Continuidad del Negocio

Heidi Paola Morales Moreno

Universidad Piloto de Colombia

Bogotá, Colombia

heidip48@hotmail.com

Resumen - Este artículo menciona algunos acontecimientos mundiales que se han presentado en los últimos años, como desastres naturales, ataques cibernéticos que alertaron a las organizaciones sobre el por qué un plan de continuidad del negocio debe ser parte importante de cualquier organización; los factores a considerar para la implementación, los estándares y las mejores prácticas existentes, que permitirán en casos de desastres naturales, fallas de infraestructura, ataques cibernéticos, fallas humanas, entre otros, asegurar la recuperación en el menor tiempo posible de los procesos críticos de la organización para continuar ofreciendo sus productos o servicios.

Abstract - This article mentions some world events that have occurred in recent years, including natural disasters, cyber attacks alerted organizations on why a business continuity plan should be an important part of any organization; Factors to consider for implementation, standards and best practices that will allow in natural disasters, infrastructure failures, cyber attacks, human errors, among others, ensure recovery in the shortest possible time critical processes the organization to continue to offer their products or services.

***Palabras clave* – Continuidad del Negocio, Análisis de Impacto, Procesos Críticos, Estrategias de Recuperación, Tiempo de Recuperación.**

I. INTRODUCCIÓN

En los últimos años se han presentado eventos a nivel mundial para los que evidentemente no se estaba preparado por su magnitud y la manera en la que se presentaron, casos como los atentados de las torres gemelas, tsunami, terremotos, incendios, delitos cibernéticos como el de Anonymous, fallas tecnológicas de empresas como BlackBerry, desastres financieros, todos éstos despertaron las alertas de las diferentes organizaciones para que se gestionara un plan de continuidad del negocio, y se entendiera la importancia de estar preparados para todos los cambios que se presentan hoy en día en cuanto a tecnología, cambios climáticos, entre otros y asimismo tener en cuenta que los factores importantes para iniciar un plan de continuidad son: Procesos, personas y tecnología.

II. CONCEPTOS GENERALES DE CONTINUIDAD DEL NEGOCIO

Plan de Contingencias: Es un documento desarrollado en forma preventiva, con el objetivo de servir de guía de acción antes, durante y después de la ocurrencia de un imprevisto. [1]

Plan de Recuperación de Desastres (DRP): Conjunto de procedimientos definidos para proteger y recuperar la infraestructura IT del negocio en caso de un evento de desastre. [1]

Plan de Continuidad del Negocio (BCP): Es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo o nulo ante una contingencia. [1]

III. PLAN CONTINUIDAD DEL NEGOCIO

Algunos estudios en el mundo muestran las siguientes cifras que hacen que se tome conciencia de la importancia de tener un plan de continuidad:

Un estudio del Disaster Recovery Institute afirma que el 90 por ciento de las empresas que tienen pérdidas significativas de datos quiebra en el plazo de tres años.

El 40 por ciento de las empresas que sufren un desastre no vuelve a abrir nunca y el 60 por ciento cierra en los siguientes tres años.

Un informe de la firma de analistas Enterprise Strategy Group indicaba que el mercado contaba con un promedio del 30 por ciento de fallos en copias de seguridad y de un 50 por ciento en

restauración de archivos. Al realizar el estudio, muchos departamentos de TI reconocían no estar seguros de ser capaces de recuperar todos los datos críticos de negocio y si se podía realizar en un tiempo aceptable.

IBM ha realizado un estudio a nivel internacional sobre los sectores que sufren más interrupciones en las actividades de negocio debido a desastres. Banca y Finanzas, con un 26 por ciento; Gobierno, Administraciones Públicas e Instituciones (19 por ciento) y Educación (11,3 por ciento) se sitúan en las primeras posiciones, seguidos por Industria (10,9 por ciento), Servicios (9,5 por ciento) y Comunicaciones (8,2 por ciento). [2]

Así que la continuidad del Negocio en las organizaciones debe ser una de sus prioridades, ya que permite continuar con la entrega a sus clientes de los productos o servicios críticos que produce, en caso de presentarse eventos como: desastres naturales, fallas técnicas, falta de recursos, fallas de servicios públicos, ataques cibernéticos, entre otros.

