Guía de AGERS sobre la función de la gestión de riesgos en las entidades aseguradoras

María Nuche Otero
Directora de Gestión de Riesgos
Consorcio de Compensación de Seguros

El 6 octubre de 2020 se presentó la Guía de AGERS (Asociación Española de Gerencia de Riesgos y Seguros) sobre la función de gestión de riesgos en las entidades aseguradoras. Esta Guía ha sido redactada por los miembros que forman la Comisión de Expertos de Riesgos en Entidades Aseguradoras de AGERS, entre los que se encuentran, en representación del Consorcio de Compensación de Seguros, Eva Valenti, Jefa del Departamento de Revisión Actuarial y María Nuche, Directora de Gestión de Riesgos.

La principal finalidad de la Guía es servir de referencia a los gestores de riesgos de las entidades aseguradoras al objeto de comprobar si están o no alineados con las prácticas y tareas comunes analizadas, de manera que permita la aplicación eficiente del sistema de gestión de riesgos. Se trata de un modelo flexible de forma que, aplicando el principio de proporcionalidad, cada entidad pueda autoevaluarse dentro del marco de actuación propuesto, teniendo en cuenta sus propias características, estructura y normativa interna.

Esta Comisión de Expertos está integrada por miembros que desempeñan la función de gestión de riesgos en entidades de seguros de diversa tipología y tamaño y han trabajado de cerca en la implementación y seguimiento de su funcionamiento.

El **objetivo de este documento** es elaborar una Guía práctica de la función de gestión de riesgos que sirva a la profesión y recoja las buenas prácticas comunes desempeñadas por esta función en las entidades de seguros, dando adicionalmente cobertura al cumplimiento de los requisitos exigidos por la normativa de Solvencia II.

La principal finalidad de la Guía es servir de referencia a los gestores de riesgos de las entidades aseguradoras al objeto de comprobar si están o no alineados con las prácticas y tareas comunes analizadas, de manera que permita la aplicación eficiente del sistema de gestión de riesgos. Se trata de un modelo flexible de forma que, aplicando el principio de proporcionalidad, cada entidad pueda autoevaluarse dentro del marco de actuación propuesto, teniendo en cuenta sus propias características, estructura y normativa interna.

El documento se dirige a todo tipo de entidades, independientemente del tamaño, del tipo de sociedad y del negocio, mediante la búsqueda de patrones comunes aplicables a todas ellas en la figura del responsable de gestión de riesgos.

También es objetivo de esta Guía mostrar al supervisor cuál es el rol y el posicionamiento adoptado por la función de gestión de riesgos y cómo se han llevado a cabo de manera práctica en las entidades de seguros tareas comunes que permitan responder a las exigencias generales de la normativa.

Entrando ya en el contenido específico de la Guía, la idea es aportar una relación de tareas y buenas prácticas en cada uno de los apartados que componen una adecuada estructura en el sistema de gestión de riesgos y en cada uno de los pasos que describen el buen funcionamiento del ciclo de riesgo implantado en las entidades.

En el **primer apartado** se analizan el **sistema de gestión de riesgos y la función de gestión de riesgos** como elementos fundamentales del sistema de gobierno en Solvencia II. Este sistema es aquel que comprende estrategias,

procesos y procedimientos de información necesarios para identificar, medir, controlar, gestionar y notificar los riesgos a los que se expone o podría exponerse una entidad y sus interdependencias.

El sistema de gestión de riesgos deberá estar integrado en la estructura organizativa y en el proceso de toma de decisiones de la entidad. Con este fin, la empresa debe:

- identificar sus objetivos y evaluar los riesgos que amenazan su consecución,
- diseñar controles internos y estrategias para gestionar o mitigar dichos riesgos y
- supervisar los controles y estrategias para asegurar que funcionen de manera eficaz.

Las entidades aseguradoras deberán además establecer una función de gestión de riesgos que facilite la aplicación del sistema de gestión de riesgos. Esta función, junto con las de cumplimiento, actuarial y auditoría interna, es una de las funciones clave en la normativa de Solvencia II. El titular de la función, por tanto, deberá reunir los requisitos de aptitud y honorabilidad necesarios para garantizar el adecuado desempeño de la función.

