Impacto de las Tecnologías Emergentes en la Gestión de la Continuidad del Negocio

Ramiro Merchán Patarroyo, Sandra Milena Suarez, Joaquín Afanador, Javier Merchán García

***Abstract*- Es necesario desarrollar habilidades en la empresa para prevenir y anticipar desastres parciales y totales; el mantener la operación de las organizaciones en caso de un siniestro es una preocupación que toma mayor relevancia día a día dada la interdependencia entre los actores de la cadena de suministro y los incidentes locales o nacionales que se han presentado en fechas recientes. Vencer la creencia que nuestras instituciones son inmunes al "peor escenario de desastre" es tal vez el principal reto que enfrentan los líderes de riesgos y continuidad del negocio, por ello, se requiere que los planes de continuidad tengan dos características esenciales: 1. Contemplen un panorama apropiado de los riesgos de la empresa y 2. Estén actualizados frente a los cambios que nos imponen las tecnologías emergentes.**

I. Introducción

LUEGO de los desastres ocurridos con posterioridad al 11 de septiembre de 2001 (terremotos, actos terroristas, ciberataques, entre otros) el fortalecimiento del BCP[1] se convirtió en una necesidad para toda compañía, pues el desarrollo del mismo permite entender los riesgos de interrupción que existen y establecer una serie de comportamientos y procedimientos para actuar en caso que un escenario de desastre se materialice.

Es necesario tener en cuenta que un BCP debe evolucionar constantemente, ya que todos los días se desarrollan nuevas tecnologías y con ellas nuevos métodos de enfrentar los riesgos pero también nuevas amenazas (la tecnología es un arma de doble filo). En este artículo se explican los conceptos relacionados con un plan de continuidad del negocio, sus componentes y las tendencias que mayor impacto tienen en la transformación del concepto de BCP, como lo son la masificación de los dispositivos móviles, el uso de las redes sociales, la virtualización, y el cloud computing (nube).

Dichas tendencias presionan hacia el concepto de continuidad del negocio en la nube. En una primera fase vemos en funcionamiento estrategias como backups, software, infraestructura y plataforma como servicios que se pueden reunir en un nuevo modelo **"DRP[2] as a Services"** y se puede afirmar que estamos ad portas de experimentar un nuevo modelo **"BCP as a Services"** pues está claro que los servicios en nube reducen el costo de operación para las empresas, dan mayor acceso a la información (difícilmente hay una pérdida total de datos, solo parcial) y permiten distribuir e integrar la responsabilidad entre especialistas por cada componente del BCP.

II. El Plan de Continuidad del Negocio (BCP).

Es un conjunto de procedimientos y estrategias encargados de asegurar la reanudación oportuna y ordenada de los procesos fundamentales del negocio, generando un impacto nulo o mínimo en una situación de desastre. Un plan de continuidad de negocio incluye, entre otros, los siguientes planes: Recuperación de desastres, Manejo de crisis, Gestión de respuesta a incidentes. SAFEID ha adoptado como marco de trabajo el modelo que propone NIST[3] 800-34 y que se observa en la figura 1.

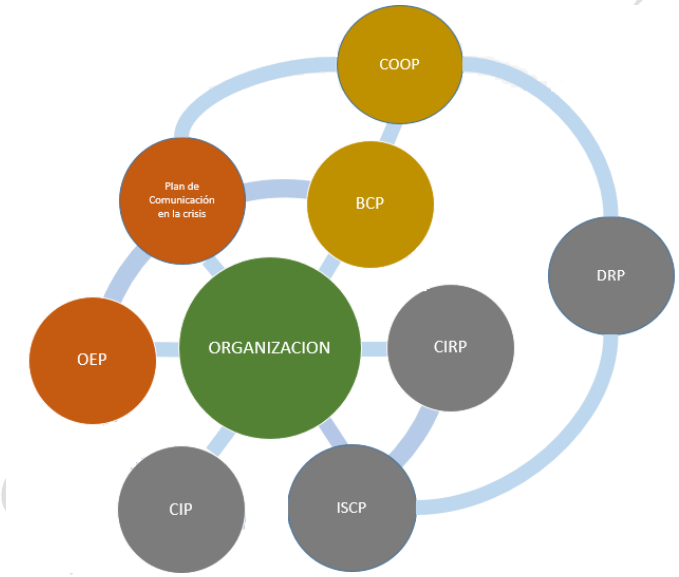

Figura 1. Planes de Continuidad del Negocio y su Interrelación, de acuerdo con el modelo NIST 800-34

[1] BCP: Business Continuity Plan

[2] DRP: Disaster Recovery Plan

[3] NIST: National Institute of Standards and Technology

A continuación se presenta un glosario resumido del significado y alcance de cada plan:

Plan	Propósito
Plan de Continuidad del Negocio – BCP	Proporcionar procedimientos para sostener operaciones críticas del negocio mientras se recupera de una interrupción significativa.
Plan de Continuidad de Operaciones (COOP)	Proporciona procedimientos y guías para sostener funciones esenciales de la organización en un sitio alterno, durante un máximo de 30 días.
Plan de Comunicaciones en Crisis	Proporciona procedimientos para difundir las comunicaciones internas y externas, así como brindar información de la situación y controlar rumores.
Plan de Protección de Infraestructura Crítica (CIP)	Proporciona las políticas y procedimientos para la protección de los componentes nacionales de infraestructura crítica. Actualmente en definición en nuestro país.
Plan de Respuesta a Ciber-Incidentes	Proporciona procedimientos para la mitigación y corrección de un ataque cibernético, como: virus, gusanos informáticos y hoy día APT´s (Amenazas Persistentes Avanzadas).
Plan de Recuperación de Desastres (DRP)	Proporciona procedimientos para la recuperación de los sistemas de información y servicios tecnológicos críticos, en una locación alterna (Centro de cómputo alterno).
Plan de Contingencias de Sistemas de Información (ISCP)	Proporciona procedimientos y capacidades para la recuperación de un sistema de información en particular.
Plan de Respuesta a Emergencias (OEP)	Proporciona procedimientos coordinados para reducir al mínimo la pérdida de vidas, lesiones y proteger daños materiales en respuesta a una amenaza física.

Tabla 1. Planes Componentes del Plan de continuidad del negocio

Como se observa, continuidad del negocio es un rompecabezas que involucra el desarrollo, el manejo y las pruebas de diferentes planes enfocados en contrarrestar la interrupción de las operaciones del negocio:

- **La recuperación de desastres** que se ocupa de la continuidad de la infraestructura de las tecnologías de la información.
- **El manejo de crisis** que determina los pasos a seguir para mitigar los efectos derivados de un evento negativo y devolver la capacidad de operación de la empresa en el menor tiempo posible.
- **La gestión de respuesta a incidentes** donde se define de forma organizada y con responsabilidades especificas la forma en la que se debe reaccionar rápida y efectivamente ante un problema para reducir sus impactos y evitar que se convierta en un desastre.

En resumen, el plan de continuidad establece una serie de procedimientos que permiten responder a la empresa ante desastres mayores que impactan las operaciones de la compañía y va más allá del plan de recuperación de TIC[4], sin embargo, es necesario tomar en cuenta que las nuevas amenazas informáticas se constituyen en un vector de ataque que pueden paralizar las operaciones y comprometer la imagen de la empresa y por ello incrementan su importancia los planes de protección de infraestructura crítica y de respuesta a ciber-incidentes.

III. TECNOLOGÍAS EMERGENTES

Actualmente el mundo continúa experimentando una serie de transformaciones derivadas del desarrollo de internet y el avance de las organizaciones en el afianzamiento de la globalización. En la figura 2 se observa la evolución reciente en términos de conectividad, masificación de redes sociales y el nuevo paradigma: La nube.

