¿Cuál es el estado de su Continuidad Empresarial?

BUSINESS CONTINUITY / DISASTER RECOVERY

El desarrollo de un plan de continuidad de negocio y el plan de recuperación de desastre puede asegurar la continuidad de la operación ante cualquier contingencia o acontecimientos inesperados que pueden tener fuertes impactos en las organizaciones.

Los riesgos y las vulnerabilidades de la información son un hecho; más aún, conforme avanza la tecnología aumenta la probabilidad de que se materialicen y dependiendo de su grado, el negocio siempre se verá afectado.

Antecedentes de la Continuidad de Negocio

La recuperación de desastres (Disaster Recovery) es un concepto desarrollado en los años 70´s, a partir de que los administradores de centros de cómputo comenzaron a reconocer la dependencia de sus empresas con sus sistemas computarizados. En esa época, la mayoría de los sistemas eran procesos en lote que corrían en grandes computadoras centrales y en muchos casos podían estar caídos por varios días antes de que impactaran significativamente a la organización.

Con el acelerado crecimiento del Internet, empresas de todos los tamaños se volvieron mucho más dependientes de la disponibilidad de sus sistemas informáticos, llegando algunas empresas a establecer niveles de disponibilidad de hasta 99.999%. Este incremento de la dependencia con los sistemas de TI, así como la conciencia de posibles desastres a gran escala, impulsaron al crecimiento de las diversas industrias relacionadas a la recuperación ante desastres, desde soluciones de alta disponibilidad, así como infraestructuras alternas, hasta la consolidación de la disciplina de continuidad de negocios.

Hoy en día, la gestión de la continuidad del negocio abarca a todas las funciones y recursos como: procesos críticos del negocio, recursos humanos, mantenimiento y respaldo del suministro eléctrico, enlaces de internet redundantes, seguridad y muchos otros factores.

Jerárquicamente, la continuidad de negocio está arriba; después está el plan de recuperación de desastres y debajo de este viene la tecnología, como el respaldo de datos, la recuperación y la restauración de TIC.

El responsable de TI, con su plan de recuperación de desastres (DRP), es un elemento clave dentro del gran escenario de la continuidad del negocio (BC); de hecho debe convertirse en el Chief Innovation Officer (CIO) y debe estar alineado totalmente a los objetivos del negocio.

Connectic Data
Tecnologías, Analítica y Comunicación

¿Cuál es la diferencia entre Business Continuity y Disaster Recovery?

Como el término lo indica, **la Continuidad de Negocio (BC)** se centra en la manera continua de la operación para minimizar eficazmente las interrupciones de su negocio, asegurando que el tiempo de inactividad se limite únicamente a los niveles aceptables del negocio. Es decir, BC, se centralizada en torno a la expectativa de alta disponibilidad de arquitecturas que soportan los sistemas esenciales de TI, pero también implícitamente cubre todos los procesos de negocio que podrían verse afectados por el incidente.

La recuperación de desastres (DR) se focaliza en la restauración de los servicios después de un evento, por lo general en una ubicación alternativa que está geográficamente distante de la ubicación principal donde ocurrió el incidente o desastre. DR hace énfasis por lo general en la infraestructura de TI que apoya las operaciones de negocio y dispone de un centro geográfico distinto que sirva como un lugar alternativo para la información crítica y de los servicios.

Definamos Desastre

Cuando se habla de desastre, lo primero que viene a nuestra mente es un desastre natural como el que genera un huracán, incendio o terremoto. Estas son preocupaciones válidas y de hecho son aspectos muy importantes para considerar en México, como parte de un plan de DR; Sin embargo, los desastres no tradicionales pueden venir en muchas formas y con frecuencia son más probables de ocurrir que los desastres naturales. Esto incluye prácticamente de todo, desde la pérdida de personal clave, huelgas laborales, explosiones, hasta las brechas de seguridad y fallas de hardware.

En realidad, los desastres tienen muchas variantes, pero pueden ser definidos como cualquier cosa que impida el acceso a los sistemas y procesos cuando estos son necesarios o vitales para el negocio.

Es necesario plantear argumentos con la probabilidad de que ocurran desastres.

Una vez que se haya cuantificado el impacto de una interrupción del servicio, podemos comenzar a evaluar la posibilidad de que un desastre ocurra. Recomendamos centrarse en los desastres más realistas, como la rotación de personal o la pérdida de conectividad de la red y entender a lo que se tiene que dar respuesta, siempre y cuando dichos eventos ocurran.

