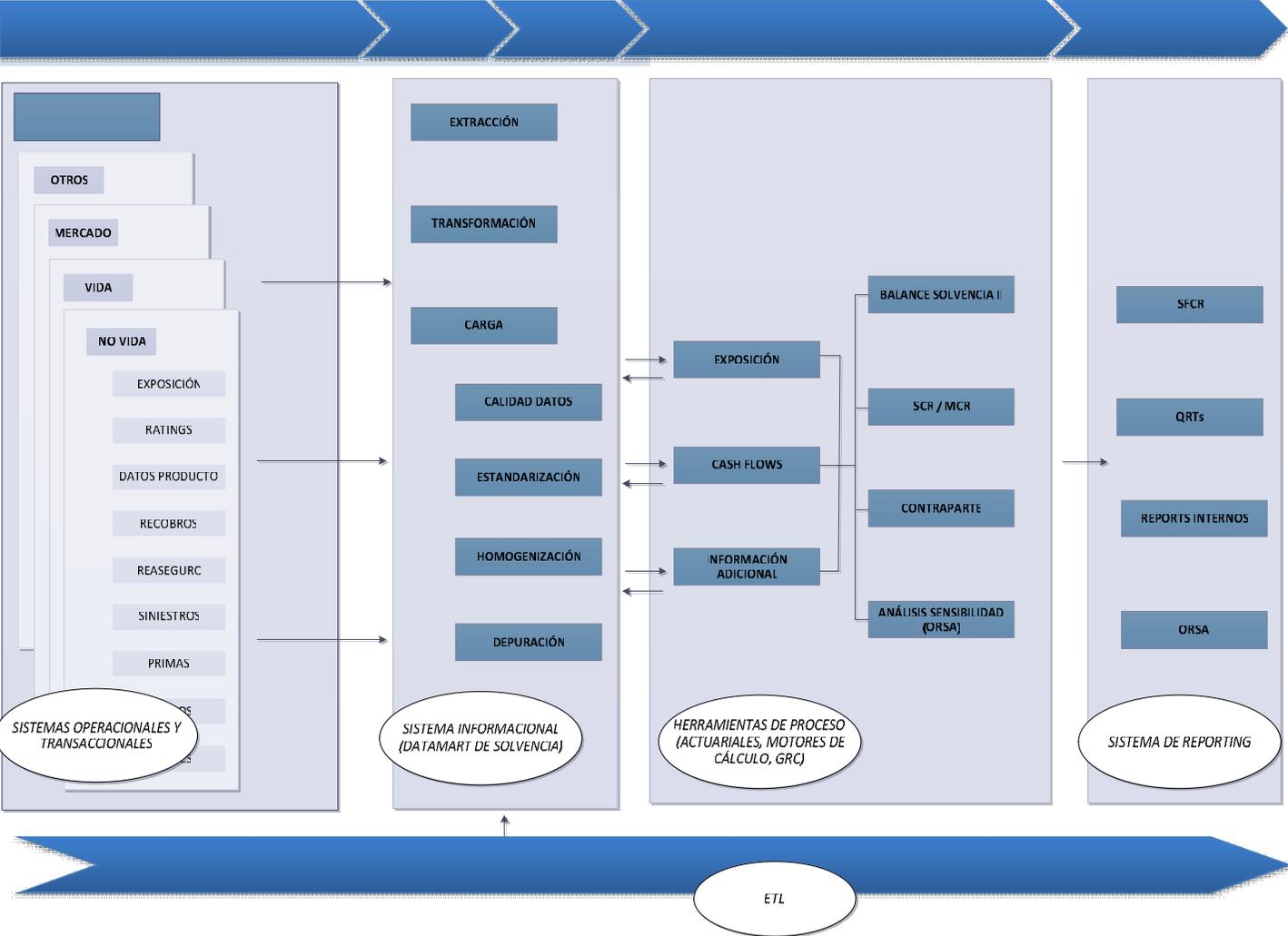
Aún sin poder identificar las aplicaciones concretas que se utilizarán por cada compañía en cada una de las partes de la plataforma (como ya hemos dicho, su elección variará en función de la situación inicial y las necesidades de cada una), después de todo este análisis, nos podemos hacer una idea muy clara del aspecto que tendrá la plataforma de la compañía para Solvencia II (ver gráfico 6, en página siguiente).

Como se puede ver en la parte superior del gráfico, la propia solución tiene un orden intrínseco de ejecución que permite distinguir 5 fases:

1. Generación de los datos. Los datos se generan en los sistemas operacionales y transaccionales, como resultado del propio funcionamiento de la compañía: se registran clientes, se emiten pólizas, se giran recibos, se ceden primas al reasegurador, etc. Sistemas implicados: sistemas operacionales y transaccionales.
2. Carga de los datos. Los datos son extraídos de los sistemas origen para ser almacenados en el datamart de Solvencia. Sistemas implicados: sistema informacional, ETL.
3. Depuración de los datos. En esta fase se deben llevar a cabo tareas que garantizarán la calidad de la información: estandarizar, depurar, eliminar duplicados, transformar, etc. Hay que pensar que la información puede tener orígenes muy diversos (en ocasiones, incluso puede venir como datos no estructurados –hojas de cálculo, tablas mantenidas manualmente, etc.) y es importante que toda la información sea homogénea antes de ser almacenada. Sistemas implicados: sistema informacional, ETL.
4. Procesos de cálculo. En esta fase se deben realizar todos los procesos actuariales, así como el cálculo de capitales regulatorios (SCR). Sistemas implicados: herramientas actuariales, motores de cálculo de capitales, sistema de gestión de riesgos.
5. Reporting. En esta fase final se genera tanto el reporting interno como externo.

Todo el movimiento de información entre aplicativos, como ya se ha dicho, debe estar controlado por procesos ETL para garantizar la trazabilidad en toda la plataforma.

Gráfico 6. La solución de Solvencia como sistema



Fuente: Elaboración propia

8. Marco de control de la calidad

Como hemos podido observar durante toda la exposición, garantizar la calidad de los datos es un aspecto fundamental de este proyecto: si no podemos estar seguros que la información es confiable, difícilmente podremos estar seguros de que las cifras estimadas de capital de solvencia son correctas y podríamos dejar a la compañía en una situación delicada.

Para poder conseguir esto es necesario establecer un marco de control que, de manera continuada, vele por que la información tenga el nivel mínimo de calidad exigible y que éste no se deteriore con el tiempo.

Los controles de la calidad de los datos pretenden evaluar los datos usados en los procesos relativos a Solvencia, con especial énfasis en:

- La valoración de activos y pasivos, en especial, el cálculo de las provisiones técnicas.
- La medición de los riesgos y la evaluación de las necesidades de capital.
- Los datos que sirven de base para estimar cualquier hipótesis usada en los cálculos anteriores.

8.1. Descripción de los tipos de controles

Es necesario definir cuáles son los controles que se realizarán a lo largo del proceso de tratamiento y transmisión de la información. Los controles deben ser diseñados en relación con los principios que deben preservarse. Se describen a continuación:

8.1.1. Controles de Precisión

Se dirá que los datos son precisos cuando no contengan errores, inexactitudes u omisiones. La recogida de información deberá comprender un ámbito suficiente de datos, y deberá efectuarse con la regularidad necesaria, garantizando así que los datos referentes a distintos momentos del tiempo sean consistentes entre sí y por tanto aptos para efectuar comparaciones y evaluar tendencias y riesgos. La compañía debe poder confiar en que los datos representan fielmente el aspecto que se está analizando. Así pues, debe ser posible proporcionar evidencias de que los datos son usados en los procesos operativos correspondientes.

Será necesario establecer pruebas de precisión como controles cruzados con otros datos, para detectar, por ejemplo, discordancias o pruebas entre los propios datos para verificar su concordancia interna. En caso que los datos sean externos será necesario comprobar adicionalmente que la metodología de generación de dichos datos es transparente y su calidad es verificada por una tercera parte ajena al proceso de suministro.

