Los desastres y los Planes de Continuidad de Negocio en las empresas de seguros

Lionel Güitta Abellán
Subdirector Continuidad de Negocio y Contingencia
MAPFRE
Madrid - España

Mundo globalizado, entorno empresarial complejo

El mundo actual está globalizado y por tanto las empresas tienen múltiples interdependencias y conexiones con compañías que son tanto sus clientes como sus proveedoras de bienes y servicios.

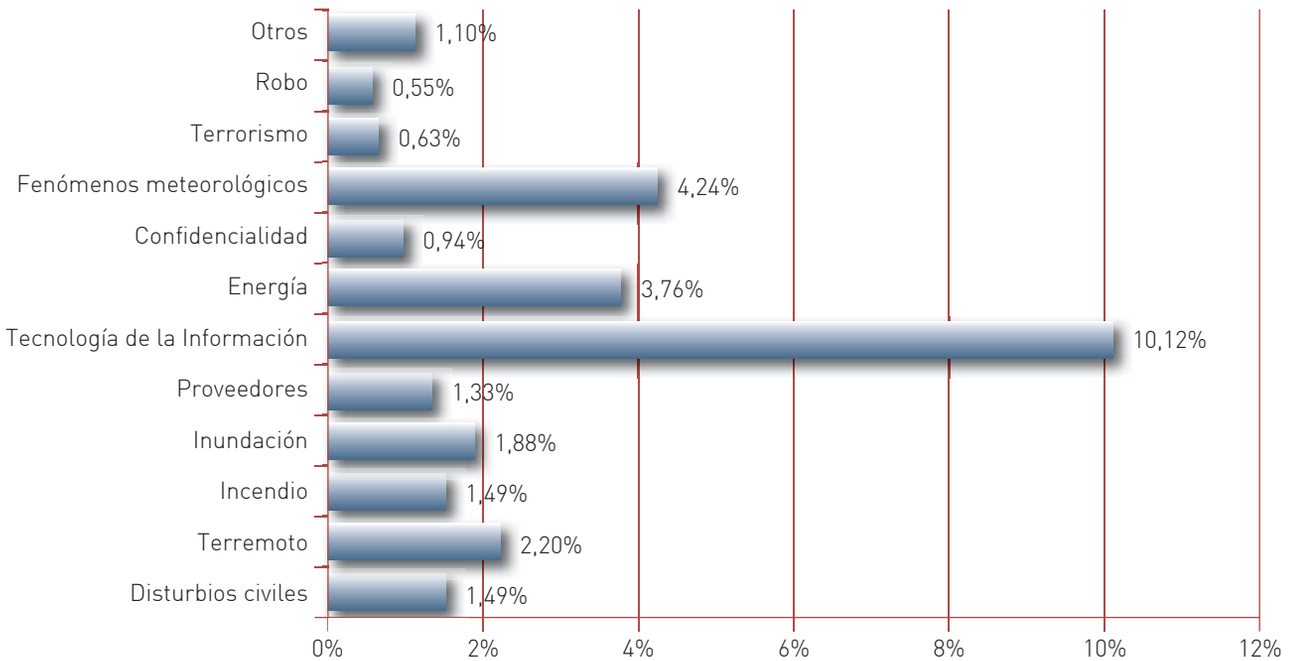
En este entorno complejo existen múltiples amenazas, algunas de las cuales, si se materializasen, podrían afectar no sólo a la supervivencia de la empresa que lo sufre, sino también a todo el entramado con el que se relaciona, así como a terceros, directa o indirectamente relacionados con ella.

La preocupación por proteger a las compañías frente a la ocurrencia de desastres se manifiesta, en un principio, en el área informática, cuando se va tomando conciencia de las consecuencias que los fallos tecnológicos pueden provocar en las empresas, como la paralización de su actividad o la pérdida de información.

Cada vez es menos frecuente encontrar organizaciones que no realicen copias de seguridad de la información almacenada en sus servidores o que incluso cuenten con soluciones alternativas que les permitan recuperar su capacidad de proceso de información en centros de procesos de datos alternativos, propios o externalizados.

La preocupación por proteger a las compañías frente a la ocurrencia de desastres nace en el área informática, cuando se va tomando conciencia de sus consecuencias, como la paralización de su actividad o la pérdida de información

Los desastres ocurren también en las compañías aseguradoras: ¿Ha tenido que activar su empresa el Plan de Continuidad de Negocio (PCN) a lo largo del último año por alguna de estas causas?
Elaboración Propia.
Fuente: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG*.



El estudio se ha realizado entre noviembre de 2011 y enero de 2012, y se ha contado con la respuesta de 685 ejecutivos de organizaciones ubicadas en más de cuarenta países, estando una cuarta parte de ellas ubicadas fuera de Estados Unidos de América. Los resultados mostrados están referidos exclusivamente a las empresas del sector asegurador, que suponen un 10,6% del total de compañías participantes en el estudio. La Tecnología de la Información es el principal elemento que desencadena la necesidad de activación de los planes de continuidad de negocio, incluyendo en este apartado, tanto las caídas de servicio programadas por actualizaciones, el mantenimiento y la gestión de cambios, así como las que no han sido programadas: ataques de virus, denegaciones de acceso o comunicaciones.

