Continuidad del Negocio y Recuperación de Desastres (BC – Business Continuity / DR – Disaster Recovery)

Autor: Norberto Figuerola

Cuanto le podría costar una hora, un día o una semana a su negocio de inactividad ? Se ha estimado que una compañía promedio experimenta un total de 87 horas de inactividad no planificada por año. Aunque las personas suelen pensar en términos de desastres naturales, lo cierto es que el error humano puede representar un asombroso 70% de las interrupciones. Independientemente de la causa, la mayoría de los negocios no conocen el precio de una sola hora de inactividad y, en consecuencia, los planes de continuidad del negocio y recuperación de desastres suelen quedar en un segundo plano frente a otros proyectos que se consideran más prioritarios y con un impacto financiero más tangible. Pero, sin dudas, el impacto del tiempo de inactividad y la pérdida de datos se siente de diversas maneras, y puede ser inmediato o tener repercusiones a largo plazo.

La continuidad del negocio tiene sus orígenes en la recuperación ante desastres, y la recuperación ante desastres básicamente se trata de tecnología de la información. Veinte o treinta años atrás, la continuidad del negocio no existía conceptualmente, pero sí la recuperación ante desastres: la principal preocupación era cómo salvar los datos si se producía un desastre. En ese momento, era muy común comprar equipos costosos y colocarlos en una ubicación remota para que todos los datos importantes de una

organización estuvieran resguardados si, por ejemplo, se produjera un terremoto. No sólo resguardados sino también que los datos se procesarían más o menos con la misma capacidad que si estuvieran en la ubicación principal. Pero después de un tiempo se hizo evidente que no tenía sentido guardar los datos si no existieran operaciones comerciales en las cuales utilizarlos. Así fue como surgió la idea de la continuidad del negocio: su objetivo es permitir que el negocio siga funcionando, aún en caso de una interrupción importante.

Continuidad del Negocio y Recuperación de Desastres (BCDR o BC / DR) son prácticas que hoy en día están estrechamente relacionadas y describen la preparación de una organización con respecto a riesgos imprevistos para la continuidad de las operaciones. La tendencia de combinar la continuidad del negocio y recuperación de desastres en un solo término es el resultado de un creciente reconocimiento de que los ejecutivos de negocios y ejecutivos de tecnología deben colaborar estrechamente en lugar de desarrollar planes de manera aislada.

En términos generales, la recuperación de desastres se refiere a las medidas concretas adoptadas para reanudar las operaciones en las consecuencias de un desastre natural catastrófico o emergencia nacional. En la tecnología de la información, tales medidas pueden incluir la restauración de servidores o mainframes con copias de seguridad, restablecimiento de centrales privadas (PBX) o redes de área local (LAN) para satisfacer las necesidades de negocio inmediatas.

La continuidad del negocio describe los procesos y procedimientos de la organización debe poner en marcha para garantizar que las funciones de misión crítica pueden continuar durante y después de un desastre. En este sentido, el concepto es intercambiable con el plan de recuperación de desastres (DRP). La continuidad del negocio, sin embargo, también se ocupa de la planificación más integral que se centra en los retos a largo plazo o crónico para el éxito organizacional. Los posibles problemas de continuidad de negocio pueden incluir la enfermedad o retiro de los miembros clave de la empresa, problemas serios en la cadena de suministro, fallas catastróficas o infecciones de malware críticos.

Definiciones

Continuidad del negocio es la “capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades operativas y comerciales en un nivel aceptable previamente definido”.

Recuperación ante desastres se refiere “al proceso, políticas y procedimientos relacionados con preparar la recuperación o continuación de la infraestructura tecnológica crítica de una organización después de un desastre natural o producido por el hombre”.

Como puede verse en las definiciones, en la recuperación ante desastres el énfasis se encuentra en la tecnología, mientras que para la continuidad del negocio son las actividades comerciales. Por lo tanto, la primera es parte de la segunda; la puede considerar como uno de los principales facilitadores de las actividades comerciales, o como la parte tecnológica de la continuidad del negocio. Una forma sencilla de acercar estos dos conceptos es ver la gestión de la continuidad como un proceso global de identificación y planificación para contrarrestar los riesgos de continuidad del negocio, y parte de dicha planificación debe incluir la recuperación del negocio desde un escenario de desastre para volver a la normalidad del trabajo.

