SOLVENCIA II Y GESTIÓN DEL RIESGO TECNOLÓGICO EN LAS COMPAÑÍAS DE SEGUROS

Versión	V1
Fecha	18-09-2012
Proyecto	Presentación CSTIC-2012
Dominio	Presentación

1. Introducción

El sector asegurador está inmerso en un profundo cambio debido a la introducción de la directiva de Solvencia II. Al amparo de dicha directiva, las compañías aseguradoras podrán tener unos requisitos de capital de solvencia en sintonía con su apetito del riesgo y la forma en que se gestiona. Para ello las compañías podrán presentar al supervisor nacional su modelo interno y será el supervisor quien deberá aprobar el mismo. Un elemento fundamental a la hora de aprobar un modelo es que dicho modelo se sustente en datos de calidad, para ello se debe analizar la situación estática de los mismos (auditoría de datos) y la situación dinámica (buen gobierno de los datos).

Por otra parte, desde el punto de vista cualitativo, Solvencia II requiere de las compañías un sistema de gobernanza el cual va a estar íntimamente relacionado con las tecnologías de la información. El supervisor deberá garantizar que dicho sistema funciona de forma adecuada y para ello deberá analizar la perspectiva tecnológica.

A continuación se presenta el papel del sector asegurador dentro de la economía nacional para luego analizar los retos tecnológicos que supone Solvencia II para las compañías de seguro y la visión que tiene la supervisión tecnológica de la Dirección General de Seguros y Fondos de Pensiones (DGSFP)

2. El sector asegurador en España.

Como ya señaló nuestra Directora General Flavia Rodríguez-Ponga en su presentación "Retos y Objetivos para el Sector Asegurador", el sector asegurador asume un papel importante dentro de la economía española. Dicha afirmación se sustenta en que el sector asegurador es:

Parte relevantes del PIB: El seguro factura al año una cifra cercana a los 60.000 millones de euros, que viene a significar el 5,5 % del Producto Interior Bruto y la pendiente de crecimiento del sector asegurador supera la tendencia del PIB.

Inversor institucional. El seguro español tiene un balance aproximado de 250.000 millones de euros (el doble que hace diez años) y genera unas inversiones financieras de 215.000 millones de las cuales, más de la mitad son de renta fija.

Creador de Empleo. Realiza más del doble de contratos fijos que la economía en su conjunto pudiéndose considerar el trabajo ofrece bastante estable. Por otra parte es financiador de primer nivel de subsectores de servicios tales como reparadores de hogar, talleres de automóvil, funerarias, médicos y otros.

Estabilizador de las economías particulares y/o empresas por medio de los seguros de vida, en crédito, caución, pérdidas pecuniarias, en daños, en autos, en responsabilidad civil en general, etc.

Prestador de servicios tales como asistencia sanitaria, defensa jurídica, decesos, asistencia en multirriesgos, accidentes, etc.

3. El Reto de Solvencia II

Durante los próximos años el se sector asegurador español se enfrenta al reto de la implantación de la directiva de Directiva 2009/138/CE del Parlamento Europeo y del Consejo sobre el seguro de vida, el acceso a la actividad de seguro y reaseguro y su ejercicio más conocida como Solvencia II.

El objeto de dicha directiva es el de garantizar el mercado interior del sector asegurador a lo largo de las fronteras de la Unión Europea armonizando, para ello, normas y estableciendo un marco de supervisión común.

La directiva se centra en tres aspectos fundamentales que tradicionalmente se denominan pilares:

Pilar I. Requisitos Cuantitativos. Se centra en los aspectos de implantación de la directiva y en especial los requisitos de capital tanto el requisito mínimo de capital (MCR) como el requisito de capital de solvencia (SCR).

Pilar II. Requisitos Cualitativos. Se relaciona con el conjunto de actividades que van a garantizar el control y el buen funcionamiento de la actividad de la entidad.

Pilar III. Disciplina de Mercado. Con este pilar se quiere garantizar la transparencia de la actividad de la aseguradora/reaseguradora tanto de cara al propio mercado como hacia el supervisor.

Una vez analizada la directiva y los objetivos que pretende, la duda que se plantea es ¿Qué papel desempeñan las tecnologías de la información a la hora de implantar Solvencia II?

Para ello nos centraremos principalmente en los Pilares I y II.

a. Pilar II. Sistema de Gobernanza

La directiva establece una serie de requisitos generales sobre la gobernanza indicando claramente que “las entidades deben de disponer de una estructura organizativa transparente y apropiada, con una clara distribución y una adecuada separación de funciones, y un sistema eficaz para garantizar la transmisión de la información”. Este requisito tiene impacto directo sobre la propia organización de las Tecnologías de la información, por una parte debe proporcionar los recursos necesarios para garantizar dichos sistema eficaz y por otra parte, la propia gobernanza de las TIC es parte de la gobernanza de corporativa.

