PLAN DE CONTINUIDAD DEL NEGOCIO

Mauricio Olivari Tavera, Carlos Elías Ramírez Coll
Mauricio_olivari@hotmail.com
Caracoll2002@hotmail.com
Universidad piloto de Colombia
Especialización en Seguridad Informática
Bogotá, Colombia

Resumen--El presente artículo describe la naturaleza de los Planes de Continuidad de Negocio o 'Business Continuity Planning' (BCP), una herramienta al servicio de la empresa cuyo objeto es garantizar la continuidad del negocio ante un evento de carácter catastrófico que afecte parcial o totalmente a la misma. Nos enfocaremos, sobre todo, en el área de TI, donde la pérdida de datos críticos para el negocio y el tiempo de inactividad de los sistemas clave son dos de los mayores riesgos a los que se enfrentan los responsables de Tecnologías de la Información a la hora de planificar un Plan de Continuidad de Negocio. Este Plan debe permitir minimizar el tiempo de recuperación e impacto que afecte los niveles aceptables de servicio de los procesos críticos del negocio. A medida que avanzan las TI, emergen nuevas herramientas que facilitan tanto el mantenimiento de los sistemas como la recuperación del mismo en caso de una eventual falla; hablamos de la virtualización, Una gran alternativa para realizar Planes de Continuidad del Negocio más efectivo y con costos más reducidos.

Abstract-- This article describes the nature of the Business Continuity Plans or 'Business Continuity Planning' (BCP), a tool for the company whose purpose is to ensure business continuity to a catastrophic event affecting part or wholly thereof. We will focus mainly in the area of IT, where the loss of critical business data and downtime of critical systems are two of the biggest risks facing those responsible for Information Technology to when planning a Business Continuity Plan. This plan should allow minimize recovery time and impact affecting acceptable levels of service for critical business processes. As IT advances, new tools emerge that facilitate both system maintenance and recovery of the same in case of an eventual failure, we talk about virtualization, a great alternative for Business Continuity Plans more effective and cost lower.

Índice de Términos—Amenaza, Análisis de Impacto al Negocio o BIA, ciclo PHVA, Plan de Continuidad de Negocios o BCP, Planes de emergencia (PE), Riesgo.

I. INTRODUCCIÓN

El riesgo de que un incidente afecte las operaciones normales de un proceso siempre está latente. En algunas ocasiones se manifiesta en forma de grandes catástrofes, como una inundación por un crudo invierno, tal como le ocurrió a la universidad de la Sabana en 2011 en Colombia, Terremotos en Chile o el Tsunami en Japón; en otras ocasiones los riesgos son originados por posibles fallas humanas o tecnológicas, sabotaje, cortes de energía, fallas en comunicaciones, transporte o de seguridad, ciber-ataques por parte de un hacker, etc.

Pero no son sólo las grandes catástrofes las que pueden acabar una empresa o afectar su normal actividad. También pueden llegar a hacerlo innumerables amenazas que llegan a poner a una organización contra las cuerdas, sea cual sea su tamaño y el sector en el que opere. La estrategia para evitar sus terribles consecuencias es un Plan de Continuidad de Negocio (BCP) probado y continuamente actualizado.

Los BCP están indicados para medianas y grandes empresas que ya disponen de planes de emergencia pero necesitan un Plan Director que

establezca pautas de actuación que van más allá de una solución inmediata a la emergencia.

Pero, ¿Qué es el Plan de Continuidad del Negocio? El Plan de Continuidad de Negocio es un plan proactivo que busca asegurar que los productos o servicios continúen siendo entregados durante una interrupción no planeada. Cualquier empresa de cualquier tamaño debería planificar la mitigación del daño producido por un desastre disponiendo de un plan de continuidad del negocio, el cual incluye:

- Planes, medidas y disposiciones para asegurar la entrega continua de los servicios y/o productos que le permitan a la Organización recuperar sus instalaciones, información y activos.
- Identificación de los recursos necesarios para respaldar la continuidad del negocio, incluyendo personal, información, equipos, recursos financieros, apoyo legal, seguridad y alojamientos en caso de ser necesarios.

La responsabilidad del establecimiento de un plan de continuidad de negocio (BCP) es de la alta gerencia. El plan deberá tratar todas las funciones y recursos humanos/materiales requeridos para que la organización sea viable después de que ocurra una interrupción, minimizando de esta forma sus consecuencias.