La continuidad del negocio es principalmente un asunto comercial, no un tema exclusivo de TI. Si el departamento de TI implementara la continuidad del negocio para toda la organización, no podría definir la criticidad de las actividades comerciales ni de la información. Probablemente la mejor forma de organizar la implementación de la continuidad del negocio es que el sector comercial lidere el proyecto; de esta forma lograría mayor concientización y aceptación de todos los sectores de la organización. El departamento de TI debe cumplir su función en ese proyecto, una función clave, preparar los planes de recuperación ante desastres.

Diferencias y Estándares

Las estadísticas indican que el 80% de las organizaciones que se enfrentan a una discontinuidad de negocios importante, y no cuentan con planes adecuados y suficientes para garantizar la continuidad del negocio, no sobreviven al evento. Organizaciones sensibles toman las medidas con suficiente antelación a posibles desastres, para asegurar que van a sobrevivir. En el clima actual, las organizaciones quieren asegurarse de que sus proveedores y las empresas en las que se han invertido van a ser capaces de hacer frente a cualquier desastre, y buscan acreditar esta evidencia a través de alguna certificación. La principal norma que existía (y sigue siendo aplicada aún) es la BS25999 que solamente habla respecto de la continuidad del negocio y no sobre recuperación de desastres. Hoy en día tenemos dos normativas:

ISO / IEC 24762:2008: Directrices para la prestación eficaz de la información y las comunicaciones (TIC) ante la Recuperación de Desastres (DR) de servicios. El asesoramiento y orientación de esta norma es genérico, por lo que es aplicable a cualquiera empresa o proveedor subcontratado de servicios TIC.

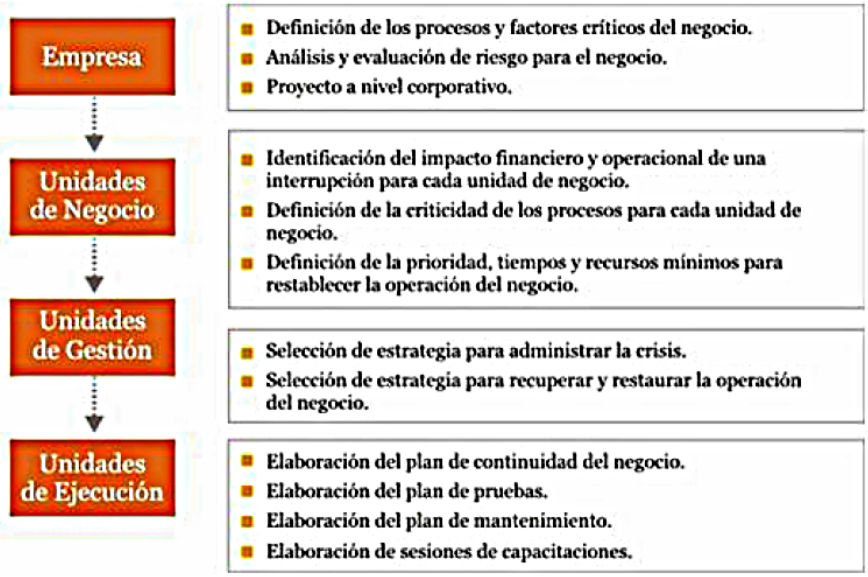
ISO 22301: 2012 : Seguridad Societaria y Continuidad de Negocio - Sistema de Gestión – Requisitos. Se publicó en mayo de 2012 y sustituye a la norma BS 25999, que se retira en noviembre de 2012. Especifica los requisitos para planificar, establecer, implementar, operar, monitorizar, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de incidentes perturbadores que puedan surgir.