Serán tareas fundamentales de la función de gestión de riesgos:

- Definir las categorías de los riesgos y los métodos para su medición y gestión.
- Coordinar los procesos de valoración y evaluación de riesgos.
- Establecer los límites de tolerancia al riesgo para cada tipo de riesgo, de acuerdo con el perfil de riesgo global de la empresa.
- Establecer contenido y frecuencia de los test de estrés.
- Monitorizar el cumplimiento de los planes de acción que deriven del tratamiento de riesgos.
- Promover la cultura de gestión de riesgos en la entidad.
- Asistir a la Alta Dirección, al Consejo de Administración y al resto de funciones clave de cara al funcionamiento eficaz del sistema de gestión de riesgos.
- Realizar la presentación periódica de información detallada sobre las exposiciones a riesgos al Consejo de Administración.
- Identificar y evaluar riesgos emergentes.
- Informar puntualmente sobre riesgos potencialmente graves.

La Guía dedica un apartado al papel que juegan el **Consejo de Administración** y las **Comisiones Delegadas** en el funcionamiento del sistema de gestión de riesgos.

El Consejo de Administración de las entidades aseguradoras será el responsable último de:

- Garantizar la eficacia del sistema de gestión de riesgos.
- Definir el apetito al riesgo y los límites de tolerancia.
- Aprobar las políticas y estrategias de gestión de riesgos.

El Consejo, por lo tanto, al objeto de dar cumplimiento a lo anterior:

- Debe interactuar con la función de gestión de riesgos, solicitando información de forma proactiva y cuestionando la información cuando sea necesario.
- Documentará las decisiones adoptadas y en qué medida se ha tenido en cuenta en las mismas la información proporcionada por el sistema de gestión de riesgos.
- Garantizará que la entidad disponga de recursos suficientes para el desempeño de la función de gestión de riesgos.
- Solucionará los conflictos de intereses que puedan surgir.

El órgano de administración, en su labor de supervisión del sistema de gestión de riesgos, debe garantizar que:

- Se tienen en cuenta todos los riesgos a los que hace frente la organización en la búsqueda de sus objetivos.
- Los riesgos son apropiados en el contexto de los objetivos de la organización.
- Los sistemas para gestionar estos riesgos se implementan y operan eficazmente.
- La información sobre estos riesgos y su gestión se comunica de la manera apropiada.
- Se asigna autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la organización.

Es habitual que las entidades creen Comisiones Delegadas del Consejo de Administración al objeto de facilitar el desempeño de sus cometidos en esta materia. En este sentido, es habitual la creación de Comisiones de Riesgos por las organizaciones y, en su defecto, la adopción de estas tareas por parte de las Comisiones de Auditoría. Estas Comisiones deberán:

- Garantizar que al Consejo le llegue toda la información relevante sobre la gestión de riesgos.
- Incluir la supervisión de riesgos en el orden del día de las reuniones de la Comisión.
- Impulsar en la organización que en todas sus decisiones el riesgo sea un factor a considerar.
- Revaluar, al menos anualmente, el mapa de riesgos.
- Utilizar controles internos para mantener los riesgos a los que se enfrenta la empresa dentro de los niveles de tolerancia definidos por el Consejo, teniendo en cuenta la relación entre coste y beneficio.
- Identificar y entender los riesgos emergentes, manteniendo reuniones con los responsables de las diferentes unidades de negocio de la organización, reforzando la idea de que es a ellos a los que corresponde la gestión eficaz de los riesgos.

En el **segundo apartado** de la Guía se analiza el **rol del gestor de riesgos en cada uno de los componentes del sistema de gestión de riesgos.**

El sistema de gestión de riesgos debe incluir:

- Una estrategia de gestión de riesgos coherente con la estrategia comercial. Se documentarán los objetivos de la estrategia, los límites de tolerancia al riesgo y la asignación de responsabilidades.
- Procedimientos sobre el proceso de toma de decisiones.
- Políticas que garanticen la definición y categorización de los riesgos y los límites de tolerancia al riesgo de cada tipo de riesgo.
- Procedimientos y procesos de información que garanticen un seguimiento y análisis de los riesgos significativos, así como la introducción de modificaciones cuando sea necesario.

Por lo tanto, se pueden identificar estos cinco componentes en todo sistema de gestión de riesgos:

- Estrategia.
- Apetito.
- Marco de Gestión de Riesgos.
- Políticas.
- Procesos y procedimientos de gestión y control.

En relación con la **estrategia,** el gestor de riesgos llevará a cabo las siguientes tareas:

- Identificación de los riesgos potenciales que pongan en peligro la consecución de la estrategia y objetivos definidos.
- Asesoramiento sobre acciones de gestión en caso de posibles materializaciones de riesgo.
- Seguimiento del cumplimiento del plan estratégico establecido dentro de los límites de riesgo aprobados.
- Análisis *ad-hoc* de operaciones corporativas.
- Asesoramiento en la adaptación del sistema de gobierno para facilitar la consecución de objetivos.