Implementar un BCP mejora la imagen de la Organización con sus empleados, accionistas y clientes al demostrar una actitud proactiva. Dentro de los beneficios adicionales podemos incluir una mejora en la eficiencia organizacional, así como también permite identificar la relación entre los activos, recursos humanos, los recursos financieros y los productos y servicios críticos de la organización.

Enfocándonos en las TI, el procesamiento de los sistemas de información suele ser un componente crítico, porque muchos de los procesos clave de negocio dependen de la disponibilidad de los recursos y de los datos que manejan.

El primer paso para construir nuestro Plan de Continuidad del Negocio es realizar un análisis de riesgos en el que se ilustren las dependencias entre los procesos críticos de negocio, las aplicaciones, los sistemas de información y los componentes de la infraestructura de TI. El resultado de este análisis es la clasificación de los componentes de TI según su importancia, con sus amenazas y vulnerabilidades. A partir de este momento es conveniente implementar un plan de acciones correctivas para proteger todos y cada uno de sus componentes. En este punto se puede llevar a cabo un Análisis de Impacto del Negocio (BIA, por sus siglas en inglés – Business Impact Analysis) para investigar las pérdidas que sufriría el negocio si se produjera una interrupción.

Este análisis permite cuantificar las posibles pérdidas después de una interrupción, con el objetivo de que la organización pueda tomar decisiones sobre los procedimientos y mecanismos para proteger sus activos clave en función del máximo tiempo posible de inactividad.

En síntesis, La ejecución de un Plan de Continuidad de Negocios permite que los productos o servicios críticos sigan siendo entregados a los clientes. En vez de enfocarse en restablecer las operaciones después de que estas se interrumpan por un desastre, un plan de continuidad se enfoca en que los procesos críticos continúen estando disponibles.

Así mismo, a medida que evolucionan las TI, también surgen nuevas herramientas en las que nos podremos apoyar y así realizar Planes de Continuidad del Negocio que respondan de manera más efectiva a eventualidades inesperadas. En este punto emergen tendencias como la virtualización de la infraestructura informática, donde las empresas

pueden minimizar riesgos y crear un entorno más flexible.

II. OBJETIVOS DEL BCP

Implementar un Plan de Continuidad del Negocio, busca que se cumplan ciertos objetivos que mencionaremos a continuación:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización, en caso de que un incidente interrumpa las operaciones informáticas en las que se apoyan.
- Proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.
- Identificar y estudiar los puntos débiles de la empresa.
- Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto, reduciendo así los impactos resultantes de interrupciones de trabajo a corto plazo.
- Mantener la buena imagen de la empresa hacia sus clientes y proveedores.
- Analizar nuevas posibles formas de comunicación e infraestructura.
- Conocer la logística de la empresa para restablecer los sistemas de la empresa.
- Ofrecer nuevas alternativas para salvaguardar el funcionamiento de la empresa ante situaciones críticas.[1]

III. GESTION DEL BCP

La Gestión de la Continuidad del Negocio es el conjunto de actividades que se llevan a cabo en una organización para asegurar que todos los procesos críticos del negocio estarán disponibles para los clientes, proveedores, y otras entidades que deben acceder a ellos.

Para ejecutar de manera organizada un BCP es necesario:

- Definir un comité responsable del plan.
- Asignar responsabilidades por cada equipo de trabajo.
- Indicar las actividades de cada una de las fases del proyecto.
- Documentar los procesos.
- Presentar los avances.
- Obtener la aprobación por parte de los directivos.

Las responsabilidades del coordinador de esta etapa son:

- Dirigir la definición de objetivos, políticas y actividades críticas.
- Coordinar y organizar directores por cada fase del proyecto.
- Controlar el proceso de BCM a través de métodos de control efectivo y gestión de cambio.
- Presentar el proceso a Directivos y personal.
- Desarrollar el plan y presupuesto para iniciar el proceso.
- Definir y recomendar procesos de estructura y gestión.
- Dirigir el proyecto a desarrollar e implementar el proceso del BCM.

Con la finalidad de hacer perdurar el plan a lo largo del tiempo, este deberá ser objeto de funciones de mantenimiento y revisión periódicas, lo que servirá para que la empresa siga adaptándose a los cambios del entorno que afectan su ejercicio.

Crear y mantener un BCP le sirve a una organización para conseguir los recursos necesarios para enfrentar cualquiera de estas situaciones.

IV. FASES DEL BCP

El alcance de un BCP no está definido. Se debe acotar con la participación de cada organización para qué tipo de amenazas se va a definir el mismo o si contemplamos todas las posibles amenazas al negocio. Normalmente, son objeto del BCP los procesos definidos como críticos en la fase inicial de evaluación de impactos al negocio.