En concreto, para verificar los estándares y requisitos de precisión de los datos, se podrían realizar los siguientes controles y acciones:

- Documentar el diseño funcional y técnico de los sistemas TI así como las bases de datos utilizadas para el almacenamiento de los datos necesarios.
- Controles que comprueben si los datos cumplen con los siguientes requisitos:
 - Los datos no contienen errores materiales.
 - Los datos de diferentes períodos de tiempo utilizados para la misma estimación son coherentes.
 - Los datos se registran de modo oportuno y coherente a lo largo del tiempo.
 - Los datos tienen un formato legible y adecuado para ser analizado posteriormente con las herramientas establecidas.
- Verificar la existencia, calidad, contenido y adecuación de la documentación referente al diseño funcional y técnico de los sistemas de TI, así como bases de datos utilizadas en el modelo interno.

8.1.2. Controles de Completitud

Se dirá que la información es completa si es suficientemente amplia para poder obtener conclusiones objetivas y fiables, es decir, debe ser integral y suficientemente extensa y se debe haber comparado y contrastado con otros datos de naturaleza similar. Por ello, debe contener el nivel de desglose necesario para identificar las tendencias en los fenómenos que se quieren observar y el comportamiento de los riesgos asociados. Se tendrá que recoger con la mayor granularidad que sea necesaria para este propósito.

Para implementar estos controles, se podría:

- Verificar que los datos son lo suficientemente granulares e incluyen la suficiente información histórica como para identificar tendencias y determinar las características del riesgo subyacente.
- Se dispone de datos que cumplen todas las condiciones previamente mencionadas para todos los parámetros del modelo relevantes y no hay ningún dato relevante que sea excluido del modelo interno sin justificación.
- Recogen toda la información del aspecto que se analiza para cada conjunto homogéneo de observaciones.

8.1.3. Controles de Adecuación

Se dirá los datos son adecuados cuando se ajusten al propósito para el cual se usan, es decir, deben contribuir a que las hipótesis sean suficientes, realistas y

creíbles para predecir el resultado de los cálculos y deben evaluar los riesgos y las necesidades asociadas. Además, deben reflejar las características y riesgos del aspecto que están evaluando, ya sea representándolo directamente o reflejando fidedignamente sus características y particularidades. En caso que los datos sean externos, serán adecuados si cumplen con estas mismas características.

Para implementar estos controles, se podría:

- Verificar que los datos son coherentes con los objetivos para los que se utilizan.
- Verificar que la cantidad y naturaleza de los datos asegura que las estimaciones del modelo interno realizadas a partir de los datos no incluyen errores de estimación indebidos.
- Verificar que los datos son coherentes con los supuestos en los que se basan las técnicas actuariales y estadísticas aplicadas a dichos datos por el modelo interno.
- Verificar que los datos reflejan de modo apropiado los riesgos a los que está expuesta la entidad de seguros y reaseguros.
- Verificar que las técnicas estadísticas están adaptadas a los datos utilizados en el modelo interno.

8.1.4. Controles de Trazabilidad de los datos

Se dirá que los datos son trazables cuando pueda trazarse todo el camino que han seguido los datos desde su origen hasta el punto de control comprobando que no ha sido alterado su contenido ni sus propiedades durante el proceso.

En concreto, para verificar los estándares y requisitos de trazabilidad de los datos, se podrían realizar los siguientes controles y acciones:

- Verificar la integridad, coherencia y consistencia de los datos en cada punto de tratamiento de éstos, incluyendo las fuentes de origen.
- Verificar la trazabilidad de los datos usados para generar los resultados del modelo interno, generando revisiones de la integridad de los datos desde la fuente de origen hasta el punto de control.

8.1.5. Controles de disponibilidad

Los datos estarán disponibles en función del estado de su sistema de almacenamiento.

8.1.6. Controles de riesgos

Será necesario analizar los riesgos del sistema relativos al tratamiento y gestión de los datos. En concreto sería importante analizar y documentar:

- El proceso para llevar a cabo las actualizaciones de datos, incluyendo la frecuencia de las actualizaciones regulares y las circunstancias que desencadenan actualizaciones adicionales y nuevos cálculos de la distribución de probabilidad prevista.
- El uso y establecimiento de supuestos para la compilación, procesamiento y aplicación de datos. En relación a estos supuestos, se requerirían las siguientes condiciones:
 - Explicar y justificar cada uno de estos supuestos, teniendo en cuenta su importancia y supuestos alternativos.
 - Las circunstancias bajo las cuales los supuestos se considerarían erróneos deberán ser claramente definidas.
 - Establecer y mantener una explicación por escrito de la metodología usada para establecer los supuestos utilizados
- El proceso para llevar a cabo las actualizaciones de datos, incluyendo la frecuencia de las actualizaciones regulares y las circunstancias que desencadenan actualizaciones adicionales y nuevos cálculos de la distribución de probabilidad prevista.

8.2. Documentación de los controles

Debería quedar un registro documental de todos los controles implementados, que debería especificar la relación entre los grupos de controles en función del principio de calidad del dato que verifican y la herramienta usada para realizar dichos controles, así como la frecuencia de realización. Esto permitiría tener un seguimiento de su uso y su localización.

La persona o grupo responsable de cada control es quien debe procurar el buen funcionamiento y la buena aplicación de éste. En el siguiente apartado se profundizará en este aspecto.

8.3. Evidencias

Con el propósito de documentar el buen funcionamiento de los controles de calidad y el cumplimiento de los principios establecidos para la calidad del dato, es necesaria la toma de evidencias que lo argumenten y lo demuestren.

En concreto, estas evidencias deberían:

- Confirmar la existencia de un inventario de todos los datos utilizados en el modelo interno que especifica su fuente, características y utilidad.

- Verificar el cumplimiento de la política de calidad de datos mediante documentación.
- Verificar que los controles definidos por TI se llevan a cabo y que satisfacen los estándares cualitativos y cuantitativos.

Las evidencias pueden consistir en los controles per se o ir acompañados de documentación que describa y verifique los resultados obtenidos. De este modo se reduce y facilita la tarea de revisión y comprensión.

8.4. Roles y responsabilidades

En el proceso de creación de procedimientos y controles para verificar la calidad de los datos es necesario establecer una serie de roles y responsabilidades que verifiquen que dichos controles se llevan a cabo y se recogen las evidencias necesarias.

8.4.1. Responsabilidades

Es preciso que las áreas que tienen contacto con la información estén implicadas en la responsabilidad de su calidad, así como las áreas de negocio que inciden sobre cómo debe ser esta información y qué cálculos o procesos deben realizarse. A pesar de que Solvencia II consta de unos procesos que requieren tanto de las áreas técnicas como de las de negocio, es importante que cada una asuma el rol y la responsabilidad que le corresponde. De este modo, los roles podrían quedar definidos del siguiente modo:

- El departamento de TI tendría asignado el rol de proveer la infraestructura y apoyar las guías de Directiva, así como de implementar los controles y pruebas desde cada área para asegurar la calidad de los datos.
- Los puestos más próximos a la definición de los datos, como son los departamentos de negocio, tendrían que definir cuáles son los criterios de calidad asociados y deberían monitorizar y gestionarlos posteriormente.

Además, sería importante establecer unos vínculos sólidos entre ambas partes y asegurar que las comunicaciones son óptimas, hecho que garantizaría un nivel de trabajo más eficiente y completo.

Normalmente la aplicación de una política para garantizar la calidad de la información no debería afectar la estructura básica de trabajo de una organización, debido a que introduce un número reducido de cambios en las responsabilidades de los diferentes miembros implicados en el tratamiento de los datos.

