Máster en Dirección Aseguradora Profesional

Curso académico 2015-2016

SOLVENCIA II
Y
CONTINUIDAD DE NEGOCIO

Alumno: Lionel Güitta Abellán

Tutor: Celedonio Villamayor Pozo

Índice

Objetivo

El objetivo del trabajo propuesto es analizar las implicaciones e impacto de los requerimientos del Reglamento de Ordenación, Supervisión y Solvencia de las Entidades Aseguradoras y Reaseguradoras (ROSSEAR) relativos a garantizar su continuidad operativa, proponiendo un modelo de sistema de gestión de la continuidad del negocio (SGCN) basado en el estándar internacional ISO 22301 que pueda ser llevado a la práctica por una entidad aseguradora.

El modelo de SGCN incluye el análisis de impacto en el negocio (base sobre la que se sustenta el diseño de las soluciones de recuperación de la actividad tras la activación del plan de continuidad de negocio) en el que se propone un método de estimación del impacto fundamentado en la correlación de los distintos tipos de impacto que se analizan.

1 Introducción

En el mundo actual las empresas se desarrollan en un entorno complejo, con múltiples dependencias e interconexiones con otras empresas, proporcionando productos o servicios o recibiendo productos o servicios. En este entorno complejo existen múltiples amenazas que, en caso de materializarse, podrían afectar a la supervivencia o viabilidad futura de la empresa que se vea afectada y con ella, en mayor o menos medida, verse afectados sus grupos de interés: empleados, clientes, proveedores, accionistas, inversores, etc.

En el caso de una empresa aseguradora, la materialización de una amenaza puede tener un efecto doble, ya que por una parte puede haberse visto afectada por el desastre pero por otra parte, sus clientes asegurados también pueden haberse visto afectados por el mismo desastre, por ejemplo un terremoto, y necesitan que la aseguradora que les ha convencido para asegurar sus bienes o proporcionarles unos determinados servicios cuando lo necesitasen, responda lo más adecuadamente posible en este tipo de situaciones.

Los planes de continuidad de negocio tratan de preparar a las empresas para hacer frente a un desastre de forma que puedan recuperar su actividad en un plazo determinado con un nivel mínimo y aceptable de calidad/servicio. Un paso en la evolución de un plan de continuidad de negocio (PCN) es el sistema de gestión de la continuidad del negocio (SGCN), que complementa el PCN añadiendo la política de continuidad de negocio, los objetivos relacionados con la continuidad y los procesos para conseguirlos.

El Estado es consciente de la importancia que tienen determinados sectores económicos en el mantenimiento de la sociedad y para ello trata de regular esas actividades económicas con el fin, entre otros, de garantizar, en la medida de lo posible, que esas empresas puedan hacer frente a situaciones adversas, tanto desde el punto de vista económico/financiero, como desde el punto de vista operacional. Así, a modo de ejemplo tenemos la Ley 8/2011, de 28 de abril, por la que se establecen medidas

para la protección de las infraestructuras críticas, que trata de mejorar la prevención, preparación y respuesta de las empresas y organismos estatales frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas.

El motivo que justifica la regulación del sector asegurador es que se trata de una actividad que gestiona los riesgos de gran parte de la sociedad, gestionándolos mediante un ciclo productivo inverso, el pago de la prima es por anticipado mientras que la indemnización o prestación es futura e incierta, ya que se producirá en el caso de que ocurra el siniestro. Por ello, la regulación aseguradora trata de garantizar que cuando ocurra el siniestro, la entidad aseguradora esté en situación de poder hacer frente a la indemnización. Esta garantía deberá cubrir tanto los aspectos que puedan afectar a la situación económico-financiera de la entidad aseguradora, como a aquellas situaciones que puedan afectar a su situación operativa.

En el sector asegurador, la garantía económico-financiera y la garantía operativa se establecen con la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (en adelante, LOSSEAR) y su desarrollo reglamentario, Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (en adelante ROSSEAR). Para el caso de la continuidad de las operaciones (garantía operativa), en el artículo 44.3 del ROSSEAR se establece:

> *Las entidades aseguradoras y reaseguradoras adoptarán medidas razonables para asegurar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de contingencia. A tal fin, las entidades emplearán sistemas, recursos y procedimientos adecuados y proporcionados.*

Adicionalmente a la buena práctica empresarial de disponer de un plan de continuidad de negocio, la legislación aseguradora a través del ROSSEAR, requiere que las aseguradoras garanticen la continuidad de sus actividades, de forma que no solo se garantice el hacer frente a situaciones que las puedan afectar financieramente (requerimientos de capital), sino que también deben poder hacer frente a situaciones que afecten a su operativa.

Respecto a la gestión de la continuidad de negocio se debe tener en cuenta que no es solo la recuperación de la actividad tras la ocurrencia de un desastre o la gestión de la crisis o la gestión de los riesgos a los que están expuestos los procesos de una entidad aseguradora, la gestión de la continuidad de negocio es una disciplina que cubre, entre otras, a todas las anteriores, dotándolas de una dimensión estratégica y que no debe

ser vista sólo como una forma de reaccionar ante unos eventos que afecten a la operativa normal de la entidad. La gestión de la continuidad de negocio puede actuar como un paraguas que permite englobar disciplinas tales como: gestión de riesgos, recuperación ante desastres, gestión de crisis, planes de emergencia, gestión de infraestructuras, seguridad, comunicación en situación de crisis, gestión de procesos,…

Es importante subrayar que el término gestión de continuidad de negocio no se refiere exclusivamente al ámbito tecnológico, a la recuperación de los sistemas informáticos afectados por una parada imprevista, este escenario es uno de los escenarios de los que se ocupa la continuidad de negocio, pero también lo son la no disponibilidad de un edificio de la entidad al verse afectado por un incendio o la pérdida del servicio proporcionado por un tercero debido a una huelga sectorial.

2 Legislación aseguradora

La legislación española en materia de seguros ha ido evolucionando de acuerdo a las necesidades del mercado, tratando de mantener un sector saneado y protegiendo a los clientes de las aseguradoras. Respecto a la protección del asegurado, veremos que es a partir de los años 80 del siglo XX cuando se trata de garantizar la solvencia de las aseguradoras con las exigencias de capitales de solvencia, con el objetivo de garantizar que la entidad pueda hacer frente a eventos inesperados.

La normativa gubernamental ha influido enormemente en la evolución de la actividad aseguradora privada, pudiendo decir que muy pocas actividades están tan condicionadas por las leyes como ésta, precisamente por su carácter social y preventivo. En este epígrafe se ofrece una reseña cronológica de normas que afectan al sector.

A continuación se expone un resumen histórico de la legislación aseguradora en España, junto a sus principales características.

Los antecedentes del Derecho del Seguro en España (y en Europa) se remontan al siglo XV con las Ordenanzas de los Magistrados de Barcelona en el Código de costumbres marítimas de Barcelona y sus ordenanzas sobre seguros marítimos de 17 de noviembre de 1458 (*llibre del consolat de mar (1300 -1400)* donde se introduce la figura del “bon home”, persona con práctica en el comercio y la navegación que por sus “…reconocidas pericia, solvencia moral y prudencia…” actuaran como árbitros para resolver diferencias en actos dudosos, dirimir disputas entre armadores, mercaderes y aseguradores y en la verificación y precisión de averías.

El Consulado de Burgos, durante el reinado de los Reyes Católicos, redactó varias Ordenanzas, entre las que destacan las Ordenanzas de seguros Marítimos, que exigían que el contrato se formalizara por escrito y establecían para los mercaderes la obligación de presentar "certificaciones y probanzas" de las averías sufridas, para la reclamación de las liquidaciones de seguros.

En los siglos XVI y siguientes se dictaron nuevas ordenanzas, destacando la de Felipe II que estuvieron en vigor hasta muy avanzado el siglo XIX. Al amparo de esas leyes se crearon los Montepíos de invalidez o vejez (precedentes de los seguros de vida), las Sociedades de Seguros Mutuos para protección de riesgos (incendios y/o las Mutualidades Aseguradoras de los Accidentes de Trabajo). Posteriormente, la regulación del Seguro apareció en el Código de Comercio de 1885.

Ley 97 de Registro y Vigilancia de entidades aseguradoras de 14 de mayo de 1908

El título completo de la ley, publicada el 15 de mayo de 1908: *Ley relativa a la inscripción, que al efecto se establece, de las Compañías, Sociedades, Asociaciones y, en general, todas las entidades que tengan por fin realizar operaciones de seguro*.

Esta Ley se centró en el control previo de la legalidad más que en los aspectos contractuales o técnicos. Regulaba las funciones de la Junta Consultiva de Seguros, órgano asesor y de audiencia pública. Este órgano sigue existiendo en la actualidad como órgano colegiado asesor del Ministerio de Economía y Competitividad en los asuntos relacionados con la ordenación, supervisión y solvencia de los seguros privados, planes y fondos de pensiones y mediación en seguros privados[1].

Ley de Ordenación de Seguros Privados de 16 de diciembre de 1954

Esta Ley modifica respecto a la anterior la verificación previa de la legalidad, ocupándose en este caso de la revisión de la documentación mercantil y técnica. Pero quizás uno de los elementos más intervencionistas fue el tener que someter a aprobación administrativa previa las pólizas y tarifas. Esto hace que el mercado asegurador español fuera muy regulado con poca posibilidad de desarrollo y con un peso reducido en la economía española. Debido a este control de productos y tarifas, la competencia es casi inexistente, además se encuentran malas prácticas en la gestión de las entidades sumadas a las limitaciones en la solidez financiera de las entidades aseguradoras. Estos problemas se manifestaron a lo largo de las crisis económicas de los años 70, cuando se detectaron problemas de solvencia patrimonial en el sector,

[1] Las funciones de este órgano se encuentran definidas en la página web de la Dirección General de Seguros y Fondos de Pensiones:
http://www.dgsfp.mineco.es/direccciongeneral/JuntaConsultiva/MenuJuntaConsultiva.asp

acompañados en algunas ocasiones de prácticas irregulares, que hicieron necesario sanear en profundidad al sector.

Ley 50/1980, de 8 de octubre, de Contrato de Seguro

Esta ley se encuentra actualmente vigente, derogando los artículos que aparecían en el Código de Comercio de 1885. En ella se estableció la regulación básica de los derechos y obligaciones de las partes de la relación contractual (aseguradora, asegurado, tomador, beneficiario), permitiendo que el supervisor pueda realizar una mejor valoración de los aspectos jurídicos del contrato de seguros.

La Ley 33/1984, de 2 de agosto, de Ordenación de Seguros Privados,

Esta Ley y su normativa de desarrollo tuvieron claramente definidos los objetivos y los mecanismos necesarios para llevar a cabo la reforma que permitiera la ordenación del mercado y mejorar el control de las entidades aseguradoras.

Por una parte la ordenación vino de la mano del fomento de la concentración empresarial y de la especialización, separando los negocios de vida y de no vida. Por otra parte, se reguló el principio de solvencia, orientándolo a los aspectos técnicos y financieros:

- mayor exigencia en las condiciones de acceso al mercado,
- mayor rigor en las garantías financieras (provisiones técnicas, margen de solvencia, fondo de garantía),
- dotación de un marco jurídico para actuar en los casos de entidades en dificultades,
- inclusión de mecanismos de expulsión del mercado para entidades que no cumplieran las obligaciones financieras mínimas para el desarrollo de la actividad

Real Decreto-Ley 10/1984, de 11 de julio, por el que se establecen medidas urgentes para el saneamiento del sector de seguros privados y para el reforzamiento del Organismo de Control.

El RDL 10/1984 creó la Comisión Liquidadora de Entidades Aseguradoras (CLEA) y se adoptaron medidas de urgencia para reforzar la actuación supervisora.

La CLEA permitió llevar a cabo el proceso de saneamiento del sector mediante la liquidación de un gran número de entidades en crisis.

A partir de este nuevo marco legal, se permitió una mayor internacionalización del sector, en primer lugar por la internacionalización de la regulación adoptando la normativa comunitaria, y en segundo lugar por la internacionalización del mercado, con la presencia de entidades extranjeras atraídas por las expectativas de crecimiento del sector asegurador español.

Ley 21/1990, de adaptación a la normativa comunitaria de la legislación de seguros privados

Introduce las directivas sobre el derecho de establecimiento en los seguros distintos del de vida y regula el nuevo régimen jurídico del Consorcio de Compensación de Seguros.

Ley 9/1992, de 30 de abril, de mediación en seguros privados

Esta Ley constituirá el equivalente reformador en el ámbito de la distribución de los seguros privados.

Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados

Su objetivo fundamental era lograr la integración de la actividad aseguradora española dentro del marco jurídico del Derecho Comunitario Europeo mediante la incorporación de la autorización administrativa única en todos los ramos de seguro.

Además esta Ley introdujo otras modificaciones normativas con el objeto de modernizar el sector:

- reforzando los mecanismos de protección del asegurado, mediante la posibilidad de la presentación de quejas y reclamaciones contra las entidades aseguradoras ante la Dirección General de Seguros y Fondos de Pensiones,
- ampliando la protección administrativa anterior a los terceros perjudicados en el ámbito del seguro de responsabilidad civil,
- introduciendo la figura del defensor del asegurado en las entidades,
- perfeccionando los mecanismos de protección del crédito que tienen los asegurados respecto a las entidades aseguradoras,
- fijando los aspectos a los que ha de ajustarse la tramitación de los procedimientos de autorización, modificación y revocación de la autorización administrativa, de disolución y liquidación de entidades aseguradoras, y de adopción de medidas de control especial.

Ley 44/2002, de medidas de reforma del sistema financiero

Una vez finalizada la función de saneamiento del sistema, suprimió la Comisión Liquidadora de Entidades Aseguradoras incorporando sus funciones al Consorcio de Compensación de Seguros.

Por otra parte, pretendió establecer un mecanismo reforzado de protección al cliente de servicios financieros mediante la imposición a todas las entidades financieras (entidades de crédito, de seguros y de valores) de la obligación de disponer de un departamento o servicio de atención al cliente,

Ley 34/2003, de modificación y adaptación a la normativa comunitaria de la legislación de seguros privados

La finalidad principal de esta Ley fue la transposición de un conjunto de directivas comunitarias que permitiese culminar la adaptación de nuestro ordenamiento jurídico al de la Unión Europea en esta materia.