Una vez sufrido un desastre, es muy complicado recuperar la operatividad completa de la empresa, por lo que será necesario realizar un análisis previo en el que se determine el orden a la hora de recuperar los procesos, los tiempos mínimos y los recursos necesarios

Sin embargo, la ocurrencia de desastres de diferente magnitud y alcance han provocado que las empresas sientan la necesidad no sólo de garantizar la recuperación tecnológica, sino también la continuidad de la operativa de sus procesos de negocio, y por tanto de todos aquellos recursos que lo soportan, como sus infraestructuras, los centros de trabajo, el personal y su red de proveedores.

Para garantizar la recuperación de la operativa de los procesos de negocio en las empresas tras un evento catastrófico, se debe trabajar en «tiempo de normalidad» analizando, diseñando e implantando soluciones que hagan posible su recuperación en «tiempo de desastre». Dichas soluciones no se refieren solo a medidas preventivas o paliativas, sino a las vitales cuando la magnitud del desastre, la falta de mantenimiento, un error de cálculo o cualquier otra causa, las haga insuficientes para que la empresa sea viable tras el desastre. Estas soluciones pasan por disponer de ubicaciones físicas alternativas, formar al personal en otras áreas del negocio, la reasignación de funciones o la duplicidad de proveedores, entre otras.

Es evidente que, una vez sufrido un desastre, es muy complicado recuperar la operatividad completa de la empresa, por lo que será necesario realizar un análisis previo en el que

se determine el orden a la hora de recuperar los procesos, los tiempos mínimos necesarios para su recuperación y los recursos necesarios para dar una calidad de servicio mínimamente aceptable. Además, se desarrollarán las soluciones que permitan proporcionar esa respuesta de la empresa para hacer frente al desastre: planes de recuperación de la actividad, planes de comunicación, planes de pruebas y formación.

A lo largo de los últimos años se han definido diversos estándares internacionales relacionados con la continuidad de negocio para ayudar a las organizaciones a gestionar los aspectos a tener en cuenta para garantizar, en la medida de lo posible, la resiliencia de la empresa que ha sufrido un desastre. En mayo de 2012 se publicó el estándar internacional más reciente: «ISO 22301 Seguridad de la Sociedad -Sistema de gestión de continuidad de negocio- Requisitos».

En el caso del sector financiero y, concretamente, en el sector asegurador, se está requiriendo, por parte del órgano regulador de la zona o del país, garantizar la continuidad operativa de las compañías. Así podemos observar cómo, en el ámbito europeo, la directiva Solvencia II, hace mención a la necesidad de garantizar la continuidad operativa:

Art. 41.4: Las empresas de seguros y de reaseguros adoptarán medidas razonables para garantizar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de emergencia. A tal fin, las empresas emplearán sistemas, recursos y procedimientos adecuados y proporcionados.

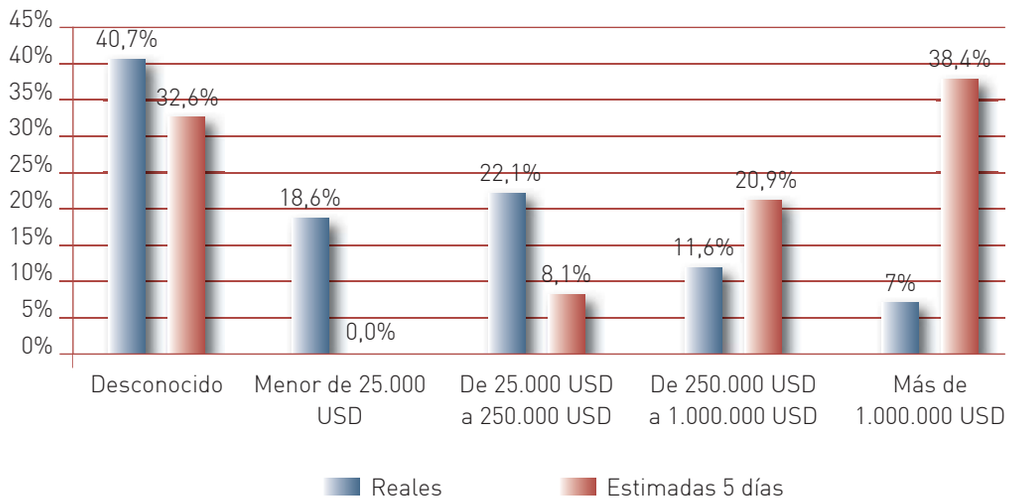
Además de definir el «Riesgo operacional» como:

El riesgo de pérdida derivado de la inadecuación o de la disfunción de procesos internos, del personal o de los sistemas, o de sucesos externos.

La medida de este Riesgo Operacional forma parte del cálculo del capital de solvencia obligatorio (*SCR: Solvency Capital Requirement*).