Las responsabilidades relacionadas con la calidad de los datos se deberían focalizar sobretudo en cuestiones que afectan más a los resultados de los modelos de cálculo que no a todo el volumen de datos en general. De este modo, el alcance de estas medidas no sería tan amplio y se reduciría la complejidad de todos los procesos.

La gestión y regulación de los datos de manera dedicada y enfocada, como se ha descrito anteriormente, es reconocida cada vez más a menudo como una buena práctica empresarial ya que está pensada para aportar beneficios para la misma.

8.4.2. Roles

Es importante asegurar que las responsabilidades asignadas a cada persona o grupo de personas refleja sus roles operacionales. Respeto a la calidad de los datos, hay tres roles principales que pueden ser asignados, en concreto:

- **Prevención:** son las funciones necesarias para administrar la gobernanza, gestionar la política de datos así como sus guías y estándares y minimizar el riesgo de comprometer el sistema a errores o a fallos de regulación normativa.
- **Suministración:** son las funciones que gestionan los datos de manera continua, en particular los directorios y sistemas de almacenamiento de datos. Un ejemplo pueden ser requerimientos básicos como la actualización de datos o el uso externo de éstos.
- **Cura:** Son los procedimientos a seguir cuando surgen problemas y los métodos para gestionar temas conocidos sobre la calidad de los datos.

9. Marco de seguridad

La información no debe únicamente cumplir unos requisitos de calidad, también debemos garantizar la seguridad de los datos.

9.1. Principios de seguridad

9.1.1. Confidencialidad

Es necesario verificar que la información sólo es accedida por aquellos que tienen autorización para ello. Para asegurar la confidencialidad de los datos pueden usarse técnicas de encriptación para la información privada y susceptible de ser interceptada, así como evitar la publicación de datos confidenciales en entornos de mayor alcance que el permitido.

9.1.2. Integridad

Para asegurar que los datos no son modificados ni borrados sin el permiso de las personas autorizadas para tal efecto, es necesario generar un sistema de control de acceso a los datos. Para ello se deben crear registros o logs de los ficheros susceptibles de ser modificados sin permiso para poder comprobar su integridad en un momento dado.

9.1.3. Disponibilidad

Los datos deben ser accesibles por las personas autorizadas en el momento en que estas necesiten hacer uso de dicha información. Para ello, los sistemas de almacenamiento deben ser robustos y confiables, y deben garantizar que la probabilidad de falta de disponibilidad sea muy baja. Para ello, deben hacerse revisiones periódicas de la accesibilidad de los servidores donde se encuentran los sistemas de almacenamiento de los datos.

9.1.4. Autenticidad

Es necesario verificar que la información ha sido generada por la persona o fuente adecuada. Esto evita problemas de falsificación o suplantación de identidad. Para ello, un sistema debe tener una gestión de usuarios y contraseñas consistente, con un sistema de permisos adecuado y cumpliendo el principio del mínimo privilegio, es decir, que cada módulo o proceso sólo debe poder ser accedido por las personas estrictamente necesarias para su uso legítimo.

9.2. Tipos de controles de seguridad

Para asegurar que los datos están protegidos es necesario llevar a cabo controles de seguridad que ayuden a tener un seguimiento del uso de la información. Para ello se proponen los siguientes tipos de controles:

9.2.1. Administrativos

Con el objetivo de tener un control de las normas de seguridad y de controlar los procesos y transacciones que sigue la información, sería necesario establecer una política de seguridad donde se detallan los mecanismos de seguridad que sigue la compañía, junto con una descripción de los procesos en los que se hace uso de la información, para detectar los posibles riesgos. También es necesario generar estándares para homogeneizar las tareas de seguridad y facilitar la detección de riesgos, y guías para que los usuarios sepan qué acciones deben realizar en cuanto a las herramientas y procedimientos de seguridad.

9.2.2. Lógicos

Sería necesario tener registrado el control de acceso a datos y a software, con el objetivo de preservar la autenticidad, la integridad y la confidencialidad de los datos.

Por ejemplo, se debería:

- Gestionar los permisos y contraseñas de acceso a los sistemas, aplicaciones y bases de datos.
- Configurar cortafuegos y demás herramientas de control de las comunicaciones para restringir el acceso externo y remoto de entidades ajenas a la información de la compañía y para preservar un sistema de permisos y de perfiles coherente con las funciones asignadas a cada usuario del sistema.
- Encriptar la información y establecer un sistema de firmas digitales.
- Verificar que los usuarios que acceden al sistema, aplicaciones y bases de datos relacionadas con el modelo interno están autorizados y que sus permisos de acceso se corresponden con sus funciones.
- Llevar a cabo un registro de accesos al sistema, a las aplicaciones y a las bases de datos.
- La aplicación del principio del privilegio mínimo

Para asegurar la integridad de los datos y para solventar posibles pérdidas de información es imprescindible necesario realizar copias de seguridad periódicas de toda la información. Por lo tanto, deberían crearse procedimientos para la creación, almacenamiento, reciclaje y destrucción de copias de seguridad.

9.2.3. Físicos

Con el propósito final de que los datos estén protegidos físicamente, es recomendable establecer unos mecanismos de seguridad para los medios de alma-

cenamiento de éstos. Esto permite asegurar la integridad y la disponibilidad de la información almacenada en dichos medios. Por ejemplo, sería necesario:

- Gestionar el control de acceso a los medios de almacenamiento.
- Crear un sistema de protección del entorno de los medios.
- Asegurar un mantenimiento periódico de los medios y de su entorno.

9.3. Directrices de seguridad de los Sistemas de Información

Las directrices de la política de seguridad mencionada anteriormente podrían ser definidas apoyándose en alguna de los estándares existentes, por ejemplo, el estándar ISO/IEC 27001, que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente. Este marco tecnológico, organizativo y procedimental de seguridad se soportaría en un conjunto de normas, estándares, procedimientos y herramientas de seguridad para la protección de activos de información.

9.4. Gestión de continuidad del negocio

Se deben establecer procesos de gestión de continuidad de negocio para minimizar el impacto en las funciones y procesos críticos de la compañía en caso de desastre, de forma que se reduzca el tiempo de indisponibilidad a los niveles establecidos. Dichos procesos deben contar con la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

Estos procesos se deben apoyar en un Plan de Continuidad de Negocio que deberá ser probado de forma periódica, manteniéndose actualizado en todo momento. Para ello se debe evaluar el riesgo ante amenazas y el impacto asociado ocasionado por la ausencia de continuidad de los activos de información que den soporte o estén implicados en los procesos de negocio de la compañía.

9.5. Cumplimiento normativo y legal

Los Sistemas de Información y comunicaciones han de estar adecuados permanentemente a las exigencias legales y normativas generales así como a las propias del negocio asegurador en sus diferentes vertientes.

El acceso por parte de personal externo a los sistemas de la compañía deberá estar amparado por un contrato de prestación de servicios en el que figurarán las correspondientes cláusulas de confidencialidad y deber de secreto, así como las normas de seguridad y las responsabilidades que se derivan de la política de seguridad de la compañía.

Los intercambios de información entre organizaciones se regularán mediante acuerdos formales, y el establecimiento de normas y procedimientos para proteger la información en tránsito.

Con el objeto de evitar perjuicios derivados de la incorrecta utilización de la información automatizada y de los sistemas que la tratan y soportan por parte de terceros, la compañía deberá realizar comprobaciones sobre el uso que se realiza de los mismos, cumpliendo en todo momento con la legislación vigente y preservando los derechos fundamentales de las personas propietarias o titulares de la información y de las personas que los utilizan.

En este sentido, se deben llevar a cabo revisiones periódicas y auditorías para verificar el grado de cumplimiento de las medidas de protección que derivan del marco de seguridad.

Así mismo, se deberán establecer mecanismos y procedimientos que determinen los criterios a seguir para la generación, almacenamiento y explotación de los registros de eventos de seguridad y pistas de auditoría, teniendo presente en todo momento la necesidad de mantener, en lo necesario, la confidencialidad, integridad y validez legal de los mismos.