Dentro de la transposición de normativa comunitaria, se lleva a cabo la referente a la liquidación de entidades aseguradoras y a las últimas directivas sobre el margen de solvencia. Las primeras directivas sobre seguros exigieron que las empresas de seguros mantuviesen un margen de solvencia, de cálculo simple, para amortiguar las posibles situaciones adversas de su actividad. Con esta solución de cálculo del margen de solvencia, aunque funcionaba correctamente, se detectaron ciertas debilidades en los aspectos sensibles desde el punto de vista del riesgo. A raíz de esto, las Directivas del 2002 establecieron nuevos requisitos para el margen de solvencia. Además de reforzar las exigencias cuantitativas, del fondo de garantía como al margen de solvencia obligatorio, se prevé también que en situaciones concretas en que se vean amenazados los derechos de los asegurados, las autoridades competentes estarán facultadas para intervenir con la suficiente antelación, incluso aun cuando no se haya producido todavía una situación de crisis. En tres pueden concretarse las medidas que a tales efectos prevén las directivas:

- la exigencia de un plan de recuperación financiera;
- la obligación a las empresas de seguros a tener un margen de solvencia obligatorio más alto que el reglamentario
- la revisión a la baja de los elementos que pueden integrar el margen de solvencia disponible.

Estas medidas incorporan por primera vez en la regulación comunitaria de seguros un enfoque dinámico y preventivo.

Ley 5/2005, sobre supervisión de los conglomerados financieros y por la que se modifican otras normas del sector financiero

Esta normativa, con origen en una directiva comunitaria de 2002/11, regula el tercer nivel de la supervisión financiera, adicional a la supervisión de entidades individuales y a la de los grupos financieros homogéneos (constituidos por entidades sólo de seguros, sólo de bancos o sólo de valores). El conglomerado financiero es aquel grupo empresarial constituido por varias entidades financieras en el que, al menos, una es necesariamente una entidad aseguradora y otra una entidad bancaria o de servicios de inversión.

2.1 Solvencia II

La continuación de esta evolución de la legislación aseguradora nos lleva a la trasposición de la Directiva 2009/138/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y reaseguro y su ejercicio (Solvencia II), que fue modificada fundamentalmente por la Directiva 2014/51/UE del Parlamento Europeo y del Consejo, en los aspectos relativos a los poderes de la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación – EIOPA -) y de la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados – ESMA -), llamada Ómnibus II.

Esta Directiva, Solvencia II es un ejercicio de armonización para facilitar el acceso y ejercicio de la actividad aseguradora y reaseguradora dela unión Europea, eliminando las principales diferencias entre las legislaciones de los estados miembros.

La Directiva Solvencia II trata la solvencia de las entidades aseguradoras y reaseguradoras basándose en tres pilares:

- **Pilar I:** En el que se definen los requisitos cuantitativos, estableciendo como deben valorarse los activos (valor de mercado), las reservas técnicas, el cálculo del capital de solvencia obligatorio y mínimo bien a través de la fórmula estándar o bien mediante un modelo interno desarrollado por la entidad que deberá ser previamente aprobado por la Dirección General de Seguros y Fondos de Pensiones. A diferencia de la anterior fórmula de cálculo del capital de solvencia,

en el que este valor se determinaba en función de las primas y los siniestros (seguros distinto del de vida) y de las provisiones matemáticas (seguros de vida), la nueva fórmula está basada en el riesgo asumido por la entidad, entrando en juego los distintos tipos de riesgos (y subriesgos asociados a cada uno de ellos).

- **Pilar II:** Establece las características del sistema de supervisión para la mejora de la gestión interna de los riesgos por parte de las entidades. En definitiva, define el sistema de gobernanza y el proceso de revisión del supervisor.
- **Pilar III:** Se centra en la divulgación de información sobre el nivel de solvencia y transparencia hacia el mercado de los riesgos asumidos y su forma de gestión.

La integración de todas estas Directivas Europeas se realiza con su trasposición a la legislación española en la **Ley20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (LOSSEAR)** y en su reglamento: **Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras (ROSSEAR).**

La parte central de este trabajo está centrada en el artículo 44 del ROSSEAR, que está englobado en el Pilar II, en el que se establece:

TÍTULO III

Ejercicio de la actividad

CAPÍTULO I

Sistema de gobierno de las entidades aseguradoras y reaseguradoras

Artículo 44. Requisitos generales del sistema de gobierno.

1. …

3. Las entidades aseguradoras y reaseguradoras adoptarán medidas razonables para asegurar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de contingencia. A tal fin, las entidades emplearán sistemas, recursos y procedimientos adecuados y proporcionados.

Este artículo determina claramente que las entidades aseguradoras y reaseguradoras deben contar con planes de continuidad de negocio que las permitan recuperar su actividad en caso de que un evento las pueda afectar. El desarrollo de estos planes de continuidad de negocio es el objeto de este trabajo.

3 Tipos de Riesgos

La gestión del riesgo es un aspecto inherente a cualquier actividad empresarial, más aún en el caso del sector asegurador, en el que la gestión del riesgo es su motivo de ser.

La gestión de los riesgos en las entidades aseguradoras y reaseguradoras (y en general del mundo empresarial) se debe extender más allá de los riesgos financieros y asegurables, para abarcar riesgos de tipo estratégico, de reputación, regulatorios, operacionales,…

De forma resumida, los riesgos a los que está expuesta una entidad aseguradora son los siguientes (“Gestión de riesgos en entidades aseguradoras”, Jesús Pérez):

- Riesgo de Suscripción: Vida, No vida.
- Riesgo Estratégico: Riesgo en la reputación, riesgo legal, riesgo de desastres (naturales, suspensión de los mercados), pérdida de competitividad, riesgos regulatorios (cambios regulatorios, lavado de dinero).
- Riesgo Operacional: Fallos en los sistemas, errores humanos, procedimientos inadecuados, controles inadecuados, fraude, error de modelo.
- Riesgos Financieros: Riesgo de crédito (riesgo de crédito directo, riesgo de liquidación), riesgo de liquidez (liquidez del mercado, liquidez individual), riesgo de mercado (riesgo de tipo de interés, riesgo de precio de los activos, riesgo de tipo de cambio)

Estos riesgos, a su vez podrían tener las siguientes consecuencias:

- Para las entidades financieras: pérdidas económicas, pérdida de oportunidades, mayor exigencia de capital, mayor coste de los fondos, daño a la reputación, pérdida de clientes, liquidación de la entidad,…
- Para el sistema financiero: Cierre/Nacionalización delas entidades, crisis generalizadas en el sistema financiero, inestabilidad económica, incremento del riesgo país,...

De cara a la cobertura y cálculo del capital de solvencia requerido, la Directiva de Solvencia II identifica los siguientes riesgos:

- Mercado; tipo de interés, acciones, inmobiliario, diferencial, tipo de cambio, concentración.
- Suscripción salud[2]: SLT (mortalidad, longevidad, invalidez y morbilidad, caída cartera, gastos, revisión), No SLT (primas y reservas, catastrófico).
- Crédito.
- Suscripción de vida: mortalidad, longevidad, invalidez y morbilidad, caída cartera, gastos, revisión, catastrófico.
- Suscripción no vida; primas y reservas, caída cartera, catastrófico.
- Activos intangibles.

Así, el cálculo del Capital de Solvencia Básico Requerido (BSCR) se realiza mediante la suma correlada de los 6 tipos de riesgos, los cuales, a su vez, se han calculado mediante las diferentes fórmulas definidas.

A este BSCR hay que realizarle unos ajustes, el primero de ellos es mediante el cálculo de la absorción de pérdidas derivadas de las provisiones técnicas y de los impuestos diferidos. Este cálculo se resta al BSCR, reduciendo la carga de capital requerido. También, en caso de que el asegurador disponga de fondos ring-fenced, podrá ajustar el BSCR reduciéndolo en función de la cuantía de esos fondos.

El último ajuste a realizar en el BSCR para la obtención del Capital de Solvencia Requerido (SCR) es la suma de la cuantía determinada por el **riesgo operacional**.

3.1 Riesgo Operacional

La definición de riesgo operacional es compleja ya que puede incluir eventos de muy diversa naturaleza y origen. La referencia que toma Solvencia II para la definición de este tipo de riesgo es la que se recoge por el Comité de Basilea en el “Nuevo acuerdo de capital” (junio 2004):

[2] Los riesgos de suscripción salud diferencia según el tipo de seguro si es tratado como vida (SLT) o como no vida (No SLT).

> "*El riesgo operacional se define como el riesgo de pérdida resultante de una falta de adecuación o fallo de los procesos, el personal y los sistemas internos o bien de acontecimientos externos*".

El artículo 13.33 de la Directiva de Solvencia II (Directiva 2009/138) lo define como:

> "*el riesgo de pérdida derivado de la inadecuación a de la disfunción de procesos internos, del personal o de los sistemas, o de sucesos externos*"

Y en el artículo 101.4, donde se indican los riesgos que cubrirá el capital de solvencia (incluyendo el riesgo operacional en el punto f), se finaliza especificando que:

> "*El riesgo operacional a que se refiere el párrafo primero letra f) incluirá los riesgos legales, pero no los riesgos derivados de decisiones estratégicas ni los riesgos de reputación*".

El motivo de estas exclusiones, es que este riesgo se incluye en el cálculo del capital requerido y dicho capital es difícil de determinar para estas categorías.

Como queda reflejado en la definición de riesgo operacional, se incluyen en el mismo cuatro categorías:

- Riesgo de procesos: pérdidas asociadas a errores en los procesos (controles, modelos, transacciones,…)
- Riesgo de personas: acciones intencionadas o fraudulentas o no intencionadas (errores, desinformación,…)
- Riesgo de sistemas: Caídas o malfuncionamiento de los sistemas informáticos, errores de programación, fallos de las comunicaciones de datos.
- Riesgos externos: eventos físicos ajenos a la entidad sobre los que no se tienen ningún control (incendios, inundaciones, terremotos, …)

Esta clasificación se basa en las causas, no en el efecto de las mismas. Como se puede observar, cualquiera de las causas puede provocar una parada de la actividad de la entidad, ya sea parada parcial o completa.

El Comité de Basilea categoriza los riesgos operacionales en tres niveles, los dos primeros determinan las categorías y subcategorías y el tercer nivel identifica ejemplos de actividades de cada subcategoría. Esta categorización también es la utilizada por el consorcio "Operational Risk Insurance Consortium" (ORIC) creado por la "Association of British Insurers" en 2005 para promover la recopilación de información de pérdidas

derivadas de riesgos operacionales. Esta categorización identifica en el primer nivel los 7 siguientes eventos:

- Fraude interno.
- Fraude externo.
- Prácticas de empleo y seguridad laboral.
- Clientes, productos y prácticas de negocio.
- Daños a activos físicos.
- Interrupción del negocio y fallos de sistemas.
- Ejecución, entrega y gestión de procesos.

De estas 7 categorías, un plan de continuidad de negocio es una solución para aquellos riesgos que se encuadren en “Daños a activos físicos” (edificios, instalaciones, etc.), en “Interrupción del negocio y fallos de sistemas” (por ejemplo, interrupción de los servicios tecnológicos) y proporciona soluciones para la ejecución, entrega y gestión de procesos en caso de que la entidad se vea afectada por un incidente disruptivo.

Como vamos a ver en siguientes capítulos, los planes de continuidad de negocio tratan de recuperar la operatividad de las actividades afectadas por el evento disruptivo en un plazo de tiempo que minore el impacto de la parada en la organización.

4 Estándares de Continuidad de Negocio

Es evidente que, cada vez más, las empresas se preocupan por cómo responder ante un posible desastre y cómo preparar las actividades (previas, durante y posteriores) para reanudar sus procesos de negocio en el caso de verse afectada por un incidente que los interrumpa.

Como hemos visto en el capítulo 3, en el sector asegurador español la LOSSEAR establece una cultura de gestión de riesgos (art. 66). Es necesario por tanto establecer un sistema de gestión de riesgos cuyo objetivo será mitigar o eliminar, entre otros, las consecuencias de materialización del riesgo operacional. También hemos visto que en el ROSSEAR (art. 44.3) se establece que las entidades aseguradoras y reaseguradoras deberán adoptar medidas razonables para asegurar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de contingencia.

¿Qué es un Plan de Continuidad de Negocio? En la norma UNE/ISO 22301:2012, se define un Plan de Continuidad de Negocio (PCN) como:

> "*Procedimientos documentados que conducen a las organizaciones a responder, recuperar, reanudar y restaurar el nivel de operación predefinido después de una interrupción*"

Añadiendo una nota en la que se especifica:

> "*Normalmente este plan cubre los recursos, los servicios y las actividades que se requieren para asegurar la continuidad de las funciones críticas del negocio*".

Podemos ver claramente que la definición de PCN de la norma UNE/ISO 22301, responde a lo requerido por el ROSSEAR a las entidades aseguradoras y reaseguradoras.

¿Qué se consigue con un Plan de Continuidad de Negocio? Además de que las entidades aseguradoras y reaseguradoras cumplan con lo que les requiere la legislación

que las aplica, el PCN prepara a la entidad para proporcionar una respuesta inmediata tras la ocurrencia de un evento que afecte a sus actividades. Esta respuesta está diseñada conforme a una serie de posibles escenarios, como veremos posteriormente, y en función de los recursos que se requieren para ejecutar los procesos.

