Gestionando la Continuidad de nuestro negocio

Víctor Hervías
Socio Director de BSCM (Business Continuity Management)

Hay un antes y un después en el mundo de la continuidad del negocio. Hasta los tristes acontecimientos del 11 de septiembre de 2001 existía cierta conciencia de la necesidad de establecer planes de recuperación ante desastres, la mayoría de las veces circunscrita a determinados entornos (como el militar, "padre" de la Continuidad, o el sector financiero) y, muy en especial, a sus entornos de tecnologías de la información. Después de este terrible golpe, comienza a percibirse la ineludible necesidad de incluir la Continuidad como un proceso crítico más dentro de la gestión del negocio y que afecta a todas sus áreas.

Tanto es así, que, de un tiempo a esta parte, tanto la mayoría de las normativas de Buen Gobierno Corporativo (SoX, Basilea, Mifid) como las mejores prácticas de Gestión (COBIT, Itil, Coso) tienen en cuenta la evaluación de riesgos y la continuidad del negocio como uno de los aspectos clave para su buena gestión, hasta la publicación, en noviembre de 2006 de la norma BS25999, primer estándar

internacional publicado por el *British Standaras Institution,* que se convertiría en norma certificable con su segunda edición un año más tarde. Otras normas como la ISO 22399 o la 24762, y hasta un total de más de 50 normas, regulaciones, estándares y guías, nacionales o internacionales, relativas a la gestión de riesgos y la continuidad de los negocios, y otras tantas de industrias específicas, dan muestra de la importancia de este asunto en el marco empresarial actual.

El británico BCI *(Business Continuity Insitute)* y el estadounidense DRII *(Disaster Recovery Internacional Institute)* recogen las dos metodologías más extendidas para la gestión de la continuidad. El segundo define la Gestión de la Continuidad del Negocio (BCP) como el "proceso de desarrollar acuerdos previos y procedimientos que permitan a una organización responder a un evento de modo que las funciones críticas del negocio continúen con los niveles de interrupción o cambios esenciales planificados". Básicamente, el BCP pretende que la organización esté preparada para sufrir el menor impacto posible ante un incidente inesperado que ponga en riesgo sus operaciones, a través de un modelo de gestión integrado dentro de la compañía y que en muchas ocasiones no pretende inventar nada nuevo dentro de la misma, sino conocer, organizar y proteger sus activos y recursos ante los diversos riesgos a los que hoy por hoy están sometidas.

El BCP es responsabilidad de la alta dirección, en tanto que ellos son los responsables de la salvaguarda de los activos y la viabilidad de la organización, y de involucrar a todos los estamentos y áreas de la misma. Parte fundamental de estos son habitualmente los entornos TIC, no sólo por ser vitales para la supervivencia de la compañía en muchos casos, sino por constituir un factor clave de éxito en cualquier organización. Es por esto que, aunque un BCP afecta a todas las áreas (por ejemplo, el activo principal de una empresa de formación no serán tanto sus entornos TIC como sus aulas y profesorado), es habitual que exista una mayor concienciación sobre continuidad en estas áreas y pueda resultar más sencilla la implantación de un Plan de Recuperación de Sistemas de la Información para luego ampliar a un BCP de toda la compañía.

El BCP, como ya se ha comentado, es un proceso de gestión continua de la compañía, basado en un modelo PDCA *(Plan-Do-Check-Act).* En un proyecto de implantación, como en cualquier otro modelo de gestión, será clave definir, desde la alta dirección, una Política de Continuidad, que incluya los objetivos y el alcance del proyecto.

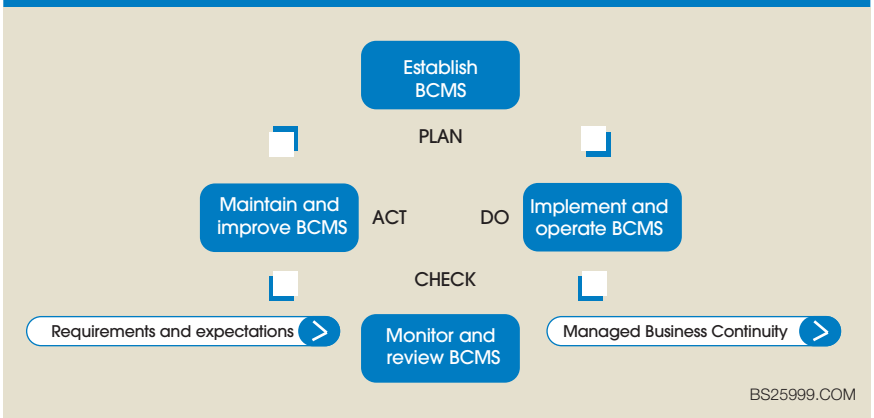
El primer paso deberá ser la identificación de los riesgos a los que está sometida la organización. Para ello deberemos identificar nuestros activos y recursos, así como la probabilidad de ocurrencia de los riesgos detectados. Éste es un proceso que muchas veces ya se ha realizado en la compañía, y de cuyos resultados podemos valernos para aquel que más incide en cuanto al BCP se refiere, el análisis de impacto *(Business Impact Analisys).*

Más allá de los riesgos a los que están sometidos nuestros activos, que muchas veces podremos evitar o minimizar tomando determinadas medidas correctoras, desde el punto de vista de la continuidad nos interesan más el riesgo residual y el impacto que éste puede provocar sobre la supervivencia de la compañía.