A su vez, dentro de los requisitos generales, se estable la necesidad de un plan de continuidad de negocio. El texto señala: “las empresas de seguros y de reaseguros adoptarán medidas razonables para garantizar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de emergencia. A tal fin, las empresas emplearán sistemas, recursos y procedimientos adecuados y proporcionados”. A la hora de abordar este punto es de obligada referencia los estándares BS 25999 o ISO 22 22301 y analizar su impacto sobre las tecnologías de la información (tiempo de recuperación, punto de recuperación, políticas de backup, centros de respaldo, etc)

Una vez establecidos los requisitos generales el sistema de gobernanza se centra en una serie de requisitos concretos en relación a los siguientes puntos:

Gestión de riesgos: el texto indica:”Las empresas de seguros y de reaseguros dispondrán 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". Como ya se indica en el Pilar I, el riesgo operacional tiene un tratamiento específico a la hora de valorar los requisitos de capital y este riesgo está estrechamente relacionado con el riesgo tecnológico.

Control interno: según se señala en artículo 46 "Las empresas de seguros y de reaseguros establecerán un sistema eficaz de control interno. Dicho sistema constará, como mínimo, de procedimientos administrativos y contables, de un marco de control interno, de mecanismos adecuados de información a todos los niveles de la empresa y de una función de verificación del cumplimiento". Las TIC como parte de la organización debe de tener definidos sus propios procesos y controles, pero a su vez, como elemento facilitador del resto de procesos debe de garantizar el funcionamientos de las herramientas relacionadas con los mismos, prestando especial atención a los controles automáticos y teniendo en cuenta las decisiones de los respectivos propietarios del negocio.

Auditoría interna: según el artículo 47. "Las empresas de seguros y de reaseguros contarán con una función eficaz de auditoría interna. La función de auditoría interna abarcará la comprobación de la adecuación y eficacia del sistema de control interno y de otros elementos del sistema de gobernanza". Las TIC deberá de estar bajo el ámbito de la auditoría interna desde una doble perspectiva, por un lado, como parte de la organización y por otra como facilitador de los recursos a las áreas a ser auditadas. A la hora de garantizar la valía de las evidencias, la auditoría informática es esencial en aquellas áreas que requieran de un soporte tecnológico importante(contabilidad, ventas, gestión de siniestros, etc)

Externalizaciones: "Los Estados miembros velarán por que las empresas de seguros y de reaseguros sigan respondiendo plenamente del cumplimiento de todas las obligaciones que para ellas se derivan de la presente Directiva cuando externalicen funciones o cualquier actividad de seguro o de reaseguro". Las tecnologías de la información son muy susceptibles de ser externalizadas. Se deberán establecer los mecanismos adecuados para garantizar el control de la actividad externalizada.

b. Pilar I. Requisitos Cuantitativos.

Según el artículo 101 de la directiva, "El capital de solvencia obligatorio se calibrará de tal modo que se garantice que todos los riesgos cuantificables a los que una empresa de seguros o de reaseguros está expuesta se tengan en cuenta. Cubrirá las actividades existentes y las nuevas actividades que se espere realizar en los siguientes doce meses. En relación con la actividad existente, deberá cubrir exclusivamente las pérdidas inesperadas.". Los riesgos que deben ser considerados son:

- riesgo de suscripción en el seguro distinto del seguro de vida
- riesgo de suscripción en el seguro de vida
- riesgo de suscripción del seguro de enfermedad
- riesgo de mercado
- riesgo de crédito
- riesgo operacional

Según se indica en la subsección 2, a la hora de calcular el capital de solvencia obligatorio, se puede acudir a la fórmula estándar:
"El capital de solvencia obligatorio calculado con arreglo a la fórmula estándar será igual a la suma de lo siguiente:

a) el capital de solvencia obligatorio básico, conforme al artículo 104;
b) el capital de solvencia obligatorio por riesgo operacional, conforme al artículo 107;

c) el importe del ajuste destinado a tener en cuenta la capacidad de absorción de pérdidas de las provisiones técnicas y los impuestos diferidos, conforme al artículo 108. "

O bien por medio del uso de modelos internos previamente aprobados por el supervisor.

La conclusión inminente desde una perspectiva de gestión de riesgo tecnológico, es que ya que éste va a tener un impacto directo sobre el riesgo operacional y éste sobe los requisitos de capital, una gestión adecuada del riesgo tecnológico propuesto en un modelo interno puede reducir los requisitos de capital respecto de la fórmula estándar.