Hay definidos diversos estándares internacionales de continuidad de negocio para garantizar, en la medida de lo posible, la resiliencia de la empresa que ha sufrido un desastre

¿Cuáles son las pérdidas económicas estimadas provocadas por los incidentes producidos en su empresa en el último año? ¿Y las pérdidas financieras estimadas por un periodo de parada del negocio durante cinco días? (USD)
Elaboración Propia.
Fuente: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.*



Es significativo ver que el 40% de las organizaciones desconocen el coste económico de las pérdidas que les han supuesto los incidentes, mientras que también casi el 40% cuantifican las pérdidas por paralización del negocio durante cinco días en más de un millón de USD.

Aspectos principales para desarrollar un Plan de Continuidad de Negocio

A la hora de la toma de decisión del desarrollo de un PCN, ya sea por requerimiento legal o por convencimiento de su necesidad, hay que valorar los siguientes aspectos:

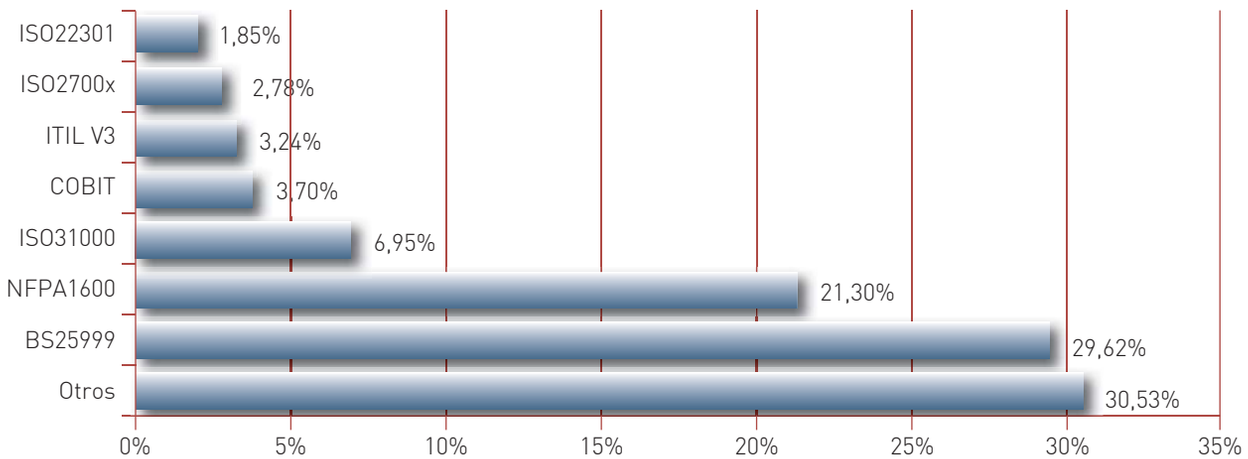
- **Existencia de compromiso de la Alta Dirección de la compañía**: Tener un promotor del proyecto con suficiente influencia en la empresa para lograr la involucración decidida de todas las áreas implicadas.

- **Alcance del plan a desarrollar**: Identificar, claramente, qué áreas de la compañía van a ser analizadas, y qué ubicaciones físicas se van a contemplar.

- **Recursos que se van a destinar al proyecto**: Pueden ser recursos humanos de la propia compañía, que deberán dedicarse casi en exclusiva al desarrollo del proyecto y/o recursos económicos para que el proyecto sea desarrollado. También puede llevarse a cabo por una empresa especializada, aunque siempre habrá que contar con la participación del propio personal de la compañía, en un porcentaje de tiempo, para proporcionar información y validar los resultados entregados.

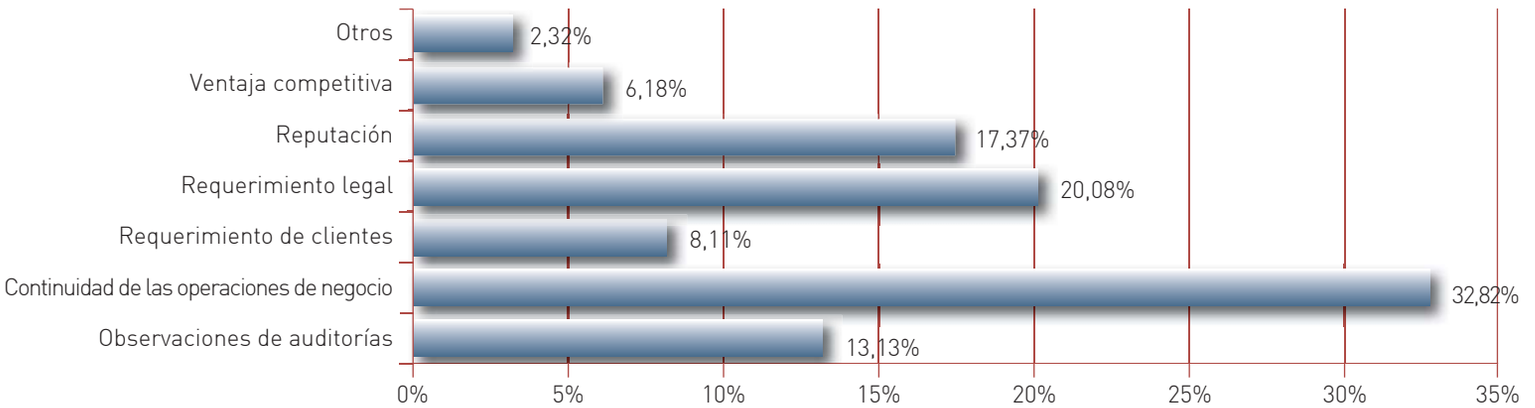
- **La continuidad de negocio se convierte en un proceso más de la compañía**: Tras la finalización del proyecto, además de la propia implantación de las soluciones, se requerirá que el plan sea actualizado periódicamente y siempre que haya cambios relevantes en la compañía. El nuevo proceso deberá contar con responsables y recursos suficientes para su desarrollo que se encargarán del diseño, preparación y realización de pruebas que garanticen la idoneidad de las soluciones implantadas, así como el entrenamiento del personal involucrado.