Con un PCN, la entidad conseguirá:

- Aumentar su resiliencia[3], es decir, su capacidad para reanudar sus actividades ante situaciones adversas (contingencias, desastres).
- Disponer de unas soluciones y procedimientos estructurados y completos que le permitan desarrollar su recuperación de forma ordenada, evitando confusiones y situaciones de tensión.
- Proporcionar una respuesta rápida y adecuada a los incidentes imprevistos, reduciendo el impacto resultante de la interrupción de las operaciones.
- Priorizar los procesos y la disponibilidad de los recursos necesarios para su ejecución. Normalmente la priorización reducirá el tiempo de recuperación de las actividades de negocio, y consecuentemente, aminorará el impacto en el negocio causado por la interrupción. Se alinean los procesos del negocio y las actividades de recuperación ante riesgos y desastres.
- Realizar un análisis de riesgos con el fin de tratar de prevenir y/o mitigar las posibles amenazas que pudieran interrumpir la actividad de la entidad, con la implantación de medidas o controles.
- Aumenta el conocimiento de los procesos, permite una revisión en profundidad de las actividades de la entidad (reingenierías de procesos), en algunos casos obliga a que se formalicen los procesos o que se actualicen. Además se realiza una identificación proactiva de los impactos derivados de la interrupción operativa.
- Mejora la reputación corporativa, genera confianza en los empleados por saber que la empresa trata de estar preparada ante situaciones adversas,
- Supone una ventaja competitiva, demostrando que la entidad aseguradora puede seguir proporcionando sus servicios,
- Puede influir en la valoración del “rating” de la entidad,
- etc.

[3] Definición del término *resiliencia* en la norma UNE/ISO 22300:2012: “*Capacidad de adaptación de una organización en un entorno ambiental complejo y cambiante”*.

4.1 Evolución de los estándares de continuidad de negocio

Se han desarrollado diversos estándares y guías de buenas prácticas para el desarrollo de un PCN, tanto a nivel nacional como a nivel internacional. La evolución en esta materia ha dado lugar a la aparición de distintos alineamientos, buenas prácticas y estándares, que han permitido a las empresas centrarse en su aplicación más que en el desarrollo desde cero de los aspectos que deberían tener en cuenta. A continuación se realiza un repaso de los principales documentos publicados.

El primer trabajo formal dedicado a la materia de continuidad de negocio fue desarrollado por la "*National Fire Protection Asociation*" (NFPA) de Estados Unidos en 1995, mediante su guía NFPA 1600. El objetivo de este documento era proporcionar a los responsables de la gestión de los desastres, tanto de organismos del sector público como del sector privado, el conjunto fundamental de procesos para valorar, mitigar, preparar, responder y recuperarse de un desastre. Trata de establecer los requerimientos para implementar y mantener un plan de gestión de desastres. Esta guía se ha ido actualizando en versiones sucesivas, siendo la más actual la publicada en 2016.

La norma BS 7799 del "*British Standard Institute*" (BSI) también se publica en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información, en la que se tratan los aspectos de recuperación de los sistemas de información tras la interrupción de sus servicios. Posteriormente, en 2005, se publicó como estándar internacional ISO 27001, a partir de cual se desarrolló esta familia de estándares.

En 1997 el "*Disaster Recovery Institute International*" (DRII) publicó las Prácticas Profesionales para la gestión de continuidad del negocio, abarcando las siguientes áreas:

- Iniciación y Gestión del proyecto
- Evaluación y control de riesgo
- Análisis de impacto del negocio
- Estrategias de la Gestión de Continuidad del Negocio
- Respuesta a emergencias y operaciones
- Elaboración y Aplicación de planes de Continuidad de Negocio
- Sensibilización y capacitación del personal

- Ejercicio y mantenimiento de los planes de Continuidad del Negocio
- Comunicaciones en las crisis y Coordinación con agencias externas

En 2003 se publica la "*Publicly Available Specification*" (PAS) 56, promovida por el la organización británica "*Business Continuity Institute"* (BCI), que proporciona una guía para la Gestión de la Continuidad de Negocio y en la que se acuñó el término de proceso para la gestión de continuidad de negocio, los principios y terminología del sistema, y una variedad de recomendaciones para la prevención de incidentes. Tres años después, publicó un documento en el que describía el ciclo de vida de la continuidad de negocio.

En 2006 el "*British Standard Institute*" (BSI) publica la norma "BS 25999-1: Gestión de continuidad de negocio – Parte 1: Código de práctica", a la que le sigue en 2007 la norma "BS 25999-2: Gestión de continuidad de negocio – Parte 2: Especificación" que es el primer estándar internacional auditable y certificable, en el que se definieron los requisitos para un enfoque de los sistemas de gestión basado en buenas prácticas y se desarrollaron guías para la provisión de información y comunicación frente a la recuperación de desastres.

Aunque no se trate de un estándar propiamente dicho, el sector financiero, a través del "Bank for International Settlements" publicó en agosto de 2006 unos principios de alto nivel de continuidad de negocio basados en los requerimientos de Basilea II: "The Joint Forum. High-level principles for business continuity", en el que se establecían los 7 principios fundamentales para conseguir disponer de continuidad de negocio.

En 2009 la "*American National Standards Institute*" (ANSI) junto con la "*American Society for Industrial Security*" (ASIS) aprueba el documento "Organizational Resilience: Security, preparedness, and Continuity Management Systems-Requirements with Guidance for Use". En él se define un marco de gestión para el plan de acción y la toma de decisiones necesarias para anticipar, prevenir, en la medida de lo posible, prepararse y responder a un incidente disruptivo. Este estándar se diseña con el objetivo de ser integrado junto a otros sistemas de gestión: ISO 9001, ISO 14000, ISO 27000.

EL PAS 200, publicado en 2001, incluye una guía y las buenas prácticas para la gestión de crisis en las empresas y organizaciones independientemente del tamaño de la misma.

Incluido en la familia de estándares ISO 27000, en 2011 se publica el ISO 27031 en el que se detallan los principios de la tecnología de la información y comunicación sobre la continuidad de negocio.

ISO 22301 se aprueba y publica en 2012, reemplazando a la BS 25999-2 como estándar de continuidad de negocio. Las principales aportaciones de esta nueva normativa respecto al estándar británico son las siguientes:

- Es necesario tener un conocimiento de la organización para una correcta planificación de las actividades a realizar. El éxito de un Sistema de Gestión de Continuidad del Negocio se basa en una eficaz definición de objetivos, apoyados en una adecuada asignación de recursos tanto materiales como humanos.
- Identificación de las "partes interesadas", sus necesidades y objetivos, mantener una buena comunicación con ellos.
- Compromiso de la alta dirección en el desarrollo del Sistema de Gestión de la Continuidad del Negocio, mediante su supervisión, control, medición.
- Se describen requisitos específicos para las comunicaciones sobre incidentes, para el control de la gestión de las comunicaciones (internas y externas), así como los elementos utilizados para las comunicaciones.
- Se establecen nuevos requisitos de medición, evaluación y análisis de la eficacia del Sistema de Gestión de la Continuidad del Negocio.

4.2 Estándar ISO 223xx

Actualmente, en Europa el estándar de continuidad de negocio más comúnmente adoptado en las organizaciones es la familia de normas ISO 223xx (Protección y seguridad de los ciudadanos), cuyos principales documentos son:

- UNE-ISO 22300:2012, Terminología.
  Como indica el propio título, contiene los términos y definiciones aplicables a la protección de los ciudadanos, con el fin de saber específicamente a qué se está refiriendo esta familia de estándares.
- UNE-ISO 22301:2012, Sistema de Gestión de la Continuidad del Negocio (SGCN). Especificaciones.
  Especifica los requisitos para la implantación y la gestión de un Sistema de Gestión de la Continuidad de Negocio (SGCN), destacando la importancia del entendimiento de las necesidades de la organización, la implantación de controles y medidas para hacer frente a incidentes disruptivos, la supervisión y revisión del rendimiento del SGCN, y la mejora continua basada en mediciones objetivas. Este estándar sigue el modelo Plan-Do-Check-Act (PDCA, "planificar-hacer-comprobar-actuar")
- UNE-ISO 22313:2012, Sistema de Gestión de Continuidad de Negocio (SGCN). Directrices.
  Proporciona las directrices, recomendaciones y autorizaciones para el desarrollo e implantación del estándar UNE-ISO 22301.

- ISO 22317, Business continuity management systems. Business Impact Analysis
  Es una guía para desarrollar, implementar y mantener un proceso de análisis de impacto en el negocio consistente con los requerimientos determinados en el estándar ISO 22301.
- UNE-ISO 22320: 2011, Gestión de emergencias. Requisitos para la respuesta a incidentes.
  Determina los requisitos mínimos para proporcionar una respuesta eficaz a los incidentes, los requisitos básicos para el mando y control, la información operacional, la coordinación y cooperación del órgano de respuesta a incidentes.
- ISO 22398:2013, Societal security. Guidelines for exercises.
  Describe los elementos para una planificación, dirección y mejora del programa de pruebas de las soluciones de continuidad de negocio:
  - proporcionando la base para comprender, desarrollar e implementar un plan de pruebas de continuidad de negocio efectivo,
  - proporcionando una guía para la planificación y dirección de las pruebas,
  - mejorando la capacidad de la organización para dirigir las pruebas involucrando a terceras partes internas y externas,
  - permite, a través de las pruebas, mejorar de forma continua, en materia de continuidad de negocio, a la organización.

Aunque no son propiamente asociados a la materia de continuidad de negocio, los estándares de gestión de riesgos de la familia ISO 310xx suelen tener cabida en algunas de las fases del desarrollo del SGCN:

- UNE-ISO 31000:2009, Gestión del riesgo. Principios y directrices.
- UNE-EN 31010:2010, Gestión del riesgo. Técnicas de apreciación del riesgo

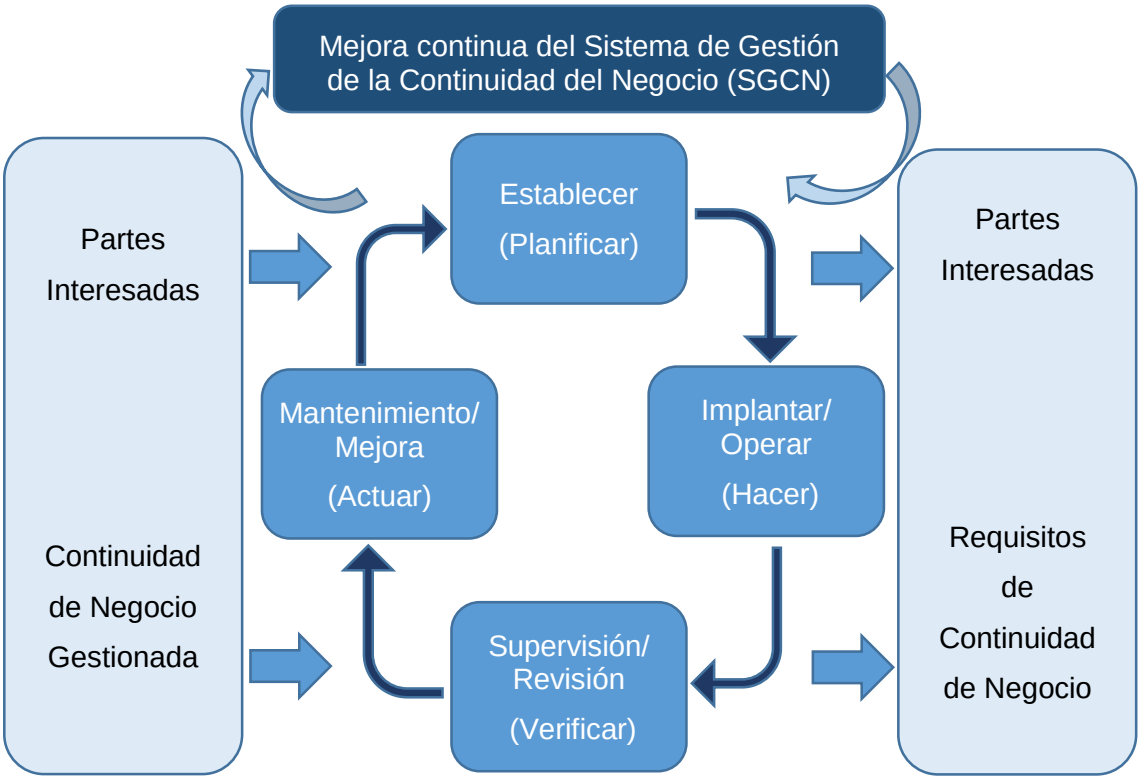
Complementariamente a los anteriores, dentro de los estándares internacionales de ISO para el desarrollo de un SGCN, centrándonos en la parte tecnológica de las entidades, también se suelen utilizar estos otros:

- ISO 27031: Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.
- ISO 27035: Information technology – Security techniques – information security incident management.

5 Desarrollo de la Continuidad del Negocio

Una vez visto el requerimiento legislativo y las alternativas que podemos utilizar para el desarrollo de la Continuidad de Negocio, a continuación se exponen los aspectos que deben tenerse en cuenta para el desarrollo y mantenimiento de la continuidad de negocio en una entidad aseguradora.

El estándar utilizado es la familia de la norma UNE-ISO 22300 descrita en el capítulo anterior. Este estándar aplica el modelo PDCA (Plan-Do-Check-Act, Planificar-Hacer, Verificar, Actuar), tal como se muestra en el siguiente esquema:



A cada una de estas fases del ciclo mostrado, le corresponden las siguientes acciones y procesos:

1. Establecer (Planificar): Establece la Política de Continuidad de Negocio, los objetivos, metas, controles, procesos y procedimientos necesarios para mejorar la continuidad del negocio.
2. Implantar y Operar (Hacer): Implantar y operar lo definido en la fase anterior: la política, los controles, los procesos y los procedimientos.
3. Supervisión y Revisión (Verificación): Supervisar y revisar el rendimiento según los objetivos y la política de continuidad de negocio, informar de los resultados a la dirección de la entidad para su revisión y determinar y autorizar las medidas para su corrección y mejora.
4. Mantenimiento y mejora (Actuar): Aplicar las medidas correctoras, basadas en la revisión de los resultados por la dirección y reevaluando el alcance del sistema de gestión, la política y los objetivos de continuidad de negocio.

Estas 4 fases se verán con mayor profundidad en los apartados de este capítulo.

Previo al inicio de los aspectos para desarrollar la continuidad de negocio, veamos algunos conceptos adicionales definidos en el estándar UNE-ISO 22301:

La **continuidad del negocio** es la "*capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo*" (UNE-ISO 22300).