Así que se indican los siguientes objetivos de un plan de continuidad del Negocio para cualquier tipo de organización:

- Proteger los intereses de sus clientes, del negocio y la imagen de la organización.
- Identificar los puntos débiles en los sistemas de la organización.
- Analizar las comunicaciones e infraestructura de la organización.
- Definir la manera para reestablecer los servicios, independientemente de los sistemas.
- Ofrecer alternativas viables a todos los procesos críticos de negocio.[3]

Teniendo en cuenta los objetivos mencionados hay dos factores indispensables para la implementación de un plan de continuidad del negocio: compromiso y conocimiento de las personas de éste y ser conscientes que este plan no involucra solamente a el área de tecnología, sino a todos los procesos de una organización.

A. Aspectos importantes de continuidad del negocio

Algunos aspectos que se definen para la implementación son:

- Realizar el análisis de riesgos que puedan afectar las actividades de la organización
- Tener una comunicación clara, en la que cada persona entienda qué debe realizar y cómo lo debe realizar para la recuperación de las actividades ante un evento.
- El plan de continuidad de negocio debe ser sencillo, ser claro para las personas las actividades que debe realizar, todos los funcionarios de la organización lo deben conocer estén directa o indirectamente involucrados con el pan de continuidad.
- Debe estar enfocado a proteger la vida humana, los activos de la información, administrar los riesgos y garantizar que los procesos críticos de la compañía continúen sus actividades.
- Debe ser flexible, ya que estos planes de recuperación se deben estar actualizando, de acuerdo a los cambios externos.
- Debe existir un comité de emergencias, encargado de gestionar la situación de crisis, organizar las personas y asegurar la recuperación
- Se deben definir escenarios y estrategias pensando en lo peor que se puede presentar

Además se debe tener en cuenta varios escenarios de desastres que se puedan presentar, de acuerdo a los procesos críticos de la organización, pensar en que se puede presentar perdida de información, en que se puede tener bloqueado el acceso a los sistemas de información, a las instalaciones, la disponibilidad de los proveedores y siempre tener presente que todos los planes se deben ejecutar de forma ordenada entre procesos, personas y tecnología.

B. Fases de la Continuidad del Negocio

Las fases sugeridas de acuerdo a las mejores prácticas para la implementación son:

1) *Definición del proyecto*, objetivos, alcance y peores escenarios
2) *Análisis de Impacto BIA*, que consiste en realizar una evaluación de los procesos y sistemas del negocio, con el objetivo de identificar:

- Áreas, funciones y/o procesos sensibles a interrupciones
- Interdependencia entre procesos internos y externos
- Impactos financieros de las interrupciones
- Impactos Operacionales de las interrupciones
- Sistemas de información críticos para la operación
- Tiempos objetivo de recuperación (RTO)
- Puntos Objetivo de recuperación (RPO)
- Clientes y proveedores críticos de la organización
- Recursos necesarios para la recuperación de operaciones
- Épocas críticas para la operación del negocio [4]

3) *Selección de estrategias*, recursos disponibles y controles, ventajas y desventajas y elegir la estrategia más conveniente de acuerdo a los procesos críticos de la organización
4) *Desarrollo de los planes de continuidad*, elaborar procedimientos para afrontar las diferentes situaciones
5) *Pruebas y mantenimiento del plan de continuidad*, debe ser probado periódicamente para identificar fallas y mejorarlas, se debe tener en cuenta como mínimo copias de seguridad, las personas y los procesos involucrados

Lo más importante y lo que hace que estos planes permitan que se recuperen en el tiempo menos posible los procesos críticos, es lo preparadas que se encuentran las personas y el conocimiento de lo que debe realizar.

