

Sistema de gestión de continuidad o BCMS - Segunda parte

Tomasi, Susana Noemí

Tercera Fase: Recuperación de desastres

Recuperación de Desastres es la capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización.

Un Plan de recuperación de Desastres, es una norma de procedimientos a fin de cubrir los aspectos esenciales respecto a las estrategias a llevarse a cabo para la restauración de la organización luego de que sucediera una catástrofe.

En todos los casos se deberá atender con prioridad aquellos elementos que sean indispensables según se halla determinado respecto los procesos críticos del negocio y considerando los tiempos máximos de interrupción identificados en cada uno de los casos.

El objetivo principal será desarrollar un programa orientado a crear y mantener conciencia en el negocio, además de mejorar las habilidades requeridas para desarrollar e implementar los planes de recuperación

En [\(1\)](#) exponen que "Como experimento, la próxima vez que esté en su centro de datos, mire a su alrededor e imagine por un momento que no hay nada. Y no solamente los computadores. Imagínesse que el edificio completo ya no existe. Luego, imagine que su trabajo es recuperar la mayor cantidad de trabajo realizado posible en el centro de datos, lo más pronto posible. ¿Qué haría?

Al pensar desde esta perspectiva, usted está dando su primer paso hacia la recuperación de desastres. La recuperación de desastres es la habilidad de recuperarse de un evento que impacta el funcionamiento del centro de datos de su organización lo más rápido y completo posible. El tipo de desastre puede variar, pero el objetivo final es siempre el mismo.

Los pasos relacionados con la recuperación a partir de un desastre son numerosos y con un rango bien amplio".

En [\(2\)](#) indican que según la fase en la que se encuentra la evolución del desastre, en términos de conducta se han descrito clásicamente cinco períodos (Doutheau C. Les comportements humains en situation de catastrophe. Con Med 1983; 2: 217-220),

"... 1. Período precrítico, que es la fase anterior, inicial o de alerta, caracterizado por ser una fase de alta tensión al conocerse la inminencia de la catástrofe y su inevitabilidad...

2. Período de crisis, generalmente bastante grave y caracterizado por el efecto sorpresa. Existe gran desorganización, fuerte estrés y aparición de miedo o inhibición tras intentos de actividad...

3. Periodo de reacción, que se caracteriza por conductas postconmocionales. El estrés y la tensión pasada, la fatiga mental y física acumulada, aflora ahora y se manifiesta en forma de desorientación témporo-espacial, impresión de extrema vulnerabilidad, lentificación de movimientos y pérdida de iniciativa....

4. Período postcrítico o de restauración, generalmente lento y donde ya se comienza a hacer un trabajo de clasificación y evaluación de los daños e incluso una mínima reconstrucción.

5. Periodo de efectos a largo plazo, caracterizada por el estrés postraumático..."

Estas fases pueden usarse como entrenamiento, para conocer el grado de preparación de la organización y permite evaluar al personal involucrado en el Plan de Continuidad, que debe actuar en la Recuperación de Desastres, su grado de cohesión, de gran importancia contra la posible desorganización que pueda surgir en un futuro inmediato, es importante que todo el personal de la organización tenga conocimiento de que la misma está capacitada para el suceso que puede ocurrir imprevistamente (como es una catástrofe natural), por lo cual no entra en pánico y procede según las indicaciones previas.

"... El pánico es uno de los comportamientos más negativos que pueden aparecer en un desastre y produce algunos de los efectos más destructivos y peligrosos conocidos. El pánico vendrá mediatizado por todo un conjunto de factores como son la ausencia de información..."

Las Estrategias de Recuperación las vamos a desarrollar adaptando lo expuesto por Ardita J. y Castellanos R. en [\(3\)](#), desde:

- * Lo Tecnológico
- * Lo Humano
- * La Infraestructura
- * Las Comunicaciones

Estrategias de recuperación desde lo tecnológico

Que se desarrollarán respecto a la Tecnología de la Información y respecto a la Tecnología de Producción:

* **Respecto a la Tecnología de la Información:** Se debe tener en cuenta la importancia de contar con la capacidad para restablecer la infraestructura tecnológica de la información de la organización en caso de una interrupción severa, y contar con:

* Un centro de cómputos alternativo, dado que si por evento acaecido el lugar físico se encuentra inhabitable, se pueda volver a operar en otro lugar realizando las restauraciones correspondientes.