La **gestión de la continuidad del negocio** (GCN) es el "*proceso de gestión holístico que identifica amenazas potenciales para la organización así como el impacto en las operaciones del negocio que tales amenazas, en caso de materialización, pueden causar, y que proporciona un marco para aumentar la capacidad de resistencia o resiliencia de la organización para dar una respuesta eficaz que salvaguarde los intereses de sus principales partes interesadas, la reputación, la marca y las actividades de creación de valor.*"

El **sistema de gestión de la continuidad del negocio** (SGCN), es la "*parte del sistema de gestión global que establece, implanta, opera, supervisa, revisa, mantiene y mejora la continuidad del negocio. El sistema de gestión incluye la estructura de la organización, las políticas, la planificación de actividades, las responsabilidades, los procedimientos, los procesos y los recursos.*"

Incluir la GCN en un sistema de gestión (SGCN) nos permite que ésta sea controlada, evaluada y mejorada de forma continua.

5.1 Establecer

Iniciamos el ciclo PDCA con esta fase: Establecer o planificar. El inicio de los trabajos que van a proporcionar a la entidad un sistema de gestión de continuidad de negocio (SGCN) viene determinado por el conocimiento propio de la entidad: el entorno en el que opera (geográfico, político, social, económico, etc.), sus intereses, organización interna (estructura organizativa, personal, etc.), requerimientos legales, productos y servicios, mapa de procesos/actividades, tecnología y cualquier otro aspecto que se considere necesario reflejar para tener la visión completa de la entidad.

Es necesario recopilar toda esta información para poder disponer de una base general que nos permitirá conocer a la entidad con el grado de profundidad adecuado. Para ello, una de las primeras tareas a desarrollar, si no se tiene ya en la entidad y que va a ser utilizada a lo largo de todo el proceso de desarrollo y gestión de la continuidad de negocio, es montar un sistema de gestión documental con una organización estructurada que permita crear, almacenar, custodiar, mantener actualizada, mantener el flujo de aprobación, consultar y compartir la documentación que se va a generar. Una de las características de la gestión de continuidad de negocio es que todas las actividades que se realizan se tratan de registrar, bien con documentos elaborados (política, objetivos, procedimientos, informes de pruebas, análisis de impacto en el negocio, valoración de riesgos, registros de pruebas, registro de incidentes, auditorías internas, etc.).

Deben identificarse y reflejarse en el SGCN los requerimientos legales a los que está obligada la entidad, legislación que afecte a las pólizas firmadas con clientes, relación con intermediadores en el caso de que los hubiera, legislación fiscal y/o contable, relaciones laborales, seguridad y salud en el trabajo, etc. Y por supuesto, como hemos estado viendo en este trabajo, la legislación que regula el negocio asegurador y reasegurador: Solvencia II.

Con la información recopilada y un conocimiento suficiente de la entidad, se debe determinar cuál va a ser el alcance del SGCN. El alcance puede definirse de varias maneras:

- limitar los trabajos a un entorno geográfico (país, región, ciudad, edificio, etc.) o a todas las ubicaciones donde haya presencia de la entidad;
- limitar los trabajos a unos servicios o productos (seguros de auto, seguros vida, seguros grandes riesgos, asistencia salud, etc.) o a todos los productos y servicios que comercialice la entidad;
- limitar los trabajos a una parte de la organización de la entidad, es decir a determinadas áreas o a determinados procesos (área de suscripción, área de atención al cliente, área de gestión de siniestros, área de tecnología, etc.) o como en las alternativas anteriores, a todas las áreas y procesos.

La solución ideal es no limitar el alcance del SGCN e incluir toda la entidad, desde el punto de vista geográfico, de productos y organizacional, sin embargo, el tamaño de la entidad o la complejidad de la misma, bien por la distribución geográfica, la cantidad de productos y servicios o la cantidad y tamaño de las áreas, pueden condicionar esta decisión, siendo aceptable iniciar los trabajos para construir el SGCN con una parte limitada de la entidad e ir posteriormente, dentro del proceso de mejora continua, ampliando ese alcance hasta cubrir la entidad completa.

En caso de que limitemos el alcance, es conveniente definir los criterios que se van a seguir para la priorización o planificación de ampliación del alcance. A modo de ejemplo, en el caso de que se decidiera desarrollar el SGCN ampliando el alcance progresivamente, uno de los criterios que se puede emplear es el volumen de pólizas generado por el país o la región, otro criterio puede ser la importancia de los servicios/productos (ejp.: la atención telefónica a clientes se considera más importante que la formación interna de los empleados).

Hay que recordar que debe quedar documentado el alcance del SGCN, reflejando en caso de que el alcance sea limitado, los motivos de esta limitación y las partes de la entidad que quedan fuera del alcance actual.

Tanto la información recopilada acerca de la entidad, como los requerimientos legislativos y el alcance del SGCN, formarán parte de la documentación a incluir en el sistema de gestión documental.

La primera condición para la implantación de un SGCN en una entidad es tener **el compromiso de la Dirección**. Tener un promotor del proyecto con suficiente influencia en la empresa facilita que la involucración decidida de todas las áreas que van a estar implicadas esté garantizada. En el caso de una entidad aseguradora, ese compromiso

debe estar garantizado por que es una demanda de la regulación actual, sin embargo, no está de más convencer a la Dirección de los beneficios de disponer de un SGCN bien desarrollado, algunos de estos beneficios ya se identificaron en el capítulo anterior, a los que habría que sumar los que el responsable de este tipo de proyectos identifique para la entidad en particular. A modo de ejemplo, una entidad aseguradora con un único centro telefónico de atención al cliente, podría detectar que este tipo de servicio es crítico para su supervivencia, ya que un desastre que dejara inoperativo este centro haría que se perdieran las llamadas de los clientes, lo que podría provocar un descrédito de la entidad ya que no es capaz de atenderlos además de una más que posible baja de la cartera de clientes por no recibir el servicio esperado cuando lo hubieran requerido. También es importante disponer del apoyo de la Alta Dirección ya que será necesaria la dotación de recursos para el desarrollo y mantenimiento del SGCN. Un SGCN se inicia como un proyecto, durante el que se analiza a la entidad, se diseñan soluciones, procedimientos a aplicar y planes para formar y probar. Una vez finalizado el proyecto, la gestión de la continuidad de negocio se convierte en un proceso más de la entidad, debiendo, a su vez disponer de recursos para este mantenimiento y actualización de soluciones, procedimientos, realización de pruebas, formación, etc.

El compromiso de la Dirección debe ser demostrable mediante el registro de evidencias. Algunas de estas evidencias se listan a continuación:

- la designación de responsable con funciones y responsabilidades asociadas a la gestión de la continuidad del negocio,
- asegurando la dotación de recursos suficientes para el desarrollo y mantenimiento del SGCN,
- la redacción, aprobación y difusión de la política de continuidad del negocio,
- la participación activa en las pruebas de los planes de continuidad de negocio.
- etc.

La **política de continuidad del negocio** debe desarrollarse con el objetivo de que sea adecuada a la entidad, proporcionando un marco para el desarrollo y mantenimiento actualizado de los aspectos relacionados con la continuidad del negocio e incluyendo los compromisos adquiridos por la Dirección.

Con el fin de que la continuidad del negocio se desarrolle y mantenga actualizada, la Dirección deberá determinar las **funciones y asignar esta responsabilidad**, que se debe asociar con una autoridad suficiente frente a todas las áreas de la entidad. Además de esta responsabilidad, también deberá informar a la Dirección de la situación y

rendimiento, por lo que tendrá que desarrollar procedimientos efectivos y eficaces para dar respuesta a posibles incidentes.

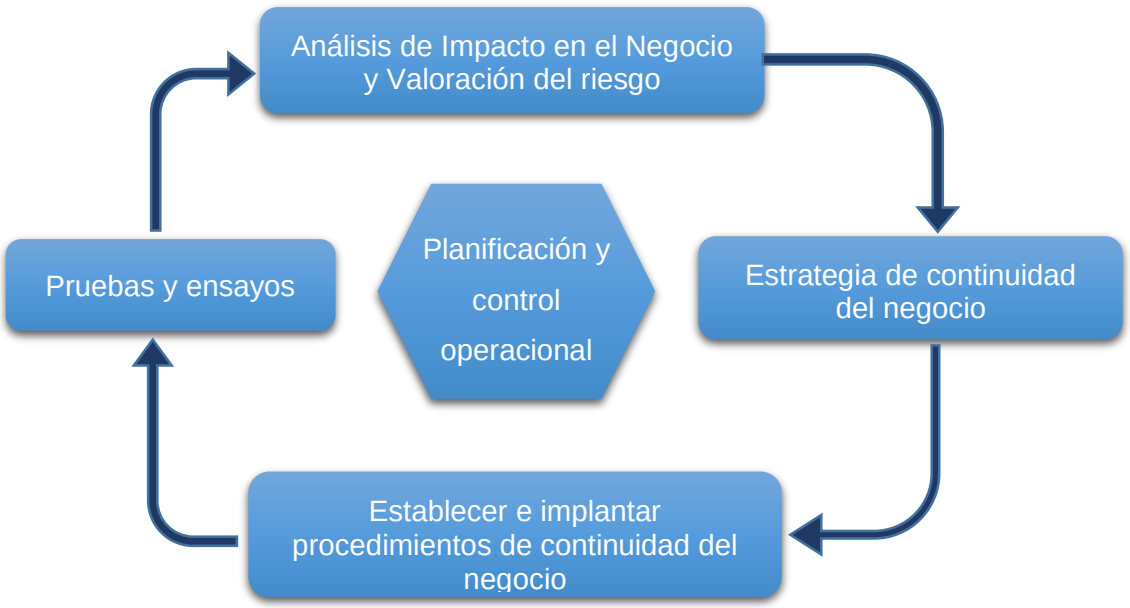
Una vez formalizada la organización que va a llevar el peso del desarrollo, implantación y mantenimiento del sistema de gestión de la continuidad de negocio, el primer trabajo de esta será determinar las acciones a llevar a cabo y los objetivos de este sistema de gestión, en definitiva, como cualquier proyecto de desarrollo e implantación, **planificar**.

Como en cualquier proyecto, para llevarlo a cabo será necesario contar con los **recursos** suficientes y adecuados: personas, tecnología, recursos económicos.

Las personas que estén asignadas al desarrollo y mantenimiento del SGCN deberán estar formadas adecuadamente. La formación técnica debe estar orientada, al menos, a las siguientes disciplinas: análisis de impactos en el negocio, valoración de riesgos, comunicación, gestión de incidentes, gestión de procesos y por supuesto, tener conocimientos del negocio asegurador/reasegurador.

5.2 Implantar y Operar.

Pasamos a la segunda fase del ciclo PDCA. La gestión de la continuidad de negocio comprende 5 elementos que se muestran en la siguiente figura:



La actividad central es la **planificación y control operacional**, es la actividad que va a controlar el resto de actividades, como en todo proyecto, la que realiza el control y coordinación.

6.2.1. *Análisis de Impacto en el Negocio y Valoración del Riesgo*

El **Análisis de Impacto en el Negocio**, es una de las principales tareas a acometer, ya que sobre los resultados de esta, se construye el resto de tareas. Su objetivo es permitir priorizar los procesos del negocio[4] en función del impacto que produce sobre él no poder realizarlas debido a una interrupción disruptiva. La clasificación de los procesos por la priorización nos permite identificar cuáles son los procesos/actividades que se deben recuperar en primer lugar, o sobre las que hay que centrar la atención en su recuperación, tras la ocurrencia de un desastre que afecte a la entidad aseguradora.

La priorización de los procesos se complementa con la determinación del tiempo de recuperación objetivo (*RTO: Recovery Time Objective*), que establece el tiempo en el que debe estar recuperado el proceso tras la ocurrencia del incidente disruptivo (al nivel de servicios que se haya predeterminado).

Es lógico pensar que en una entidad aseguradora, de forma general, los procesos prioritarios serán aquellos relacionados con la atención a los clientes y más concretamente aquellos relacionados con la gestión de siniestros o proporcionar un servicio necesario para atender a sus clientes, por ejemplo, envío de una grúa para asistencia en carretera porque nuestro cliente haya tenido una avería en su vehículo. A este apartado dedicaremos el capítulo siguiente, proponiendo un método para su realización.

Respecto a la segunda parte de este elemento, la **valoración del riesgo**, es algo intrínseco a la actividad aseguradora como ya hemos visto, se trata de identificar y cuantificar los riesgos asociados a los procesos prioritarios, así como las dependencias entre ellos, y las consecuencias potenciales de un incidente disruptivo.

[4] Se utiliza el término proceso como el "*conjunto de actividades interrelacionadas o interactivas que transforman las entradas en resultados"* (ISO 22301). Será la entidad la que deberá definir cuál es la definición que quiere dar a sus procesos de negocio.

6.2.2. *Estrategia de continuidad del negocio*

Una vez que disponemos de la priorización de procesos, se deben identificar soluciones que permitan la recuperación de la actividad dando respuesta a esa priorización, es decir, soluciones que posibiliten tener los recursos mínimos necesarios para reanudar la actividad.

Los elementos para poder ejecutar los procesos de negocio de una entidad se pueden concentrar en 4 grupos:

- Personas: los empleados que ejecutan los procesos de la entidad.
- Información, servicios de tecnología de la información y comunicaciones. En una entidad aseguradora/reaseguradora, la información y los datos están íntimamente relacionados con la tecnología de la información ya que lo habitual es que toda la información necesaria para la ejecución de los procesos esté informatizada.
- Edificios, infraestructura y servicios generales asociados. Los empleados que ejecutan los procesos y la infraestructura tecnológica asociada se ubica en edificios propiedad o no de la entidad. Estos edificios requieren de unas infraestructuras para poder "funcionar": suministro eléctrico, suministro de consumibles, etc.
- Proveedores de servicios. La entidad puede apoyarse en proveedores de servicios para la ejecución de sus procesos: consultorías, servicios de telemarketing, servicios de teleoperadores, etc.