9.6. Seguridad frente a acciones humanas

Todo el personal de la compañía deberá desarrollar sus actividades conociendo, asumiendo y aplicando las normas y procedimientos de seguridad establecidos en la normativa de seguridad vigente en la organización.

Para ello, es indispensable la formación del personal en la normativa de seguridad y en el correcto uso de los Sistemas de Información con el fin de minimizar los posibles riesgos de seguridad.

9.7. Clasificación e inventariado de activos

Se deberá conocer en todo momento el valor de la información de la compañía, para lo cual es esencial el inventariado y clasificación de la misma. Se debería crear y mantener un inventario de los activos de información, asignando a cada uno de ellos un responsable y custodio.

Cada uno de los activos será clasificado de acuerdo a su sensibilidad, criticidad y naturaleza, aspectos éstos que dependen a su vez de la actividad o función de negocio que soporta.

9.8. Adquisición, desarrollo y mantenimiento de sistemas

Los requisitos de seguridad serán considerados durante todo el ciclo de vida de desarrollo de los sistemas de la compañía, tanto en sistemas de desarrollo propio como en aquellos desarrollados por terceros, desde las fases de análisis de requerimientos y viabilidad, en las que se particularizan y evalúan dichos requisitos, a las fases de diseño, pruebas, implantación, aceptación y su posterior mantenimiento.

9.9. Seguridad física del entorno

Los Sistemas de Información deberán ubicarse en zonas con acceso restringido que estén adecuadamente protegidos mediante los mecanismos de control de acceso físico apropiados. Asimismo se deberán proteger estos sistemas frente a otro tipo de amenazas del entorno como incendios, inundaciones o cortes en el suministro eléctrico.

Dicha protección se extiende a aquellos sistemas cuya securización física esté delegada en algún proveedor. Para ello, se deberán firmar las cláusulas oportunas en los contratos y se establecerán los mecanismos de seguimiento necesarios por parte de la compañía.

El tratamiento de información fuera de los sistemas de la compañía deberá ser debidamente autorizado, una vez que se garantice el cumplimiento del nivel de seguridad correspondiente.

9.10. Gestión y operación de sistemas, redes y comunicaciones

Se deberán establecer formalmente responsabilidades y procedimientos documentados para asegurar una correcta configuración, administración, operación y monitorización de los Sistemas de Información y comunicaciones de la compañía. Para ello, se establecerá una normativa específica y se adoptarán las mejores prácticas en materia de seguridad.

Se deberá definir y establecer un procedimiento de gestión de incidencias con el fin de minimizar el impacto ocasionado debido a incidentes de seguridad o fallos en el funcionamiento de los sistemas, así como para evitar su repetición.

Se deberá garantizar una adecuada segregación de funciones en la asignación de responsabilidades con el objetivo de prevenir un uso no adecuado de los Sistemas de Información. En caso de que no sea factible, se establecerán mecanismos de control adecuados que permitan su seguimiento.

Se deberán establecer los procedimientos y controles que prevengan adecuadamente frente a la introducción de software malicioso, garantizando la integridad del software y de la información de la compañía.

Se deberán establecer medidas de salvaguarda, incluyendo las copias de seguridad necesarias, comprobando periódicamente su validez mediante su restauración, e independientemente de que se monitoricen los sistemas permanentemente.

La información transmitida por redes de comunicaciones, públicas o privadas, deberá ser adecuadamente protegida mediante los mecanismos oportunos que garanticen su confidencialidad e integridad. Se deben establecer los controles necesarios que impidan la suplantación del emisor, modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en

las redes internas, como con entidades con las que la compañía tenga relación y, también, con sistemas externos.

Se deberán establecer procedimientos que contemplen el almacenamiento, manipulación, transporte y destrucción de la información sensible soportada tanto en formato papel como en soportes informáticos (cintas, discos, ordenadores portátiles, dispositivos móviles como agendas electrónicas y teléfonos, dispositivos extraíbles, etc.), con el fin de mitigar el riesgo de acceso no autorizado y hurto.

10. La gestión del proyecto

Una vez decidida una arquitectura para la solución tecnológica de solvencia, es necesario trazar un plan para la consecución de su implantación. Con el mismo espíritu al que nos obliga referirnos a una solución genérica, vale la pena dedicar un breve espacio a hablar de las fases que un proyecto de estas características debería tener y a los riesgos asociados al mismo.

10.1. Fases del proyecto

De manera general, se pueden distinguir dos grandes fases en este proyecto:

- Una primera fase de análisis orientada a determinar cuáles son los requisitos de la Directiva y establecer las diferencias con la información y los sistemas de los que la compañía dispone actualmente, y
- Una segunda fase que es la construcción propiamente de la plataforma y las pruebas para garantizar el correcto funcionamiento.

Entremos algo más en profundidad en esta primera fase para detallar las sub-fases y algunas tareas asociadas.

1. Análisis de las bases de datos y el entorno tecnológico actual. Aquí sería necesario analizar aspectos como las variables necesarias para implementar la solución, la identificación de los orígenes de datos, así como de los usuarios involucrados, los controles existentes, etc.
2. Toma de requerimientos. Aquí se deben incluir los requerimientos de todos los tipos: regulatorios / normativos, operativos, de cálculo de capital, de reporting, etc. Esta fase puede concluir con la elección de la plataforma tecnológica.
3. Definición funcional y de procesos. Esta subfase debe incluir el diseño de las interfaces y los controles, de las tablas y vistas de las bases de datos, de los cálculos, así como la identificación de responsabilidades para cada tipo de usuario.

A la conclusión de esta primera fase, debemos estar en posesión de un diseño detallado de toda la solución, que debe incluir un detalle de toda la información y procesos necesarios, y de la arquitectura tecnológica de la plataforma para Solvencia.

Gráfico 7. Fases del proyecto



Fuente: Elaboración propia

En el caso de la segunda fase, el detalle podría ser parecido al siguiente:

1. Implementación en sistemas, que comprende tanto el diseño técnico como la construcción de la plataforma de software propiamente dicha.
2. Pruebas unitarias y de integración. En primer lugar se debe definir un plan de pruebas y luego hay que llevarlo a cabo. Las pruebas deben ser exhaustivas y cubrir todos los ámbitos de la solución.
3. Aprovisionamiento y estabilización. En último lugar, se procederá a cargar la información histórica y, una vez hecho, la plataforma tecnológica entrará en un periodo de seguimiento y ajuste final.

Como todas las plataformas tecnológicas, una vez implementadas, deben ser mantenidas. Este caso no será una excepción y deberemos estar atentos tanto a cambios regulatorios que obliguen a realizar adaptaciones, como a la posible obsolescencia de la tecnología utilizada. Se podría argumentar que un proyecto de software no termina nunca.

10.2. Riesgos del proyecto

Como todo proyecto de implantación, lleva asociados unos riesgos que pueden comprometer su éxito. Destacamos a continuación algunos de los principales.

- El (siempre complicado) marco regulatorio. Como hemos visto con la propia Directiva de Solvencia II, una nueva regulación puede sufrir retrasos o modificaciones de última hora, que obliguen a cambiar o incluso rehacer partes de la plataforma de software. También pueden aparecer nuevas normas, que nos fuercen a tener que hacerlas compatibles con los sistemas que estamos construyendo. A modo de ejemplo, ya debe tenerse en cuenta qué se va a hacer para hacer compatible Solvencia II con la entrada en vigor de IFRS4, prevista para 2018. ¿Qué se hace durante el periodo interino en que una ya está en vigor pero la otra no? ¿Se mantienen dos sistemas independientes?
- La implicación de las áreas de negocio. Para que este proyecto sea un éxito es fundamental que todas las áreas involucradas en Solvencia (que son muy numerosas) estén perfectamente alineadas con los objetivos y participen activamente para garantizar una comunicación eficaz. La comunicación entre departamentos, no acostumbra a ser un punto fuerte en las compañías que tienen una cierta dimensión.
- Las soluciones comerciales. Si bien ya hemos visto que optar por soluciones comerciales puede tener ventajas, también es cierto que, en este caso, las empresas de software han tenido que desarrollar sus programas luchando contra la misma incertidumbre de la normativa que han sufrido las empresas aseguradoras. A unos meses vista de la entrada en vigor de la normativa, todavía hay aspectos que no han sido publicados.