Se trata de identificar los activos y recursos críticos de la organización y el impacto financiero, humano y sobre la reputación, que pueden llegar a suponer la no disponibilidad de esos recursos ante un eventual incidente. Será necesario definir en este proceso el punto de recuperación, que determina la tolerancia a pérdida (de datos en SI) que consideramos aceptable (desde el punto de vista de los SI, se marcarán también las políticas de *backups*) y el tiempo de recuperación, o el tiempo de no disponibilidad que consideramos aceptable en caso de una interrupción de las operaciones (que, recurriendo al mismo ejemplo de los SI, definirá la opción para el centro de respaldo). Habrá que tener en cuenta, a la hora de definir ambos aspectos, la evolución de los impactos en el tiempo (un incidente pequeño en principio, como una pequeña fuga en una tubería, puede convertirse en un desastre si no se trata a tiempo, y se provoca una inundación) y el equilibrio entre los costes de interrupción y el de las medidas tomadas para paliarlos.

Un análisis de impacto correctamente realizado será clave para el éxito del BCP y la identificación de los activos, recursos y procesos que realmente son

Figura 1. The Plan-Do-Check-Act (PDCA) Method



críticos para el negocio, en función de su potencial impacto sobre el mismo. El siguiente paso será, por tanto, el establecimiento de las estrategias para la recuperación y/o alternativas en función de la probabilidad de ocurrencia y su impacto. Esto dependerá de cada organización, pero, por ejemplo, en sistemas de información deberemos establecer procedimientos de *backup* y recuperación, necesidades de un centro de proceso de datos alternativo, almacenamiento externo de la información y otras necesidades de infraestructura como las comunicaciones.

Común a cualquier BCP debería ser el establecimiento de un centro de control desde el que coordinaremos las actividades de respuesta y recuperación en caso de desastre que puede establecerse, por ejemplo, en otras localizaciones de la propia compañía, una vivienda adecuada o incluso la suite de un hotel, teniendo en cuenta que ha de reunir ciertos requisitos de distancia, dimensión, disponibilidad, medios, etc.

Estas estrategias de recuperación nos guiarán en el propio desarrollo del plan, con el establecimiento de los procedimientos de respuesta y recuperación, la definición de responsabilidades y equipos (equipo de gestión de incidentes, logística, instalaciones, recursos humanos, etc.) y la adquisición en caso necesario de los recursos alternativos que hayamos definido, así como planes específicos de emergencia que hayamos podido identificar. No debemos olvidar en este proceso la definición de un plan de vuelta a la normalidad, que en ocasiones puede ser una situación tanto o más crítica que la propia de contingencia.

Como señalábamos al principio de este artículo, mucha de la información necesaria para el desarrollo del plan ya existe en la compañía (planes de emergencia y evacuación, prevención de riesgos laborales, procedimientos de operación, etc.), y el esfuerzo debe centrarse en recopilarla, organizarla y complementarla cuando sea necesario. En definitiva, hacerla útil en el momento de una contingencia.

Un punto importante será la identificación de las personas adecuadas para cada situación, atendiendo a sus capacidades y aptitudes, y teniendo en cuenta la potencial situación de estrés en que pueden verse obligados a cumplir con sus responsabilidades dentro del plan, así como un eficiente plan de comunicación, tanto interno como externo, que permita que las crisis se gestionen de manera coordinada y eficiente.

El desarrollo del plan dará como resultado un manual de procedimientos donde debemos buscar, ante todo, la accesibilidad para todos los miembros involucrados, intentando que sea un documento accesible, claro y conciso, exento de tecnicismos.

La última fase de la implantación será el programa de comunicación, formación y entrenamiento, que debe incluir a todos los estamentos de la compañía (y quizá a algunos de los externos) y estar enfocado hacia los distintos niveles de involucración en el plan. Habrá que poner especial atención a aquellas habilidades especiales en función de las responsabilidades dentro del mismo (por ejemplo, habilidades de comunicación ante los medios).

Una de las mejores formas de entrenar será la utilización de simulaciones, bien completamente ficticias, bien simulacros reales, parciales o no, de situaciones de contingencia.

Si bien es cierto que un plan que no está probado resultará seguramente inútil en el momento del incidente, también es recomendable ser prudente con las pruebas en escenarios reales, pues una prueba mal dimensionada o preparada puede resultar en un incidente real.

Hasta aquí la implantación. Pero las organizaciones son cambiantes por definición, y el esfuerzo realizado en la implantación pronto será en vano si no mantenemos nuestro plan actualizado, cerrando el ciclo PDCA comentado al inicio. La revisión periódica del sistema y, sobre todo, el uso de simulacros nos permitirán comprobar que nuestro BCP está actualizado y alimentarlo y mejorarlo con las experiencias obtenidas de los propios ejercicios.

Por último, enfatizar en lo que consideramos son los principales factores de éxito para la exitosa implantación de un sistema de gestión de continuidad de negocio, que no son otros que el necesario liderazgo de la alta dirección, desde el primer impulso del proyecto, así como el aprovechamiento del conocimiento de los miembros de la organización, pues son ellos los que conocen los procesos, muchas veces los que ya cuentan con las alternativas aunque no estén documentadas. Sólo tenemos que organizar ese conocimiento y ponerlo al servicio del negocio. ■