La indisponibilidad de cualquiera de estos elementos, o de una combinación de ellos, provoca un escenario de indisponibilidad que puede derivar en una situación de crisis o incidente disruptivo o desastre. Las estrategias de continuidad de negocio deben proveer soluciones para hacer frente a cualquiera de estos escenarios de indisponibilidad

Las estrategias estarán orientadas a una o varias de las siguientes opciones:

a) Proteger los procesos prioritarios, mediante alguna de las siguientes soluciones o combinación de ellas:
    - la reducción de los riesgos asociados al proceso e identificados en la valoración de riesgos. Esta es una medida a implantar y ejecutar previamente a la declaración del desastre, introduciendo medidas mitigatorias tales como utilizar soluciones de alta disponibilidad en la

infraestructura tecnológica, de forma que, en caso de incidente en uno de los equipos, el proceso de negocio al que estén prestando servicio no se vea afectado.

- traspasando el proceso a un tercero, por ejemplo, desviando las llamadas de los clientes a un proveedor de servicios de atención telefónica, quien ya estaría proporcionando ese servicio aunque con un acuerdo de nivel de servicio inferior al que se solicite en el momento de la activación de la demanda motivada por el incidente disruptivo.
- suprimiendo el proceso, ya que, aunque todos los procesos son importantes para la entidad, en caso de que se produzca un incidente que afecte a la operativa, la entidad debe centrar los esfuerzos y recursos disponibles en recuperar los procesos prioritarios, lo que puede motivar la decisión de suprimir temporalmente los procesos menos prioritarios para dedicar sus recursos a los procesos prioritarios.

b) Estabilizar, continuar, reanudar y recuperar los procesos principales, mediante alguna de las siguientes alternativas o con una combinación de ellas (en cada una de ellas se añade un ejemplo):

- la reubicación de la ejecución de los procesos. En caso de que el centro de proceso de datos (CPD) donde se ubica la infraestructura tecnológica de la entidad se haya visto afectado por un desastre, la entidad podría haber tenido la precaución de disponer de un segundo CPD alternativo, en otra ubicación geográfica, para recuperar los servicios tecnológicos de la entidad.
- reubicación de los recursos. Si uno de los edificios de la entidad no está disponible (incendio, inundación, etc.), el personal que trabaja en ese centro puede desplazarse a uno o varios centros de trabajo adicionales que disponga la entidad o alquilar ese espacio necesario o haber montado previamente la infraestructura tecnológica y organizativa necesaria para que los empleados puedan realizar el trabajo desde sus domicilios.
- con procesos alternativos temporales, desarrollando soluciones que permitan proporcionar los servicios sin los recursos normalmente disponibles. El pago de la nómina mensual a los empleados, si no se ha podido completar el proceso por cualquier tipo de incidente, podría realizarse solicitando al banco (con todas las autorizaciones necesarias)

que repita la remesa de transferencias del mes anterior, posteriormente se regularizaría esta remesa (actualización de variables, empleados de baja, etc.).

- sustitución de recursos, incorporando perfiles profesionales que puedan acometer los procesos afectados. Normalmente, este tipo de estrategia se circunscribe a perfiles administrativos ya que los procesos técnicos de una entidad aseguradora requieren tener formación previa tanto del proceso en si como de cómo funciona internamente la entidad.

c) Mitigar y gestionar los impactos, estas estrategias están orientadas a lo que hay que prever tras la ocurrencia del desastre:
   - Disponer de un seguro, paradójico resultaría que una entidad aseguradora no esté asegurada: edificios, tecnología, etc. No obstante, no todo se puede asegurar: reputación o imagen de marca, conocimiento de las personas, etc.
   - Restaurar los bienes, los edificios afectados por una inundación deben ser limpiados, los equipos afectados por un incendio, reparados (cuadros eléctricos, generadores eléctricos, etc.)
   - Gestionar la reputación, es uno de los aspectos fundamentales de la gestión de crisis, es necesario desarrollar una estrategia de comunicación.

Para la toma de decisión de las estrategias a implantar se debe recabar la información necesaria para dimensionarlas adecuadamente, ya que la implantación de las estrategias requerirá de una inversión económica que deberá ser aprobada por la Dirección.

La estrategia de continuidad de negocio para hacer frente a un escenario de **indisponibilidad de personas**, requiere un análisis previo del número de personas necesarias para ejecutar cada proceso (cuantos puestos de trabajo serían necesarios en caso de reubicar las personas), los perfiles profesionales requeridos por cada proceso (suscriptores, actuarios, tecnólogos, etc.), incluso los conocimientos técnicos adicionales que disponen por si pudieran incorporarse en la estrategia de sustitución de recursos y ejecutar procesos que no están bajo su ámbito de responsabilidad normalmente.

Las soluciones de estrategias para un escenario de indisponibilidad de personas pueden ser: reorganización y reasignación de responsabilidades, contratación temporal, externalización de procesos, etc.

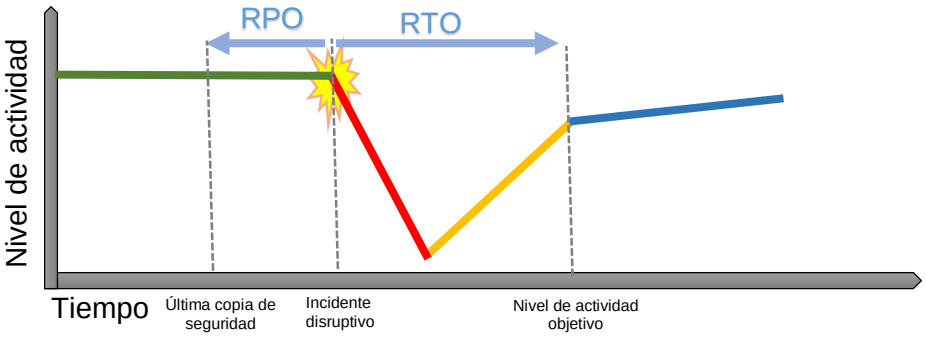
La definición de una estrategia para hacer frente a un escenario de **indisponibilidad de la tecnología** (información, servicios de tecnología de la información y comunicaciones) requiere disponer de información acerca de:

- los tipos de líneas de comunicaciones (voz, líneas dedicadas con terceros, conexiones públicas, radioenlaces, etc.) y su capacidad,
- inventario de los elementos de comunicación,
- inventario de las aplicaciones informáticas y asociarlas a los procesos de negocio a los que dan soporte,
- dependencias entre aplicaciones informáticas y/o servicios tecnológicos.
- inventario de los servidores en los que están funcionando las aplicaciones y donde se alojan las bases de datos y ficheros, así como las capacidades de estos servidores (almacenamiento local, capacidad de procesamiento, capacidad de enlaces de red, etc.), la capacidad.
- tipo de almacenamiento de información necesaria.

La información involucrada en la recuperación de la actividad, debe mantener las características de seguridad previas a la ocurrencia del incidente: confidencialidad (la información sólo es accedida por quien tiene los permisos necesarios), integridad (la información es fidedigna), disponibilidad (la información es accesible cuando se requiera), vigente (la información permite el buen funcionamiento de los procesos).

Cuando ocurre un incidente que obliga a la recuperación de la información, la disponibilidad se ve afectada por el RTO que, como ya se ha señalado anteriormente, será el tiempo para la recuperación del proceso, incluyendo la recuperación de la información. También se ve afectada la vigencia de la información, aunque para esta característica existe otro parámetro denominado “Punto de Recuperación Objetivo” (RPO*: Recovery Point Objective*), el cual determina la cantidad de pérdida de información asumible por la entidad debido a un desastre, Este parámetro nos va a determinar la frecuencia de realización de las copias de seguridad de la información, es decir, si el RPO de un proceso o de una aplicación es de 4 horas, el negocio puede asumir perder 4 horas de trabajo, bien porque lo puede recuperar por otros medios o bien porque asume sin más esa pérdida. Este RPO indica al área de tecnología que debe realizar copias de seguridad de la aplicación cada 4 horas (totales, incrementales,

diferenciales, etc.), de forma que, si en el peor de los casos la interrupción del negocio se produjera justo antes del inicio del proceso de las copias de seguridad, la última copia de seguridad, realizada 4 horas antes, cubriría el riesgo asumido por el negocio en cuanto a la pérdida de información. El término RPO es aplicable fundamentalmente al escenario de indisponibilidad de la tecnología, mientras que el término RTO es aplicable a cualquiera de los escenarios de indisponibilidad. El esquema siguiente muestra gráficamente ambos conceptos:



Las estrategias posibles a aplicar para un escenario de indisponibilidad de la tecnología pueden ser disponer de un CPD alternativo, propio o de un tercero, en modo "*Hot site*" (las aplicaciones y servicios se están ejecutando simultáneamente en ambos CPD Activo –Activo, o en caso de caída del CPD principal, entra inmediatamente en funcionamiento el CPD alternativo, Activo-Pasivo), "*Warm site*" (el CPD de respaldo cuenta con los equipos, información e infraestructura necesaria para la recuperación), "*Cold site*" (el CPD de respaldo sólo cuenta con la infraestructura).

La estrategia de **indisponibilidad de edificio** (edificios, infraestructura y servicios generales asociados) requiere información del número de personas a reubicar, de las necesidades de estas personas (puestos de trabajo, equipamiento, etc.), infraestructura de comunicaciones, suministro de consumibles, material de oficina, etc. También es conveniente conocer los requerimientos de suministros básicos que se requieren; suministro eléctrico mínimo, capacidad de las líneas de comunicaciones.

Además de proporcionar espacio de trabajo para las personas reubicadas, no hay que olvidar la necesidad de contar con un espacio para el equipo que gestiona la crisis.

Las soluciones para este tipo de indisponibilidad pueden ser reubicación en edificios de la propia entidad, alquiler de espacio e infraestructura durante la crisis hasta que esté de nuevo disponible el edificio original, complementar las soluciones anteriores con teletrabajo de una parte de los empleados.

Como en las anteriores estrategias, la determinación de la estrategia de **indisponibilidad de proveedores de servicios** requiere de información previa: servicios externalizados, nivel de servicio requerido al proveedor, número de proveedores que proporcionan el servicio, requerimientos para que el proveedor provea el servicio (tecnología, recursos materiales, etc.).

Previo a la contratación de un servicio externalizado, es una buena práctica seleccionar proveedores con capacidad para hacer frente a un desastre que les afecte, que tengan un plan de continuidad de negocio desarrollado. Para ello, debe incluirse en la valoración de los proveedores que opten a proporcionar un servicio, un parámetro que valore esta capacidad. Adicionalmente, se puede acordar un nivel de servicio determinado para la operación normal y prever una capacidad adicional del proveedor en caso de que la entidad lo requiera por haberse visto afectada por un incidente (indisponibilidad de edificio, de personas o de tecnología).

Además de la solución anterior, otras posibles soluciones para el diseño de la estrategia ante el escenario de indisponibilidad del proveedor, pueden ser las siguientes: diversificar los proveedores (tener más de un proveedor para el mismo servicio), asunción del servicio por parte de la entidad.

Tras la obtención de toda la información necesaria para los escenarios de indisponibilidad que pueden producirse en una entidad aseguradora, el equipo determinado para la gestión de la continuidad del negocio, deberá diseñar las soluciones que permitan recuperar la actividad, conforme a las capacidades identificadas y a los tiempos determinados en el análisis de impacto en el negocio de cada proceso incluido en el alcance del SGCN.

Las soluciones diseñadas deberán someterse a la aprobación de la Dirección ya que normalmente requerirán inversiones económicas para su implantación. Para ello, es recomendable proporcionar el diseño de más de una estrategia junto el coste estimado (coste de implantación, coste de mantenimiento, coste de activación) de cada una de ellas, así la Dirección podrá disponer de un parámetro adicional para la valoración de la decisión.

6.2.3. *Establecer e implantar procedimientos de continuidad del negocio*

Cuando se produce un incidente disruptivo la entidad debe estar preparada para darle respuesta efectiva y eficiente, para ello la entidad debe establecer una estructura de respuesta simple y que pueda ser activada rápidamente. En función del tamaño y complejidad de la entidad, esta estructura de respuesta puede ser escalonada con distintos niveles de equipos involucrados que actuarían de acuerdo a la gravedad y alcance del incidente.

Uno de los elementos a gestionar adecuadamente durante una crisis es la comunicación interna y externa. Tras la ocurrencia de un incidente, la información que permita valorar el incidente y la situación debe ser recibida por el equipo de respuesta, por lo que es necesario articular los procedimientos para realizar esta comunicación y las siguientes para actuar en función de la evolución. La comunicación externa podemos diferenciarla en dos vertientes, la primera de ellas la comunicación con los servicios de emergencia y la segunda la comunicación con los clientes, proveedores, etc.

La comunicación interna, también la podemos diferenciar en dos vertientes, por una parte la información que debe intercambiarse con las personas que están participando activamente en la gestión de crisis y la segunda vertiente, la información dirigida a los empleados de la entidad, proporcionándoles información de la situación y de las acciones que deban realizar.