¿Cuál es el estándar de gestión de continuidad de negocio que se ha aplicado en su empresa aseguradora?
Elaboración Propia.
Fuente: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG*.



Se puede observar que un tercio de las compañías basan su sistema de gestión de la continuidad de negocio en estándares locales del país o estándares no específicos de continuidad de negocio (Otros). El elevado porcentaje de la aplicación del estándar NFPA1600 está motivado principalmente porque la mayoría de las compañías intervinientes en este estudio están localizadas en EE.UU. La normativa ISO22301, que sustituye a la BS25999, aparece con bajo porcentaje porque a la fecha del estudio estaba en fase de borrador (publicada en mayo 2012). También es destacable que casi un 7% de las compañías basan su sistema de gestión de continuidad de negocio en estándares relacionados principalmente con la tecnología (ITIL, COBIT).

¿Cuáles son las razones principales para la implantación de un sistema de gestión de continuidad de negocio en su compañía aseguradora?
Elaboración Propia.
Fuente: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG.*



Una de cada tres compañías aseguradoras han desarrollado un PCN (o está en proceso), fundamentalmente para mantener la continuidad de sus operaciones, mientras que una de cada cinco lo hace para cumplir con los requisitos legales.

Fases de desarrollo del PCN

Un PCN tiene por objeto dotar a una organización de la capacidad de reacción necesaria para conseguir la vuelta a la normalidad, de la manera más efectiva, tras una interrupción de las actividades del negocio causadas por un desastre. De manera formal, el estándar ISO 22301, define un Plan de Continuidad de Negocio como:

> ***Conjunto de procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar, tras una interrupción, a un nivel predefinido de operación. Normalmente esto cubre los recursos, servicios y actividades necesarias para garantizar la continuidad de las funciones críticas del negocio.***

El desarrollo de un PCN en una compañía de seguros contempla cuatro fases, que se describen a continuación:

1. Análisis de riesgos de los escenarios de indisponibilidad

Los procesos de una compañía aseguradora necesitan de cinco grupos de elementos para poder realizarse:

- Personas.
- Edificios/Infraestructuras.
- Información.
- Tecnología.
- Proveedores.

Se analizan entonces los riesgos de ocurrencia de un escenario de indisponibilidad de cada uno de ellos, cuantificando la probabilidad de materialización de las amenazas. Así se determinarán las medidas adicionales a aplicar para detectar o mitigar sus consecuencias. Constituye además una herramienta de decisión para priorizar las soluciones de estrategias de recuperación. Las dificultades asociadas a esta fase son las propias de un análisis de riesgos, entre otros:

- Disponer de histórico de incidentes que hayan afectado a la compañía.
- Acceso a la información necesaria.

2. Análisis de Impacto en el Negocio

Se trata de analizar el impacto que supone en la empresa la no realización de cada uno de los procesos, obteniendo como resultado de la misma la lista ordenada de procesos según su criticidad y determinando el tiempo en el que se requiere su recuperación tras la declaración del desastre.

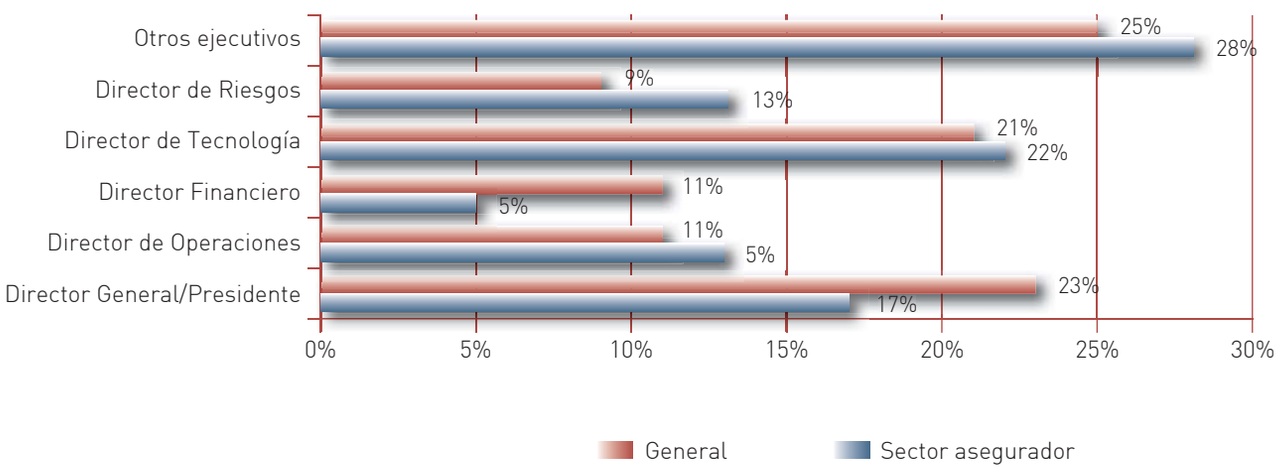
Esta es la actividad más importante en la definición de un Plan de Continuidad de Negocio, ya que el resto de los trabajos a realizar estarán basados en los resultados que obtengamos en esta fase.