Se debe definir cuánto tiempo de inactividad es aceptable

- Utilice datos históricos para elaborar una lluvia de ideas sobre cuánto tiempo de inactividad es aceptable para su negocio.
- Tenga en cuenta que, para algunas empresas, el tiempo de inactividad puede tener un impacto casi irreparable a la reputación de una marca.
- Se debe entender y concientizar sobre las implicaciones de este tipo de eventos y asegúrese de tomar las medidas correctas para mantener el funcionamiento en el tiempo necesario.
- **OPR= Objetivo de Punto de Recuperación**, calcule el objetivo de recuperar el nivel de información dentro del tiempo establecido.
- **OTR= Objetivo de Tiempo de Recuperación**, calcule la cantidad de tiempo aceptable en que la recuperación debe llevarse a cabo.

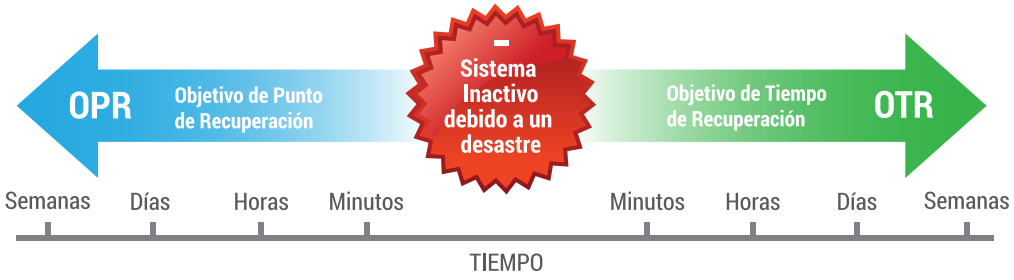
El OPR, se refiere a la cantidad de datos que su empresa puede darse el lujo de perder, ya sea de 2 horas de valor de datos o valor de 2 días.

El OTR, se centra más en el tiempo efectivo en el que se llevan a cabo las operaciones normales.

Por ejemplo, algunas empresas podrían estar tranquilas si sus negocios fueran cerrados por unos días, mientras que otras organizaciones estarían en serios problemas si sus sistemas o redes colapsaran por más de una hora.

Acote a la vez un OPR y OTR, estos son esenciales para determinar qué tipo de medidas se deben tomar para garantizar la continuidad apropiada de su negocio y permita una rápida recuperación después de un desastre.

¿En dónde se encuentra su organización y en qué punto debe estar?



Gestión del Riesgo

La realización de un Business Impact Analysis (BIA) permite a una organización tomar decisiones de riesgo significativamente más informadas. Las buenas prácticas de gestión de riesgos se traducen en una o más de las siguientes estrategias:

Limitación de riesgo y mitigación

Esta estrategia abarca los controles, arquitecturas, topologías, etc., que están diseñados para reducir la probabilidad de una interrupción del servicio. El detalle derivado del esfuerzo BIA ayuda a determinar la justificación económica o la falta de este, para la adopción de diversos enfoques de mitigación de riesgos.

Anulación de riesgo

Evitar el riesgo es esencialmente una decisión de negocios para evitar determinadas actividades o modelos de negocio teniendo en cuenta sus características de riesgo.

Transferencia de riesgo

La transferencia de riesgo se puede lograr de varias maneras, desde la compra de seguros para cubrir las pérdidas potenciales a través de la contratación de servicios de otras organizaciones que están mejor equipadas para limitar o mitigar el riesgo en cuestión. Esto incluye a los proveedores o aliados de negocio, que brindan servicios gestionados de seguridad, servicios de conectividad empresarial, servicios de centro de datos remoto, etc; así como a la línea de negocio, tales como la nómina y Recursos Humanos. Con una adecuada gestión, el riesgo transferido realmente puede ser una estrategia exitosa dado que muchos de los proveedores y aliados de negocio, ofrecen estos servicios de una forma en función de sus economías de escala, infraestructura y personal.

Riesgo asumido

En última instancia, el asumir los riesgos no es una estrategia, sino la aceptación de una cierta cantidad residual de riesgo que sea apropiada y aceptable a la luz del OPR y OTR establecido en el BIA.

Análisis de Impacto de Negocio (BIA)

Planes de contingencia eficaces ilustran con una multitud de escenarios de riesgo y evalúan estos en términos de su probabilidad y su impacto, en caso de que ocurran. Para facilitar esta comprensión, el análisis de impacto del negocio (BIA) es el que generalmente se realiza.