* Equipamiento y software necesario, se indica que se debería tener en el almacén en stock aquellos repuestos trascendentales para la prosecución del sistema, y que si se tienen "sistemas completos se tiende a reducir el tiempo fuera de servicio y requiere habilidades mínimas para instalar, pero sería muchísimo más costoso que tener un CPU y un módulo RAM de repuestos. Sin embargo, este costo puede ser justificado si su organización tiene varias docenas de servidores idénticos que se podrían beneficiar de tener un sistema adicional de repuesto..."

* Redes de comunicaciones alternativas, se deberá tener diseñado la configuración topológica de interconexión de equipos en red que responda adecuadamente a las necesidades de la recuperación, con las etapas de implementación de la misma.

* Recuperación de datos: Se debería enviar respaldos fuera de sitio semanalmente para que en el peor de los casos no se pierda más que los datos de una semana.

* Soporte Técnico, puede estar acordado con empresas externas, o utilizar el personal propio de la organización.

* Procedimiento de carga y puesta en marcha del sitio de recuperación, con verificación de pruebas correspondientes.

Se determina que "... Un plan de recuperación de desastres indica cada faceta del proceso de recuperación, incluyendo (pero no limitado) a:

- * Los eventos que denotan posibles desastres
- * Las personas en la organización que tienen la autoridad para declarar un desastre y por ende, colocar el plan en efecto
- * La secuencia de eventos necesaria para preparar el sitio de respaldo una vez que se ha declarado un desastre
- * Los papeles y responsabilidades de todo el personal clave con respecto a llevar a cabo el plan
- * Un inventario del hardware necesario y del software requerido para restaurar la producción
- * Un plan listando el personal a cubrir el sitio de respaldo, incluyendo un horario de rotación para soportar las operaciones continuas sin quemar a los miembros del equipo de desastres
- * La secuencia de eventos necesaria para mover las operaciones desde el sitio de respaldo al nuevo/restaurado centro de datos

Los planes de recuperación de desastres a menudo llenan múltiples carpetas de hojas sueltas. Este nivel de detalle es vital porque en el evento de una emergencia, el plan quizás sea lo único que quede de su centro de datos anterior (además de los otros sitios de respaldo, por supuesto) para ayudarlo a reconstruir y restaurar las operaciones.... Mientras que los planes de recuperación de desastres deberían de estar a la mano en su sitio de trabajo, también se deberían conservar copias fuera de sus instalaciones. De esta forma, si un desastre destruye sus instalaciones no se eliminarán todas las copias de su plan de recuperación..."

Ante emergencias, puede especificar:

— **Que cualquier centro de datos perteneciente a la organización, aunque sea de otra área o empresa del grupo, puede actuar como un sitio de recuperación de desastre para cualquier otro centro de datos.**

— **Que las funciones comerciales no deben estar atadas a una máquina específica, de manera tal que dicha máquina pueda ser reemplazada por otra en caso de desastres.**

— **Que los recursos de hardware puedan ser compartidos o distribuidos entre los distintos sectores de la organización en caso de catástrofes.**

Además: se pueden reducir los costos de soporte y formación de personal, y aumentar la eficiencia, la compatibilidad, capacidad de recuperación y disponibilidad de los recursos, si una misma normativa es utilizada por distintas empresas de la organización, y que las mismas acuerdan los procedimientos y utilización de los recursos ya sea tecnológico, logísticos,

humanos, etc. en común.

* **Respecto a la Tecnología de Producción:** se debe tener en cuenta el valor económico de contar con la capacidad para restablecer la infraestructura tecnológica de producción de la organización en caso de una disrupción severa, y contar con:

* Uno o varios lugares de trabajo alternativos, en caso de que el suceso hubiera afectado una parte o varias de la planta, unidad de servicios, (bancarios, de seguros, estatales, etc.), se deberán utilizar sitios de contingencia, que pueden proceder de distintos orígenes:

— Empresas especializadas en suministrar servicios de recuperación de desastres, a las que se las debe tener contactadas previamente.