Los planes de continuidad de negocio están compuestos por uno o varios documentos en los que deben estar definidos y desarrollados los siguientes aspectos:

- Las funciones y responsabilidades de todas las personas que participarán en los distintos procedimientos de recuperación de la actividad, estableciendo quien o quienes tienen la autoridad para la activación de los procedimientos y las circunstancias bajo las cuales se puede producir esta activación.
- La gestión del incidente, incluyendo el procedimiento para la activación y desactivación de los equipos de respuesta a incidentes, con el objetivo es que la respuesta que de la entidad sea efectiva. En este procedimiento deberá incluirse información acerca de: ubicación desde donde se va a gestionar el incidente (incluyendo una ubicación alternativa por si la ubicación principal se hubiera visto afectada), la información necesaria para poder valorar el incidente y realizar el

escalado y el seguimiento de la evolución del mismo, los medios necesarios para realizar las comunicaciones,

- Datos de contacto de los miembros del equipo de gestión de la respuesta a los incidentes, de organismos relacionados con el sector asegurador (Une spa, DGSFP), organismos relacionados con el sector financiero (CNMV, Ministerio de Economía y Competitividad), medios de comunicación (prensa, radio, televisión). Sin olvidar la presencia en redes sociales.
- La estrategia de comunicaciones con empleados, familiares, partes interesadas y medios de comunicación. Un aspecto clave en la estrategia de comunicación y que debe ser difundido a toda la entidad, es que sólo están autorizados a hacer declaraciones a los medios de comunicación o publicar en las redes sociales información relativa al incidente, las personas autorizadas expresamente para ello por la entidad.
- Procedimientos para la reanudación de la actividad de negocio, especificando bajo qué circunstancias debe aplicarse el procedimiento, la prioridad de las actividades a reanudar, el tiempo determinado para su reanudación, el nivel de servicio a alcanzar, los recursos necesarios: personas, perfiles, elementos tecnológicos necesarios (sistemas de tecnología de información y comunicaciones), etc.
- Procedimientos para la recuperación de los sistemas de tecnología de la información y comunicaciones. Son un caso especial de recuperación de la actividad, que puede aplicarse en la misma situación de gestión del desastre que la recuperación de las actividades de negocio o, como hemos visto, ser un escenario de indisponibilidad por sí mismo. Las aplicaciones informáticas y la infraestructura tecnológica que las soporta llevan asociados los tiempos de recuperación (RTO) de los procesos que las utilizan, esta característica determina como deben estar configurados todos los elementos tecnológicos para no rebasar esos tiempos objetivos (implantando elementos que garanticen alta disponibilidad, teniendo reservada la infraestructura para la recuperación, etc.). La generalidad determina que a menor tiempo de recuperación, el coste de la estrategia de recuperación es mayor, aspecto a tener en cuenta de cara a implantar medidas de recuperación proporcionadas, ya que en el caso más absurdo podríamos implantar medidas de recuperación cuyo coste superaran el coste estimado de los impactos.

Incluidos en estos procedimientos de recuperación de la tecnología, se deben describir las acciones para la comprobación de la integridad de la información. Supongamos dos sistemas de información, el primero gestiona las pólizas de un ramo y el segundo gestiona los siniestros, es evidente que ambos sistemas estarán interconectados, tras recuperar ambos sistemas, el usuario no debería encontrarse situaciones tales como que hubiera un siniestro asociado a una póliza que no estuviera dada de alta en el primer sistema que gestiona las pólizas. Esta situación extrema podría ocurrir si las copias de seguridad de ambos sistemas que se han utilizado para recuperar los sistemas de información se realizaron en distintos instantes de tiempo.

- Procedimientos para la vuelta a la normalidad. Una vez estabilizada la situación, la operativa del negocio debe volver a la situación previa al incidente disruptivo, habrá que deshacer de forma ordenada todas las acciones realizadas para reanudar la actividad. Estos procedimientos son complejos y dependen de la gravedad del incidente, si el desastre hubiera afectado al edificio donde se desarrolla el negocio, podríamos estar valorando tener que reconstruir el edificio afectado, para lo cual habrá que reservar fondos económicos o utilizar la póliza de seguro del edificio, hasta realizar una limpieza del mismo porque sólo se ha visto afectado por el humo de un incendio. Sin olvidar la comunicación a las partes interesadas: empleados, clientes, accionistas, proveedores, reguladores, etc.

6.2.4. *Pruebas de procedimientos*

La mayoría del trabajo realizado para construir el sistema de gestión de la continuidad de negocio: la planificación, el análisis de los procesos, el diseño de las estrategias, el desarrollo de los procedimientos para recuperar la actividad, etc. Se quedaría en nada si no se comprueba su eficacia mediante la realización de pruebas que identifiquen los aspectos de mejora.

Una entidad puede decir que dispone de un plan de continuidad de negocio cuando lo tiene desarrollado, difundido a lo largo de la organización y PROBADO.

Determinar un plan de pruebas ayuda a desarrollar las pruebas de forma sistemática permitiendo controlar y ampliar paulatinamente el alcance de las mismas garantizando que en un periodo de tiempo la entidad tenga la confianza suficiente de que los procedimientos y soluciones de continuidad del negocio funcionan adecuadamente.

La realización de las pruebas permite a la entidad:

- Formar, entrenar y generar confianza en el personal en la respuesta a los incidentes y en la realización de las actividades que permiten reanudar la actividad.
- Evaluar las capacidades individuales y de la entidad, midiendo el grado de conocimiento del personal de los procedimientos.
- Estimar los tiempos “reales” de recuperación de la actividad.
- Determinar si las estrategias de recuperación y los recursos estimados son suficientes.
- Comprobar que los procedimientos desarrollados son adecuados y detectar posibles áreas de mejora.

Tras la realización de las pruebas, se debe redactar un informe con la descripción del escenario simulado, los participantes, recursos implicados (tecnología, proveedores, edificios, etc.), los objetivos de la prueba, los eventos simulados, las acciones ejecutadas, los tiempos de recuperación de las actividades, los resultados obtenidos.

Además el informe se completará con un análisis de los resultados obtenidos frente a los objetivos iniciales y un plan de acción que identifique las acciones de mejora con los responsables de las tareas identificadas y el calendario para su realización.

5.3 Supervisar y Revisar

La tercera fase del ciclo PDCA del SGCN: Verificar y evaluar el rendimiento del SGCN, la protección de los procesos prioritarios, las evidencias de los trabajos realizados y de que estén adecuadamente documentados.

El SGCN debe ser evaluado periódicamente para comprobar los siguientes aspectos:

- La política de continuidad del negocio, las estrategias y procedimientos reflejan los objetivos de la entidad;
- Las estrategias de continuidad de negocio y sus procedimientos contemplan todos los servicios esenciales y sus procesos asociados, están actualizadas, son eficaces para la reanudación de las actividades y son comunicados al personal;
- Las personas están formadas para responder adecuadamente a un incidente.
- Existen y están implantados eficazmente programas de mantenimiento, pruebas y procesos de control de cambios.

Complementariamente a las evaluaciones planificadas, tras la ocurrencia de un incidente debería valorarse la respuesta proporcionada: causa del incidente, eficacia de la respuesta, capacidad de la entidad para hacer frente al incidente, analizar el impacto real frente al impacto estimado en los análisis.

Otro tipo de valoraciones que deberían planificarse son las auditorías, internas o externas, para garantizar que el SGCN se desarrolla, implanta y opera conforme a los propios requisitos de la entidad. Los resultados de las auditorías formarían parten de las acciones correctoras que deberán entrar en el ciclo de mejora continua del SGCN.

Además de las valoraciones y evaluaciones anteriores, hay determinados aspectos que pueden motivar la necesidad de revisar el SGCN, como pueden ser nuevos requisitos reguladores (Solvencia II), experiencia adquirida en incidentes, evolución tecnológica, evolución del propio negocio asegurador de la entidad aseguradora (nuevos productos, cambios en alcance geográfico, etc.)

5.4 Mantener y mejorar

La última fase del ciclo PDCA: Actuar. Los resultados de las revisiones realizadas y los resultados obtenidos en las pruebas y en los incidentes gestionados reales nos dan una visión de los aspectos a mejorar en el SGCN.

La entidad debe desarrollar los procedimientos que garanticen que no cumplir un requisito, el incumplimiento de la planificación y las debilidades asociadas al SGCN se identifiquen y comuniquen adecuadamente para solventarlas con las acciones correctoras necesarias.

Las acciones correctoras deberán tener asignadas quien es la persona o equipo responsable de su aplicación y su planificación. Todos los cambios relacionados con estas acciones correctoras deben quedar registrados en el SGCN.

Además de las acciones correctoras, también se pueden identificar acciones para la mejora del SGCN. La implantación de ambos tipos de acciones, correctoras para cubrir deficiencias y de mejora que aportan un nivel superior de eficacia, evidencian el compromiso de la entidad con la mejora continua, que es otra característica de este sistema de gestión.

6 Análisis de Impacto en el Negocio

El objetivo del análisis de impacto en el negocio (BIA por sus siglas en inglés: Business Impact Analysis) es priorizar los procesos analizados en función del impacto que suponga para la entidad su paralización por un incidente disruptivo.

Las ventajas de realizar un BIA son las siguientes:

- Identifica las relaciones entre productos, procesos y recursos requeridos para la actividad de la entidad.
- Recopila y proporciona información de la entidad que puede servir para abordar un proyecto de mejora de la eficiencia de los procesos.
- Permite diseñar las estrategias de recuperación de la actividad que minoren el impacto y con los costes adecuados a los recursos necesarios.
- Complementariamente al objetivo de priorizar los procesos, sirve para determinar el orden de la actividades a realizar para reanudar los procesos.

El proceso para la realización del BIA se puede dividir en las siguientes etapas:

a) Definición del BIA: En esta primera etapa la entidad debe determinar que clases de impactos quiere incorporar en el método de cálculo de la criticidad de los procesos, de forma que a mayor criticidad del proceso mayor impacto y, por tanto, mayor priorización del mismo. El objetivo secundario de este trabajo, como se indica en el capítulo Objetivo, es proponer un método de cálculo del impacto, este método de cálculo se desarrolla en el siguiente apartado de este capítulo.

   A continuación se muestran algunos tipos de impacto que pueden incluirse en el método de cálculo de la criticidad, teniendo en cuenta que en la tercera etapa, toma de información de negocio, las personas seleccionadas deberán aportar información acerca de los tipos de impacto que se seleccionen:

   - Financiero/Económico: Pérdidas económicas

- Legal/Regulatorio: Incumplimiento de la legislación/regulación que afecte a la entidad aseguradora
- Reputación: Imagen negativa de la entidad
- Estratégico: Incumplimiento de los objetivos estratégicos de la entidad
- Externo: Afectación a clientes o terceras partes

Para cada uno de los tipos de impactos que se incorporen al método de cálculo se deben definir criterios de valoración así como criterios temporales para la valoración de los impactos.

b) Toma de Información preliminar: Definidos los aspectos internos del BIA en la etapa anterior, se debe disponer del organigrama de la entidad y obtener el mapa de procesos o inventario de procesos con las personas responsables de cada uno de ellos, ya que normalmente serán las que aporten información de los recursos necesarios para ejecutar el proceso y valorar los impactos de acuerdo a los criterios de valoración previamente definidos.

El modo de recopilación de la información de cada proceso se realiza normalmente a través de un formulario, el cual puede ser completado de forma individual por cada responsable de procesos, de forma colectiva mediante talleres de trabajo o una mediante combinación de ambas.

El formulario debe recoger información de los procesos relativa a los flujos de entrada y salida de información, formato de la información de entrada y salida, recursos necesarios para ejecutar el proceso (recursos humanos, tecnológicos, aplicaciones informáticas, registros vitales, etc.) y, como parte fundamental de la información recogida de cada proceso, la valoración de los tipos de impacto que haya determinado la entidad.

Antes de la toma de información de negocio, es conveniente convocar una sesión de formación a los responsables, exponiendo el motivo de la toma de datos y presentando el formulario que van a completar.

c) Toma de información de negocio: Tras la sesión formativa, los responsables completan los formularios conforme al método determinado previamente (talleres, individualmente, combinación de ambas).

d) Consolidación y Análisis: Se consolida toda la información recibida en los formularios, se procesa (ver método de valoración de impactos en el siguiente apartado) y se analizan los resultados obtenidos del impacto de cada proceso derivado de su parada debida a un incidente disruptivo, calculado en función de la valoración de los tipos de impactos. El análisis puede detectar alguna incoherencia en los valores de impactos

que deberá ser comprobada con los responsables por si esta se debiera a algún error en la toma de información.

e) Aprobación de resultados: Una vez analizados y revisados los resultados, el orden de priorización debe ser aprobados por el Comité de Dirección de la entidad ya que debe ser conocedor de que en caso de activación del plan de continuidad de negocio, ese será el orden que se seguirá para reanudar la actividad.

Una vez aprobado el orden de priorización y con los datos que ya se recogieron de los recursos necesarios para la ejecución de cada proceso, se pueden diseñar las estrategias de recuperación.

6.1 Método valoración de impactos

El valor de impacto que se va a calcular es un número sin unidades de medida, no es una medida económica, no es una medida de las primas perdidas, no es una medida de siniestros sin atender,…es un valor que nos permitirá comparar los procesos analizados y poder priorizarlos cuando haya que reanudarlos tras un desastre o incidente disruptivo.

Previo al inicio del método, se deben concretar algunos términos:

a) Tipos de impactos: qué tipos de impacto van a incluirse en el cálculo del impacto de los procesos. En la descripción de la etapa de la definición del BIA se proponían los siguientes: Financiero/Económico, Legal/Regulatorio, Reputación, Estratégico, Externo; para el ejemplo de cálculo serán los que se utilizarán.

b) La valoración de los impactos evolucionan normalmente de forma creciente con el tiempo de parada del proceso. Para reflejar esta evolución, cada tipo de impacto debe valorarse en función del tiempo de parada, por lo que hay que definir intervalos de tiempo a valorar. Estos intervalos de tiempo podrán ser los mismos que se utilicen posteriormente para asignar los RTO de cada proceso. Para el ejemplo de cálculo que se va a realizar, se utilizarán los siguientes intervalos temporales:
    - 0h < t <= 6h: impacto que se produce desde la ocurrencia del incidente hasta las 6 horas.
    - 6h < t <= 12h: impacto que se produce desde la ocurrencia del incidente hasta las 12 horas.
    - 12h < t <= 24h: impacto que se produce desde la ocurrencia del incidente hasta las 24 horas.

- 24h < t <= 48h: impacto que se produce desde la ocurrencia del incidente hasta las 48 horas.
- 48h < t <= 96h: impacto que se produce desde la ocurrencia del incidente hasta las 96 horas.
- t > 96h: impacto que se produce pasadas 96 horas desde la ocurrencia del incidente.