Como cualquier plan que se desea implementar, el BCP consta de varias fases o etapas:

A. *La fase inicial*. En esta fase se establece la necesidad de desarrollar el BCP en la organización, de tal manera que se comunica la importancia de realizar este plan, involucrando a los directivos y el personal de la empresa. Se establecen los roles y recursos que participarán para la construcción del mismo; de lo cual se escribió en el capítulo anterior(Gestión del BCP).

B. *Evaluación y Control.* Consiste en realizar un análisis de riesgos en el que se ilustren las dependencias entre los procesos críticos de negocio, las aplicaciones, los sistemas de información y los componentes de la infraestructura de TI. Lo anterior se convierte en el principal insumo para la detección de los posibles impactos os pérdidas que sufriría el negocio si se produjera una interrupción en los procesos del negocio (BIA). La organización deberá analizar todos los puntos críticos de su proceso de producción o servicio en los que se debe centrar el BCP. Se establecerán indicadores que serán el punto de partida del plan e informarán sobre el grado de respuesta que éste ofrece. Es necesaria una exhaustiva evaluación de riesgos que incluya tanto aquellos accidentes y eventos cuya materialización pueda implicar la desaparición del negocio, como otros que perturben gravemente su normal desarrollo.

C. *Desarrollo e implementación del BCP*. Tomando como base la información que arrojan los resultados del Análisis de Riesgo y el BIA, se prepara la estrategia y la logística necesaria para garantizar la continuidad de cada uno de los procesos críticos identificados.

D. *Concientización y Capacitación*. Ante la imprevisible evolución de cada emergencia/contingencia, los BCP no incluyen, en la mayoría de los casos, pautas concretas de actuación, sino pautas de carácter general. Esto implica un conocimiento exhaustivo del negocio por parte del personal involucrado en el BCP, así como una rápida capacidad de respuesta. Sin embargo es necesario que la organización prepare a sus empleados ante la presencia de un cambio, logrando minimizar esa resistencia y obteniendo mejor disposición ante situaciones de este tipo creando una cultura de aceptación ante un evento que perturbe su labor.

E. *Mantenimiento.* En un BCP también se debe manejar el ciclo PHVA(Planear – Hacer – Verificar – Actuar), el cual permite que siempre se encuentre actualizado y mejorado.

F. *Plan de comunicaciones de Crisis*. Se debe concretar el plan de comunicaciones como complemento al BCP o como parte integrante del mismo. En este punto se propone desarrollar, coordinar, evaluar y ejercitar planes para comunicarlos a directivos, personal, usuarios, proveedores y medios de comunicación, de tal forma que el entorno de la organización se entere de su estado y en caso de crisis poder reaccionar de forma adecuada.

G. *Coordinación con Autoridades Públicas.* En esta etapa se quiere que la organización tenga una clara definición y documentación de las políticas a implementar como un documento obligatorio

en la organización. Por lo tanto, en este proceso la organización vera los resultados en la mejoría de los procesos de toda su organización, teniendo en cuenta que las políticas están dirigidas a la organización como un todo.[2]

Revisando cada una de las fases referenciadas anteriormente, podríamos decir que hay una que constituye la base fundamental para la creación de un buen Plan de Continuidad del Negocio, y esta es el Análisis de Impacto al Negocio (BIA), sobre el cual trataremos en el siguiente capítulo.

V. ANALISIS DE IMPACTO AL NEGOCIO (BIA)

Como lo comentábamos anteriormente, la base fundamental para crear un buen plan de negocio es la realización del (BIA). Éste es básicamente un informe que nos muestra los costos o pérdidas que se generarían la interrupción de los procesos de negocio.

Una vez obtenido este informe, la compañía tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial).

Al realizar una clasificación de los activos, que son los bienes y derechos que representan un valor para la empresa, y apoyándonos en el BIA (Análisis de Impacto de Negocio) se identifica que los componentes claves requeridos para continuar con las Operaciones de Negocio luego de un incidente, son principalmente los siguientes:

- Capital Humano
- Activos materiales
- Áreas de trabajo
- Registros vitales- Backups de información
- Aplicativos Críticos
- Dependencias con Terceras partes
- Imagen de empresa

Tres aspectos claves para realizar este análisis (BIA) son:

- Criticidad de los recursos de información relacionados con los procesos críticos del negocio
- Período de recuperación crítico antes de incurrir en pérdidas significativas
- Sistema de clasificación de riesgos

VI. GOBIERNO DEL BCP

Un BCP contiene una estructura de gobierno, a menudo en la forma de un comité que asegura un compromiso de alta dirección y define las funciones de alta dirección y sus responsabilidades. Este comité es el responsable de la supervisión, inicio, planeación, aprobación, ensayos y auditorias al BCP. Asimismo implementa el BCP, coordina actividades, aprueba los resultados que arroje el BIA, supervisa la creación de planes de continuidad y revisa los resultados de actividades de aseguramiento de calidad.