Parece una tarea complicada que los vendedores de software puedan llegar a tiempo.

- Los usuarios de la plataforma. Cómo siempre que se producen cambios en tecnología, las organizaciones deben luchar contra la resistencia al cambio que presentan los usuarios. En este caso, en el que además, es más que probable la aparición de nuevos procesos, y la modificación de algunos de larga tradición, este riesgo es especialmente probable.
- El proceso de implantación. Todo el proceso de implantación debe ser supervisado de manera muy estrecha, de tal modo que las eventualidades sean abordadas de inmediato. Cualquier retraso, por la dependencia de las tareas, puede comprometer el cumplimiento del calendario regulatorio.

11. Conclusiones

Es innegable que la Directiva de Solvencia II va a tener un impacto importante en el sector asegurador. Lo ha tenido durante el proceso de aprobación de la misma, plagado de retrasos e incertidumbres que, en ocasiones, han hecho temer que jamás se llegara a implantar, y que han provocado un incremento de costes del proyecto; lo tendrá a partir de la entrada en vigor, con unos más que probables aumentos de las cifras de capital que las empresas deberán reservar para como capital de solvencia y con la obligación de enfocar la gestión del día a día de las compañías entorno a la mentalidad de la orientación al riesgo que la Directiva propugna.

Obviamente, todos estos cambios deben ser trasladados a los Sistemas de Información de las empresas aseguradoras; no en vano, se precisan nuevos motores de cálculo, la creación de nuevos informes, etc.

Esta tarea es intensiva en recursos tanto económicos cuanto personales, en un momento en que el sector está especialmente preocupado por el crecimiento y no puede descuidar su objetivo principal: mantener –o si es posible incrementar– la facturación, mejorar la eficiencia, controlar los costes y, todo esto, en un entorno fuertemente competitivo.

Como hemos podido ver durante todo este trabajo, las implicaciones que la entrada en vigor de la Directiva tiene en las áreas de TI son importantes y muy diversas: no sólo será necesario hacer nuevos desarrollos (o comprar y adaptar nuevas soluciones comerciales), sino que tendrán que implantarse unos marcos de control y seguridad que garanticen la calidad de la información que se utilizará para satisfacer los requerimientos de la Directiva, así como la trazabilidad de todo el proceso.

Pero aun siendo complejo y costoso, todo esto es asumible. La verdadera clave fundamental del éxito de la implantación de la Directiva de Solvencia II en las compañías es la confianza que las organizaciones puedan tener en que la información de la que disponen es correcta. La compañía que no pueda estar segura que sus datos base son correctos vivirá en la incertidumbre constante de no saber si está provisionando demasiado para Solvencia, perdiendo la oportunidad de sacar rendimiento económico a ese excedente, y con las consiguientes pérdidas para sus accionistas, o si, por el contrario, se haya insuficientemente cubierta ante posibles situaciones de riesgo, generando una situación de peligro para sus clientes.

Disponer de una información de calidad es responsabilidad de todas las áreas de una compañía, pero especialmente, de la unidad de Sistemas de Información, que es la que dispone de las herramientas necesarias para garantizarla.

Por todo ello, en nuestra opinión, es de vital importancia que el área de Sistemas de Información juegue un papel muy destacado en el proyecto de desarrollo de la Directiva en las organizaciones y, también, que se dediquen todos los recursos necesarios a garantizar que se dispone de una información de calidad, aunque inicialmente suponga una inversión importante. Seguramente, en

el entorno tan competitivo en el que nos movemos actualmente en el sector asegurador, de ello dependa el éxito de la empresa a medio plazo.

No querríamos acabar sin hacer una última reflexión en torno a lo que significa todo esto para aquellas compañías de tamaño más pequeño. No se puede obviar que, el esfuerzo del que hemos hablado, puede ser difícilmente asumible por compañías que no dispongan ya de una infraestructura mínima. Esto las va a obligar a ser imaginativas con las soluciones, si quieren cumplir la normativa, quizás estableciendo alianzas con otras pequeñas compañías para aprovechar sinergias. Su reto es, si cabe, todavía mayor.

12. Bibliografía

ABRIL, R.M.; MACAU, R. "Visión estratégica de la tecnología de los Sistemas de Información", *Datamation* (ed. española), núm. 41, enero (1989), págs. 28-37.

BARRIC, A.; BURWEISTER, C. "The Solvency II Scenarios: four perspectives on SII compliance", *THINK ALGO*, núm Junio (2010), págs. 29-33.

CLARK, K.B. "Para competir con éxito, no basta una tecnología avanzada", *Harvard-Deusto Business Review*, núm. 42, segundo trimestre (1990), págs. 101-106.

ICEA. Enfoque TI para el éxito en la implantación de Solvencia II. Documento núm. 225. Madrid, 2013.

FORRESTER, J.W. *Industrial Dynamics*. 5ª ed. Massachusetts: MIT Press, 1968.

Fundación de Estudios Financieros. Estudio sobre el sector asegurador en España 2010: los aspectos cualitativos de Solvencia II. Madrid. Papeles de la fundación nº 38, 2010.

OCDE. *Las nuevas tecnologías en la década de los noventa*. Madrid. Centro de publicaciones Ministerio de Trabajo y Seguridad Social, 1990.

PORTER, M.E.; MILLAR, V.E. "Cómo obtener ventajas competitivas por medio de la información". *Harvard-Deusto Business Review*, núm. 25, primer trimestre . (1968), págs. 3-20.

REVILLA GUTIÉRREZ, E. "Reflexiones en torno al valor estratégico de la tecnología de la información", *Anales de Estudios de Economía y Empresa*, núm. 6 (1991), págs. 67-81.

Javier Portales Pau

Ingeniero técnico en Informática por la Universidad Politécnica de Cataluña (FIB-UPC), empezó su carrera profesional en el mundo de la consultoría informática, hasta que se incorporó al Grupo Catalana Occidente. Actualmente es responsable del departamento de Proyectos Especiales de TI.

COLECCIÓN “CUADERNOS DE DIRECCIÓN ASEGURADORA”

Master en Dirección de Entidades Aseguradoras y Financieras
Facultad de Economía y Empresa. Universidad de Barcelona