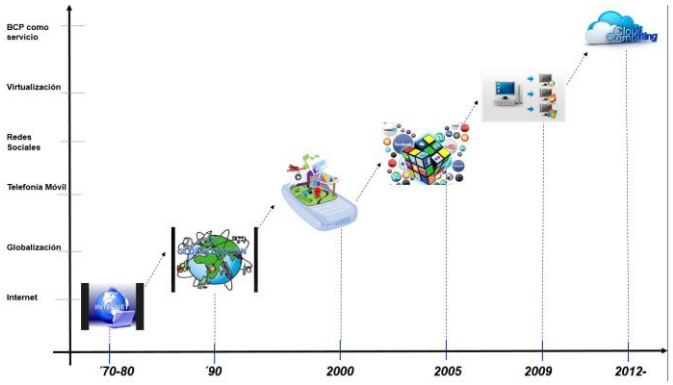

Figura 2. Tecnologías emergentes y su impacto en las relaciones de negocios.

La masificación de las **comunicaciones móviles** ha tenido gran impacto en el funcionamiento de las empresas debido a que constantemente se está mejorando la capacidad de almacenamiento de estos dispositivos además de la gran cantidad de aplicaciones que se pueden descargar y permiten llevar la empresa en la mano; Smartphones, Tablets, computadores de última generación, dan acceso a las bases de datos de una compañía en cualquier instante y desde cualquier lugar.

Las redes sociales se han convertido en un método instantáneo de comunicación reemplazando las llamadas telefónicas gracias a su alcance mundial, a su capacidad de transmitir archivos y primordialmente su bajo costo (vale más una llamada que un mensaje por correo electrónico, Facebook o WhatsApp).

[4] TIC: Tecnología de Información y Comunicaciones

La virtualización, concepto propuesto hace varios años pero que hasta ahora deja ver todo su potencial gracias a compañías como VMware, Microsoft, Oracle y Google, que la han posicionado por las mejoras en sus interfaces y facilidad de uso, es otra gran tendencia que consiste en la creación de un entorno simulado para algún recurso tecnológico como un sistema operativo o un dispositivo de almacenamiento. A manera de ejemplo, puede imaginarse un emulador, el cual permite correr sobre un computador una película sin necesidad de tener un lector de DVD instalado en él; esto gracias a que el emulador simula y hace las veces de lector. La virtualización reduce notablemente el costo de operación pues no necesita comprarse un computador por cada sistema operativo que necesite la empresa sino que valiéndose de ella se puede elegir el sistema a trabajar.

La **computación en la nube** hace referencia al procesamiento y almacenamiento de datos en servidores remotos, contrario a los datacenter locales donde los servidores son normalmente propios de la empresa o más importante aún, se tienen claro cuáles son, sus características y donde se localizan.

Una gran ventaja de la nube es el fácil acceso a las bases de datos pues solo requiere de una conexión a internet sin importar el lugar del mundo donde se encuentre, inclusive ya todos nosotros hemos hecho uso de la computación en la nube cuando ingresamos al correo electrónico; este es el ejemplo más claro de la nube: La información guardada en el correo (contactos, registros, calendarios) es almacenada en los servidores correspondientes de quien provee el servicio (Google, Microsoft, Yahoo, etc.) y al momento de ingresar la contraseña queda a nuestra disposición la información pero no tenemos idea exacta de cuales son dichos servidores y donde se encuentran.

La replicación es una estrategia que facilita la toma de backups remotos y debe cubrir tanto los datos críticos como no críticos. La toma de réplicas se debe planificar detalladamente pues un error en cualquier software, cualquier interrupción en el envío de los datos de un centro de cómputo a otro, fallas en los canales o cualquier otro imprevisto puede ser fatal en la recuperación hasta el punto de perder totalmente la información.

IV. IMPACTO DE LAS TECNOLOGÍAS EMERGENTES EN EL PLAN DE CONTINUIDAD DEL NEGOCIO.

Sin duda alguna las tecnologías emergentes cambiaron la forma de realizar las operaciones en la compañía: Las áreas de mercadeo y publicidad se apoyan en redes sociales, el procesamiento de datos cada vez más se soporta en la virtualización y las tecnologías actuales no están diseñadas para heredar sistemas no virtualizables, los dispositivos móviles replantearon la forma de trabajar de las fuerzas de ventas y en general dieron vida al concepto de transparencia a la localización geográfica de los usuarios y la nube al de trasparencia del procesamiento.