Los directivos de un Comité BCP normalmente:

- Aprueban la estructura de gobierno
- Aclaran cuáles son sus funciones y las de todos los que participan en el programa
- Revisan la creación de comités, grupos de trabajo y equipos que van a desarrollar y ejecutar el plan
- Suministran orientación estratégica
- Aprueban los resultados del BIA
- Revisan los productos y servicios críticos que se han identificado
- Aprueban los Planes de Continuidad
- Monitorean las actividades de aseguramiento de calidad,
- Resuelven conflictos de interés

El comité del BCP normalmente está compuesto por los siguientes miembros:

- Líder Ejecutivo, quien tiene la responsabilidad general del comité del BCP; solicita el apoyo de la alta dirección y dirección, y asegura la financiación adecuada para el BCP.
- Coordinador del BCP asegura el apoyo de la alta dirección, estima requisitos de financiación, desarrolla la política del BCP, coordina y supervisa el proceso de BIA, asegura participaciones eficaces de los lideres de procesos, coordina y supervisa el desarrollo de los planes y disposiciones para la continuidad del negocio; establece grupos de trabajo y equipos y define sus responsabilidades; coordina jornadas de capacitación, y establece la revisión periódica, pruebas y de auditorías del BCP.
- Oficial de Seguridad, quien trabaja para garantizar que todos los aspectos del BCP cumplen con los requisitos de seguridad de la organización.
- Jefe de Información el cual coopera estrechamente con el coordinador del BCP y especialistas IT en planes de continuidad.
- Líderes de proceso, quienes suministran información valiosa sobre las actividades de la organización, y revisan los resultados del BIA.[3]

VII. PLAN DE CONTINUIDAD DEL NEGOCIO Vs PLAN DE CONTINGENCIA

A menudo se las personas suelen confundir estos dos términos para referirse a lo mismo, Para un mayor entendimiento, podemos decir que un Plan de Contingencia consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil que soportan la información y los procesos de negocio considerados críticos en el PCN de la compañía.

Por su parte, el Plan de Continuidad de Negocio puede ser definido como un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto en los procesos de negocio de una compañía.[4]

VIII. TENDENCIA DEL BCP EN LAS TI

Virtualización.

El mantenimiento de sistemas es una de las responsabilidades de los departamentos de TI. Asegurar la continuidad de negocio es importante en la mayoría de las empresas, debido a la dependencia que tienen de las infraestructuras informáticas. La virtualización puede ayudar a las organizaciones a estar más protegidas.

No todas las empresas pueden invertir en hardware redundante o en instalaciones de recuperación frente a desastres. La mayoría de las empresas se limitan a usar cintas para sus copias de seguridad, y mientras que esto es aceptable para almacenamiento a largo plazo, no facilita mucho el proceso de recuperación en caso de algún fallo.

La virtualización facilita mucho esta situación: gracias a la creación de una máquina virtual, junto con su sistema operativo, aplicaciones y datos, se puede tratar cada entorno como si fuera un fichero. Esto significa que una organización puede estar más protegida contra los riesgos de caídas del sistema y recuperarse más rápido después de experimentar cualquier problema.

Emplear la virtualización para asegurar la continuidad de negocio y la recuperación frente a desastres permite a las empresas beneficiarse de dos puntos clave: una máquina virtual se puede copiar y mover de sitio, y es independiente del hardware que lo ejecuta. Desde el punto de vista de continuidad, esto conlleva varias ventajas importantes. La copia de una máquina virtual significa que se puede

mantener una réplica exacta en un centro remoto, ya sea como parte de un sistema stand-by en caliente o guardado en una cinta. En el caso de un fallo, se puede arrancar la máquina virtual almacenada en otro sistema y los usuarios pueden acceder al servicio de forma rápida y sencilla.

En segundo lugar, la independencia del hardware de la máquina virtual significa que la organización no tiene por qué invertir en hardware de respaldo específico; cualquier plataforma servidor que ejecute el mismo hipervisor puede funcionar como host a la máquina virtual. Esto significa que incluso las pequeñas organizaciones pueden implementar una estrategia completa en caso de desastre.