La Continuidad del Negocio es un concepto fundamentalmente **Proactivo:** ¿Cómo evito o mitigo el impacto de un riesgo?. Algunos de los objetivos de la Gestión de la Continuidad del Negocio (*Business Continuity Management*) son:

- Definición de los procesos y factores críticos del negocio
- Evaluar los riesgos potenciales y preparar contingencias para acontecimientos imprevistos.
- Minimizar las interrupciones en las operaciones normales.
- Definición de la criticidad de los procesos para cada unidad del negocio
- Establecer mecanismos alternativos de operación de antemano.
- Mantener un mínimo nivel de servicio, mientras se restauran las operaciones.
- Proteger las funciones de negocio que ofrecen productos o servicios.
- Minimizar el impacto económico de las interrupciones.
- Capacitar al personal con los procedimientos de emergencia.

La Recuperación de Desastres (*Disaster Recovery*) es un concepto fundamentalmente **Reactivo:** ¿Cómo me recupero de un desastre y restauro la organización a un estado normal de operación una vez que un riesgo se ha materializado?. El Plan de Recuperación de Desastres (*Disaster Recovery Plan*) debe establecer los procedimientos para recuperar los procesos y sistemas después de una interrupción. El plan debe incluir:

- Definición de los sistemas, recursos y procesos necesarios para restaurar el servicio a los niveles previos al desastre.
- Definición de las fases de notificación y activación para detectar y evaluar los daños.
- Definición de las actividades, recursos y procedimientos necesarios durante la interrupción de las operaciones.
- Asignación de responsabilidades al personal autorizado para garantizar la coordinación.



Plan de Continuidad de Negocios

Rara vez estamos preparados para que ocurra un desastre, sin embargo, varias cosas pueden salir mal. Cada incidente es único y se desarrolla de forma inesperada. Aquí es donde un Plan de Continuidad de Negocios entra en juego. Para darle a la organización la mejor oportunidad de éxito, es necesario poner el plan en las manos de todo el personal responsable de llevar a cabo cualquier parte del mismo. La falta de un plan no sólo significa que a la organización le tomará más tiempo del necesario para recuperarse de un evento o incidente, sino que podría quedar fuera del negocio para siempre.

La Continuidad de Negocio (BC) se refiere al mantenimiento de las funciones de negocio o como podemos rápidamente reanudarlas en caso de una interrupción importante, ya sea causada por un incendio, una inundación, una enfermedad epidémica o un ataque malicioso a través de Internet . Un plan de BC describe los procedimientos e instrucciones que una organización debe seguir para encarar ese tipo de desastres, y cubrir los procesos de negocio, activos, recursos humanos , etc. El futuro de cualquier empresa depende de sus personas y procesos. Ser capaz de manejar cualquier incidente efectivamente puede tener un efecto positivo en la reputación y el valor de mercado, y aumenta la confianza de los clientes.

El Plan de Continuidad de Negocios es el proceso desarrollado para prevenir interrupciones que afecten el desempeño de las actividades normales del Negocio. En caso que un evento de riesgo no pueda ser evitado, este plan debe tender a minimizar su impacto (duración y económico). Tiene un alcance Operativo y Tecnológico.

Componentes

1.- Definir Estrategia de Continuidad

- Comprensión de los riesgos e impactos que enfrenta la organización
- Considerar la contratación de seguros
- Elaboración y documentación de una estrategia y planes de continuidad de los negocios
- Pruebas y actualización periódicas de los planes y procesos implementados;
- Garantizar que la administración de la continuidad de los negocios esté incorpora a los procesos y estructura de la organización.

2.- Análisis de Impacto (BIA)

El objetivo es determinar qué impacto podría llegar a tener un desastre sobre las funciones críticas del negocio. Éste es básicamente un informe que nos muestra el costo ocasionado por 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).

En el BIA se identifican los componentes claves requeridos para continuar con las Operaciones de Negocio luego de un incidente, dentro de estos componentes se encuentran:

- Personal requerido
- Áreas de trabajo
- Registros vitales
- Aplicativos críticos
- Dependencias de otras áreas
- Dependencias de terceras partes
- Criticidad de los recursos de información
- Participación del personal de seguridad informática y los usuarios finales
- Análisis de todos los tipos de recursos de información

Tres aspectos claves para el análisis:

- 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

3.- Diseño y Desarrollo del Plan

Preparar y documentar un plan detallado para la recuperación de los sistemas y procesos críticos del negocio. En primer lugar, crear un Plan de Continuidad de Negocio implica empezar por evaluar sus procesos de negocio, determinar qué áreas son vulnerables, y las pérdidas potenciales si esos procesos están inactivos por un día, unos días o una semana. Esto es esencialmente un (BIA). Se pueden utilizar cualquier número de plantillas gratuitas disponibles en línea o encontrar un plan real publicado por una organización similar a la suya y modificarlo si es necesario.