– Más del 40% de los negocios nunca vuelven a abrir después de un desastre –

*** ¡2 de cada 5 empresas que experimentan un desastre pueden quedar fuera de su negocio hasta por 5 años!**

* Las principales causas de inactividad en una organización en México son:

- Caída del sistema: 43.1%
- Errores Humanos: 25.5%
- Caída de la aplicación: 15.7%
- Desastre Natural: 11.8%
- Actos maliciosos: 3.9%

*Fuente: IDC Latin America Data Center Survey.

Un análisis de impacto de negocio (BIA) es el paso más crítico en cualquier esfuerzo de planificación exitoso de BC/DR. El objetivo de un esfuerzo BIA eficaz, es lograr la comprensión de la criticidad de los procesos de negocio específicos y la infraestructura de TI implícita que soporta estos procesos.

Entendamos la función de aplicaciones de gestión esenciales

Si su empresa utiliza sistemas ERP como SAP, Oracle y Microsoft Dynamics, o se basa en sistemas de correo electrónico como Exchange, estas son las probables aplicaciones que son esenciales para la actividad empresarial normal del día a día. Comprendamos que estos sistemas deben ser prioritarios, como las primeras cosas que se deben restaurar en caso de un desastre.

Inventariar los sistemas críticos y personal

Cada pieza de la infraestructura de TI de su empresa debe estar documentado, desde servidores a redes para respaldar los medios de comunicación. Además, la información de contacto del personal crítico, de terceros, de proveedores de servicios y grupos de interés críticos como clientes, debe ser fácilmente accesible en caso de un desastre.

Cuantifique el impacto de una interrupción de servicio

Se debe tener muy presente las consecuencias financieras, contractuales y regulatorias en caso de experimentar un evento. Por ejemplo, si usted opera un sitio de comercio electrónico, determinar cuántos ingresos se pierden por cada minuto que el sitio está abajo. Si usted brinda servicio a los clientes, entender lo que su contrato dice acerca de su nivel de servicio. Es necesario comprender lo que se perdería al sufrir una interrupción del servicio.

Implementación de una estrategia de BCP/DRP

Entonces, ¿cómo vincular si necesitamos un sitio DR para BCP/DRP? Deje que el BIA haga el trabajo pesado. Cuando una organización lleva a cabo un BIA, esta puede determinar el mejor enfoque para la continuidad o recuperación en función del valor económico o comercial.

No es evaluar el riesgo y proteger las funciones esenciales del negocio y sus sistemas de TI, es negligente y en última instancia puede resultar en graves consecuencias para el negocio. Los objetivos OPR y OTR que se derivan de los análisis BIA ayudan a las organizaciones para pensar, en el apropiado control preventivo y diseños arquitectónicos necesarios para cumplir estos objetivos.

Los sistemas que requieren mayor tolerancia a las fallas requerirán una arquitectura de alta disponibilidad, que minimice los impactos de falla en el diseño del sistema. Aunque no hay una única solución, hay una variedad de opciones que pueden hacer las organizaciones para seguir adelante con su estrategia de BCP/DRP.

¿Sabe cuál es el estado actual de su plan de recuperación de desastres?

Nulo
No existe prevención (respaldos, capacitación, documentación) ni una estrategia formal de respuesta.

Bajo
Existe un seguro, un Plan de Protección Civil y una prevención de respaldos independientes de información pero no hay estrategia formal de respuesta.

Medio
Existe un DRP (estrategia de IT) o un BCP (estrategia de negocio) pero no ambos.

Alto
Existe prevención, estrategia formal de respuesta (DRP y BCP), se han realizado pruebas, así como capacitación y la administración del plan la lleva manualmente un equipo especializado.

Óptimo
Existe prevención, estrategia formal de respuesta (DRP y BCP), se han realizado pruebas y capacitación. Además, se cuenta con una solución de administración y activación de Continuidad.

Importancia de Sitios Calientes / Fríos

La Infraestructura de TIC es el centro de recuperación de desastres que por lo general tiene menos tolerancia a fallas. Como ejemplo, sitios remotos fríos (centros de datos u otras instalaciones donde el equipo puede enviarse a las operaciones de restauración), y el sitio caliente (centros de datos donde se haya la conectividad de red y hardware pre-posicionados) estos son generalmente parte de una estrategia DRP y está en sincronía con la idea y esfuerzos de recuperación a un desastre, suelen ser más reactivas; mientras que los métodos de continuidad del negocio son más proactivas y preventivas. Independientemente, ambos requieren del esfuerzo de planificación.