- Consideración de los conceptos capital y riesgo en la toma de decisiones.
- Incorporación del plan estratégico al proceso ORSA (i).

Un elemento clave de la estrategia de riesgos que ha de definir el Consejo de Administración, asesorado por la función de gestión de riesgos, es el **apetito de riesgo** deseado. Una vez definido, la función de gestión de riesgos debe garantizar que se hace un seguimiento periódico de este apetito, comprobando que el perfil de riesgo asumido en cada momento se mantiene dentro de los niveles de riesgos previamente establecidos.

El apetito de riesgo es la cantidad y tipología de riesgos que la entidad está dispuesta a asumir para la consecución de sus objetivos. Tiene que estar vinculado a la estrategia de la entidad y es un punto de referencia para la planificación del negocio y la toma de decisiones. La fijación de este umbral permite optimizar el binomio riesgo-rentabilidad.

Para que este parámetro de carácter global pueda ser utilizado en la práctica, debe traducirse en límites más detallados que nos permiten utilizar métricas concretas y medibles para la gestión del negocio en el día a día.

Es necesario, asimismo, definir dos parámetros adicionales:

- Tolerancia al riesgo: Se define como el nivel aceptable de variación del objetivo de apetito de riesgo.
- Capacidad: Es el nivel máximo de riesgo que la entidad puede soportar en la consecución de sus objetivos estratégicos. La tolerancia al riesgo servirá como alerta para evitar que la entidad llegue al nivel establecido por su capacidad, algo que pondría en peligro la solvencia.

Es esencial que el gestor de riesgos lidere el seguimiento periódico del cumplimiento de los límites de riesgo establecidos.

Deberá compararse el perfil de riesgo, entendiendo este como el nivel de riesgo incurrido en cada cierre periódico o en un momento determinado, con el apetito de riesgo deseado aprobado por el Consejo de Administración.

Se verificará si cada uno de los riesgos se encuentra dentro de los límites especificados en las políticas. Si existen brechas o incumplimientos de límites, deberían proponerse y desarrollarse los correspondientes planes de acción que permitan mantenerse dentro los límites e intervalos de riesgo aprobados.

El resultado de la comparación periódica entre el perfil de riesgo (el asumido en un momento determinado) y el apetito de riesgo deseado es recogido en un informe que se remite al Consejo para su aprobación, bien directamente o a través de las Comisiones Delegadas, si estas existen.

El **marco de gestión de riesgos y control interno** resume los procesos y metodologías de gestión de riesgos que deben aplicarse e implementarse en la compañía y se basa en tres pilares fundamentales:

1. Una estructura adecuada donde se definan claramente las responsabilidades frente a la propiedad, el control y la supervisión de los riesgos. Dicha estructura se manifestará en unos organigramas jerárquicos y funcionales y en los correspondientes flujos de información, comunicación y toma de decisiones a lo largo de la organización.

2. Unas políticas corporativas que fijen los principios clave de funcionamiento en aras a la consecución de los objetivos marcados, así como unos límites de riesgo y unos niveles de tolerancia.

3. Unos procesos de gestión, documentados, formalizados y comunicados a la organización, que materializarán el sistema de gestión de la compañía en base a los cuales se identifica cómo han de realizarse las tareas y definirse las actividades de control que mitiguen dichos riesgos. Estas actividades de control deberán cumplir, tal y como dicta la normativa, el requisito de ser proporcionales a los riesgos derivados de las actividades y procesos a controlar.

(i) ORSA (acrónimo inglés de Own Risk Solvency Assessment, evaluación propia de los riesgos para la solvencia) es el conjunto de procesos y procedimientos que establece la directiva europea Solvencia II (2009/138/CE) para que las entidades aseguradoras y reaseguradoras puedan evaluar los riesgos a corto y largo plazo que pueden afrontar conforme a sus disponibilidades y necesidades internas de capital.

El marco de gestión de riesgos debería revisarse periódicamente. Es una buena práctica que dicha revisión se lleve a cabo anualmente.

El conjunto de **políticas corporativas** define los principios en base a los cuales la entidad debe gestionar determinadas áreas de riesgo y ayuda a garantizar que se cumplen los objetivos de negocio y los requerimientos regulatorios de las jurisdicciones en las que se opera.