Estos intervalos de tiempo podrán ser los mismos que se utilicen posteriormente para asignar los RTO de cada proceso.

c) Criterios de valoración de los tipos de impacto: Para que las valoraciones realizadas por los distintos responsables sigan un criterio homogéneo es necesario determinar los criterios de valoración. Los tipos de impacto se pueden valorar de forma cuantitativa o de forma cualitativa. Los tipos de impacto propuestos se valoran de forma cualitativa, excepto el Financiero/Económico en el que podemos proporcionar el criterio de valoración del impacto por la cantidad de euros que se pierden o dejan de ganar. Se definen 5 valoraciones de criterios para cada tipo de impacto: Muy Bajo, Bajo, Medio, Alto, Muy Alto, a cada uno de estos criterios se le asigna una cuantificación numérica (Muy bajo = 1; Bajo = 2; Medio = 3; Alto = 4; Muy Alto = 5).
Por último, queda determinar a que corresponde cada valoración de criterio para cada tipo de impacto, ejemplos de criterios:
   - Tipo impacto Económico:
     - Muy Bajo: el impacto económico es inferior a 100.000€
     - Bajo: el impacto económico es inferior a 250.000€
     - Medio: el impacto económico es inferior a 750.000€
     - Alto: el impacto económico es inferior a 2.000.000€
     - Muy Alto: el impacto económico es superior a 10.000.000€
   - Tipo impacto Legal:
     - Muy Bajo: Los posibles incumplimientos no generarían apenas consecuencias.
     - Bajo: Podría afectar a alguna normativa o cláusula contractual, pero serían fácilmente subsanables y tendrían una escasa repercusión
     - Medio: Provocarían incumplimientos legales o contractuales que podrían ser subsanados con dificultades y en un espacio temporal medio (3-6 meses).

- Alto: Implicaría el incumplimiento de las obligaciones legales y contractuales que podrían ocasionar penalizaciones o sanciones, incluyendo denuncias de contratos.
- Muy Alto: Implicaría el incumplimiento de obligaciones legales y contractuales que podrían provocar pérdida de licencias o contratos actuales y futuros.

- Tipo impacto Estratégico:
  - Muy Bajo: El cumplimiento de los objetivos estratégicos se ve comprometido en menos de un 5%, aunque con ligero esfuerzo en dedicación/recursos se puede revertir la situación.
  - Bajo: El cumplimiento de los objetivos estratégicos se ve comprometido en menos de un 5%, requiriendo un esfuerzo importante en dedicación/recursos se puede revertir la situación.
  - Medio: El cumplimiento de los objetivos estratégicos se ve comprometido entre un 5% y un 10%, requiriendo un esfuerzo importante en dedicación/recursos se puede revertir la situación.
  - Alto: El cumplimiento de los objetivos estratégicos se ve comprometido entre un 10% y un 15% sin posibilidad de recuperación antes del plazo de cumplimiento de los objetivos.
  - Muy Alto: El cumplimiento de los objetivos estratégicos se ve comprometido en más de un 15%.
- Tipo impacto Externo:
  - Muy Bajo: Cierto grado de malestar en los clientes.
  - Bajo: Provocaría un incremento cuantitativo de reclamaciones de clientes actuales o potenciales, sin otro tipo de repercusiones.
  - Medio: Podría provocar cancelaciones o anulaciones de pólizas o pérdidas de futuras contrataciones.
  - Alto: Provocaría un incremento en las cancelaciones o anulaciones de pólizas o bien una pérdida de futuras contrataciones.
  - Muy Alto: Provocaría la cancelación o anulación masiva de pólizas o bien la pérdida masiva de nuevas contrataciones.
- Tipo impacto Reputación:
  - Muy Bajo: Tendría consecuencias mínimas para la reputación, afectaría exclusivamente a la percepción de los empleados.

- Bajo: Podría afectar a algún grupo de interés tal como proveedores o empleados, pero no en la organización, ni en sus clientes, en socios estratégicos, ni en la sociedad.
- Medio: Podría tener consecuencias moderadas afectando únicamente a la propia organización y sus empleados y proveedores, pero no al resto de grupos de interés.
- Alto: Tendría consecuencias graves que impactarían en la mayor parte de los grupos de interés: En la propia organización, clientes, empleados, proveedores, aunque no en los socios estratégicos, ni en la sociedad.
- Muy Alto: Tendría consecuencias catastróficas para la reputación de la entidad, impactaría en todos los grupos de interés, clientes, empleados, proveedores, socios estratégicos y sociedad en general

Una vez definidos todos los elementos necesarios para la valoración del impacto, pasamos a la formulación matemática del método propuesto.

Para el cálculo del valor del impacto asociado a cada tipo de impacto se realiza el sumatorio de los productos del valor asignado al intervalo por la cuantificación realizada al valor del criterio seleccionado:

$$VTI(I) = \sum_{i} (10^{Valoración_i} \times Intervalo_i)$$

Siendo:

- VTI = Valoración del Tipo de Impacto
- I = Tipo de impacto a valorar
- i = número del intervalo de tiempo
- Valoración = Valor del impacto determinado por el responsable
- Intervalo = Valor asignado al intervalo (V), de acuerdo a la siguiente tabla:

INTERVALO					V		INTERVALO					V
0h	<	t	<=	6h	32		24h	<	t	<=	48h	4
6h	<	t	<=	12h	16		48h	<	t	<=	96h	2
12h	<	t	<=	24h	8		96h	<	t			1

Así, siguiendo con un ejemplo de valoración del tipo de impacto financiero, si el responsable de uno de los procesos analizados hubiera proporcionado la siguiente información:

Tipo impacto	Intervalos temporales					
	0h<t<=6h	6h<t<=12h	12h<t<=24h	24h<t<=48h	48h<t<=96h	t>96h
Financiero	--	Muy Bajo	Muy Bajo	Medio	Medio	Alto
Significado criterio	Sin impacto	<100.000€	<100.000€	<750.000€	<750.000€	<2.000.000€
Valoración intervalo	0	1	1	3	3	4

$$VTI\ (Financiero) = \ 10^0\ x\ 32 + \ 10^1\ x\ 16 + 10^1\ x\ 8 + \ 10^3\ x\ 4 + \ 10^3\ x\ 2 + \ 10^4\ x\ 1$$

$$VTI\ (Financiero) = \ 32 + \ 160 + 80 + \ 4.000 + \ 2.000 + \ 10.000 = 16.272$$

El intervalo de valores que puede tomar cualquier VTI es: 63 <= VTI <= 6.300.000, recordemos que este valor no tiene unidades.

Este cálculo se realiza con el resto de tipos de impactos que se están midiendo, la siguiente tabla muestra el resto de información proporcionada por el responsable:

Tipo impacto	Intervalos temporales					
	0h<t<=6h	6h<t<=12h	12h<t<=24h	24h<t<=48h	48h<t<=96h	t>96h
Financiero	--	Muy Bajo	Muy Bajo	Medio	Medio	Alto
Legal	--	--	--	Bajo	Bajo	Medio
Estratégico	--	--	--	--	--	Bajo
Externo	Bajo	Bajo	Medio	Medio	Alto	Muy Alto
Reputación	--	Bajo	Bajo	Medio	Medio	Alto

$$VTI\ (Legal) = 10^0\ x\ 32 + 10^0\ x\ 16 + 10^0\ x\ 8 + 10^2\ x\ 4 + 10^2\ x\ 2 + 10^3\ x\ 1 = 1.656$$

$$VTI\ (Estratégico) = 10^0\ x\ 32 + 10^0\ x\ 16 + 10^0\ x\ 8 + 10^0\ x\ 4 + 10^0\ x\ 2 + 10^1\ x\ 1 = 72$$

$$VTI\ (Externo) = 10^2\ x\ 32 + 10^2\ x\ 16 + 10^3\ x\ 8 + 10^3\ x\ 4 + 10^4\ x\ 2 + 10^5\ x\ 1 = 136.800$$

$$VTI\ (Reputación) = 10^0\ x\ 32 + 10^2\ x\ 16 + 10^2\ x\ 8 + 10^3\ x\ 4 + 10^3\ x\ 2 + 10^4\ x\ 1 = 18.432$$

Con el fin de que la presentación de los resultados de los valores de impacto de todos los procesos sea más comprensible, se realiza un cambio de escala de los VTI, de forma que los valores de los tipos de impactos que se presentarían al Comité de Dirección de la entidad, se ubiquen en un rango de 0 a 5. Como la fórmula de los VTI no es lineal, hay que determinar la fórmula de escalado para cada intervalo, identificando los límites de cada intervalo por el valor que tendría el VTI si las valoraciones a lo largo de todos los intervalos temporales fueran constantes:

Intervalos temporales						
0h<t<=6h	**6h<t<=12h**	**12h<t<=24h**	**24h<t<=48h**	**48h<t<=96h**	**t>96h**	**VTI**
--	--	--	--	--	--	63
Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo	630
Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	6.300
Medio	Medio	Medio	Medio	Medio	Medio	63.000
Alto	Alto	Alto	Alto	Alto	Alto	630.000
Muy Alto	Muy Alto	Muy Alto	Muy Alto	Muy Alto	Muy Alto	6.300.000

- 63 <= VTI < 630 → 0 <= VTIe < 1
- 630 <= VTI < 6.300 → 1 <= VTIe < 2
- 6.300 <= VTI < 63.000 → 2 <= VTIe < 3

- 63.000 <= VTI < 630.000 → 3 <= VTIe < 4
- 630.000 <= VTI <= 6.300.000 → 4 <= VTIe <= 5

La fórmula general para realizar el escalado sería:

$$VTIe = \frac{VTI - vtim}{vtiM - vtim} + vtiem$$

Siendo:

- VTIe = Valor Tipo de Impacto Escalado
- VTI = Valor Tipo Impacto
- vtim = valor mínimo del intervalo al que corresponde VTI
- vtiM = valor máximo del intervalo al que corresponde VTI
- vtiem = valor mínimo del intervalo al que corresponde VTIe

Para el ejemplo que se está siguiendo:

$$VTIe(Financiero) = \frac{16.272 - 6.300}{63.000 - 6.300} + 2 = 2{,}176$$

$$VTIe(Legal) = \frac{1.656 - 630}{6.300 - 630} + 1 = 1{,}181$$

$$VTIe(Estratégico) = \frac{72 - 63}{630 - 63} + 0 = 0{,}016$$

$$VTIe(Externo) = \frac{136.800 - 63.000}{630.000 - 63.000} + 3 = 3{,}130$$

$$VTIe(Reputación) = \frac{18.432 - 6.300}{63.000 - 6.300} + 2 = 2{,}214$$

Una vez calculados los valores escalados para cada tipo de impacto, hay que calcular el Valor del Impacto asociado al proceso que se está valorando, para ello se realiza la suma correlada de los valores de los VTI. Utilizando la siguiente matriz de correlación, basada en la experiencia:

McorrVI	Financiero	Legal	Estratégico	Externo	Reputación
Financiero	1	0,5	0,75	0,5	0,5
Legal	0,5	1	0,25	0,25	0,5
Estratégico	0,75	0,25	1	0,1	0,25
Externo	0,5	0,25	0,1	1	0,75
Reputación	0,5	0,5	0,25	0,75	1

$$VI\ (P) = \sqrt{\overrightarrow{VTIe}\ x\ MCorrVI\ x\ \overrightarrow{VTIe^T}}$$

Siendo:

- VI = Valoración del Impacto
- P = Proceso que se está valorando
- VTIe = Vector de valoraciones de tipo de impacto escalado del proceso P
- MCorrVI = Matriz de correlación de tipos de impacto

Aplicando la fórmula al ejemplo:

$$VI\ (P) = \sqrt{(2{,}176 \quad \ldots \quad 2{,}214)\ x \begin{pmatrix} 1 & \cdots & 0{,}5 \\ \vdots & \ddots & \vdots \\ 0{,}5 & \cdots & 1 \end{pmatrix} x\ (2{,}176 \quad \ldots \quad 2{,}214)^T} = 7{,}069$$

Los valores de la matriz de correlación determinan que los valores de VI se encuentran en el intervalo: 0 <= VI <= 18,507 (valor obtenido con el vector VTIe = (5, 5, 5, 5, 5)).

Este valor VI asociado a cada proceso es el que utilizamos para priorizar el orden de recuperación, objetivo del BIA.

Por último, quedaría asignar los RTO al proceso. Los RTO están asociados a la priorización y para ser más eficientes en el diseño de las estrategias de recuperación e incluso durante la propia recuperación de la actividad, los procesos se agrupan por intervalos de recuperación. Lo más habitual es que los intervalos de recuperación se definan con los mismos valores que los intervalos temporales utilizados para valorar los impactos. La asignación de cada proceso al RTO que le corresponda se realiza dividiendo el valor máximo posible del VI, en nuestro ejemplo 18,507, entre el número de intervalos definidos, en nuestro caso 6 (0h < t <= 6h; 6h < t <= 12h; 12h < t <= 24h; 24h < t <= 48h; 48h < t <= 96h; t > 96h): 3,084, de forma que podemos construir la tabla de asignación de RTO en función del VI como sigue:

VI mínimo	VI Máximo	RTO
0	3,084	<= 6h
3,084	6,169	<= 12h
6,169	9,253	<= 24h
9,253	12,338	<= 48h
12,338	15,422	<= 96h
15,422	18,507	>96h

Este proceso de valoración del impacto se sigue con el resto de procesos, construyendo la lista ordenada por el VI obtenido y el RTO asignado. Esta lista es el resultado del BIA que, junto a los recursos necesarios para poder realizar los procesos constituyen la entrada para la siguiente etapa, el diseño de las estrategias de recuperación.

7 Conclusiones

La evolución de la legislación aseguradora muestra una tendencia hacia la protección del cliente frente a la aseguradora. Esto se debe a:

- Normalmente se trata de un contrato de adhesión, por el que el cliente acepta un contrato redactado por la aseguradora.
- Algunos tipos de contrato se firman a largo plazo, seguros de vida, y se trata de garantizar la prestación firmada por ambas partes.
- Se trata de un ciclo productivo inverso, el cliente paga por anticipado la posible prestación, sin tener certeza de que vaya a tener que recibirla o recibirla a largo plazo como se ha indicado anteriormente.
- El cliente, normalmente tiene menos conocimientos para y menos medios para enfrentarse a una aseguradora en caso de que hubiera diferencias respecto a la prestación recibida.
- Tratar de evitar que una mala gestión de la entidad aseguradora afecte a las prestaciones contratadas por los clientes.
- La entidad aseguradora debe poder hacer frente a eventos no esperados o con poca probabilidad de ocurrencia que afecten a sus compromisos adquiridos.

