¿Cómo podemos identificar, gestionar y cuantificar el riesgo operacional en las empresas de seguros y reaseguros?

Por Isabel Casares San José-Martí
Economista y Actuario de Seguros

La identificación, gestión y cuantificación del riesgo operacional en las empresas de seguros y reaseguros es fundamental en el proceso de implementación de Solvencia II, ya que nos va a permitir evaluar la efectividad de los sistemas de control interno en las empresas. Para una eficaz gestión y cuantificación del riesgo operacional se necesita recopilar eventos históricos, tanto propios de las empresas como los datos del sector asegurador en el mayor periodo de tiempo que sea posible.

El riesgo operacional es el riesgo de pérdida derivado de la inadecuación o la disfunción de procesos internos, del personal o de los sistemas, o de sucesos externos, es decir, la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallos del personal, de la tecnología de información o eventos externos, en el que podemos incluir el riesgo legal, pero suele excluirse el riesgo estratégico y reputacional.

Las empresas de seguros y reaseguros, deben realizar una eficaz gestión del riesgo operacional al que se enfrentan, por lo que partimos por detallar los principales factores que originan el riesgo operacional:

1. **Procesos internos:** Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos, políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

2. **Personal**: Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, etc.

3. **Tecnología de información**: Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallos en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, etc.

4. **Eventos externos**: Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallos en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, etc.

Los eventos de pérdida por riesgo operacional con que nos encontramos en las empresas de seguros y reaseguros, son los siguientes:

a. **Fraude interno**.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

b. **Fraude externo**.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c. **Relaciones laborales y seguridad en el puesto de trabajo**.- Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de siniestros por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d. **Clientes, productos y prácticas empresariales**.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes, de la naturaleza o diseño de un producto.

e. **Daños a activos materiales**.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f. **Interrupción del negocio y fallos en los sistemas**.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g. **Ejecución, entrega y gestión de procesos**.- Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

A modo de ejemplo, se presenta un cuadro de los tipos de eventos de pérdida por riesgo operacional:

Tipo de evento (Nivel 1)	**Definición**	**Tipo de evento (Nivel 2)**	**Ejemplos**
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa.	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).
		Robo y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	Robo y fraude	Robo, falsificación.
		Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación.	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
		Higiene y seguridad en el trabajo	Casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores.
		Diversidad y discriminación	Todo tipo de discriminación.
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información

Tipo de evento (Nivel 1)	Definición	Tipo de evento (Nivel 2)	Ejemplos
	concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.		(conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.
		Prácticas empresariales o de mercado improcedentes	Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la empresa), lavado de dinero.
		Productos defectuosos	Defectos del producto (no autorizado, etc.), error de los modelos.
		Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes.
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento.
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos	Desastres y otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).
Interrupción del negocio y fallos en los sistemas	Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas	Sistemas	Pérdidas por fallos en equipos de hardware, software o telecomunicaciones; fallo en energía eléctrica.
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo.
		Seguimiento y presentación de informes	Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).
		Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos.

Tipo de evento (Nivel 1)	Definición	Tipo de evento (Nivel 2)	Ejemplos
		Gestión de cuentas de clientes	Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia.
		Contrapartes comerciales	Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.
		Distribuidores y proveedores	Subcontratación, litigios con proveedores.

La implementación de estrategias, políticas y procedimientos en las empresas de seguros y reaseguros respecto a la gestión del riesgo operacional es un requisito necesario para asegurar que cualquier empresa identifique, analice, trate y controle de una forma eficaz el riesgo operacional tanto de los riesgos propios como de los riesgos de los servicios externalizados.