La figura 1 muestra el costo de una interrupción del negocio, y de las estrategias de recuperación

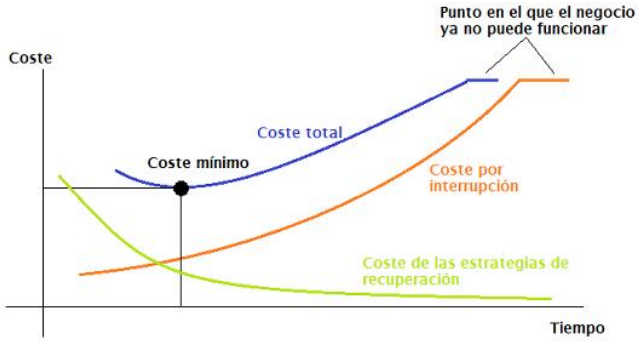

Fig.1 Costo de una interrupción del negocio. [5]

En la figura 2 se muestra las bases de la planeación de la Continuidad del Negocio

Fig2. Planeación de la Continuidad del Negocio. [6]

La figura 3 muestra el ciclo de vida de la planeación de la Continuidad del Negocio

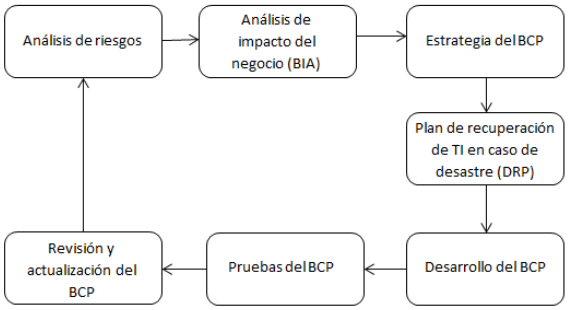

Fig.3 Ciclo de vida de la planeación de la continuidad del negocio. [5]

IV. PASOS A SEGUIR CUANDO SE PRESENTA LA INTERRUPCIÓN DEL NEGOCIO

Al presentarse la interrupción de los procesos críticos del negocio se deberían seguir las siguientes etapas, de acuerdo a lo indicado en los numerales anteriores:

A. Respuesta

La respuesta a incidentes involucra el despliegue de todos los equipos, planes, medidas y estrategias. Las siguientes tareas se ejecutan durante la fase de respuesta:

1) *Gestión del Incidente:* La gestión del incidente incluye las siguientes actividades:
   - Notificar a la Alta Dirección, empleados y accionistas
   - Asumir el control de la situación
   - Identificar el rango y el alcance del daño
   - Implementar planes de acción
   - Identificación de daños a la infraestructura.
   - Coordinar el apoyo de personas externas e internas.
2) *Gestión de Comunicaciones: L*a Gestión de Comunicaciones es fundamental para evitar la creación de rumores, mantener contacto con la prensa, servicios de emergencia y proveedores, empleados, accionistas y terceros interesados. Los requerimientos de comunicaciones pueden requerir sistemas redundantes, así como la creación de un plan para establecer todos los requerimientos de comunicaciones bajo una situación no deseada.

3) *Gestión de Operaciones:* Cuando se presente una interrupción, la Organización puede manejarse desde un Centro de Operaciones de Emergencia, lo cual garantiza que se centraliza la información, se coordinan los recursos y se asegura una respuesta efectiva a la situación. Por esto es importante contar como parte de las estrategias de un centro alterno de operaciones, a donde se puedan desplazar los empleados claves para la recuperación de los procesos críticos.

B. Continuidad

La continuidad tiene como propósito asegurarse de que los servicios o productos críticos continúan siendo entregados a los clientes, o en caso contrario, que el tiempo de espera no sea mayor a los límites establecidos en el análisis de Impacto (BIA)

C. Recuperación y Restauración

La meta de la recuperación y restauración es recobrar la operatividad de la organización manteniendo la entrega de productos y servicios críticos. En esta etapa se incluyen las siguientes actividades:

- Decidir donde reiniciar operaciones: utilizar un sitio alterno de operaciones
- Regreso del personal a las instalaciones
- Adquirir los recursos adicionales para restaurar por completo la operación.
- Restablecer las operaciones normales de la organización.
- Reanudación de las operaciones en los niveles anteriores a la interrupción [7]

V. ESTÁNDARES Y BUENAS PRÁCTICAS PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO

En esta sección mostramos los estándares y buenas prácticas existentes para la implementación del Plan de Continuidad del Negocio.