La legislación actual se ha orientado a la gestión de riesgos financieros, tratando de garantizar que la entidad aseguradora podrá cumplir con las obligaciones contraídas con sus clientes disponiendo de capital suficiente que le permita hacer frente a situaciones extraordinarias e imprevistas. Se ha introducido el concepto de riesgo operacional, desde un punto de vista financiero ya que interviene en el cálculo del capital de solvencia requerido (Solvency Capital Requirement) y también desde el punto de vista de garantizar la continuidad de su operativa, aunque en este último aspecto parece que no se ha entrado en tanto detalle o exigencia como en otros sectores (Basilea II en el sector bancario o protección de infraestructuras críticas).

En materia de continuidad de negocio, hasta el momento en España la Dirección General de Seguros y Fondos de Pensiones (DGSFP), no ha tenido un papel tan intervencionista como se ha podido observar en países de América Latina donde las aseguradoras deben presentar información de detalle de sus planes de continuidad de negocio, como por ejemplo, los resultados de su análisis de impacto en el negocio incorporando el modo de realización del mismo. Esta exigencia puede estar fundamentada en que en esta zona geográfica las catástrofes naturales, terremotos, tienen mayor probabilidad de ocurrencia y, en línea con la necesidad de protección de los clientes, el regulador quiere constatar que las entidades aseguradoras están suficientemente preparadas para recuperar su actividad y poder prestar los servicios y prestaciones a sus clientes.

También ha evolucionado la continuidad de negocio, la sociedad ha ido madurando en este aspecto a consecuencia de los desastres a los que ha tenido que enfrentarse, adoptando nuevos términos: recuperación del CPD (Centro de Proceso de Datos), recuperación ante desastres, contingencia informática, planes de continuidad del negocio, gestión de la continuidad del negocio, resiliencia. Todos ellos orientados a devolver la normalidad en las actividades de negocio, cada uno de ellos más completo que el anterior, abarcando un alcance mayor dentro de las organizaciones. La continuidad de negocio ha pasado de ser un aspecto que se contemplaba exclusivamente en las tecnologías de la información a ser una materia que abarca a todas las áreas de la entidad. Las entidades y los reguladores comprenden que la continuidad de negocio es un proceso holístico, que debe ser gestionado de forma continua, siendo esta característica la base por la que los planes de continuidad de negocio evolucionan a sistemas de gestión de continuidad de negocio, comportándose como un proceso transversal que abarca toda la entidad.

Esta evolución ha tenido su reflejo en la publicación de las distintas guías y estándares, las cuales han ido contemplando además de los propios aspectos para recuperar la actividad, hacerlo de forma eficiente mediante actividades previas a la ocurrencia de incidentes: análisis de impacto en el negocio, análisis de riesgos, diseño de estrategias de recuperación, preparación de procedimientos; e identificando claramente los aspectos a gestionar durante la situación de crisis: acciones a realizar, comunicación interna y externa, recursos necesarios, etc.

El desarrollo de un sistema para la gestión de la continuidad del negocio requiere de unos factores mínimos para garantizar el éxito en su despliegue e implantación: el compromiso de la Alta Dirección de la entidad, la formación de un equipo cualificado y con la autoridad suficiente dentro de la entidad para impulsar su desarrollo y mantenimiento, dotar de los recursos suficientes y proporcionados para garantizar que las soluciones diseñadas se implanten y, como en cualquier proyecto, realizar una buena planificación.

Cada vez con mayor frecuencia es común que las auditorías financieras soliciten información acerca de la disponibilidad de un plan de continuidad de negocio, apareciendo como "hecho observado" si no se dispone de él. Lo mismo ocurre con auditorías de control interno y, desde hace bastantes años, en las auditorías de tecnologías de la información, aunque en este último caso, centrándose específicamente en la disponibilidad de un plan de contingencia informática, el cual debe estar sustentado en un análisis de impacto en el negocio que permita establecer la priorización en la reanudación de las aplicaciones informáticas.

La base sobre la que se sustentan los planes de continuidad de negocio es el análisis de impacto en el negocio, a partir de los resultados obtenidos en esta etapa, se diseñan las estrategias de recuperación y los procedimientos para la reanudación de la actividad, sin olvidar las necesidades de comunicación.

El cálculo del impacto debe tener en cuenta los distintos tipos de impacto que pueden afectar a la entidad y, además, su evolución con el tiempo de parada de los procesos. Lo normal es que el impacto vaya creciendo según transcurre el tiempo de parada de los procesos.

El desarrollo del sistema de gestión de la continuidad del negocio no puede quedarse en la fase de análisis y diseño, no puede quedarse en papel. Lo diseñado debe implantarse en la realidad, contar con un centro alternativo o proporcionar accesos remotos a los sistemas de información o diversificar los proveedores de servicios o … las estrategias de recuperación diseñadas deben implantarse, pero no solo eso, también deben probarse, pero no solo eso, también debe formarse al personal de la entidad para que sepa cómo actuar en caso de activación del plan de continuidad de negocio, pero no solo eso, también debe mantenerse actualizado ya que las entidades cambian, cambia la organización, los responsables, los sistemas de información, los productos,

los servicios,… todos estos cambios afectan en mayor o menor medida al sistema de gestión de la continuidad del negocio.

Por último para finalizar este trabajo, señalar que una entidad puede decir que cuenta con un plan de continuidad de negocio cuando lo ha desarrollado, implantado y probado con éxito.

8 Bibliografía

ÁLVAREZ CAMIÑA, Sergio. "*La regulación de los seguros privados: objetivos, evolución y nuevas tendencias*". Revista ICE Noviembre-Diciembre 2006 nº 833. Disponible en: http://www.revistasice.com/CachePDF/ICE_833_101-114__6A65E0C239E67DB605B503CA4481D015.pdf

ASIS INTERNATIONAL. "*ASIS SPC.1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems-Requirements with Guidance for Use*". 2009. American National Standard Institute, Inc.

BANK FOR INTERNATIONAL SETTLEMENTS. "*The Joint Forum. High-level principles for business continuity*". Agosto 2006.

BSI British Standards. "*BS 25777:2008. Information and communications technology continuity management – Code of practice*". 2008. British Standards Institution.

BUSINESS CONTINUITY INSTITUTE. "*Manual de buenas prácticas 2007. Guía para instaurar Buenas Prácticas Globales en Gestión de Continuidad de Negocio*" (Traducción ISMS Forum Spain). Disponible en: https://es.scribd.com/doc/163918527/Buenas-Practicas-Continuidad-Negocio-2007-BCI

HERRERO BRAÑAS, Ana Belén. "*Riesgo operacional en el marco de Solvencia II*". 2012. Madrid. FUNDACIÓN MAPFRE.

ISO/DTS 22317. "Societal security – Business continuity management systems – Business impact analysis". Dciembre 2014. International Organization for Standardization.

ISO 22398. "*Societal security – Guidelines for exercises*". Septiembre 2013. International Organization for Standardization.

ISO/IEC 27031. "*Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*". Marzo 2011. International Organization for Standardization.

ISO/IEC 27035. "*Information technology – Security techniques – Information security incident management*". Septiembre 2011. International Organization for Standardization.

MAESTRO MARTÍNEZ, Jose Luis. "*Guía práctica para documentar el cumplimiento de los requisitos del sistema de gobierno en Solvencia II*". Disponible en: http://www.ideas-sa.es/extra/Guia_practica_documentar_Solvencia_II.pdf

PÉREZ PÉREZ, Jesús. "*Gestión de riesgos en entidades aseguradoras. Solvencia II y su impacto regulatorio*". 1ª edición. Madrid. Delta, Publicaciones universitarias, 2016.

PONS PONS, Jerónia. "*Las entidades aseguradoras y la canalización del ahorro en España, 1908-1940*". Disponible en: http://www.unizar.es/eueez/cahe/pons.pdf

RITTINGHOUSE, John W., RANSOME, James F. "*Business Continuity and Disaster Recovery for Infosec Managers*". Edición 2005. Elsevier Digital Press.

RODRÍGUEZ-PONGA SALAMANCA, Mª Flavia, BRUNA LÓPEZ-POLÍN, María. "*Las entidades aseguradoras ante la nueva regulación*". Revista Española de Control Externo, vol. XVIII, nº 52 (Enero 2016), págs. 33-57. Disponible en: http://www.tcu.es/export/sites/default/.content/PdfAbsys/52RodriguezPongaLasentidadesaseguradoras.pdf

SANS INSTITUTE. "*Introduction to Business Continuity Planning*". 2002. Disponible en: https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559

SNEDAKER, Susan. "*Business Continuity & Disaster Recovery for IT Professionals*". Edición 2007. Syngress Publishing, Inc.

UNE-ISO 22300. "*Protección y seguridad de los ciudadanos. Terminología*". Diciembre 2013. Asociación Española de Normalización y Certificación (AENOR).

UNE-ISO 22301. "*Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio (SGCN). Especificaciones*". Diciembre 2013. Asociación Española de Normalización y Certificación (AENOR).

UNE-ISO 22313. "*Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio (SGCN). Directrices*". Diciembre 2013. Asociación Española de Normalización y Certificación (AENOR).

UNE-ISO 22320. "*Protección y seguridad de los ciudadanos. Gestión de emergencias. Requisitos para la respuesta a incidentes*". Diciembre 2013. Asociación Española de Normalización y Certificación (AENOR).

UNESPA. "*Solvencia II. De un vistazo*". Disponible en: http://www.unespa.es/adjuntos/fichero_4100_20151119.pdf

WITTY, Roberta J. "Ten Best Practices for Creating and Maintaining Effective Business Continuity Management Plans". Febrero 2010. Gartner.

9 Normativa Legal

Ley núm. 97 – Fomento – 14 de mayo, pub. el 15. "*Ley relativa a la inscripción, que al efecto se establece, de las Compañías, Sociedades, Asociaciones y, en general, todas las entidades que tengan por fin realizar operaciones de seguro.".* Legislación y Disposiciones de la Administración Central. Volumen 2 de 1908 (págs. 265 a 282). Disponible en:

http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_10/spl_79/pdfs/4.pdf

Ley de 16 de diciembre de 1954 sobre ordenación de los Seguros privados.

BOE núm. 353, de 19 de diciembre de 1954. (págs. 8365 a 8372). Disponible en: https://www.boe.es/datos/pdfs/BOE/1954/353/A08365-08372.pdf

Ley 50/1980, de 8 de octubre, de Contrato de Seguro.

BOE núm. 250, de 17 de octubre de 1980 (págs. 23126 a 23133). Disponible en: http://www.boe.es/boe/dias/1980/10/17/pdfs/A23126-23133.pdf

Real Decreto-Ley 10/1984, de 11 de julio, por el que se establecen medidas urgentes para el saneamiento del sector de seguros privados y para el reforzamiento del Organismo de Control.

BOE núm. 168, de 14 de julio de 1984 (págs. 20725 a 20726). Disponible en: http://www.boe.es/boe/dias/1984/07/14/pdfs/A20725-20726.pdf

La Ley 33/1984, de 2 de agosto, de Ordenación de Seguros Privados,

BOE núm. 186, de 4 de agosto de 1984 (págs. 22736 a 22747). Disponible en: http://www.boe.es/boe/dias/1984/08/04/pdfs/A22736-22747.pdf

Ley 21/1990, de 19 de diciembre, para adaptar el Derecho español a la Directiva 88/357/CEE, sobre libertad de servicios en seguros distintos al de vida, y de actualización de la legislación de seguros privados.

BOE núm. 304, de 20 de diciembre de 1990 (págs. 37977 a 37991). Disponible en: http://www.boe.es/boe/dias/1990/12/20/pdfs/A37977-37991.pdf

Ley 9/1992, de 30 de abril, de mediación en seguros privados.

BOE núm. 106, de 2 de mayo de 1992 (págs. 14929 a 14937). Disponible en: http://www.boe.es/boe/dias/1992/05/02/pdfs/A14929-14937.pdf

Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados.

BOE núm. 268, de 9 de noviembre de 1995 (págs. 32480 a 32567). Disponible en: http://www.boe.es/boe/dias/1995/11/09/pdfs/A32480-32567.pdf

Ley 44/2002, de medidas de reforma del sistema financiero.

BOE núm. 281, de 23 de noviembre de 2002 (págs. 41273 a 41331). Disponible en: http://www.boe.es/boe/dias/2002/11/23/pdfs/A41273-41331.pdf

Ley 34/2003, de modificación y adaptación a la normativa comunitaria de la legislación de seguros privados

BOE núm. 265, de 5 de noviembre de 2003 (págs. 39190 a 39220). Disponible en: http://www.boe.es/boe/dias/2003/11/05/pdfs/A39190-39220.pdf

Ley 5/2005, sobre supervisión de los conglomerados financieros y por la que se modifican otras normas del sector financiero

BOE núm. 97, de 23 de abril de 2005 (págs. 13901 a 13912). Disponible en: http://www.boe.es/boe/dias/2005/04/23/pdfs/A13901-13912.pdf

Directiva 2009/138/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y reaseguro y su ejercicio (Solvencia II)

DOUE de 17 de diciembre de 2009, págs. 335/1 a 35/155. Disponible en: https://www.boe.es/doue/2009/335/L00001-00155.pdf

Directiva 2014/51/UE del Parlamento Europeo y del Consejo de 16 de abril de 2014 por la que se modifican las Directivas 2003/71/CE y 2009/138/CE y los

Reglamentos (CE) no 1060/2009, (UE) no 1094/2010 y (UE) no 1095/2010 en lo que respecta a los poderes de la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación) y de la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados)

DOUE de 22 de mayo de 2014, págs. 153/1 a 153/61. Disponible en: http://www.boe.es/doue/2014/153/L00001-00061.pdf

Ley20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

BOE núm. 168, de 15 de julio de 2015 (págs. 58455 a 58611). Disponible en: http://www.boe.es/boe/dias/2015/07/15/pdfs/BOE-A-2015-7897.pdf

Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

BOE núm. 288, de 2 de diciembre de 2015 (págs. 113617 a 113816). Disponible en: http://www.boe.es/boe/dias/2015/12/02/pdfs/BOE-A-2015-13057.pdf