Las principales dificultades del Análisis del Impacto de Negocio son las siguientes:

- **Necesidad de dedicación de los responsables de los procesos para la determinación de los impactos**. Aportar la información necesaria para el análisis a realizar, requiere

Un PCN tiene por objeto dotar a una organización de la capacidad de reacción necesaria para conseguir la vuelta a la normalidad, de la manera más efectiva, tras una interrupción de las actividades del negocio causadas por un desastre

¿Quién es el principal promotor del desarrollo de los sistemas de gestión de continuidad de negocio?
Elaboración Propia.
Fuentes: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG y Business Continuity Preparedness Survey, Q4 2011. Forrester/Disaster recovery Journal.*



En el gráfico no se aprecian diferencias significativas entre los resultados obtenidos entre las compañías del sector asegurador y los resultados que contemplan todos los sectores empresariales. Hay que señalar la influencia que tiene el máximo responsable de la tecnología en la implantación de un sistema de gestión de continuidad de negocio.

un tiempo que, si se suma a las labores del día a día, supone un esfuerzo adicional de los responsables.

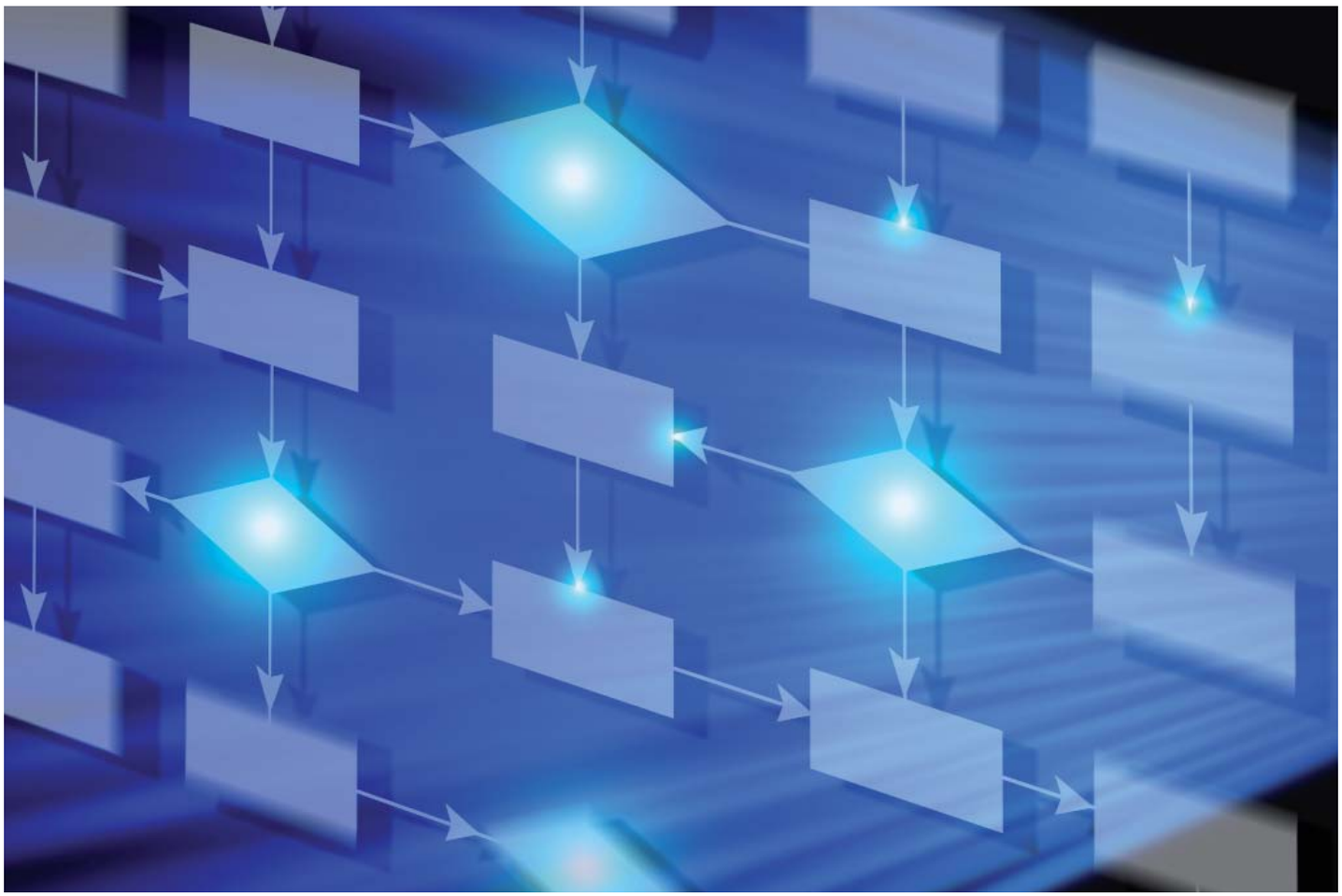
- **Minorar la subjetividad personal de cada responsable en la determinación del impacto de los procesos**. Para evitar que los resultados se vean sesgados por quienes se consideran especialmente imprescindibles para la empresa o los que consideran que su trabajo aporta poco valor, se puede impartir charlas formativas o talleres que expliquen el objetivo que se pretende, y/o recoger la información del impacto de forma no directa. Esta última técnica requiere un trabajo previo para escoger las cuestiones a plantear, los criterios de respuesta a emplear, las ponderaciones de cada una de las cuestiones y el proceso matemático que realiza el cálculo final. Adicionalmente, los resultados obtenidos se deben revisar con los responsables superiores, ya que tienen una visión de conjunto con la que pueden detectar incongruencias en la clasificación de los procesos que estén bajo su responsabilidad.

