

## CONTINUIDAD DE NEGOCIOS ©

### Abstract

Ing. Carlos Ormella Meyer

El objetivo de la **Continuidad de Negocios, BC**, es asegurar que los procesos primordiales sean o bien no interrumpidos, o bien efectiva y eficientemente restaurados de acuerdo con la misión de negocios de una empresa, asegurando directamente el éxito total de la misma. Para ello la Continuidad de Negocios se enfoca en la resiliencia de la gente, procesos, lugar de trabajo, sistemas, seguridad física, comunicaciones, etc.

En tal sentido, la Continuidad de Negocios se refiere a las actividades necesarias que aseguren la supervivencia de una empresa frente a un incidente que provoque una interrupción en la operatoria normal de negocios.

La determinación de tales actividades ordenadas adecuadamente constituye el llamado **BCP o Plan de Continuidad de Negocios**.

El BCP confronta la posibilidad de un desastre, cómo un desastre interrumpe el proceso de negocios, y cómo los negocios pueden continuar en operación.

En la preparación de un BCP es importante tener en cuenta que el desafío número 1 no es la tecnología que sustenta las operaciones de la empresa, sino la visión de los negocios y las estrategias a establecer para mantener las operaciones comerciales y en definitiva los objetivos/misión de la misma. Como consecuencia, los sistemas de información se consideran en el BCP sólo en términos de su soporte para los procesos de negocios.

A grandes rasgos, el BCP tiene que establecer la gestión de riesgos y los procesos de recuperación de desastres para identificar, valorar y responder a los riesgos asociados con la pérdida de posibilidad de ejecutar los procesos de negocios habituales de la organización.

Siguiendo el lineamiento comentado, especialmente en cuanto al alcance de un BCP en todas las actividades de una empresa, en el desarrollo de un BCP no sólo hay que formar un *equipo o comité del proyecto* sino también contar con el apoyo de la alta gerencia y los propietarios de los servicios/procesos de negocios, incluso bajo la forma de un *steering committee*, involucrándolo en forma consistente desde el principio del proyecto, para la evaluación del progreso y éxito de la implementación del plan.

### Bases para la Preparación de un BCP

Una forma simplificada de considerar la preparación de un BCP pasa por fases como las que siguen:

- 1) Análisis de Impacto en los Negocios
- 2) Valuación de Riesgos
- 3) Estrategias de gestión
- 4) Pruebas
- 5) Mantenimiento

#### 1) Análisis de Impacto en los Negocios

Uno de los puntos más trascendentes del BCP es el **BIA o Análisis de Impacto en los Negocios**. El BIA consiste básicamente en la valuación de los impactos potenciales que resulten de diferentes incidentes o desastres que afecten funciones críticas de negocios de una empresa.

Esquemáticamente se puede decir que el BIA consiste en:

- a) Identificar los procesos (o servicios) de negocio, datos e infraestructura tecnológica importantes para la empresa, determinando cuáles son especialmente críticos para el negocio. Las necesidades críticas se pueden relevar de manera consistente usando cuestionarios especiales. Estos cuestionarios se enfocan en documentar las actividades críticas de cada área, y en identificar los requerimientos mínimos relacionados con el personal, equipamiento, documentación, facilidades, y otros recursos.

- b) Identificar los riesgos asociados, el impacto de los mismos y el RTO (*Objetivo de Tiempo de Recuperación*), que asegure la viabilidad de las operaciones de negocios para los diferentes procesos críticos, a través de las funciones y recursos que generalmente incluye cada proceso de negocio. Con referencia a los impactos, hay que determinar el costo de las interrupciones no sólo en cuanto a productividad y/o ingresos perdidos sino también considerando los gastos de recuperación. Además, puede haber otros costos indirectos asociados, tales como una baja o inestabilidad en la situación financiera, reputación dañada, pérdida de personal, y hasta quizás penalidades según leyes o regulaciones.
- Un punto importante en todo este análisis reside en el verdadero costo de una interrupción, tomado como el resumen de los gastos y pérdidas que resulten de un evento adverso determinado. El costo monetario es un factor de productividad e ingresos perdidos, más los gastos de recuperación. En conexión con el RTO se define el MAO o MAD (Máxima Interrupción o Indisponibilidad de Servicios), referido al tiempo máximo tolerable, antes de que se produzcan daños irreparables para los negocios. En este sentido el RTO corresponde a un lapso de tiempo menor que el del MAD. A RTO suele dársele diferentes significados. Hay quienes lo consideran un parámetro exclusivamente para las aplicaciones y sistemas IT, reservando el MAD para las funciones de negocios. Sin embargo, tal distinción no es muy sostenible.
- Finalmente, otro factor adicional lo constituye el RPO (*Objetivo del Punto de Recuperación*), que indica el momento en el tiempo pasado al incidente, a partir del cual se deben restaurar los datos para poder reasumir las transacciones de negocios.
- c) Asignar las prioridades de recuperación correspondientes a las funciones y recursos categorizándolos, por ejemplo, como críticos, esenciales y de soporte. Esta clasificación generalmente se basa en el lapso máximo de interrupción (por ejemplo 1 día, 1 semana, o más de 1 semana) antes de poner seriamente en peligro las operaciones de una empresa, y todo lo que se deriva de tal situación. Adicionalmente, hay que considerar la posibilidad o no de suplir los sistemas computacionales con el trabajo manual.