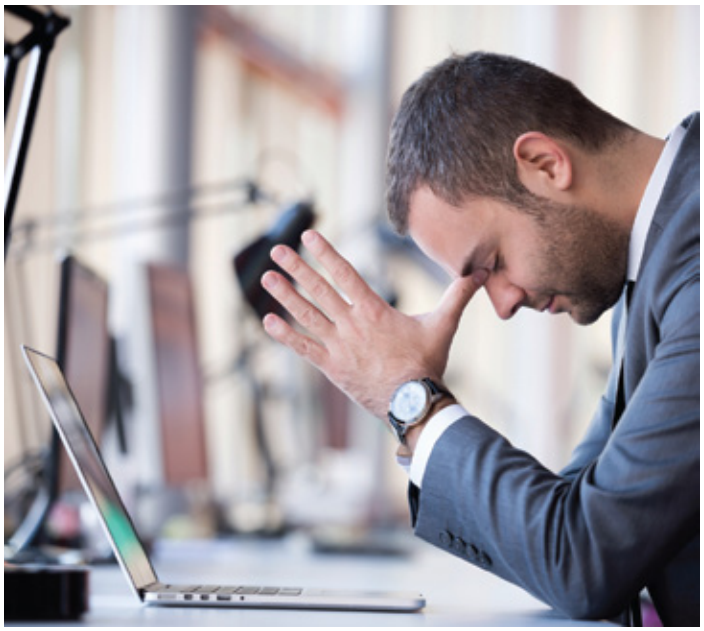
Seguridad

Los requisitos de seguridad de los datos derivados de las leyes locales y federales, es fundamental para incluir la seguridad y la mitigación del incumplimiento de cualquier esfuerzo de planificación BC/DR.

La restauración de los procesos de negocio claves o sistemas de TIC de una manera insegura en última instancia, aumentan el daño causado por una interrupción del servicio. Pocos escenarios son peores, que la restauración de servicios después de un desastre, sólo para encontrar que los expedientes clave de la organización y los datos han sido comprometidos, ya sea por falta de cifrado o la falta de aplicación de las políticas apropiadas y prácticas de seguridad en el sitio de recuperación o fallas.

Acuerdo de Nivel de Servicios

Para ayudar a pensar en la tolerancia a fallas y el tiempo de inactividad, es importante tener en cuenta las métricas de disponibilidad y el tiempo de inactividad permisible. En realidad, se basa en los objetivos de los SLA. Estos números deben ser evaluados en conjunto con su organización para determinar qué tipo de SLA se necesita.



Consideraciones

Se debe minimizar el riesgo de indisponibilidad en los servicios y procesos críticos de su organización, con los planes de recuperación más avanzados que actualmente están al alcance de las organizaciones. Ya existen herramientas, proveedores y aliados de negocios que su único fin es automatizar el proceso de administración de planes de continuidad de negocio, que permiten a las organizaciones tener planes actualizados, responder ante contingencias en tiempos de tolerancia ideales y que garantizan un excelente manejo de los incidentes.

Con demasiada frecuencia se observa como las compañías luchan por recuperarse después de un desastre y pensar: Nunca nos va a pasar a nosotros. Sin embargo, este exceso de confianza es exactamente lo que inevitablemente lleva a las empresas a su propia desaparición. Cada organización solo tiene que pensar en BCP/DRP, sin excepción alguna. Los desastres se producen en cualquier momento y las empresas que sobreviven a estos, son las que realmente entienden el valor de la continuidad del negocio, si se espera hasta después de un evento para empezar a considerar un BCP/DRP, es muy probable que las empresas afectadas nunca se recuperen.

Acerca de Connectic Data

Connectic Data, apoya a la comunidad de TIC en México a ser facilitadores y simplificadores de soluciones y servicios de TIC, asistimos a las empresas en la planificación, integración, desarrollo, implementación y administración de su infraestructura de TIC con el fin de maximizar su disponibilidad, capacidad de respuesta y su continuidad de negocio.

Connectic Data, particulariza una estrategia de TI que puede ser escalable a largo plazo, con un costo total de inversión competitivo a través de las economías de escala.

Connectic Data
Tecnologías, Analítica y Comunicación

www.connecticdata.com