Como ocurre para el resto de los riesgos, el Consejo de Administración de las empresas son los máximos responsables del cumplimiento de una eficaz gestión dinámica de los riesgos operacionales, asumiendo la responsabilidad de:

a) Definir la política general para la gestión del riesgo operacional.

b) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, a fin de contar con la infraestructura, metodología y personal apropiados.

c) Establecer un sistema de incentivos que fomente la adecuada gestión del riesgo operacional y que no favorezca la toma inapropiada de riesgos.

d) Aprobar el manual de gestión del riesgo operacional.

e) Conocer los principales riesgos operacionales afrontados por la entidad, estableciendo cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.

f) Establecer un sistema adecuado de delegación de facultades y de segregación de funciones a través de toda la organización.

g) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión del riesgo operacional, y que los principales riesgos identificados se encuentran bajo control dentro de los límites que han establecido.

El sistema de gestión de riesgos, evaluación interna de riesgos y solvencia, sistema de control interno y funciones del sistema de gobierno recoge la gestión eficaz del riesgo operacional.

La Unidad de Riesgos de las empresas de seguros y reaseguros deberá tener especialistas en gestión del riesgo operacional que cumplan al menos con las siguientes funciones:

a) Proponer políticas para la gestión del riesgo operacional.

b) Participar en el diseño y permanente actualización del manual de gestión del riesgo operacional.

c) Desarrollar la metodología para la gestión del riesgo operacional.

d) Apoyar y asistir a las demás unidades de la empresa para la aplicación de la metodología de gestión del riesgo operacional.

e) Evaluación del riesgo operacional, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.

f) Consolidación y desarrollo de reportes e informes sobre la gestión del riesgo operacional por proceso, o unidades de negocio y apoyo.

g) Identificación de las necesidades de capacitación y difusión para una adecuada gestión del riesgo operacional.

Las empresas deberán asignar recursos suficientes para la gestión del riesgo operacional, que les permita un adecuado cumplimiento de dichas funciones y asegurar una adecuada independencia entre el área que asuma las funciones de gestión del riesgo y aquellas otras unidades de negocio o de apoyo.

¿Qué metodología es la más adecuada para la gestión del riesgo operacional?

A priori, podemos decir que deben cumplirse, al menos, los siguientes criterios:

1. La metodología debe ser implementada en toda la empresa.

2. La empresa debe asignar recursos suficientes para aplicar su metodología en las principales líneas de negocio, y en los procesos de control y de apoyo.

3. La aplicación de la metodología debe estar integrada a los procesos de gestión de riesgos de la empresa.

4. Deben establecerse incentivos que permitan una mejora continua de la gestión del riesgo operacional.

5. La aplicación de la metodología de gestión del riesgo operacional debe estar adecuadamente documentada.

6. Deben establecerse procedimientos que permitan asegurar el cumplimiento de su metodología de gestión del riesgo operacional.

Para poder cuantificar el riesgo operacional, las empresas deberán contar con una base de datos de los eventos de pérdida por estos riesgos, destacando que un mismo evento puede tener como efecto una o más pérdidas, por lo cual las empresas deben tener capacidad de agrupar las pérdidas ocurridas por evento.

¿Cómo elaboramos la base de datos de eventos de riesgos operacionales?.

1. Debemos registrar los eventos de pérdida originados en toda la empresa, para lo cual se diseñarán políticas, procedimientos de captura, y formación al personal que interviene en el proceso.

2. Debemos definir y documentar criterios objetivos para asignar los eventos de pérdida a los tipos de evento y a las líneas de negocio.

3. Debemos definir un importe mínimo de pérdida a partir del cual se registrará un evento en la base de datos, un expediente físico o electrónico que contenga información adicional y que permita conocer el modo en que se produjo el evento, características especiales y otra información relevante, así como las acciones que hubiera tomado la empresa, incluyendo entre otras las mejoras o cambios requeridos en sus políticas o procedimientos.

Como parte de una eficaz gestión del riesgo operacional, las empresas deben:

- Implementar un **sistema de gestión de la continuidad del negocio** que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

- Implementar un **sistema de gestión de la seguridad de la información**, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Con el fin de gestionar los riesgos operacionales asociados a los **servicios externalizados**, las empresas deberán establecer políticas y procedimientos apropiados para evaluar, administrar y supervisar los procesos de los servicios externalizados considerando, al menos:

a) El proceso de selección del proveedor del servicio.

b) La elaboración del acuerdo de subcontratación.

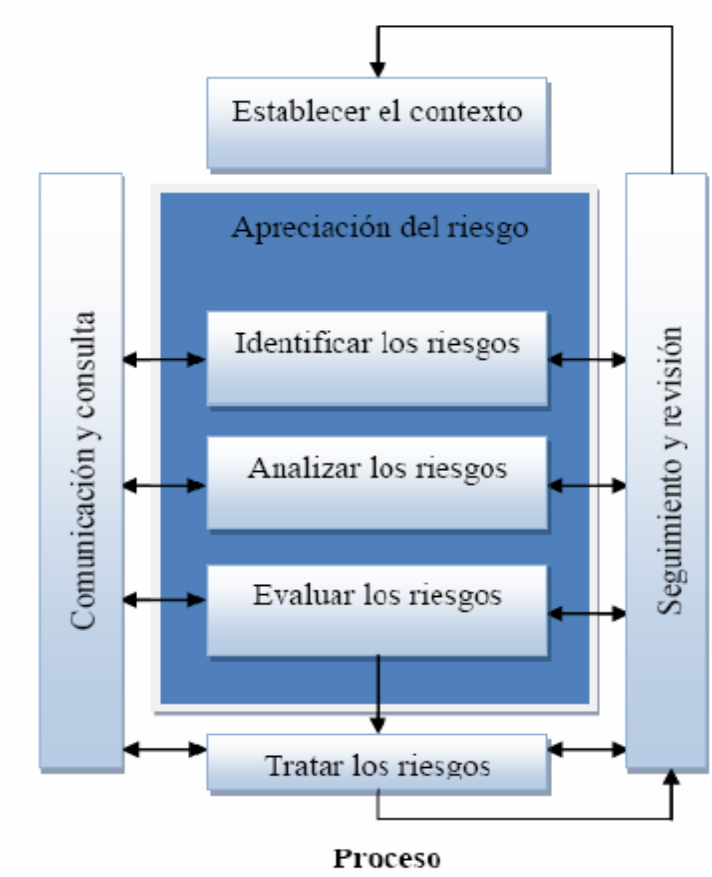
c) La gestión y supervisión de los riesgos asociados con el acuerdo de subcontratación.

d) La implementación de un entorno de control efectivo.

e) Establecimiento de planes de continuidad.

Los acuerdos de subcontratación deberán formalizarse mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, y definir claramente las responsabilidades del proveedor y de la empresa.

El proceso de la implementación de la gestión del riesgo operacional recoge las siguientes fases:



Proceso

Fase de identificación del riesgo: Consiste en determinar, según la clasificación de los riesgos operacionales, cuáles son riesgo existentes y cuál es su influencia en las actividades de la entidad. Para ello debemos conocer el origen de los riesgos, realizar un inventario de riesgos y analizar las causas de los eventos que los generan.

Fase del análisis y evaluación del riesgo: En esta fase, partimos de los datos históricos y de la opinión de expertos para construir un mapa de riesgos inherente (antes de controles) a través de una matriz de doble entrada: probabilidad o frecuencia e intensidad de ocurrencia por cada uno de los riesgos. Al incorporar los controles internos de la empresa, obtenemos el mapa de riesgos residuales mediante los indicadores de riesgo, *Key Risk Indicators* (KRI).

Fase de tratamiento del riesgo: Una vez implementado un sistema eficaz de riesgo operacional, los responsables de las líneas de negocio reportarán y validarán la información de riesgos a través de una infraestructura informática y los responsables del departamento de riesgos o auditoría interna realizarán una validación cruzada para determinar, fundamentalmente, la efectividad de los controles internos, externos y la monitorización de los planes de mitigación de riesgos.

A continuación, la empresa debe desarrollar planes de acción para el tratamiento de los riesgos y estos planes pueden ser: aceptar el riesgo, disminuir la probabilidad de ocurrencia, disminuir el impacto, transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo al nivel de tolerancia al riesgo definido.