Frente al panorama anterior, un reto que tienen hoy día las áreas de riesgos y continuidad del negocio es determinar si sus estrategias de mitigación y continuidad del negocio están acordes frente a los riesgos y ventajas que dichas tecnologías introducen en la organización y en caso contrario dar el giro requerido. Revisemos algunos de dichos impactos:

Backups como Servicio: Consiste en instalar un software especial en cualquier ordenador el cual genera copias de información que se almacenan en un servidor virtual externo y que mitiga la pérdida de datos. Se debe verificar la eficiencia y mitigación de riesgos que ofrecen las estrategias de backups en funcionamiento.

DRP como Servicio: Hay que aprovechar el modelo de Software como Servicio (SaaS) donde el usuario renta un software en lugar de comprarlo o instalarlo en su propia infraestructura de procesamiento. Indudablemente esta opción optimiza los recursos de cómputo pues el procesamiento se aloja en los servidores del proveedor. En contraposición, se debe confiar en el proveedor pues se incrementan los riesgos de privacidad de la información, conectividad y seguridad en línea. Es necesario que en este tipo de contratos se defina claramente la responsabilidad del proveedor en participar en las pruebas y simulacros del BCP / DRP que planifique la empresa.

Las Redes Sociales y las Comunicaciones Móviles facilitan la notificación masiva requerida en situaciones de desastre y de primera mano tienden a remplazar los *"arboles de llamadas"* pero tienen dos talones de Aquiles: 1. Dependen del funcionamiento de las telecomunicaciones y 2. Son herramientas de dominio público, lo cual las hace vulnerables a ataques, por ello se recomienda restringirlas a casos de emergencia.

La Replicación es necesaria frente a otro tema que estamos experimentando las empresas: **Big Data**. Las estrategias de respaldo y recuperación de datos basados en métodos convencionales no ofrecen los tiempos de recuperación que exigen las condiciones de operación actuales. Los principales retos en esta tecnología se concentran en la capacidad de los canales, la capacidad de almacenamiento, la tolerancia a fallas y según nuestro criterio tener la certeza que se están respaldando apropiadamente los datos críticos del negocio.

V. CONCLUSIÓN

Las tecnologías emergentes impactaron la forma de llevar a cabo las relaciones de negocio y por ende los planes de continuidad. Se debe evaluar si nuestros planes están acordes a los nuevos modelos de trabajo y si consideran el uso de dichas tecnologías para brindar mayores niveles de eficiencia en la recuperación ante desastres, de igual manera se debe realizar una evaluación de los riesgos que las tecnologías emergentes introducen en los planes de continuidad.

Dejamos a consideración de los responsables de riesgos y continuidad del negocio los siguientes interrogantes:

1. ¿Nuestros planes de continuidad contemplan todos los componentes que requiere la empresa?
2. ¿Se han valorado los costos de operación de los planes de continuidad existentes frente a las tecnologías emergentes?
3. ¿Se tienen identificados los riesgos de operar en contingencia?
4. ¿Qué pasa si fallan nuestros planes de continuidad definidos? ¿Tenemos un plan C?
5. ¿En las pruebas realizadas a los planes de continuidad se han verificado los planes de retorno a la normalidad?

REFERENCIAS

[1] ISACA, Advanced Persistent Threat Awareness Study Results

[2] ISACA, Business Continuity Management: Emerging Trends, 2012

[3] NIST 800-34, Contingency Planning Guide For Federal Information Systems.

[4] Portafolio Safety in Deep, Ramiro Merchán, Sandra Suarez.

[5] SAFEID, artículo 1: ¿Conozco los riesgos de mi cadena de suministro?, Julio de 2015

info@safeid-sas.com www.safeid-sas.com