Las responsabilidades de la primera y segunda línea con respecto al contenido, revisión, aprobación, operación, supervisión, seguimiento y comunicación de las políticas deben estar definidas en las mismas. Es buena práctica que el gestor de riesgos participe directamente en la elaboración de la política específica de la función de gestión de riesgos, que definirá sus actividades como función clave de control, sus derechos, obligaciones y relaciones y flujos de comunicación y reporte a lo largo de la organización. Esta política debe ser aprobada por el Consejo de Administración y revisada anualmente.

El gestor de riesgos ayuda y asesora a las áreas operativas propietarias de los riesgos a proponer el contenido de las políticas específicas de riesgos. Lo que es esencial en la entidad es que se asignen responsabilidades respecto a la gestión y control de los riesgos por sus propietarios.

Las políticas específicas de gestión de riesgos deben dar cobertura, como mínimo, a las áreas de riesgos recogidas en la normativa:

- Política de gestión de riesgos de suscripción y constitución de reservas.
- Política de gestión de activos y pasivos.
- Política de gestión del riesgo de inversión.
- Política de gestión del riesgo de liquidez.
- Política de gestión del riesgo de concentración.
- Política de gestión del riesgo operacional.
- Política de reaseguro u otras técnicas de mitigación.

Es necesario que las actividades de gestión de riesgos sean transversales, abarcando todos los procesos e involucrando a las diferentes áreas operativas de la entidad.

Resulta indispensable, por tanto, establecer **procedimientos bien definidos de control y gestión de los riesgos** mediante los cuales se pueda identificar, vigilar y medir el impacto de las distintas categorías de riesgo. Deben describirse las áreas responsables de gestionar y controlar cada categoría, la frecuencia y el contenido de los controles y las situaciones que requieren mayor atención, y un plan específico; deben asegurar, igualmente, que los riesgos están descritos y son conocidos por las personas del área donde puedan producirse.

La existencia de estos procedimientos, adecuadamente documentados, garantiza la eficacia del sistema, asegurando que la entidad se mantenga dentro del umbral de riesgo fijado por el Consejo de Administración, de manera que se garantice su solvencia.

El establecimiento de procedimientos de gestión y control de riesgos debe abarcar la realización de los siguientes procesos:

1. Proceso de elaboración de un catálogo de riesgos.

   El proceso base de cualquier sistema de gestión de riesgos consiste en el trazado del mapa de riesgos de la entidad. Este mapa puede incluir únicamente riesgos operacionales o también riesgos reputacionales, estratégicos, de cumplimiento, de negocio, financieros, etc.

   Un procedimiento habitual para elaborar este catálogo consiste en ir identificando los riesgos por áreas de actividad y por procesos (o viceversa, en el que el centro es el proceso, con independencia de las áreas en particular que lideran o vertebran el mismo). A cada riesgo se le asignará una valoración inherente de impacto y probabilidad de ocurrencia. Se le asociarán una serie de controles que mitiguen dicho impacto y probabilidad de ocurrencia, con lo que se obtendrá la valoración residual. Dichas valoraciones servirán para hacer el seguimiento de la evolución del riesgo.

   Adicionalmente, pueden incluirse en el catálogo otros datos del riesgo, como las personas encargadas de ejecutar los distintos roles de control, los planes de acción asociados, indicadores clave de riesgo (KRI, por sus siglas en inglés), marcas de riesgo clave, etc.

2. Proceso de identificación y actualización anual de los riesgos.

   El procedimiento para la identificación y actualización de los riesgos, que debe involucrar a todas las áreas operativas y actividades de la entidad, consiste en revisar todos los riesgos identificados en el catálogo de riesgos, validando su vigencia, pudiendo redefinirse o eliminarse, y permitiendo, en su caso, la inclusión de nuevos riesgos.

   El gestor de riesgos debe dar el visto bueno a las modificaciones propuestas por las distintas áreas operativas, que serán seguidamente incorporadas al catálogo de riesgos. Dicho proceso incluye la actualización de procesos y actividades, riesgos, controles y planes de acción asociados. Adicionalmente pueden incorporarse los planes de acción que se estimen oportunos para asegurar que la entidad se ajusta al apetito de riesgo definido.

3. Proceso de evaluación periódica de riesgos.

   El procedimiento de valoración periódico, que involucra de nuevo a todas las áreas de la empresa y a sus actividades más relevantes, consiste en actualizar la valoración residual de los riesgos recogidos en el mapa y el grado de efectividad de sus controles. Se obtiene así un mapa actualizado del posible impacto en la gestión de los riesgos identificados.

   La periodicidad del proceso puede establecerse en función de la prioridad de las actividades que se estén controlando y de si se trata de actividades de negocio o de soporte.