PUBLICACIONES

- 1.- Francisco Abián Rodríguez: “Modelo Global de un Servicio de Prestaciones Vida y su interrelación con Suscripción” 2005/2006
- 2.- Erika Johanna Aguilar Olaya: “Gobierno Corporativo en las Mutualidades de Seguros” 2005/2006
- 3.- Alex Aguyé Casademunt: “La Entidad Multicanal. Elementos clave para la implantación de la Estrategia Multicanal en una entidad aseguradora” 2009/2010
- 4.- José María Alonso-Rodríguez Piedra: “Creación de una plataforma de servicios de siniestros orientada al cliente” 2007/2008
- 5.- Jorge Alvez Jiménez: “innovación y excelencia en retención de clientes” 2009/2010
- 6.- Anna Aragonés Palom: “El Cuadro de Mando Integral en el Entorno de los seguros Multirriesgo” 2008/2009
- 7.- Maribel Avila Ostos: “La tele-suscripción de Riesgos en los Seguros de Vida” 2009/20010
- 8.- Mercé Bascompte Riquelme: “El Seguro de Hogar en España. Análisis y tendencias” 2005/2006
- 9.- Aurelio Beltrán Cortés: “Bancaseguros. Canal Estratégico de crecimiento del sector asegurador” 2010/2011
- 10.- Manuel Blanco Alpunte: “Delimitación temporal de cobertura en el seguro de responsabilidad civil. Las cláusulas claims made” 2008/2009
- 11.- Eduard Blanxart Raventós: “El Gobierno Corporativo y el Seguro D & O” 2004/2005
- 12.- Rubén Bouso López: “El Sector Industrial en España y su respuesta aseguradora: el Multirriesgo Industrial. Protección de la empresa frente a las grandes pérdidas patrimoniales” 2006/2007
- 13.- Kevin van den Boom: “El Mercado Reasegurador (Cedentes, Brokers y Reaseguradores). Nuevas Tendencias y Retos Futuros” 2008/2009
- 14.- Laia Bruno Sazatornil: “L'ètica i la rentabilitat en les companyies asseguradores. Proposta de codi deontològic” 2004/2005
- 15.- María Dolores Caldés Llopis: “Centro Integral de Operaciones Vida” 2007/2008
- 16.- Adolfo Calvo Llorca: “Instrumentos legales para el recobro en el marco del seguro de crédito” 2010/2011
- 17.- Ferran Camprubí Baiges: “La gestión de las inversiones en las entidades aseguradoras. Selección de inversiones” 2010/2011
- 18.- Joan Antoni Carbonell Aregall: “La Gestió Internacional de Sinistres d'Automòbil amb Resultat de Danys Materials” 2003-2004
- 19.- Susana Carmona Llevadot: “Viabilidad de la creación de un sistema de Obra Social en una entidad aseguradora” 2007/2008
- 20.- Sergi Casas del Alcazar: “El PPlan de Contingencias en la Empresa de Seguros” 2010/2011
- 21.- Francisco Javier Cortés Martínez: “Análisis Global del Seguro de Decesos” 2003-2004
- 22.- María Carmen Ceña Nogué: “El Seguro de Comunidades y su Gestión” 2009/2010
- 23.- Jordi Cots Paltor: “Control Interno. El auto-control en los Centros de Siniestros de Automóviles” 2007/2008
- 24.- Montserrat Cunillé Salgado: “Los riesgos operacionales en las Entidades Aseguradoras” 2003-2004

- 25.- Ricard Doménech Pagés: "La realidad 2.0. La percepción del cliente, más importante que nunca" 2010/2011
- 26.- Luis Domínguez Martínez: "Formas alternativas para la Cobertura de Riesgos" 2003-2004
- 27.- Marta Escudero Cutal: "Solvencia II. Aplicación práctica en una entidad de Vida" 2007/2008
- 28.- Salvador Esteve Casablanca: "La Dirección de Reaseguro. Manual de Reaseguro" 2005/2006
- 29.- Alvaro de Falguera Gaminde: "Plan Estratégico de una Correduría de Seguros Náuticos" 2004/2005
- 30.- Isabel M^a Fernández García: "Nuevos aires para las Rentas Vitalicias" 2006/2007
- 31.- Eduard Fillet Catarina: "Contratación y Gestión de un Programa Internacional de Seguros" 2009/2010
- 32.- Pablo Follana Murcia: "Métodos de Valoración de una Compañía de Seguros. Modelos Financieros de Proyección y Valoración consistentes" 2004/2005
- 33.- Juan Fuentes Jassé: "El fraude en el seguro del Automóvil" 2007/2008
- 34.- Xavier Gabarró Navarro: ""El Seguro de Protección Jurídica. Una oportunidad de Negocio"" 2009/2010
- 35.- Josep María Galcerá Gombau: "La Responsabilidad Civil del Automóvil y el Daño Corporal. La gestión de siniestros. Adaptación a los cambios legislativos y propuestas de futuro" 2003-2004
- 36.- Luisa García Martínez: "El Carácter tuitivo de la LCS y los sistemas de Defensa del Asegurado. Perspectiva de un Operador de Banca Seguros" 2006/2007
- 37.- Fernando García Giralt: "Control de Gestión en las Entidades Aseguradoras" 2006/2007
- 38.- Jordi García-Muret Ubis: "Dirección de la Sucursal. D. A. F. O." 2006/2007
- 39.- David Giménez Rodríguez: "El seguro de Crédito: Evolución y sus Canales de Distribución" 2008/2009
- 40.- Juan Antonio González Arriete: "Línea de Descuento Asegurada" 2007/2008
- 41.- Miquel Gotés Grau: "Assegurances Agràries a BancaSeguros. Potencial i Sistema de Comercialització" 2010/2011
- 42.- Jesús Gracia León: "Los Centros de Siniestros de Seguros Generales. De Centros Operativos a Centros Resolutivos. De la optimización de recursos a la calidad de servicio" 2006/2007
- 43.- José Antonio Guerra Díez: "Creación de unas Tablas de Mortalidad Dinámicas" 2007/2008
- 44.- Santiago Guerrero Caballero: "La politización de las pensiones en España" 2010/2011
- 45.- Francisco J. Herencia Conde: "El Seguro de Dependencia. Estudio comparativo a nivel internacional y posibilidades de desarrollo en España" 2006/2007
- 46.- Francisco Javier Herrera Ruiz: "Selección de riesgos en el seguro de Salud" 2009/2010
- 47.- Alicia Hoya Hernández: "Impacto del cambio climático en el reaseguro" 2008/2009
- 48.- Jordi Jiménez Baena: "Creación de una Red de Agentes Exclusivos" 2007/2008
- 49.- Oriol Jorba Cartoixà: "La oportunidad aseguradora en el sector de las energías renovables" 2008/2009
- 50.- Anna Juncá Puig: "Una nueva metodología de fidelización en el sector asegurador" 2003/2004
- 51.- Ignacio Lacalle Goría: "El artículo 38 Ley Contrato de Seguro en la Gestión de Siniestros. El procedimiento de peritos" 2004/2005
- 52.- M^a Carmen Lara Ortíz: "Solvencia II. Riesgo de ALM en Vida" 2003/2004
- 53.- Haydée Noemí Lara Téllez: "El nuevo sistema de Pensiones en México" 2004/2005