- **Valorar la criticidad de las actividades**. Debido al profundo análisis que se realiza, el personal responsable puede interpretar que se está valorando su importancia para la empresa. Es un aspecto importante a aclarar, sobre todo dada la situación económica actual. Se debe insistir en que el objetivo es medir la criticidad de cada una de las actividades en caso de que la compañía se vea afectada por un desastre, no la importancia de la actividad realizada. Todas las que se desarrollan en una compañía son importantes, pero en caso de verse afectada por un desastre, la compañía debe priorizar la recuperación de unas frente a otras. Inicialmente, debe centrar sus esfuerzos en reanudar las actividades cuya no realización puedan suponer un ma-

Debido a la profundidad del Análisis de Impacto de Negocio, el personal responsable puede interpretar que se está valorando su importancia para la empresa. Es un aspecto importante que debe aclararse, sobre todo dada la situación económica actual

Número de empleados en FTE (*Full-Time Equivalent*) dedicados a la Gestión de la Continuidad de Negocio en las compañías aseguradoras.
Elaboración Propia.
Fuente: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report. Continuity Insights/KPMG.*

Nº FTE	0/2	3/5	6/9	10/20	+20
Nivel Corporativo	22,89%	7,63%	3,21%	1,61%	0,40%
Unidades de Negocio	15,26%	4,82%	2,41%	2,81%	5,62%
Tecnología de la Información	16,47%	8,43%	2,41%	3,61%	2,41%



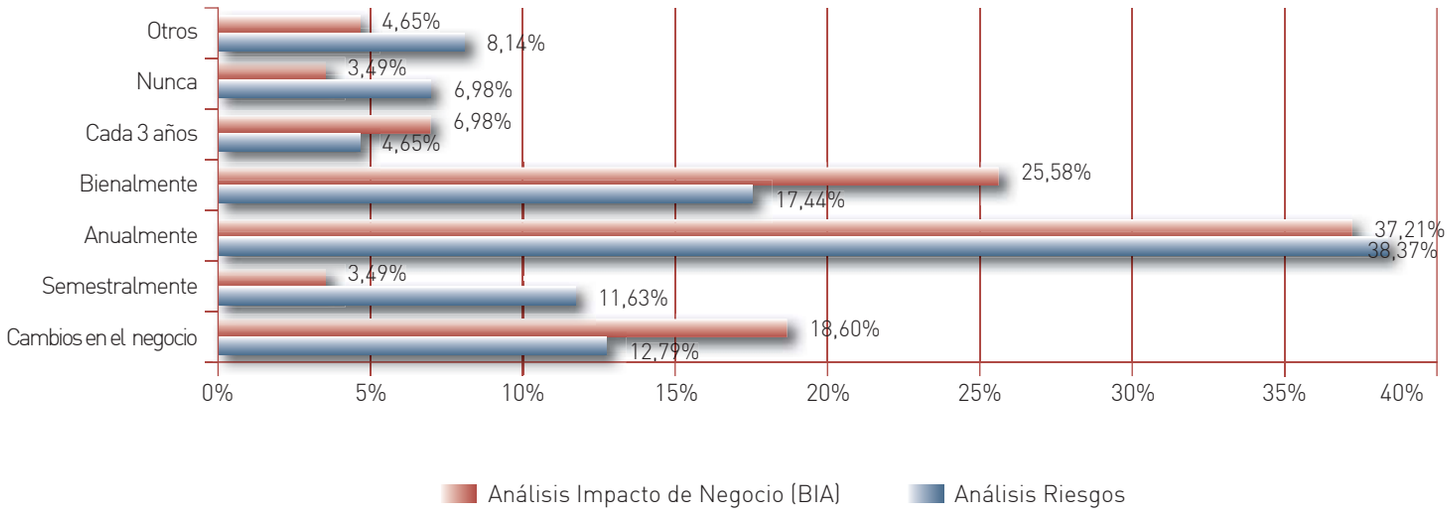
Una parte importante de la Gestión de Crisis es la relacionada con los aspectos de la comunicación de la situación y su evolución, tanto hacia el exterior de la compañía como hacia el interior

yor perjuicio para la compañía (mayor nivel de criticidad), para continuar con las del siguiente nivel y así sucesivamente hasta restablecer todas las actividades o haber utilizado todos los recursos disponibles.