Hay seis pasos generales involucrados en la creación de un plan de continuidad del negocio :

1 . Alcance del plan

2 . Identificar las áreas clave del negocio.

3 . Identificar las funciones críticas.

4 . Identificar las dependencias entre las distintas áreas de negocio y funciones.

5 . Determinar el tiempo de inactividad aceptable para cada función crítica.

6 . Crear un plan para mantener las operaciones

Una herramienta común de planificación de continuidad del negocio es una lista que incluya suministros y equipo, la ubicación de copias de seguridad de datos y sitios de respaldo, disponibilidad del plan y quien debería tenerlo, información de contacto de los servicios de emergencia, personal clave y los proveedores de sitios de respaldo. El plan de Recuperación de Desastres es parte del Plan de Continuidad del Negocio, así que se debería consultar con el departamento de TI.

Este plan debe ser una guía de implementación. Debe incluir identificación de funciones críticas, identificación de sistemas que son necesarios, estimación del daño potencial y cálculo de los recursos mínimo para recuperar los servicios, selección de estrategia de recuperación y determinación de personal crítico para la recuperación.

5.- Pruebas y Mantenimiento

Se debe probar rigurosamente un plan para saber si es completo y cumple con los fines previstos. Muchas organizaciones ponen a prueba un plan de continuidad de negocios de dos a cuatro veces al año.

Los exámenes comunes incluyen ejercicios de mesa , paseos virtuales estructurados y simulaciones. Los equipos de los exámenes generalmente están compuestos por el coordinador de la recuperación y los miembros de cada unidad funcional. Un ejercicio de simulación por lo general ocurre en una sala de conferencias con el equipo estudiando minuciosamente el plan, buscando debilidades y asegurando que todas las unidades de negocio están representadas en el mismo. A menudo, el equipo trabaja a través de la prueba con un desastre específico en mente.

Es también una buena idea llevar a cabo un simulacro de evacuación de emergencia completo al menos una vez al año. Este tipo de prueba le permite determinar si es necesario tomar medidas especiales para evacuar a los miembros del personal que tienen limitaciones físicas Las pruebas de simulación de desastres pueden ser un poco complicadas y se debe realizar al menos anualmente.

Las pruebas del plan son extremadamente críticas, dado que sin ellas no podemos evaluar si el plan funcionará o no. Existen 5 posibilidades de pruebas:

• Checklist: Consiste en distribuir copias del plan a todos los involucrados, los cuales deben revisar el plan y aceptarlo. No es una prueba formal, pero siempre es un buen comienzo.

• Discusión en mesa redonda: Consiste en reunir a todos los involucrados y seguir el plan línea por línea. Este mecanismo permite descubrir dependencia o relaciones entre los distintos departamentos.

• Ensayo (walkthrough): Esta es una simulación en terreno de la contingencia, siguiendo paso a paso el plan. Permite comprobar que todos los involucrados pueden cumplir con su deber.

• Funcional: Permite aplicar el plan de contingencia, moviendo los servicios a un sitio alternativo (el cual queda corriendo en paralelo).

• Interrupción Total: Consiste en interrumpir intencionalmente el servicio productivo y aplicar el plan de contingencia. Esta es claramente la alternativa de mayor costo y consumidora de tiempo.

6.- Necesidad de Entrenamiento

Además de las pruebas, es necesario un programa de entrenamiento que entregue la información y la capacitación del personal adscrito al plan. Deben realizarse cursos que deben de contemplar en detalle los siguientes aspectos:

- Descripción general del plan.
- Funciones y obligaciones del personal adscrito a cada uno de los equipos de emergencias.
- Descripción de las posibles emergencias que pueden afectar a organización.