## 2) **Valuación de Riesgos**

En parte en forma paralela al BIA, hay que realizar una **Valuación de Riesgos** que consiste en considerar los riesgos que pueden existir y afectar precisamente a las funciones y recursos críticos determinados antes. Más precisamente se trata de analizar el espectro de amenazas que pueden afectar los recursos y realizar una valuación de riesgos para identificar las que podrían concretarse causando impacto y daño en las operaciones.

La valuación de riesgos de los diferentes procesos o funciones permite identificar los *controles de seguridad* que mitiguen las vulnerabilidades de los activos y/o la reducción de frecuencia de ocurrencia de incidentes provocados por ataques, errores o fallas.

De esta manera y con un análisis de costo-beneficio para su posible implementación, los riesgos se reduzcan a niveles residuales aceptables para las condiciones operativas. En este punto hay que tener presente que generalmente siempre será más efectivo en costo aplicar ciertas medidas que intentar la recuperación luego de una interrupción.

La actividad de valuación de riesgos debe considerarse como crítica puesto que de sus resultados dependen, llegado el caso, las directivas y esfuerzos del grupo encargado de la recuperación de desastres. Ocurre que este equipo encarará la gestión de riesgos sólo en los riesgos identificados y de manera priorizada.

La norma ISO 17799 y su complemento de implementación la nueva ISO 27001 (antes BS 7799-2) constituyen la herramienta idónea para determinar e implementar los controles de seguridad y contramedidas o salvaguardas necesarias para reducir adecuadamente los riesgos en cuestión. Esto se lleva adelante a partir de un análisis gap entre los resultados de la valuación de riesgos y los controles de seguridad de las normas.

## 3) **Estrategias de Gestión**

Con los resultados de las dos fases anteriores, por un lado los impactos sobre recursos críticos convenientemente priorizados del BIA y por el otro los riesgos residuales a considerar, el desarrollo de un

BCP sigue con la etapa de determinación de las estrategias para el tratamiento de riesgos e impactos, así como la preparación de los procedimientos correspondientes, las pruebas y aceptación, y finalmente el mantenimiento y actualización posterior.

Se trata de decidir sobre qué medidas adoptar respecto a diferentes momentos de todo el proceso de continuidad de negocios:

- Prevención
- Respuesta o reacción a incidentes
- Reanudación o recuperación
- Restauración/Reconstitución

En el caso de la *Prevención*, como se dijo antes, las decisiones a tomar pasan por considerar que un posible paso de recuperación posterior sólo tenga que trabajar con los riesgos residuales, habida cuenta de las medidas de prevención que mitiguen los riesgos originales en cada caso. Para el caso se usan contramedidas disuasivas y preventivas.

La *Respuesta* implica una cadena de información, contactos y toma de decisiones frente a las diferentes eventualidades que se pudieren presentar según el tipo y nivel de incidentes.

La *Recuperación* comienza siempre primero por los procesos críticos de negocios incluso en un sitio alternativo. Esta eventualidad se analiza teniendo presente que en general tienen mayor costo para menor tiempo de recuperación. Algunas de dichas opciones son las que siguen:

- 1) Sitio espejado: un sistema idéntico al de producción.
- 2) Remote journaling: transmisión en línea de cambios y actualizaciones de bases de datos.
- 3) Hot site: sitio compatible con el de producción.
- 4) Cold site: sitio vacío con la infraestructura como para la instalación.

Para la elección de un sitio alternativo el principal criterio de comparación generalmente es el costo de cada opción, dado por la ubicación, el equipamiento de hardware, telecomunicaciones, documentación, y tiempo de puesta en operación.