Los “Snapshots” (instantáneas) son otra de las ventajas clave de la virtualización: gracias a que una máquina virtual puede tener múltiples versiones de sí misma guardadas en el tiempo, las empresas pueden guardar copias que saben que funcionan. En el caso de tener que implementar un parche, se puede probar en un entorno virtual primero y luego ponerlo en producción. Si surgiera algún problema que afectase a la máquina virtual, la empresa puede recuperar la versión anterior y utilizarla.

Mediante la virtualización de la infraestructura informática, las empresas pueden minimizar riesgos y crear un entorno más flexible.

La virtualización también puede usarse para reducir el tiempo requerido por los tiempos de inactividad programados: gracias a herramientas como VMotion, las máquinas virtuales se pueden mover por la infraestructura de una empresa. En el caso de que algún servidor físico requiera algún tipo de mantenimiento preventivo, las máquinas virtuales que lo soportan se pueden mover a otros hosts dentro de la infraestructura virtual mientras se realizan los trabajos. Una vez completada la tarea, se vuelven a migrar las máquinas virtuales.

Mantener la continuidad del negocio implica entender los procesos de negocio de la empresa y cómo un fallo del sistema puede ocasionar una reducción de ingresos y una mala reputación. Mediante la virtualización de la infraestructura informática, las empresas pueden minimizar estos riesgos y crear un entorno más flexible. La posibilidad de recuperar el servidor de correo electrónico de forma rápida gracias a una máquina virtual de respaldo, no sólo ahorra gastos en hardware y mantenimiento, sino que permitirá al técnico salir de la oficina el viernes por la noche.[5]

IX. Conclusiones

Después de realizar el estudio acerca de un Plan de Negocio, mediante la lectura de gran cantidad de información al respecto, llegamos a las siguientes conclusiones:

- Garantiza la continuidad de los procesos ante desastres y eventualidades.
- Es un plan maestro de planes de contingencia de áreas de negocio y de contingencia de las infraestructuras en las que se soporta el negocio, entre ellas los sistemas de información y las comunicaciones.
- Mejora en la eficiencia organizacional, así como también permite identificar la relación entre los activos, recursos humanos, los recursos financieros y los productos y servicios críticos de la organización.
- Una apropiada respuesta a una crisis que se presente requiere de equipos que lideren y respalden las operaciones de respuesta.
- Los miembros del equipo deben seleccionarse teniendo en cuenta capacitación y experiencia para asignarles tal responsabilidad.
- La meta de la recuperación y restauración es recobrar la operatividad de la organización

manteniendo la entrega de productos y servicios críticos.

- El Plan de Contingencia es uno de los elementos más importantes de Plan de Continuidad del Negocio, que lo veríamos como un orquestador de planes.
- No debemos tener dudas al afirmar que el Plan de Contingencia es uno de los elementos más relevantes de un Plan de Continuidad de Negocio, y que si tenemos en cuenta la dependencia casi absoluta que las organizaciones y empresas de cualquier tipo tienen de los Sistemas de Información y de las Comunicaciones, nos daremos cuenta rápidamente de que a día de hoy es difícil dar Continuidad sin tener Contingencia de las TIC. Y decimos "difícil" y no "imposible", pues en ocasiones podremos buscar alternativas "manuales" para aquellas actividades que en condiciones normales realizamos apoyándonos en las TIC.

X. Reconocimientos

Ing. Ramiro Merchán. Experto en Planeación de la Continuidad del Negocio (CISA, CBCP).

XI. Referencias

[1] Juan Gaspar Martínez. Plan de Continuidad del Negocio. Guía práctica para su elaboración. Diaz de Santos, Madrid, México, Buenos Aires, 2006

[2] BS-25999.

[3] Art. Seguridad de la Información en Colombia. [Online].
Available: http://blog.segu-info.com.ar/2010/06/plan-de-continuidad-de-negocios-o.html#axzz2R1hSENld

[4] Art. Contingencia TIC vs Continuidad de negocio. Manuel Díaz Sampedro. [Online].
Available:
http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios//Contingencia_vs_Continuidad.

[5] Art. Seguridad de la Información en Colombia. [Online].
Available:
http://www.itcio.es/virtualizacion/opinion/1005195010102/virtualizacion-continuidad-negocio.1.html

Autores

Olivari Tavera Juan Mauricio ingeniero de sistemas de la universidad el bosque. Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia

Ramírez Coll Carlos Elías ingeniero de sistemas de la universidad el bosque. Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia