EL SUBVALORADO BCP Y DRP EN LAS EMPRESAS: ¿IGNORANCIA O INCAPACIDAD?

Carlos Emilio Osorio Lobo
Universidad Piloto de Colombia
Bogotá, Colombia
millo12@gmail.com

Resumen - A continuación se mostrará de una manera superficial y a grosso modo aspectos inherentes a los planes de continuidad del negocio y de recuperación ante un desastre y de cómo el ultimo es uno de los tantos aspectos que debe tener el primero para solventar de una manera eficiente y sobre todo efectiva, una situación imprevista, crítica y accidental en una compañía o negocio.

Abstract - Then it will be shown in a superficial way and grosso inherent aspects plans business continuity and recovery disaster and how the latter is one of many aspects that should be the first to solve in an efficient way and all effective , an unexpected critical and accidental situation in a company or business.

Figura 1 – Bussiness Continuity Planning y Disaster Recovery Plan [1]

Palabras Claves - BCP, DRP, BIA, Amenazas, Desastre, Ataque, Virus, Activos, AR, RTO.

I. INTRODUCCIÓN

El término desastre se define como un evento cuyas consecuencias rebasan la capacidad de la entidad afectada para restablecerse por sí misma; es decir, si una empresa se declara "en desastre", acepta que no podrá regresar a la normalidad con recursos propios y por lo tanto, requiere ayuda de una entidad externa. Una empresa no esta exenta de padecer una situación de este tipo y como tal, es posible categorizarlo de la siguiente manera:

Desastres generados por procesos dinámicos en el interior de la tierra:

- Sismos.
- Tsunamis.
- Erupciones volcánicas.

Desastres generados por procesos dinámicos en la superficie de la tierra:

- Deslizamiento de tierras.
- Derrumbes.
- Aludes.
- Aluviones.

Desastres generados por fenómenos meteorológicos o hidrológicos:

- Inundaciones.
- Sequías.
- Heladas.
- Tormentas.
- Granizadas.
- Tornados.
- Huracanes.

Desastres de origen biológico:

- Plagas.
- Epidemias.
- Pandemias.

Desastres tecnológicos:

- Ataques.
- Virus.
- Pérdida de información.

Desastres varios:

- Incendios.
- Explosiones.
- Derrames de sustancias químicas.
- Contaminación ambiental.
- Guerras.

- Subversión.
- Terrorismo.

Sin importar su tamaño, ninguna organización puede darse el lujo de interrumpir su actividad económica, así se presenten obstáculos internos, o situaciones críticas externas. Para lograr esto, deben existir programas de continuidad de negocio (BCP) y recuperación ante desastre (DRP); dichos programas no se tratan de conceptos o procesos complejos o de implementaciones muy costosas o demoradas, su propósito es mitigar riesgos y evitar perdidas significativas que comprometan la estabilidad de el negocio.

Entre los interrogantes que se pueden plantear las organizaciones, sin importar su actividad económica, son los siguientes: ¿Cuál seria el impacto para una entidad financiera, si se interrumpe la plataforma de la banca electrónica? ¿Cómo se vería afectada la reputación de una empresa de transporte, si se cayera la plataforma de venta de boletos? ¿Cuánto dinero podría perder una cadena de almacenes, si la infraestructura tecnológica de un punto de venta se cae?

Estas incógnitas tienen en común que son procesos vitales del negocio y que mantiene una estrecha interdependencia con la tecnología, si uno de estos procesos se interrumpe de forma prolongada, la organización podrían sufrir consecuencias negativas como obtener una mala reputación, perdidas financieras o incluso el cierre definitivo de la organización.

La implementación del plan de continuidad del negocio (BCP, DRP), se enfoca en proteger los procesos vitales del negocio, contra desastres o fallas mayores a partir de la deducción de las posibles consecuencias que se puedan tener. La existencia de un plan de continuidad del negocio (BCP,DRP), permite la pronta recuperación de la operación, en caso de presentarse alguna situación que afecte el flujo normal de las actividades.