7.-Mantenimiento y Reevaluación del Plan

La tecnología y el negocio evolucionan, y la gente va y viene, por lo que el plan debe ser actualizado. Revisar por lo menos anualmente el plan y discutir las áreas que han de ser modificadas. Antes de la revisión, solicitar la retroalimentación del personal para incorporar en el plan. Solicitar a todos los departamentos o unidades de negocios que revisen el plan, incluyendo las sucursales u otras unidades remotas. Si se ha tenido la desgracia de enfrentarse a un desastre y tuvo que poner el plan en acción, asegurarse de incorporar las lecciones aprendidas.

Cada plan de continuidad del negocio debe ser apoyado desde arriba hacia abajo. Esto significa que la alta dirección debe estar representada en la creación y la actualización del plan, nadie puede delegar su responsabilidad en subordinados. La gestión es también la

clave para promover el conocimiento del usuario. Si los empleados no saben sobre el plan, cómo van a ser capaces de reaccionar adecuadamente cuando cada minuto cuenta. Aunque la distribución y formación puede llevarse a cabo por los gestores de las unidades de negocios o personal de recursos humanos, el inicio de la concientización y formación debe generarse en la capa superior de la organización para acentuar su importancia y lograr un mayor impacto en todos los empleados, dando al plan más credibilidad y urgencia.

Para lograr que el plan se mantenga actualizado y permita la recuperación ante un desastre, es necesario documentar las responsabilidades de su mantenimiento, elaborando una matriz que indique para cada una de las secciones del plan:

• El responsable de las revisiones periódicas de cada uno de los planes de continuidad del negocio.

• La periodicidad con la que realizará una revisión.

• Una descripción con los principales aspectos a revisar.

• Identificación de cambios en las disposiciones relativas al negocio aún no reflejadas en los planes de continuidad

Plan de Recuperación ante Desastres (DRP)

Es el proceso de retomar el desarrollo normal del Negocio, luego de declarado un evento que afecta la continuidad del mismo. Generalmente está focalizado en los aspectos Tecnológicos. Es el conjunto de acciones necesarias de ejecutar para volver a la situación que existía antes del desastre. Este plan puede dividirse en 2 roles:

• Salvamento: Restaurar la funcionalidad de los sistemas dañados, unidades y de las instalaciones. Incluye los siguiente pasos:

- Evaluar los daños
- Recuperación del equipamiento reparable.
- Reparación y limpieza de las instalaciones. Recuperación del equipamiento faltante.
- Restauración de las instalaciones a su estado original.

- Recuperación**:** Se focaliza en la responsabilidad de migrar los servicios a un sitio alternativo.

Alternativas de Recuperación

- Opciones ante Desastres o No Hacer Nada
- Procedimientos Manuales
- Acuerdos Recíprocos
- Recuperación Gradual (Standby Frio)
- Recuperación Intermedia (Standby Templado)
- Recuperación Inmediata (Standby Caliente)
- Tipos de Respaldo (Backup) o Full: Respalda toda la información disponible a la fecha de ejecución.
    - Incremental: Respalda todos los archivos modificados desde el último backup ejecutado.
    - Diferencial: Respalda todos los archivos modificados desde el último backup full.

Estrategia de Backup o Incremental, Delta o Full

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
I	I	I	I	I	I	D
I	I	I	I	I	I	D
I	I	I	I	I	I	D
I	I	I	I	I	I	F

Plan de DR

Como cualquier proyecto importante, el DR comienza con una planificación, seguido de plantillas y procedimientos de mejores prácticas, que a su vez se implementan, en parte con herramientas adecuadas.

Además de identificar las aplicaciones de misión crítica y de infraestructura, se basan en identificar los datos de estas aplicaciones y las tareas que necesitan tener acceso a las mismas. Esto puede incluir correo electrónico, bases de datos de los clientes, y todos los documentos, hojas de cálculo, presentaciones y otros archivos "no estructurados" utilizados por la gestión de proyectos / productos, desarrollo, ventas, manufactura, etc. Las empresas acumulan una cantidad considerable de datos en el tiempo, cientos de

gigabytes, terabytes o quizás petabytes. Pero sólo algunos, a menudo una pequeña fracción, de estos datos los que tienen que estar disponibles nueva y rápidamente.