- **Determinar qué procesos deben analizarse**. Es recomendable analizar todos los procesos de la compañía para no realizar ningún juicio previo, sin análisis formal, de su criticidad, ya que se puede correr el riesgo de no incluir alguno de ellos que posteriormente pueda catalogarse con una criticidad elevada. La definición del alcance del análisis de los procesos puede organizarse estableciendo distintas fases hasta completar la totalidad de los mismos. Así, por ejemplo, se empieza contemplando todos los procesos de una única área de la compañía, para continuar el alcance a otros de otras áreas, de forma que al finalizar todas las fases se haya recorrido completamente el mapa de procesos de la compañía. Esta aproximación de análisis puede suponer un trabajo adicional por tener que ir consolidando los nuevos resultados con los obtenidos en fases anteriores, hecho que se produce fundamentalmente con los procesos transversales a varias áreas. En cualquier caso, en grandes compañías, esta puede ser la mejor aproximación para tener un análisis completo, se trata de la estrategia de «divide y vencerás», intentando evitar que, por el número de procesos a analizar y los recursos disponibles, el PCN no pueda desarrollarse adecuadamente.

- **Estudiar las dependencias entre procesos**. Este aspecto está relacionado con el punto anterior y estudia las posibles dependencias entre los procesos. Si, por ejemplo, un proceso A aparece con un valor de criticidad determinado, los procesos de los que dependa, deberán tener un valor de criticidad superior, para que cuando se reanude dicho proceso A, se

¿Con qué frecuencia realiza el Análisis de Riesgos en su compañía aseguradora? ¿Y el Análisis de Impacto en el Negocio?
Elaboración Propia.
Fuente: 2011-2012 *Global Business Continuity Management Program Benchmarking Study (Insurance Segment Report). Continuity Insights/KPMG*.



La mitad de las compañías aseguradoras revisan los resultados de sus análisis de riesgos en el año siguiente, o antes (11,63%), de la última revisión. En el caso del análisis del impacto en el negocio, un 40% de las compañías realizan la revisión de resultados al año siguiente a su última revisión (o antes: 3,49%). Es importante señalar que son relativamente pocas las compañías que realizan las revisiones cuando se han producido cambios en la compañía.

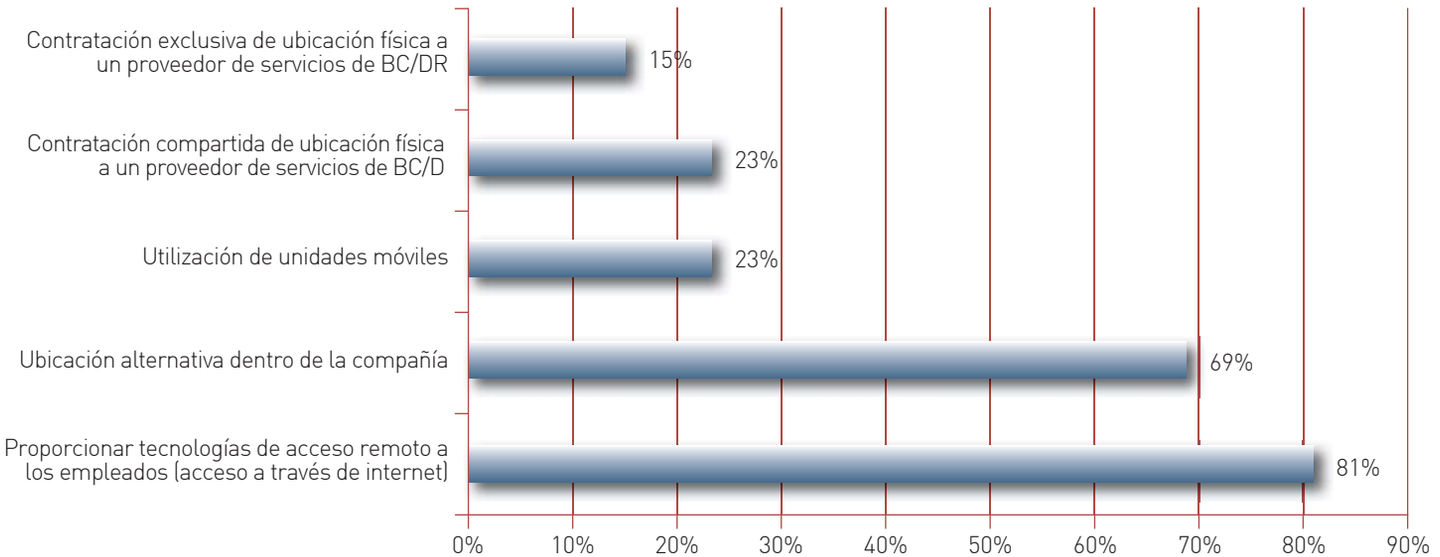
hayan restablecido previamente los procesos que requiere para operar.