A. ISO 22301:2012

En el año 2007, se publicó la norma británica BS 25999, se divide en dos partes:

Primera parte: Código de buenas prácticas, que proporciona una guía de recomendaciones de buenas prácticas en cuanto a Gestión de la Continuidad del Negocio (BCM)

Segunda parte: Publicada el 20 de noviembre 2007, proporciona los requisitos de un Sistema de Gestión de Continuidad de Negocio (SGCN) basado en las mejores prácticas de SGC. Incluye un estándar que sirve para demostrar el cumplimiento vía auditoría y proceso de certificación.

Y luego fue reemplazada en el año 2012 por la norma ISO 22301:2012 Sistemas de Continuidad del Negocio-Requisitos. [8]

En la figura 4 se muestra los elementos de continuidad del negocio, mediante el ciclo PDCA en ISO 22301:2012

Fig. 4 Elementos de continuidad del negocio mediante el ciclo PDCA. [8]

El modelo anterior ha sido creado con consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000-1:2011, ISO 14001:2004 y con ISO 28000:2007.

B. Metodología DRII (Disaster Recovery Institute International)

Constituye el conjunto de prácticas profesionales para la Gestión de Continuidad de Negocio, cuyo objetivo principal es permitir a las operaciones comerciales de la empresa, el seguir operando bajo condiciones adversas, al implantar: iniciación y manejo del proyecto, evaluación de riesgos, análisis de impacto al negocio (BIA), selección de estrategias de continuidad, respuesta a emergencias, desarrollo de los planes de continuidad, ejercicios y mantenimiento de los planes de continuidad, sensibilización y programas de entrenamiento.[9]

C. ISO/IEC 27001:2013

Esta norma define cómo organizar la seguridad de la información en cualquier tipo de organización. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información [10], y en su Anexo A.17 está enfocado a los aspectos de seguridad de la información en la gestión de continuidad del negocio distribuidos así: A.17.1.1 Planificación de la continuidad de la seguridad de la información, A.17.1.2. Implementación de la continuidad de la seguridad de la información. A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

D. ITIL V3

ITIL V3 es un marco para la gestión de servicios de TI que se ocupa de la planificación, aprovisionamiento, diseño, implementación, operación, soporte y mejora de los servicios de TI que sean adecuados para las necesidades del negocio, así que proporciona buenas prácticas para lo que se hace para el diseño de la recuperación ante desastres de TI.[11]

E. BCI (Business Continuity Institute)

Es la principal organización de certificación de profesionales en Continuidad de Negocio. El BCI busca promover y facilitar la adopción de buenas prácticas de continuidad de negocio en todo el mundo a través de:

- Mejora de los estándares en la continuidad del negocio.
- Investigación de las organizaciones
- Compromiso
- Liderazgo de conocimiento en la continuidad del negocio.
- Facilitar el intercambio de las mejores prácticas en la continuidad del negocio.
- Capacitación y certificación de profesionales de BC [12].

En el año 2013 se publicó la nueva Guía de Buenas Prácticas (Good Practice Guidelines – 2013).

F. COBIT

Es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI). Así que es una herramienta que proporciona un enfoque a la continuidad de las operaciones, ya que cuenta en el dominio de Entrega y Soporte, en el proceso DS4 con 13 objetivos de control los cuales permitirán

asegurar la continuidad del servicio y asimismo la continuidad de las operaciones. [13]

G. NIST 800 – 34

Es una guía para la implementación de planes de contingencia para TI, identifica principios fundamentales de planificación basándose en el ámbito del gobierno de TI. La planificación de contingencia se refiere a las medidas provisionales para recuperar los servicios del sistema de información después de una interrupción. Las medidas provisionales pueden incluir la reubicación de los sistemas de información y un sitio alterno de operaciones, la recuperación de las funciones de los sistemas de información que utilizan equipos, o el rendimiento de las funciones del sistema de información que utilizan métodos manuales. Así que esta guía se dirige a los planes de contingencia específicos, recomendaciones de tres tipos de plataformas y proporciona estrategias y técnicas comunes a todos los sistemas.