La *Restauración*, finalmente, se refiere a las tareas necesarias para la reanudación de actividades normales en el sitio original mientras sigue funcionando el sitio alternativo. A veces se hace la distinción entre *reanudación* (resumption) y *recuperación* (recovery). En tal caso se dice que la reanudación es la recuperación de operaciones críticas de negocios, mientras que la recuperación se refiere a operaciones de negocios menos sensibles al tiempo.

La decisión sobre todas las medidas comentadas debe tomarse en función de un análisis de costo-beneficio para las diferentes estrategias analizadas.

#### **4) Pruebas**

Las **Pruebas** también constituyen una etapa importante en el proceso de un BCP, puesto que por un lado se trata de ver si el mismo funcionará cuando realmente haga falta, y por el otro que las pruebas sirvan también como entrenamiento para el equipo encargado de las mismas permitiéndoles familiarizarse con los procedimientos correspondientes.

En consecuencia, las pruebas deben planificarse con enfoque realístico. Hay que establecer adecuadamente el alcance de las mismas así como la logística, es decir los recursos necesarios para las mismas.

En muchos casos resulta conveniente realizar primero pruebas de escritorio (o de clase como también se le llaman), donde un buen análisis puede poner de manifiesto la necesidad de correcciones. A partir de estos resultados se pueden programar pruebas funcionales en un escenario de simulación de interrupción de negocios.

El resultado final de las pruebas muestra casi siempre los cambios que hay que realizar para mejorar los procedimientos seguidos en la aplicación del BCP.

### 5) Mantenimiento

La revisión del plan debe ser periódica y programada adecuadamente conforme procedimientos especialmente preparados al efecto. Un punto importante en este paso es la determinación de cuáles son los factores de posibles cambios y los procedimientos correspondientes. Considerar las actualizaciones, por ejemplo, cuando hay un equipamiento nuevo, cambios de funciones de personal clave, procesos de negocios, nuevas localizaciones de la empresa, reglamentaciones, normas, y situaciones de riesgo en general.

### Adicionales y comentarios

Una herramienta adicional que puede resultar muy útil es el conocido **Scorecard**, en este caso bajo la forma de un **tablero de control** simplificado de alcance gerencial especialmente a cuanto al área IT. Preparado como un checklist, puede usarse como base de un análisis preliminar al desarrollo de un BCP, para establecer en qué medida está preparada una organización a situaciones que afecten la continuidad de las operaciones de negocios.

El BCP incluye generalmente otros documentos, tales como:

- Plan de Recuperación de Desastres (DRP).
- Planes de Contingencia, aplicables generalmente a los sistemas IT involucrados.

Por otra parte, también es usual agregar a la documentación del BCP, los resultados del BIA y de la Valuación de Riesgos.

La norma ISO 17799 tiene un capítulo específico para la propia Gestión de Continuidad de Negocios, desarrollado en cinco controles específicos:

- 14.1.1: Inclusión de la seguridad de la información en el proceso de gestión de continuidad de negocios.
- 14.1.2: Continuidad de negocios y valuación de riesgos.
- 14.1.3: Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información.
- 14.1.4: Marco de referencia para la planificación de continuidad de negocios.
- 14.1.5: Prueba, mantenimiento y revaluación de los planes de continuidad de negocios.

Bajo la implementación establecida por la ISO 27001, el plan mismo se enmarca dentro de los controles 14.1.2, 14.1.3 y 14.1.5. El control 14.1.4, por su parte, establece los criterios unificados para la estructura del propio BCP, así como para los planes que lo complementan como el DRP y los diferentes planes de contingencia. Finalmente el control 14.1.1 contempla lo relacionado con la gestión propiamente dicha de un proyecto BCP, tal como el establecimiento del comité del proyecto, el proyecto de desarrollo y el programa de concientización y entrenamiento, la coordinación respecto de leyes y reglamentaciones, el mantenimiento del plan preparado y su ejecución, etc.

Por otra parte, la ISO 17799 tiene otras secciones también importantes desde el punto de vista de un BCP. Entonces, también pueden verse como componentes de un BCP, las áreas tratadas por la norma con referencia a la organización, seguridad en los recursos humanos, seguridad física y ambiental, control de acceso, y cumplimiento.

Las ventajas de trabajar dentro del marco establecido por las normas ISO 17799 y 27001, es que el desarrollo en cuestión adquiere características de universalidad por fuera de enfoques particulares. Con esto se gana también libertad de cambios y contrataciones de terceros en el futuro. Por otra parte, puesto que el BCP es una de las áreas que cubren estas normas, cuando en algún momento ulterior la empresa proyecte un plan de seguridad conforme las mismas, e incluso su certificación, ya el área del BCP estará conforme dichas normas, y no serán necesarias modificaciones en los puntos cubiertos.