- **Determinar el nivel de profundidad a analizar**. Las compañías pueden tener determinado un mapa de procesos a distintos niveles (procesos, subprocesos, actividades, tareas), o en caso de que no lo dispongan, se puede analizar en función de la estructura organizativa (direcciones, áreas, departamentos, jefaturas). En cualquiera de los dos casos, se debe determinar cuál es el nivel a analizar, de forma que los resultados sean homogéneos. Tampoco debe ser muy genérico ya que esto obligaría a buscar soluciones que implicasen la utilización de muchos recursos sin que se llegase a especificar su cometido. Ni debe analizarse a un nivel demasiado detallado ya que, a pesar de ser muy precisos en los recursos a emplear, en caso de vernos afectado por un desastre, las soluciones planteadas deben ser lo suficientemente flexibles como para hacer frente al escenario real.
- Determinar los umbrales de los valores de criticidad y su correspondencia con los tiempos de recuperación objetivo (RTO: *Recovery Time Objective*). El RTO se mide desde la detección del incidente hasta la recuperación de la actividad. Este tiempo debe determinarse para cada uno de los procesos y dependerá de la criticidad del proceso analizado. Hay que tener en cuenta que normalmente a menor RTO requerido por los procesos, le corresponde una solución de recuperación que requiere mayor inversión económica y/o mayor esfuerzo en la preparación de los procedimientos de reactivación de la actividad, ya que se dispone de menos tiempo para reaccionar.

3. Selección y diseño de soluciones para la recuperación de la actividad

Una vez analizados los impactos que puede producir la no realización de los procesos cuando la compañía se vea afectada por un

¿Qué soluciones de Continuidad de Negocio aplica en su compañía?
Fuente: *Business Continuity Preparedness Survey, Q4 2011. Forrester/Disaster recovery Journal.*



Las soluciones que aparecen en el gráfico están relacionadas fundamentalmente con un escenario de desastre que haya afectado a los edificios de la compañía y que requiera realojar al personal o permitir el acceso remoto a los sistemas informáticos, siendo esta última la opción mas implantada. (BD/DR: *Business Continuity and Disaster Recovery*).

desastre y determinado el tiempo en el que deberían recuperarse las actividades, se deben diseñar soluciones que permitan cumplir con esos requerimientos del negocio: tiempo de recuperación y recursos mínimos necesarios. Estas soluciones se definirán en función de los escenarios de indisponibilidad de los elementos necesarios para ejecutar los procesos.

Las principales dificultades durante esta fase son:

- **Determinar el grado mínimo de servicio que se debe ofrecer**. Las soluciones que se concreten para la situación de desastre deberán considerar el mínimo de recursos imprescindibles para desarrollar las actividades.

- **Estimar los costes de desarrollo de las soluciones**. Es un factor crucial para la toma de decisión, sobre todo cuando haya varias alternativas. Habrá que identificar los parámetros que intervienen en el coste de las propuestas y aplicarlos a las variables de los recursos que se van precisar para reanudar la actividad.

- **La Alta Dirección de la compañía ha de aprobar el PCN y costes**. Derivado del punto anterior, el desarrollo de las soluciones propuestas puede exceder las competencias del área que gestiona la continuidad de negocio, por lo que requerirá la aprobación por parte de la Alta Dirección y la comunicación a las áreas involucradas para su implantación.

Además de la selección e implantación de las soluciones, se tendrán que especificar los procedimientos para la Gestión de Crisis y el operativo para la puesta en marcha de las actividades afectadas. Una parte importante de la Gestión de Crisis es la relacionada con los aspectos de la comunicación de la situación y su evolución, tanto hacia el exterior de la compañía como hacia el interior.

4. Realización de pruebas

Para poder determinar si la compañía está preparada para hacer frente a un desastre, han de ponerse en práctica ejercicios que permitan:

- Comprobar que las soluciones implantadas y los procedimientos desarrollados son correctos y suficientes para cumplir con los requerimientos del negocio.

- Identificar los aspectos a revisar o mejorar.

Las pruebas pueden realizarse escalonadamente de acuerdo a la madurez del desarrollo e implantación de las soluciones y procedimientos. Se puede empezar con «pruebas de escritorio», para comprobar que están reflejadas todas las tareas a realizar así como la sincronización entre ellas. Posteriormente, se organiza el «simulacro», en el que se ensayan operativamente los procedimientos y las soluciones. La compañía sólo podrá confirmar que dispone de un PCN si ha realizado pruebas y el resultado de estas se considera satisfactorio.

Conclusión

El PCN debe enmarcarse dentro de un Sistema de Gestión de Continuidad de Negocio que permita su desarrollo, monitorización, revisión, mantenimiento y mejora continua, lo que incluirá la definición de una estructura organizativa y sus responsabilidades, la redacción de unas políticas, los recursos necesarios y la planificación de actividades a desarrollar.

Desde entonces la continuidad de negocio se convierte en un proceso más de la compañía y como tal, debe gestionarse adecuadamente para que no quede desfasado y así, cuando desgraciadamente haya que hacer uso de él, realmente sea eficiente para garantizar la supervivencia de la compañía.