4. Análisis de Modelos Internos. Perspectiva de Tecnologías de la Información

A la hora de evaluar los modelos internos, la supervisión tecnológica (Informática de la DGSFP) considera necesario hacer uso de las mejores prácticas y estándares reconocidos internacionalmente y en especial por el sector financiero. Por esta razón, se ha considerado la idoneidad del empleo de COBIT 4.1 (marco de trabajo de ISACA), como punto de partida.

Según la información recogida en COBIT 4.1, para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. En este marco de trabajo se definen los siguientes siete criterios de información: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Partiendo de los criterios indicados, se ha considerado la necesidad de analizar la situación de la compañía desde dos perspectivas distintas:

a. Perspectiva Estática

Se pretende analizar el flujo de la información concreta de pólizas y siniestros que la entidad emplea en la propuesta de modelo interno. Dicho análisis utilizará como punto de partida los procesos de la compañía y analizará los sistemas informático que los sustentan haciendo uso para ello de la documentación que se disponga de arquitectura de empresa. El objetivo fundamental de este análisis es comprobar que los datos con los que se generan los modelos por parte del departamento actuarial, sean los reales de la compañía.

Para poder desarrollar esta perspectiva, serían necesarios trabajos de auditoría de datos. Dicha auditoría debería estar sustentada con la información de una arquitectura de empresa y tenida en consideración en los planes de auditoría de la entidad.

Se considera esta perspectiva como estática, porque nos muestra el estado de dicha información en un momento determinado, en concreto en el momento y las condiciones del análisis, sin garantizar que en otro momento o condiciones se obtengan los mismos resultados

b. Perspectiva Dinámica

Bajo esta perspectiva se va a analizar lo que podríamos llamar buen gobierno de la información. El buen gobierno de la información nos va a indicar el alineamiento estratégico de los sistemas de información con los objetivos de la entidad y en particular con la gestión del riesgo. Esta perspectiva, nos va a mostrar la capacidad que tiene la entidad para gestionar de forma adecuada la información para asegurar la calidad de la misma ante diferentes eventos.

El análisis de la perspectiva dinámica se va a fundamentar en dos visiones complementarias de la realidad de las tecnologías de la información:

1. Visión corporativa de las tecnologías de la Información. Se analizará el papel que desempeña las tecnologías de la información dentro de la entidad desde el punto de vista tanto estratégico como operativo. Se prestará especial atención a la forma en que los procesos de control interno, gestión de riesgos y en especial el de auditoría interna, tienen en consideración los sistemas de información de la entidad. Este análisis lo situaremos bajo el capítulo de Gobierno Corporativo y tecnología de la información.

2. Visión del marco de gobierno de TI. Se evaluarán los procesos de los sistemas información de la entidad acorde a lo establecido en la ISO/IEC 15504 Software Process Improvement Capability Determination utilizando la metodología de ISACA "COBIT Process Assessment Model (PAM)". Con esta metodología se evaluarán aquellos procesos de los sistemas de información directamente implicados en el modelo interno comparando dicha evaluación con el resto del sector (benchmarking). Este análisis lo situaremos bajo el capítulo Marco de trabajo del gobierno de TI.

Como ya se ha indicado, ambas visiones deben de ser complementarias y consistentes siendo un elemento crítico del análisis del modelo la no existencia de incoherencias entre ambas visiones.

Los puntos a estudiar se pueden estructurar de la siguiente forma:

- Gobierno Corporativo y las Tecnologías de las Información
  - La estrategia corporativa y las tecnologías de la información.
  - Visión operativa de las tecnologías de la información
  - Auditoría Interna
- Marco de Trabajo del Gobierno de TI
  - Gobierno de las tecnologías de la información
  - Control interno
  - Gestión de procesos
- Alineamiento con el Negocio
  - Arquitectura de Empresa
  - Gestión de Configuración
- Entrega de Valor
  - Inversión
  - Ciclo de Vida de desarrollo del sistema
  - Gestión de Servicios
  - Gestión de Proyectos
- Gestión de Riesgos
- Recursos Humanos
- Gestión de la Continuidad de Negocio
- Outsourcing
- Seguridad

5. Conclusiones

A la hora implantar de forma adecuado Solvencia II en las compañías de seguro/reaseguro es necesario tener en cuenta las tecnologías de la información. Pero en este caso, más que nunca, es necesario tener una visión corporativa de las tecnologías de la información y las comunicaciones y garantizar así el alineamiento estratégico. Por lo tanto, va requerir una profunda implicación no solo de los profesionales de seguros sino también de los especialistas en tecnologías de la información y las comunicaciones dando lugar una simbiosis entre ambos roles dando lugar a nuevos perfiles multidisciplinares.