II. GLOSARIO DE TÉRMINOS

- ***DRP - Disaster Recovery Plan***: Plan de recuperación de desastre.
- ***BCP - Bussiness Continuity Planning***: Plan de continuidad de negocios.
- ***BIA - Business Impact Analysis***: Análisis del impacto al negocio.
- ***AR - Risk Analysis***: Análisis de riesgo.
- ***RPO - Recovery Point Objective***: Objetivos de punto de recuperación.
- ***RTO - Recovery Time Objetive***: Tiempo objetivo de recuperación.
- ***Activos***: Los activos son todos aquellos recursos del sistema de información o relacionados con éste. *[2]*

III. DIFERENCIAS ENTRE BCP Y DRP

A. Plan de continuidad del negocio

Un plan de continuidad del negocio (Business Continuity Plan) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo determinado después de una interrupción no deseada o desastre.

El factor crítico durante el desastre, será el nivel de prevención, preparación y anticipación con que se generen las acciones y medidas a tomar en una situación de riesgo.

B. Plan de recuperación ante desastres

Un plan de recuperación ante desastres (Disaster Recovery Plan) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones, en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave.

Asumiendo que se ha completado una evaluación de riesgos e identificado amenazas potenciales a nuestra infraestructura de TI, lo siguiente será determinar qué elementos de dicha infraestructura son los más importantes para las operaciones corporativas. Además, suponiendo que todos los sistemas y redes TI funcionan con normalidad, la compañía debería ser plenamente viable, competitiva y sólida desde el punto de vista financiero. *[3]*

C. Diferencias

Aunque en ocasiones los dos conceptos se manejan indistintamente existen pequeños matices que los diferencian.

Un plan de recuperación ante desastres, describe como enfrenta una organización a posibles desastres. Así como un desastre es un evento que imposibilita la continuación de las funciones normales, un plan de recuperación de desastres se compone de las precauciones tomadas para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente funciones de misión crítica. Este plan establece las acciones que deberán ejecutarse para recuperar la operaciones fundamentales de una organización tras un desastre. El plan debe incluir también las

medidas para evitar determinados riesgos, mitigarlos o transferirlos a terceras partes. El DRP suele centrarse en la recuperación de las operaciones relacionadas con el procesado de datos y en general lo concerniente a IT. A medida que la infraestructura de IT aumenta, el plan de recuperación ante desastre también crece, las interrupciones del servicio o perdida de información tiene un impacto muy critico. Por esto la implementación de un DRP se vuelve cada vez más relevante dentro de las organizaciones.

El plan de continuidad de negocio (BCP) es el más global y se compone a su vez de planes que describen como la organización puede operar, durante o después de una emergencia. El BCP debe describir como gestionar cualquier incidencia que afecte a la organización y que interrumpa o detenga su operación normal, no solo grandes desastres.

Un aspecto a tener en cuenta, es que un plan de continuidad de negocio no es un lugar donde se describe detalladamente como solventar cada problema que nos podamos encontrar durante un incidente, por ejemplo, que se detenga el aire acondicionado en el centro de computo, lo cual es un contratiempo importante, sin embargo, no se puede esperar que el plan de continuidad de negocio explique como reparar el aire acondicionado pero sí deberá describir qué hacer: si hay que apagar los equipos o no y en qué orden y las indicaciones necesarias para llamar a los técnicos que deben reparar el aire acondicionado, entre otras.

IV. ¿POR QUE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO?

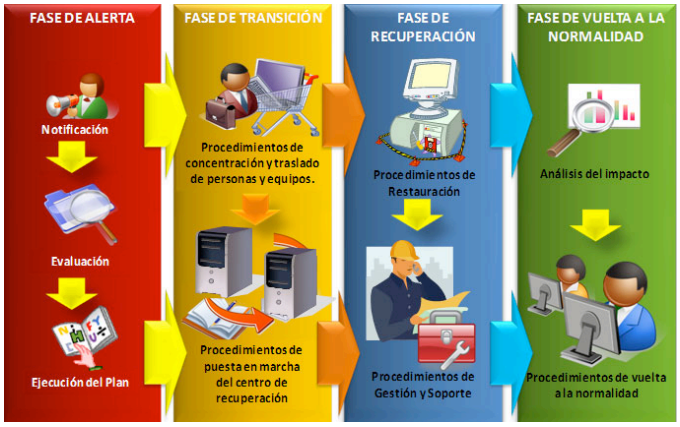

Figura 2 – Ciclo de vida de BCP [4]

La implantación de un sistema de gestión de continuidad del negocio, permite a las organizaciones demostrar su capacidad para seguir funcionando con normalidad en caso de producirse una interrupción, minimizando sus debilidades y reforzando así sus fortalezas, permitiendo a las organizaciones:

- Establecer, implementar, mantener y mejorar los sistemas de gestión de continuidad de negocio.
- Cumplir con los requisitos de la política de continuidad de negocio.
- Protección de los empleados y de la reputación de marca.
- Asegura la continuidad de negocio y de la comercialización de productos y servicios proporciona una base de entendimiento, desarrollo e implantación de la continuidad de negocio, aportando confianza tanto de negocio a negocio como de negocio a cliente.
- La continuidad de negocio forma parte de la gestión general del riesgo dentro de una organización, por lo que tiene áreas y aspectos comunes con la gestión de la seguridad de la información.

Debido a que cualquier interrupción en los procesos de negocio afecta la operación y su continuidad, es responsabilidad de la dirección general aprobar, implementar y probar formalmente un plan de continuidad de negocio que cubra las actividades de recuperación e identifique los aspectos críticos necesarias. En esta política, se deben considerar entre otros:

- Definir los procedimientos para generar los respaldos o back-ups de la información sensible e importante.
- Elementos de seguridad física necesarios.
- Integración y enlace formal del BCP con el DRP.
- Mantenimiento continuo del plan BCP/DRP.
- Pruebas del plan, las cuales deben incluir las simulaciones e intentos de restauración necesarios.
- Establecer políticas necesarias de seguridad física.
- Crear un centro de operación de emergencia en caso de que se presente una contingencia que imposibilite continuar operando en las instalaciones de la empresa (plantas, fábricas, almacenes, centros de servicio, tiendas, etcétera). Éste deberá contar con la infraestructura tecnológica adecuada y suficiente para soportar las aplicaciones clave del negocio, tanto operativas como financieras.
- Los roles y responsabilidades de las diferentes áreas y procesos dentro de la organización que incluyen el entrenamiento necesario al personal doliente.

V. NORMATIVIDAD

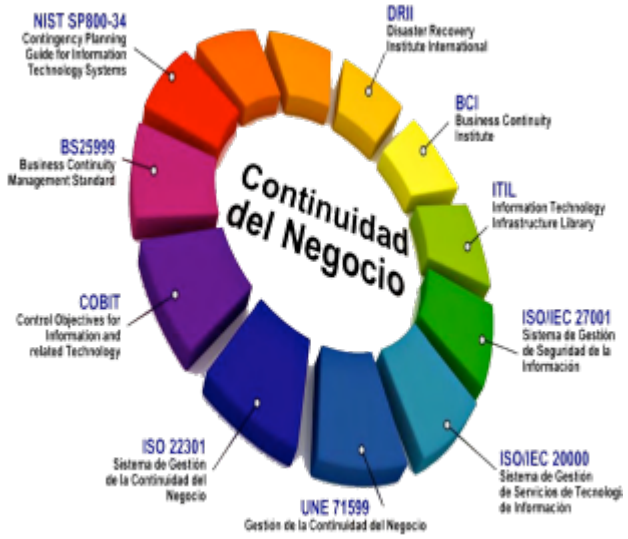

Figura 3 – Normatividad [5]

A continuación se citaran algunas de las normas que rigen un plan de continuidad del negocio son:

A. BSI 25999 Partes 1 y 2.

Se trata de una norma certificable en la que se tiene como objeto la gestión o plan de continuidad del negocio fundamentalmente enfocado a la disponibilidad de la información, uno de los activos más importantes hoy en día para cualquier organización. *[6]*