La causa de un desastre de TI no necesariamente tiene que ser relevante, puede ser pequeña y específica. Una fuente de alimentación, CPU, tarjeta de interfaz de red, memoria RAM, refrigeración, u otro componente en un servidor individual que pueda fallar. Una breve fluctuación de energía puede codificar datos o interrumpir la actividad de un programa. La caída de un centro de cómputos completo es raro, pero puede suceder. El daño por fuego, inundación, o terremoto son causas que pueden hacer caer toda la sala de cómputos o centro de datos.

Un marco de planificación de DR generalmente consiste de 4 pasos:

- evaluación del impacto de negocio,
- evaluación de riesgos,
- gestión de riesgos
- pruebas de recuperación

Paso 1 : Análisis de Impacto al Negocio

Un Análisis de Impacto al Negocio (BIA) define las capacidades que tiene la empresa de no poder funcionar sin la disponibilidad de algunas áreas de negocios. Este es el primer paso en la creación de un Plan de Recuperación de Desastres.

Hacer un BIA debe involucrar el manejo de nivel superior, para identificar y ponerse de acuerdo sobre la lista de aplicaciones que se consideran esenciales, junto con la infraestructura y otros servicios necesarios para el funcionamiento y el uso de estas aplicaciones asociado.

Todas las principales partes interesadas deben participar en este análisis. Básicamente todo lo descripto para la Continuidad del Negocio respecto del BIA es utilizable en este plan también. Dos métricas esenciales se utilizan especialmente en el análisis de impacto de DR el RTO y el RPO.

RTO y RPO

Objetivo de Punto de Recuperación (RPO) y Recovery Time Objective (RTO)
El objetivo de hacer copias de seguridad de los datos que consideramos críticas para el negocio es estar en disposición de recuperarlas en caso de desastre o pérdida de datos.

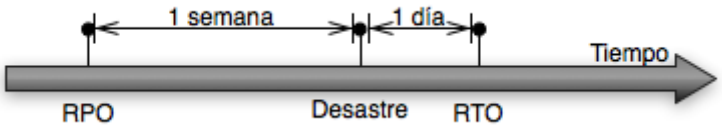
Teniendo claro que el objetivo de las copias de seguridad es garantizar la recuperación de los datos, es decir, la disponibilidad de los datos, hay que tener claro en qué condiciones recuperamos estos datos.

Para identificar las condiciones de recuperación de los datos hay dos valores temporales que siempre debemos valorar a la hora de diseñar un sistema de copias de seguridad y que se conocen como RTO y RPO.

El **RTO (Recovery Time Objective)** es el tiempo en que se tarda en recuperar los datos en caso de pérdida.

El **RPO (Recovery Point Objective)** es el punto de recuperación de los datos. Es decir, en qué momento temporal anterior a la pérdida se recuperan los datos.

Para entender mejor el significado de estos dos valores, a continuación se representan en modo de ejemplo en una escala temporal.



En el ejemplo se observa que el RTO es de 1 día y el RPO es de 1 semana. Esto significa que en caso de pérdida de datos, tardaremos 1 día a recuperar los datos y que después de la recuperación, los datos que obtendremos tendrán una semana de antigüedad como mucho. Es decir, que habremos perdido los datos de la semana anterior a la pérdida de datos.

Estos dos conceptos, el RTO y el RPO, determinarán las políticas de copias de seguridad. Estas se dimensionarán según el impacto que tiene la pérdida de los datos. Por eso nos tenemos que preguntar cuáles son los efectos de perder los datos de un día, dos, una semana o un mes. Y también cuáles son los efectos de no disponer de los datos durante un día, dos,

Paso 2: Evaluación del riesgo

El segundo paso para un plan de DR completo incluye la cartografía de los 2 tipos de infraestructura de TI:

1. Infraestructura de TI a controlar, ya sea ubicado en sus oficinas o en las instalaciones de co-localización y de TI.

2 Infraestructura de TI que no controla, como servicios web y en la nube o en los sitios Web que se ejecutan en un centro de alojamiento.