- 54.- Marta Leiva Costa: "La reforma de pensiones públicas y el impacto que esta modificación supone en la previsión social" 2010/2011
- 55.- Victoria León Rodríguez: "Problemática del aseguramiento de los Jóvenes en la política comercial de las aseguradoras" 2010/2011
- 56.- Pilar Lindín Soriano: "Gestión eficiente de pólizas colectivas de vida" 2003/2004
- 57.- Victor Lombardero Guarner: "La Dirección Económico Financiera en el Sector Asegurador" 2010/2011
- 58.- Maite López Aladros: "Análisis de los Comercios en España. Composición, Evolución y Oportunidades de negocio para el mercado asegurador" 2008/2009
- 59.- Josep March Arranz: "Los Riesgos Personales de Autónomos y Trabajadores por cuenta propia. Una visión de la oferta aseguradora" 2005/2006
- 60.- Miquel Maresch Camprubí: "Necesidades de organización en las estructuras de distribución por mediadores" 2010/2011
- 61.- José Luis Marín de Alcaraz: "El seguro de impago de alquiler de viviendas" 2007/2008
- 62.- Miguel Ángel Martínez Boix: "Creatividad, innovación y tecnología en la empresa de seguros" 2005/2006
- 63.- Susana Martínez Corveira: "Propuesta de Reforma del Baremo de Autos" 2009/2010
- 64.- Inmaculada Martínez Lozano: "La Tributación en el mundo del seguro" 2008/2009
- 65.- Dolors Melero Montero: "Distribución en bancaseguros: Actuación en productos de empresas y gerencia de riesgos" 2008/2009
- 66.- Josep Mena Font: "La Internalización de la Empresa Española" 2009/2010
- 67.- Angela Milla Molina: "La Gestión de la Previsión Social Complementaria en las Compañías de Seguros. Hacia un nuevo modelo de Gestión" 2004/2005
- 68.- Montserrat Montull Rossón: "Control de entidades aseguradoras" 2004/2005
- 69.- Eugenio Morales González: "Oferta de licuación de patrimonio inmobiliario en España" 2007/2008
- 70.- Lluís Morales Navarro: "Plan de Marketing. División de Bancaseguros" 2003/2004
- 71.- Sonia Moya Fernández: "Creación de un seguro de vida. El éxito de su diseño" 2006/2007
- 72.- Rocio Moya Morón: "Creación y desarrollo de nuevos Modelos de Facturación Electrónica en el Seguro de Salud y ampliación de los modelos existentes" 2008/2009
- 73.- María Eugenia Muguerra Goya: "Bancaseguros. La comercialización de Productos de Seguros No Vida a través de redes bancarias" 2005/2006
- 74.- Ana Isabel Mullor Cabo: "Impacto del Envejecimiento en el Seguro" 2003/2004
- 75.- Estefanía Nicolás Ramos: "Programas Multinacionales de Seguros" 2003/2004
- 76.- Santiago de la Nogal Mesa: "Control interno en las Entidades Aseguradoras" 2005/2006
- 77.- Antonio Nolasco Gutiérrez: "Venta Cruzada. Mediación de Seguros de Riesgo en la Entidad Financiera" 2006/2007
- 78.- Francesc Ocaña Herrera: "Bonus-Malus en seguros de asistencia sanitaria" 2006/2007
- 79.- Antonio Olmos Francino: "El Cuadro de Mando Integral: Perspectiva Presente y Futura" 2004/2005
- 80.- Luis Palacios García: "El Contrato de Prestación de Servicios Logísticos y la Gerencia de Riesgos en Operadores Logísticos" 2004/2005
- 81.- Jaume Paris Martínez: "Segmento Discapacitados. Una oportunidad de Negocio" 2009/2010
- 82.- Martín Pascual San Martín: "El incremento de la Longevidad y sus efectos colaterales" 2004/2005

- 83.- Montserrat Pascual Villacampa: "Proceso de Tarificación en el Seguro del Automóvil. Una perspectiva técnica" 2005/2006
- 84.- Marco Antonio Payo Aguirre: "La Gerencia de Riesgos. Las Compañías Cautivas como alternativa y tendencia en el Risk Management" 2006/2007
- 85.- Patricia Pérez Julián: "Impacto de las nuevas tecnologías en el sector asegurador" 2008/2009
- 86.- María Felicidad Pérez Soro: "La atención telefónica como transmisora de imagen" 2009/2010
- 87.- Marco José Piccirillo: "Ley de Ordenación de la Edificación y Seguro. Garantía Decenal de Daños" 2006/2007
- 88.- Irene Plana Güell: "Sistemas d'Informació Geogràfica en el Sector Assegurador" 2010/2011
- 89.- Sonia Plaza López: "La Ley 15/1999 de Protección de Datos de carácter personal" 2003/2004
- 90.- Pere Pons Pena: "Identificación de Oportunidades comerciales en la Provincia de Tarragona" 2007/2008
- 91.- María Luisa Postigo Díaz: "La Responsabilidad Civil Empresarial por accidentes del trabajo. La Prevención de Riesgos Laborales, una asignatura pendiente" 2006/2007
- 92.- Jordi Pozo Tamarit: "Gerencia de Riesgos de Terminales Marítimas" 2003/2004
- 93.- Francesc Pujol Niñerola: "La Gerencia de Riesgos en los grupos multisectoriales" 2003-2004
- 94.- M^a del Carmen Puyol Rodríguez: "Recursos Humanos. Breve mirada en el sector de Seguros" 2003/2004
- 95.- Antonio Miguel Reina Vidal: "Sistema de Control Interno, Compañía de Vida. Bancaseguros" 2006/2007
- 96.- Marta Rodríguez Carreiras: "Internet en el Sector Asegurador" 2003/2004
- 97.- Juan Carlos Rodríguez García: "Seguro de Asistencia Sanitaria. Análisis del proceso de tramitación de Actos Médicos" 2004/2005
- 98.- Mónica Rodríguez Nogueiras: "La Cobertura de Riesgos Catastróficos en el Mundo y soluciones alternativas en el sector asegurador" 2005/2006
- 99.- Susana Roquet Palma: "Fusiones y Adquisiciones. La integración y su impacto cultural" 2008/2009
- 100.- Santiago Rovira Obradors: "El Servei d'Assegurances. Identificació de les variables clau" 2007/2008
- 101.- Carlos Ruano Espí: "Microseguro. Una oportunidad para todos" 2008/2009
- 102.- Mireia Rubio Cantisano: "El Comercio Electrónico en el sector asegurador" 2009/2010
- 103.- María Elena Ruíz Rodríguez: "Análisis del sistema español de Pensiones. Evolución hacia un modelo europeo de Pensiones único y viabilidad del mismo" 2005/2006
- 104.- Eduardo Ruiz-Cuevas García: "Fases y etapas en el desarrollo de un nuevo producto. El Taller de Productos" 2006/2007
- 105.- Pablo Martín Sáenz de la Pascua: "Solvencia II y Modelos de Solvencia en Latinoamérica. Sistemas de Seguros de Chile, México y Perú" 2005/2006
- 106.- Carlos Sala Farré: "Distribución de seguros. Pasado, presente y tendencias de futuro" 2008/2009
- 107.- Ana Isabel Salguero Matarín: "Quién es quién en el mundo del Plan de Pensiones de Empleo en España" 2006/2007
- 108.- Jorge Sánchez García: "El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras" 2006/2007
- 109.- María Angels Serral Floreta: "El lucro cesante derivado de los daños personales en un accidente de circulación" 2010/2011

- 110.- David Serrano Solano: "Metodología para planificar acciones comerciales mediante el análisis de su impacto en los resultados de una compañía aseguradora de No Vida" 2003/2004
- 111.- Jaume Siberta Durán: "Calidad. Obtención de la Normativa ISO 9000 en un centro de Atención Telefónica" 2003/2004
- 112.- María Jesús Suárez González: "Los Poolings Multinacionales" 2005/2006
- 113.- Miguel Torres Juan: "Los siniestros IBNR y el Seguro de Responsabilidad Civil" 2004/2005
- 114.- Carlos Travé Babiano: "Provisiones Técnicas en Solvencia II. Valoración de las provisiones de siniestros" 2010/2011
- 115.- Rosa Viciano García: "Banca-Seguros. Evolución, regulación y nuevos retos" 2007/2008
- 116.- Ramón Vidal Escobosa: "El baremo de Daños Personales en el Seguro de Automóviles" 2009/2010
- 117.- Tomás Wong-Kit Ching: "Análisis del Reaseguro como mitigador del capital de riesgo" 2008/2009
- 118.- Yibo Xiong: "Estudio del mercado chino de Seguros: La actualidad y la tendencia" 2005/2006
- 119.- Beatriz Bernal Callizo: "Póliza de Servicios Asistenciales" 2003/2004
- 120.- Marta Bové Badell: "Estudio comparativo de evaluación del Riesgo de Incendio en la Industria Química" 2003/2004
- 121.- Ernest Castellón Teixidó: "La edificación. Fases del proceso, riesgos y seguros" 2004/2005
- 122.- Sandra Clusella Giménez: "Gestió d'Actius i Passius. Inmunització Financera" 2004/2005
- 123.- Miquel Crespí Argemí: "El Seguro de Todo Riesgo Construcción" 2005/2006
- 124.- Yolanda Dengra Martínez: "Modelos para la oferta de seguros de Hogar en una Caja de Ahorros" 2007/2008
- 125.- Marta Fernández Ayala: "El futuro del Seguro. Bancaseguros" 2003/2004
- 126.- Antonio Galí Isus: "Inclusión de las Energías Renovables en el sistema Eléctrico Español" 2009/2010
- 127.- Gloria Gorbea Bretones: "El control interno en una entidad aseguradora" 2006/2007
- 128.- Marta Jiménez Rubio: "El procedimiento de tramitación de siniestros de daños materiales de automóvil: análisis, ventajas y desventajas" 2008/2009
- 129.- Lorena Alejandra Libson: "Protección de las víctimas de los accidentes de circulación. Comparación entre el sistema español y el argentino" 2003/2004
- 130.- Mario Manzano Gómez: "La responsabilidad civil por productos defectuosos. Solución aseguradora" 2005/2006
- 131.- Àlvar Martín Botí: "El Ahorro Previsión en España y Europa. Retos y Oportunidades de Futuro" 2006/2007
- 132.- Sergio Martínez Olivé: "Construcción de un modelo de previsión de resultados en una Entidad Aseguradora de Seguros No Vida" 2003/2004
- 133.- Pilar Miracle Vázquez: "Alternativas de implementación de un Departamento de Gestión Global del Riesgo. Aplicado a empresas industriales de mediana dimensión" 2003/2004
- 134.- María José Morales Muñoz: "La Gestión de los Servicios de Asistencia en los Multirriesgo de Hogar" 2007/2008
- 135.- Juan Luis Moreno Pedroso: "El Seguro de Caución. Situación actual y perspectivas" 2003/2004
- 136.- Rosario Isabel Pastrana Gutiérrez: "Creació d'una empresa de serveis socials d'atenció a la dependència de les persones grans enfocada a productes d'assegurances" 2007/2008
- 137.- Joan Prat Rifà: "La Previsió Social Complementaria a l'Empresa" 2003/2004