B. NIST 800-34, Contingency Planning Guide for Information Technology.

Provee instrucciones, recomendaciones y planes de contingencia para los sistemas de información federal. Los planes de contingencia se refieren a medidas provisionales para la recuperación de los sistemas de información después de una ruptura; estas medidas pueden incluir la reubicación de estos sistemas de información y operación a un sitio alterno, recuperación de sus funciones usando equipos alternativos o recuperar su desempeño por medio de métodos manuales. *[7]*

C. ISO 27031 Continuidad del negocio.

El estándar explica los principios y conceptos de la tecnología de información y comunicación (TIC), la preparación para que continúe el negocio, y la descripción de los procesos y métodos necesarios para señalar e identificar todos los aspectos que sirvan para mejorar la preparación de las TIC de una empresa con la finalidad de garantizar la continuidad del negocio. *[8]*

D. ISO/PAS 22399:2007 Incident preparedness and operational continuity management.

Proporciona la dirección general de una organización - las organizaciones privadas, gubernamentales y no gubernamentales - para desarrollar sus propios criterios de rendimiento específicos de preparación para incidentes y continuidad operativa, y el diseño de un sistema de gestión apropiado. *[9]*

VI. PASOS PARA UNA CORRECTA IMPLEMENTACIÓN

Para una correcta implementación en el desarrollo y aplicación del DRP en una empresa, se deben tener en cuenta los siguientes paso:

A. Desarrollar una política de continuidad del negocio.

Todas las actividades deben estar alineadas con los objetivos de continuidad del negocio, por lo tanto se debe comenzar por establecer un punto de partida consistente en una política encargada de establecer la planeación de las estrategias, así como la clasificación de los sistemas o aplicaciones para identificar aquellos que sean considerados como críticos.

B. Realizar una evaluación de riesgos.

Llevar a cabo una evaluación de riesgos permite identificar, analizar y evaluar las amenazas que podrían afectar a la organización, especialmente aquellos que puedan provocar una situación que se incluya en la categoría de desastre.

C. Realizar un análisis de impacto al negocio (BIA).

Aquí se definen principalmente los objetivos de recuperación para los sistemas que soportan los procesos de negocio. Se define el tiempo objetivo de recuperación (RTO), que es el período máximo permitido para la recuperación de una función o recurso de negocio a un nivel aceptable luego de un desastre y el punto objetivo de recuperación (RPO) que es la antigüedad máxima de los datos para su restauración, con base en los requisitos del negocio.

D. Desarrollar estrategias de recuperación y continuidad del negocio.

En este punto se busca dejar en claro todas las medidas requeridas para regresar a la operación tan pronto como sea posible, con base en una priorización derivada de la clasificación de la política de continuidad del negocio.

E. Concientizar, capacitar y probar los planes.

Un elemento necesario con relación a los planes consiste en realizar su difusión entre los miembros de la organización, especialmente entre aquellos que serán los encargados de ejecutarlo en caso de ser requerido. Además, se deben realizar pruebas del mismo, para ello, se puede hacer uso de diferentes opciones, desde una revisión de la lista de verificación de la recuperación hasta una prueba de interrupción completa, donde las operaciones se paralizan en el sitio primario y se transfieren a un sitio de recuperación.

F. Mantener y mejorar el plan de recuperación ante desastres.

A partir de los resultados de la prueba de los planes de recuperación, se deben suministrar los ajustes correspondientes para contar con documentación actualizada y apropiada a los intereses de la organización, una vez que han sido consideradas las situaciones de desastre que podrían afectarla, las actividades y recursos necesarias para restablecer las operaciones críticas.

De manera general, las organizaciones que desarrollan los planes de recuperación, deberán considerar los recursos a su alcance, los servicios previamente identificados y que se desean recuperar tan pronto como sea posible, así como los tipos y severidad de las amenazas que enfrenta la organización y pueden llegar a convertirse en un problema de mayor magnitud.

Otro elemento necesario es la propensión al riesgo de la organización, ya que de ello también dependerán los esfuerzos y recursos destinados al desarrollo y aplicación del DRP. La consideración de este plan ofrece la ventaja de responder de forma planeada ante una catástrofe y minimizar su impacto en las actividades y objeto social de la compañía.