Una vez que la infraestructura de TI ha sido asignada, buscar los puntos únicos de fallo (SPOF), como un servidor con sólo una tarjeta de red. Estos son los primeros lugares a considerar "fortificar" con redundancia.

Paso 3 : Gestión de Riesgos

Para disminuir el riesgo de que ocurra un desastre de datos, la organización deberá fortalecerse y protegerse contra los problemas más comunes el 90% -95 % de los pequeños incidentes que puedan afectarla. La redundancia es un método general para evitar o minimizar los varios eventos de desastres de TI. Por ejemplo, los servidores, el almacenamiento y equipos de red se pueden configurar con dos fuentes de alimentación, conectado a su vez a las fuentes de alimentación independientes. Servidores, firewalls, UPS y otro equipo, incluso sitios enteros, se puede duplicar. La Red y servicio eléctrico pueden ser suministrados por dos empresas independientes por cables separados. Los datos pueden ser almacenados en varios discos duros.

Paso 4 : Pruebas de Recuperación

Sólo hay dos maneras de determinar si un plan de Plan de DR funciona. Una es cuando hay un desastre. Esto, por supuesto, es la forma equivocada de deteminar si el Plan ha fallado, por ejemplo en incluír una aplicación crítica. La otra forma es realizar periódicamente pruebas. Es mejor descubrir un defecto en la infraestructura probando escenarios de fallo en circunstancias controladas. Por ejemplo, en una prueba controlada, si se descubre que una tarjeta de red no funciona correctamente, se puede detener la prueba, instalar una nueva tarjeta, y ejecutar la prueba de nuevo.

Las auditorías externas pueden ayudar a identificar si existe algún elemento del Plan de DR que aún necesita elaboración. No todas las organizaciones pueden simular un escenario completo de desastre, o llevaran a cabo actividades para confirmar una recuperación completa. Las auditorías externas pueden mantener un nivel más alto de lo que la empresa pueda configurar, y llevar a cabo pruebas más rigurosas, completas, y obligar a seguir las mejores prácticas de TI.

Enfoques de copia de Seguridad Off-Site

En la mayoría de los eventos de desastres de TI, la recuperación implica la restauración de los datos, debido a que la copia principal ha sido dañada, destruida o resulta inaccesible.

Para asegurarse de que una copia de los datos está disponible cuando se produce un desastre, una copia de seguridad fuera del sitio es fundamental. Debe estar geográficamente tan lejos que un gran evento como fuego, inundación, terremoto, corte de luz, o una explosión no haga daño o aisle el respaldo.

El backup en cinta o cartuchos fue lo que se usó generalmente como copia de seguridad fuera del sitio durante décadas. Pero existen problemas con las copias de seguridad

basadas en cinta, toman tiempo para encontrar y recuperar información, si la cinta está defectuosa, no se descubre hasta que se la utilice, para leer cintas de generaciones anteriores, es necesario tener una unidad de cinta de trabajo que los apoya y altos costos de infraestructura. Actualmente en un mundo de 24x7x365una copia de seguridad que no es rápida y de fácil acceso puede resultar buena para la preservación de importantes datos de la empresa, pero no es útil para la recuperación de desastres. El RTO de hoy se mide en horas o incluso minutos.

Está prohibida la difusión, transmisión, modificación, copia, reproducción y/o distribución total o parcial del presente Documento, en cualquier forma y por cualquier medio, sin la previa autorización escrita del autor, encontrándose protegidos por las Leyes de Derecho de Autor, Marcas, Lealtad Comercial, Bases de Datos y otras normas Asimismo, queda prohibido cualquier uso de los Documentos o parte de los mismos con fines comerciales. La violación de los derechos antes señalados puede acarrear condenas civiles y/o penales establecidas en las normas precedentemente citadas. Se exigirán responsabilidades a los infractores por todas las vías disponibles en derecho.
Fecha y lugar de publicación: Buenos Aires, Abril de 2014. Queda hecho el depósito que establece la Ley 11.723.