- Los sistemas cliente / servidor;
- Los sistemas de telecomunicaciones; y
- Sistemas mainframe. [14]

VI. CONCLUSIONES

Toda organización sea grande, mediana o pequeña, debe contar con un plan de continuidad de negocio.

La continuidad de negocio no depende solamente del área de tecnología, se encuentran involucrados todos los procesos, áreas y personas de una organización

La planeación de la continuidad del negocio debe estar enfocada a la gestión de riesgos de la organización

Al definir estrategias y escenarios de desastres es necesario pensar en el peor de estos y así estar mejor preparados.

La capacitación de las personas y el conocimiento del plan de continuidad son factores importantes para el mejoramiento de éste.

Un Plan de continuidad se debe enfocar en mantener la continuidad de los procesos críticos de la organización.

Las pruebas del plan de continuidad se deben realizar periódicamente, para evaluar si los procedimientos corresponden a la realidad y si arrojan los resultados esperados, y así poder mejorar e identificar los puntos débiles de la organización

El plan de continuidad debe estar actualizando constantemente de acuerdo a los cambios en la tecnología, personal y procesos.

Para el plan de continuidad se deben tener los recursos suficientes disponibles en cuanto a personas y tecnología, para que sea exitoso.

Para la implementación de un plan de continuidad del negocio es necesario implementar unas de las metodologías existentes de acuerdo a su organización y que permita tenerlo a corto plazo.

REFERENCIAS

[1] *Etek Reycom (2010). Plan de continuidad de negocios*. http://www.reycom.com.ar/mail/10/enero10/bcp.html
[2] *Almudena Jiménez. Itcio.es* http://www.itcio.es/planes-contingencia/informes/1003551016902/plan-continuidad-negocio-salvavidas-empresa.2.html
[3] *Federico Pineda(2012). 4 puntos clave para la continuidad en el negocio.* http://www.logisticamx.enfasis.com/notas/65226-4-puntos-clave-la-continuidad-el-negocio
[4] *Sisteseg(2013). Plan para la continuidad del negocio (bcp y drp).*http://www.sisteseg.com/sindustrial.html
[5] Pilar González (2012). El plan de continuidad de negocio (BCP). http://www.seinhe.com/blog/84-el-plan-de-continuidad-de-negocio-bcp
[6] Presentación continuidad del negocio
[7] http://seguridadinformacioncolombia.blogspot.com/2010/06/plan-de-continuidad-de-negocios-o.html
[8] Dijan Kosutic blog (2012). ISO 22301 vs. BS 25999-2 – Infografía http://blog.iso27001standard.com/es/2012/05/22/iso-22301-vs-bs-25999-2-infografia/
[9] *Plan de Continuidad de Operaciones.* http://www.safety-management.eu/PDF/normas_bcm.pdf
[10] *Academy 27001. Conceptos básicos sobre ISO 27001.* http://www.iso27001standard.com/es/que-es-la-norma-iso-27001
[11] Paul Kirvan. Proyectar con COBIT e ITIL el plan de recuperación de desastres (2014). http://searchdatacenter.techtarget.com/es/consejo/Proyectar-con-COBIT-e-ITIL-el-plan-de-recuperacion-de-desastres
[12] *(2014) Business Continuity Institute Website*. http://www.thebci.org/index.php/about/generalinfo
[13] *Jose Angel Peña(2013). COBIT aplicado para asegurar la continuidad de las operaciones.* http://www.isaca.org/chapters7/Monterrey/Events/Documents/20050920%20Cobit%20para%20asegurar%20continuidad%20operaciones.pdf
[14] Planes de Contingencia. http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations/2-2b-contingency-planning-swanson-nist.pdf
[15] *Dri International. Website*. https://drii.org/
[16] *Disaster Recovery Journal. Website*. http://www.drj.com/
[17] *Group Global Continuity*. http://www.globalcontinuity.com/