VII. CONSECUENCIAS DE NO IMPLEMENTAR DRP

Cuando se habla de un desastre no aplica solamente a una catástrofe natural como un terremoto, inundación, huracán o fenómeno similar que paralizan una región, sino también la inexperiencia de un usuario que desconecta una base de datos, el caso fortuito de la rotura de un tubo del acueducto que afecta la conectividad de internet de la fuente de los datos o la súbita caída del servicio de energía tan común en nuestro entorno tradicional.

Existen empresas que no cuentan con planes de predicción y/o contingencia de desastres, por lo tanto, en caso de alguna contingencia no cuentan con los recursos que garanticen la continuidad de sus servicios; arriesgando grandes sumas de dinero y muchas veces la disponibilidad de la información es escasa o nula y en algunos casos esta información llega a perderse.

Además de lo anterior, algunas de las consecuencias a las que está expuesta una organización son:

- Incapacidad para mantener la continuidad de los servicios relacionados con la TIC del negocio.
- No tener protegido al negocio de fallas generales en los servicios informáticos.
- Se aumentan exponencialmente los riesgos generados por la falta de servicios.
- No se tiene la forma de garantizar el acceso a la información empresarial.
- No es posible mantener la disponibilidad de los recursos informáticos.
- Aumenta el riesgo en la toma de decisiones erróneas al presentarse algún desastre.
- En una situación de este tipo no es posible dar atención continua a los clientes, proveedores, accionistas y colaboradores.
- Incapacidad de mantener los servicios críticos al cliente.
- Daño en la participación de mercado, la imagen, reputación o marca.
- No poder proteger los activos de la compañía, incluyendo propiedad intelectual y personal.
- Falla de control de negocio.
- No poder cumplir los requerimientos legales.

VIII. CASOS DE ÉXITO

A continuación se citaran algunos casos de éxito en la implementación de BCP/DRP:

- ***Vodafone Reino Unido.***

Fue el primer operador de móviles en el mundo en lograr la certificación ISO 22301. Esta certificación demuestra los esfuerzos de la compañía en proporciona a los clientes el servicio más uniformemente confiable, sin importar las circunstancias. También les proporciona un servicio de diferenciación y una ventaja competitiva, así como también la capacidad de satisfacer los requisitos de contingencias legales y civiles. *[10]*

- ***Wal-Mart.***

Tras cinco años de intentos infructuosos para implementar un DRP completo y operativo, Wal-Mart consiguió su objetivo con una inversión justa aprovechando su infraestructura al máximo. La solución permitió a la compañía contar con un DRP que garantice un alto nivel de autosuficiencia en su área de continuidad de sistemas. El proceso les permitió identificar los riesgos existentes y tomar medidas apropiadas de control preventivo. *[11]*

- ***LaSalle Bank de Chicago .***

Su sede principal se incendió en diciembre del 2004; al día siguiente estaba funcionando sin problemas para sus clientes gracias a una combinación de sedes alternas y de trabajo "en remoto", es decir desde sus casas, para una parte del personal.

- ***Banco HSBC.***

Fue uno de los más afectados por una gigantesca bomba del grupo terrorista IRA en la ciudad de Londres; su sede londinense fue destrozada, pero ya desde el 1993, el banco, luego de una bomba en ese año, había decidido replicar y proteger toda su data en otra ubicación, por lo que no le fue muy difícil reanudar sus operaciones, pues además, el personal estaba preparado para lo peor.

- ***Lehman Brothers.***

El 11 de septiembre de 2001, en el atentado a las torres gemelas, la sede en Manhattan del banco logró según John Manville, director de redes y telecomunicaciones: "Fuimos capaces de casi inmediatamente poner a trabajar al personal más crítico, darles el back-up del negocio y poner en marcha las aplicaciones". *[12]*

- ***El Gobierno Alemán.***

Cuando Berlín sufrió bombardeos, supieron asegurar su continuidad administrativa durante mucho tiempo con una red de bunkers, algo bastante sorprendente por la magnitud de dichos bombardeos. Cabe añadir que incluso habían preparado un escenario de derrota militar durante el cual seguiría funcionando una suerte de "gobierno subterráneo" que debería estar listo para un eventual resurgimiento.