   El gestor de riesgos debe ofrecer a las distintas áreas operativas la posibilidad de comunicar cambios en sus procesos, riesgos, controles y planes de acción o bien la realización de una nueva autoevaluación de los riesgos y controles ya existentes.

La operativa de ejecución de los tres procedimientos anteriores debe recogerse por escrito en un manual de procedimiento de gestión de riesgos.

4. Proceso de notificación de los riesgos.

   Los resultados de los procesos anteriores pueden divulgarse a las partes interesadas a través de informes que recojan el marco general de gestión de riesgos y control interno de la entidad, con una descripción de la metodología de valoración de riesgos y controles utilizados y el resultado anual de dicha valoración.

   La periodicidad de estos informes debe ser fijada en la política de gestión de riesgos, pudiendo ser distinta según la criticidad de los riesgos valorados. Es necesario, pues, que las actividades de gestión de riesgos sean transversales, abarcando todos los procesos e involucrando a las diferentes áreas operativas de la entidad.

En el **tercer apartado,** el documento centra de forma particular su atención en el papel que juega el gestor de riesgos en el **proceso ORSA,** al constituir esta evaluación interna de los riesgos y de la solvencia una herramienta indispensable sobre la que debe pivotar toda la gestión de riesgos de las entidades aseguradoras.

El proceso ORSA desempeña un papel esencial en la confección de la estrategia y en la planificación del negocio, ya que proporciona una visión global de los riesgos actuales y futuros a los que podría verse expuesta la entidad, así como el patrimonio libre del que la entidad debe disponer para hacer frente a las eventuales pérdidas que puedan acontecer en el horizonte temporal considerado.

Los gestores de riesgos y, en especial, el responsable de la función de gestión de riesgos, tienen un papel esencial en las distintas fases del proceso ORSA. El alcance de sus funciones debería recogerse de manera general en la política escrita del proceso, junto con los procedimientos y métodos de elaboración del análisis ORSA, las normas de calidad de los datos y la frecuencia de la evaluación.

Los resultados obtenidos tras la realización del proceso ORSA deben contrastarse con el apetito al riesgo de la entidad, de tal forma que, en caso de que vayan a superarse los umbrales de riesgo establecidos, se adopten las medidas de gestión previstas para cada caso concreto.

De acuerdo con lo dispuesto en la normativa de Solvencia II, el análisis ORSA debe incluir como mínimo:

(i) la determinación de las necesidades globales de solvencia de la entidad, teniendo en consideración todos los riesgos inherentes a su actividad con el propósito de facilitar la correcta toma de decisiones a corto y medio plazo en base a sus necesidades de capital económico;

(ii) la verificación del cumplimiento continuado de los requisitos de capital y en materia de provisiones técnicas;

(iii) la medida en la que el perfil de riesgo de la entidad se aparta de las hipótesis de cálculo del capital de solvencia obligatorio mediante la fórmula estándar.

El Informe ORSA debe ser presentado a la Alta Dirección y al Consejo de Administración de la entidad para su aprobación y ratificación. Debe ser enviado al supervisor (Dirección General de Seguros y Fondos de Pensiones) en las dos semanas siguientes a su conclusión (fecha coincidente con la aprobación del informe por el órgano de administración) y, a su vez, se recomienda que sea antes del 30 de junio del primer año proyectado en el mencionado informe. El Informe ORSA aprobado se pondrá también en conocimiento del personal clave de la entidad.

En el **cuarto apartado** de la Guía se desarrolla el papel del gestor de riesgos en **diversos aspectos incardinados dentro de la normativa de Solvencia II,** como su participación en el cálculo del capital de solvencia obligatorio y capital mínimo obligatorio, su rol en el cumplimiento de las obligaciones de información y transparencia recogidas en

el Pilar III de la norma, las particularidades de la función de gestión de riesgos en los grupos de entidades aseguradoras o el papel del gestor de riesgos en la externalización.

En el **quinto y último apartado,** dada la coyuntura actual que se está viviendo en todos las organizaciones a raíz de la pandemia provocada por la COVID-19, la Guía ha considerado esencial incorporar el papel de la gestión de riesgos en caso de contingencia grave, entendida esta como un evento inesperado que pueda constituir una amenaza para la continuidad de las operaciones. Sobre este aspecto resulta interesante analizar el rol del gestor de riesgos, tanto en las etapas previas a la contingencia como responsable de impulsar la aprobación de un **Plan de Continuidad de Negocio** en la organización, como durante la gestión de la propia contingencia en el momento que se produce y en un momento posterior, haciendo el seguimiento hasta la total recuperación de la normalidad en el desempeño de la actividad de la organización.