— Otras ubicaciones que pertenecen y son operadas por la organización, y que se encuentran disponibles.

— Un acuerdo mutuo con otra organización para compartir las facilidades de un lugar utilizable en el evento de un desastre.

* El equipamiento necesario para operar.

Estrategias de recuperación desde lo humano

Que se desarrollarán respecto a los siguientes recursos humanos:

Coordinador del Plan de Continuidad del negocio a cargo de un Comité de contingencias, que incluya líderes de cada uno de los sectores de la organización, según el organigrama previamente estipulado.

Recursos humanos necesarios para operar en la recuperación, se debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave.

Lógica de movimiento del personal, contar con la manera de contactarse y notificar a todo el personal clave del problema y asignarles tareas enfocadas hacia el plan de recuperación, ya sea por medio de teléfonos de línea, celulares, correos electrónicos, notificaciones a los domicilios, la lista de contactos del Plan debe disponerla más de uno de los miembros del Comité de contingencias, y ser utilizada rápidamente.

Además se debe poseer con la lista de contactos del resto del personal, sabiendo quienes pueden reemplazar a personal al que no se ha podido contactar y designarles a todo el personal de la organización las actividades que correspondan.

Si se cuenta con proveedores externos contratados para casos de contingencias, realizar rápidamente las solicitudes de actividad correspondiente.

En (4) se expresa que: "... Es imperativo que tus empleados sepan a dónde ir y qué hacer si tu oficina o computadoras están in-operativas. Algunos roles y funciones que deberías designar serian, identificar las funciones críticas y determinar quién va a llenar. Por ejemplo, quien se pondrá en contacto con los clientes y gestionara el seguro?

* Determinar los puntos de encuentro para los escenarios de evacuación.

* Designar y preparar lugares alternativos de trabajo y sugerir instalaciones remotas de trabajo para un período temporal.

* Distribuir el plan a todos los empleados y cargar una copia donde sea accesible a todo el

mundo (cualificado).

- * Coloca una copia del plan en alguna parte que en la que no se viera afectada por la falta de datos o la evacuación de oficinas.

- * No coloques la copia única en el servidor.

- * Comparte el plan con todas las nuevas contrataciones como parte de su introducción en la compañía. Además, revisa el plan con todos los empleados sobre una base trimestral.

Todos los negocios experimentan algún tipo de insuficiencia de datos o alguna situación de emergencia. Es sólo cuestión de tiempo y magnitud. La mayoría de la gente piensa que nunca les va a pasar con ellos, pero todo lo que necesitas es un pequeño ejemplo para arruinar una empresa. **La mejor protección** contra este tipo de escenario es un bien pensado plan que haya sido probado y comunicado a todo el mundo. Asegúrate de que estás preparado. ¿Y tu dispones de algún tipo de plan de recuperación de desastres?..."

Estrategias de recuperación desde la infraestructura

Que se desarrollarán respecto a:

Las facilidades edilicias, que impliquen la recuperación de las actividades desde lo más crítico hasta lo menos.

La provisión de energía

La provisión de suministros

El servicio telefónico, de internet, etc.

La seguridad física

Estrategias de recuperación desde las comunicaciones

Que se desarrollarán respecto a:

La declaración de estado de contingencia

La Notificación a Personal — Proveedores — Clientes — Legales (Organismos competentes) — Prensa — Comunidad en general, sobre todo de la región que compete a la organización, en caso de ser necesario.

Todo aquello que se entienda necesario para la recuperación del desastre.

Cuarta Fase: gestión de incidentes

En ITIL [\(5\)](#) se indica que "La **Gestión de Incidentes** tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible"

Ocurrido un suceso que afecta la continuidad total o parcial del negocio, se debe efectuar una notificación a las más altas autoridades de la organización, y el coordinador general deberá poner en práctica el Sistema de Gestión de Continuidad correspondiente.