- 138.- Alberto Sanz Moreno: "Beneficios del Seguro de Protección de Pagos" 2004/2005
- 139.- Judith Safont González: "Efectes de la contaminació i del estils de vida sobre les assegurances de salut i vida" 2009/2010
- 140.- Carles Soldevila Mejías: "Models de gestió en companyies d'assegurances. Outsourcing / Insourcing" 2005/2006
- 141.- Olga Torrente Pascual: "IFRS-19 Retribuciones post-empleo" 2003/2004
- 142.- Annabel Roig Navarro: "La importancia de las mutualidades de previsión social como complementarias al sistema publico" 2009/2010
- 143.- José Angel Ansón Tortosa: "Gerencia de Riesgos en la Empresa española" 2011/2012
- 144.- María Mercedes Bernués Burillo: "El permiso por puntos y su solución aseguradora" 2011/2012
- 145.- Sònia Beulas Boix: "Prevención del blanqueo de capitales en el seguro de vida" 2011/2012
- 146.- Ana Borràs Pons: "Teletrabajo y Recursos Humanos en el sector Asegurador" 2011/2012
- 147.- María Asunción Cabezas Bono: "La gestión del cliente en el sector de bancaseguros" 2011/2012
- 148.- María Carrasco Mora: "Matching Premium. New approach to calculate technical provisions Life insurance companies" 2011/2012
- 149.- Eduard Huguet Palouzie: "Las redes sociales en el Sector Asegurador. Plan social-media. El Community Manager" 2011/2012
- 150.- Laura Monedero Ramírez: "Tratamiento del Riesgo Operacional en los 3 pilares de Solvencia II" 2011/2012
- 151.- Salvador Obregón Gomá: "La Gestión de Intangibles en la Empresa de Seguros" 2011/2012
- 152.- Elisabet Ordóñez Somolinos: "El sistema de control Interno de la Información Financiera en las Entidades Cotizadas" 2011/2012
- 153.- Gemma Ortega Vidal: "La Mediación. Técnica de resolución de conflictos aplicada al Sector Asegurador" 2011/2012
- 154.- Miguel Ángel Pino García: "Seguro de Crédito: Implantación en una aseguradora multirramo" 2011/2012
- 155.- Genevieve Thibault: "The Costumer Experience as a Sorce of Competitive Advantage" 2011/2012
- 156.- Francesc Vidal Bueno: "La Mediación como método alternativo de gestión de conflictos y su aplicación en el ámbito asegurador" 2011/2012
- 157.- Mireia Arenas López: "El Fraude en los Seguros de Asistencia. Asistencia en Carretera, Viaje y Multirriesgo" 2012/2013
- 158.- Lluís Fernández Rabat: "El proyecto de contratos de Seguro-IFRS4. Expectativas y realidades" 2012/2013
- 159.- Josep Ferrer Arilla: "El seguro de decesos. Presente y tendencias de futuro" 2012/2013
- 160.- Alicia García Rodríguez: "El Cuadro de Mando Integral en el Ramo de Defensa Jurídica" 2012/2013
- 161.- David Jarque Solsona: "Nuevos sistemas de suscripción en el negocio de vida. Aplicación en el canal bancaseguros" 2012/2013
- 162.- Kamal Mustafá Gondolbeu: "Estrategias de Expansión en el Sector Asegurador. Matriz de Madurez del Mercado de Seguros Mundial" 2012/2013
- 163.- Jordi Núñez García: "Redes Periciales. Eficacia de la Red y Calidad en el Servicio" 2012/2013
- 164.- Paula Núñez García: "Benchmarking de Autoevaluación del Control en un Centro de Sinistros Diversos" 2012/2013

- 165.- Cristina Riera Asensio: "Agregadores. Nuevo modelo de negocio en el Sector Asegurador" 2012/2013
- 166.- Joan Carles Simón Robles: "Responsabilidad Social Empresarial. Propuesta para el canal de agentes y agencias de una compañía de seguros generalista" 2012/2013
- 167.- Marc Vilardebó Miró: "La política de inversión de las compañías aseguradoras ¿Influirá Solvencia II en la toma de decisiones?" 2012/2013
- 168.- Josep María Bertrán Aranés: "Segmentación de la oferta aseguradora para el sector agrícola en la provincia de Lleida" 2013/2014
- 169.- María Buendía Pérez: "Estrategia: Formulación, implementación, valoración y control" 2013/2014
- 170.- Gabriella Fernández Andrade: "Oportunidades de mejora en el mercado de seguros de Panamá" 2013/2014
- 171.- Alejandro Galcerán Rosal: "El Plan Estratégico de la Mediación: cómo una Entidad Aseguradora puede ayudar a un Mediador a implementar el PEM" 2013/2014
- 172.- Raquel Gómez Fernández: "La Previsión Social Complementaria: una apuesta de futuro" 2013/2014
- 173.- Xoan Jovaní Guiral: "Combinaciones de negocios en entidades aseguradoras: una aproximación práctica" 2013/2014
- 174.- Àlex Lansac Font: "Visión 360 de cliente: desarrollo, gestión y fidelización" 2013/2014
- 175.- Albert Llambrich Moreno: "Distribución: Evolución y retos de futuro: la evolución tecnológica" 2013/2014
- 176.- Montserrat Pastor Ventura: "Gestión de la Red de Mediadores en una Entidad Aseguradora. Presente y futuro de los agentes exclusivos" 2013/2014
- 177.- Javier Portalés Pau: "El impacto de Solvencia II en el área de TI" 2013/2014
- 178.- Jesús Rey Pulido: "El Seguro de Impago de Alquileres: Nuevas Tendencias" 2013/2014
- 179.- Anna Solé Serra: "Del cliente satisfecho al cliente entusiasmado. La experiencia cliente en los seguros de vida" 2013/2014
- 180.- Eva Tejedor Escorihuela: "Implantación de un Programa Internacional de Seguro por una compañía española sin sucursales o filiales propias en el extranjero. Caso práctico: Seguro de Daños Materiales y RC" 2013/2014