- ***El Gobierno Japonés***

Enfrentando a los masivos bombardeos de Tokio a partir de 1943, todavía seguía funcionando cuando decidió capitular luego de las dos bombas atómicas de Hiroshima y Nagasaki. Su recuperación fue tal, que su "agencia de estabilización económica" llamada luego de "planeación económica" fue uno de los jugadores clave de la recuperación del Japón en la pos-guerra.

- ***Banco Crédit Lyonnais***

El 5 de mayo de 1996, un domingo, la sede del banco francés se incendió casi completamente con un fuego que se inició en su gigantesca sala de mercados de capitales. Al día siguiente, estaba funcionando de nuevo, gracias a una sede alterna en las afueras de Paris, a todo un dispositivo de replicación y back-up informático y de relaciones estrechas con proveedores clave, y al uso inteligente de las salas de mercados de otras sedes (como Londres, New York y Tokio) y otros locales parisinos, que le permitió reconstituir su central telefónica en poquísimo tiempo, e instalar oficinas temporales para parte del personal en pocos días. *[13]*

IX. CONCLUSIONES

Sin lugar a dudas, contar un con plan de continuidad de negocio, apoyado entre otros con un plan de recuperación ante el desastre en una organización, asegura en gran medida, solventar y minimizar el impacto que pueda ocasionar un suceso de esta naturaleza, que en la gran mayoría de los casos, sucede en el momento menos indicado y menos esperado, además de tomar las medidas necesarias para reducir al máximo el impacto negativo que esto produzca al interior de la compañía, a sus empleados, proveedores y clientes.

De la misma forma, estos planes demandan una parte importante del presupuesto de una empresa, invierto en el desarrollo, implementación, seguimiento y mantenimiento con el objetivo de tener un sistema de garantice la continuidad del negocio.

Una parte clave y fundamental a la hora de recuperarse de un desastre es, sin lugar a dudas, la preparación del personal involucrado tanto operativa como sicológicamente, su grado de conocimiento y su liderazgo en cada una de las áreas, un trabajo integrado, coordinado e interdisciplinario que logre restablecer todos los servicios y la operación de la compañía lo mas pronto y eficientemente posible.

X. REFERENCIAS

[1] Bussiness Continuity Planning y Disaster Recovery Plan. Tomada de: https://thebullrun.wordpress.com/2013/02/19/what-is-disaster-recovery-and-business-continuity-planning/

[2] Glosario de términos. Disponible en: http://searchdatacenter.techtarget.com/es/cronica/Pasos-para-un-Plan-de-Recuperacion-de-Desastres-DRP

[3] DRP y BCP. Disponible en: https://prezi.com/uum9mha0dkj7/bussines-continuity-plan-bcp-y-disaster-recovery-plan-drp/

[4] Ciclo de vida de BCP.
Tomada de : http://bit.ly/1MyFJNl

[5] Normatividad.
Tomada de: http://bit.ly/22XZy4U

[6] Norma certificable BS 25999. Disponible en: https://es.wikipedia.org/wiki/BS_25999

[7] Norma certificable BS 25999. Disponible en: http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations/2-2b-contingency-planning-swanson-nist.pdf

[8] ISO 27031 Continuidad del negocio. Disponible en: http://www.pmg-ssi.com/2014/04/iso-27031-continuidad-del-negocio/

[9] ISO/PAS 22399:2007 Incident preparedness and operational continuity management. Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=50295

[10] Casos de éxito de Gestión de Continuidad del Negocio. Disponible en: http://www.bsigroup.com/es-MX/continuidad-delnegocio-ISO-22301/casos-ISO-22301/

[11] Walmart: http://www.gcpglobal.com/casos-walmart.php

[12] Un caso real: cómo Lehman Brothers sobrevivió al desastre. Disponible en: http://www.networkworld.es/archive/un-caso-real-como-lehman-brothers-sobrevivio-al-desastre

[13] Continuidad Operativa o del Negocio – Ejemplos de Éxito Disponible en: http://blogs.gestion.pe/riesgosfinancieros/2014/09/continuidad-operativa-o-del-negocio-ejemplos-de-exito.html