Determinando el nivel de prioridad para la resolución del incidente, tal como se ha explicitado en el Plan de Gestión de Continuidad del Negocio.

El nivel de prioridad se basa esencialmente en dos parámetros:

- Impacto del incidente y de cómo éste afecta a los procesos de negocio y/o del número de usuarios y procesos perjudicados, según lo determinado en: Análisis del impacto de una

interrupción en el normal funcionamiento del negocio.

— Premura: dependiendo del tiempo máximo de retraso que se necesite para la resolución del incidente, según lo determinado en: Relevamiento, análisis y definición de un plan de continuidad de negocios.

Para una buena Gestión de un Incidente se deberá:

1. Asentar el incidente, con el registro de un número de referencia único para el mismo con el que lo identificará, con la fecha correspondiente y la hora, descripción del suceso ocurrido, daños producidos, en sistemas, mamposterías, edificios, recursos humanos afectados, etc., con los datos precisos de quienes van a hacerse cargo en las distintas etapas de la solución del mismo, de acuerdo a los planes pre-establecidos.

2. Catalogar el incidente, por la gravedad del mismo, los servicios afectados, la prioridad que se le tuvo que asignar, el término de la resolución del mismo y como perjudicó a la organización en su conjunto.

3. Analizar los informes, que deberán ser correctamente confeccionados, a fin de elaborar estadísticas, y monitorizar el rendimiento de los planes elaborados, realizar las mejoras técnicas que se crean necesarias en los mismos y optimizar los recursos.

Se debe tener en cuenta, que para una organización, no importa el tamaño que tenga, no es lo mismo, un incidente que ocurre en el sector de sistemas, porque el acceso a los datos se interrumpe por vulnerabilidades que afectan al mismo, que catástrofes naturales, como ser un terremoto como ocurrieron en distintas zonas del planeta, o un atentado, en el momento en que acaece algo de semejante magnitud, el personal de la organización, debería estar muy, pero muy preparado para afrontar con entereza semejante catástrofe, y pedir que registren todo lo ejecutado, seguramente será dificultoso.

Conclusiones

El sistema de gestión de continuidad (BCMS) es un procedimiento que abarca una serie de actividades a través de las cuales se obtiene una previsión eficaz para afrontar situaciones que lleven a interrumpir el normal funcionamiento de la organización y por lo tanto la operatividad del ente se encuentre en peligro y garantizar el desempeño continuo de las funciones esenciales de una compañía durante una crisis.

Un BCMS, abarca las fases de

- * Análisis del impacto de una interrupción en el normal funcionamiento del negocio
- * Plan de Continuidad del Negocio o BCP (Business Continuity Planning)
- * Recuperación de Desastres
- * Gestión de Incidentes.

Todas ellas deben llevarse a cabo, ya que derivada de una contingencia surgen los daños económicos causados por cada hora de no operatividad de la organización, ya sea bancaria, comercial industrial, de seguros, en los sistemas de distribución, del propio estado, en organismos como la AFIP, el ANSES, los ministerios, etc., que hacen que contar con un Sistema de Gestión de Continuidad, a la medida del organismo de que se trate, y con una inversión acorde, sea indispensable en toda empresa.

(1) Red Hat Enterprise Linux 4, Introducción a la administración de sistemas, Red Hat, Inc, 2005.

(2) Arcos González P., et-al, La ayuda sanitaria en desastres, Fundación para la Cooperación y Salud Internacional Carlos III, Madrid, 2006.

(3) Ardita Julio, Castellanos Raúl, Apuntes de la materia: Gestión, Auditoria y Normas de Seguridad, de la Carrera de Especialización en Criptografía y Seguridad Teleinformática, Facultad de Ingeniería, Dto. De Posgrados, Instituto Universitario del Ejército Argentino, 08/09-2009.

(4) Juan Rodríguez, El Plan de recuperación de desastres en la empresa, 15-02-2012, <http://www.tecnologiapyme.com/productividad/el-plan-de-recuperacion-de-desastres-en-la-empresa>.

(5) ITIL, Information Technology Infrastructure Library, <http://www.ital-officialsite.com/>