arcserve®

eBook

CÓMO ELABORAR UN PLAN DE RECUPERACIÓN DE DESASTRES

MEJORES PRÁCTICAS

CÓMO ELABORAR UN PLAN EXITOSO DE RECUPERACIÓN DE DESASTRES

Los desastres suceden, y no hay dinero ni planificación que puedan detenerlos. Sin embargo, un buen plan de recuperación de desastres (DR) puede reducir el tiempo de inactividad en su empresa de semanas o días a solo horas o incluso unos pocos minutos.

Al igual que todo proyecto importante, un proceso exitoso de DR comienza con una planificación, seguida de modelos y procedimientos de mejores prácticas, que son implementados utilizando las herramientas adecuadas.

Además de identificar las aplicaciones críticas y la infraestructura en la que se basan, es necesario también determinar los datos a los que estas aplicaciones y tareas necesitan acceder.

Es probable que, a lo largo del tiempo, su empresa haya acumulado una cantidad significativa de datos: cientos de gigabytes, terabytes o, por qué no, petabytes. Pero siempre es necesario recuperar rápidamente una pequeña fracción de estos datos.

PASO 1: Análisis de impacto en el negocio

Un análisis de impacto en el negocio (BIA) define cuáles son las funcionalidades sin las que su empresa no podría operar. Este es el primer paso en la creación de un plan útil de recuperación de desastres.

El BIA debe contar con la participación de directores externos al departamento de TI para identificar y acordar un listado de aplicaciones consideradas esenciales, además de los directores de TI para coordinar las tareas sobre las aplicaciones, y también para analizar la infraestructura asociada y otros servicios que se requieran para ejecutarlas y utilizarlas.

Todas las partes interesadas deben participar del análisis. Esto permite asegurar que estén cubiertas todas las aplicaciones que los ejecutivos consideran esenciales en el caso de inactividad.

PASO 2: Evaluación de riesgos

El segundo paso en el proceso de elaboración de un plan de DR consiste en analizar los dos tipos de infraestructura de TI:

1. Infraestructura de TI bajo control de la empresa, ya sea que esté ubicada en oficinas propias o en instalaciones compartidas.
2. Infraestructura de TI fuera del control de la empresa, como servicios web y de nube o sitios web que se ejecutan en un entorno alojado

Una vez analizada la infraestructura de TI, busque puntos únicos de falla, como servidores con una sola tarjeta de red.

Estos son los primeros elementos que debe considerar para "reforzar" sus sistemas con redundancia.

¿CUÁLES SON LAS CAUSAS DE LOS DESASTRES DE TI?

La causa de un desastre de TI puede relacionarse con algo pequeño y específico. Puede existir una falla en una unidad de alimentación, CPU, tarjeta de interfaz de red, memoria RAM, ventilador u otro componente de un determinado servidor. Una mínima fluctuación en la alimentación puede alterar los datos o la actividad de un programa.
No es habitual que se interrumpa un centro de datos en su totalidad, pero puede suceder. También hay cuestiones climáticas que pueden cortar la energía o la conectividad. Los incendios, las inundaciones o los daños en los edificios pueden hacer estragos en sus centros de datos o salas de informática.

PASO 3: Gestión de riesgos

Para disminuir el riesgo de que suceda un desastre de TI, refuerce sus sistemas contra los problemas más comunes. Así, estará protegido contra el 90-95% de los pequeños incidentes que podrían afectar a su empresa.

La redundancia es un enfoque popular que se adopta a la hora de evitar, o minimizar, muchos de los desastres de TI. Por ejemplo, los sistemas de servidores, almacenamiento y redes pueden configurarse con dos unidades de alimentación conectadas, a su vez, a dos fuentes independientes de energía. Servidores, firewalls, UPS y otros dispositivos, incluso sitios enteros, pueden duplicarse. Los servicios de redes y electricidad pueden ser provistos por dos empresas diferentes, incluso a través de un cableado diferente. Los datos pueden almacenarse en múltiples discos duros.

PASO 4: Pruebas de DR

Existen solo dos formas de determinar la efectividad de un plan de DR.

En primer lugar, ante la ocurrencia de un desastre. Este, por supuesto, no sería un momento ideal para detectar errores de planificación, fallas en las herramientas o servicios, o incluso alguna aplicación crítica faltante.

En segundo lugar, es posible llevar a cabo pruebas periódicas. Es mejor descubrir los potenciales errores en su infraestructura probando escenarios de fallas bajo condiciones controladas.

Las auditorías externas permiten identificar si existen elementos de su plan de DR que necesitan ajustarse. No todas las organizaciones pueden simular un escenario de desastre total, o llevar adelante pruebas que permitan confirmar una recuperación plena. Con una auditoría externa, podrá aplicar un estándar más estricto y efectuar pruebas completas y rigurosas, lo que lo obligará a seguir las mejores prácticas de TI.

Enfoques de backup externo

En la mayoría de los desastres de TI, la recuperación implica recuperar datos, ya sea porque la copia principal se ha dañado o destruido o no se puede acceder a ella.

Para garantizar que una copia de sus datos esté disponible en caso de desastres de TI, es crítico contar con un backup externo. Estas copias de seguridad deben estar lo suficientemente alejadas geográficamente, para asegurar que, ante la ocurrencia de un evento significativo, como incendios, inundaciones, cortes de energía, explosiones o sismos, la ubicación de backup no se dañe o aísle.

Durante décadas, la cinta fue el método de backup externo más popular. Sin embargo, existen desventajas:

- Lleva tiempo solicitar, encontrar y recuperar cintas externas.
- Si una cinta se encuentra dañada, es imposible reconocerlo hasta necesitarla.
- Para usar cintas de generaciones anteriores, es necesario contar con una unidad adecuada que sea compatible. En caso de que sus instalaciones sean inaccesibles, también necesitará una ubicación alternativa, lo que incrementa los costos de infraestructura.
- Es posible que deba examinar la totalidad de una cinta para recuperar solo algunos archivos.
- Muchas copias de seguridad basadas en cintas usan formatos propietarios, lo que requiere un software especial de proveedor para acceder a ellas; esto, a su vez, aumenta aún más los costos.

En el mundo actual de actividad ininterrumpida, una copia de seguridad a la que no pueda acceder con facilidad y rapidez puede representar un buen método para preservar información importante de la empresa, pero no será de utilidad a la hora de recuperarse ante un desastre. Los RTO actuales se miden en horas o incluso en solo minutos.

OBJETIVO DE PUNTO DE RECUPERACIÓN (RPO) Y OBJETIVO DE TIEMPO DE RECUPERACIÓN (RTO)

El objetivo de punto de recuperación (RPO) hace referencia a los datos a los que desea volver a tener acceso rápidamente.
Por su parte, el objetivo de tiempo de recuperación (RTO), hace referencia a la rapidez con la que desea volver a tener acceso a esos datos.
El tiempo de inactividad aceptable para datos y aplicaciones críticos depende de muchos factores (principalmente, de los costos) y varía según la empresa. En general, actualmente este tiempo de inactividad aceptable se reduce a minutos u horas, y no a días o semanas, como sucedía hace algunos años.

ALOJAMIENTO VS. TERCERIZACIÓN DE APLICACIONES

Otro elemento crítico a la hora de administrar el riesgo de desastres de TI consiste en evaluar si es necesario tercerizar sus aplicaciones y servicios de TI, y migrarlos a la nube.

ACERCA DE ARCSERVE

Arcserve ofrece soluciones extraordinarias que permiten proteger los valiosos activos digitales de las organizaciones que necesitan una protección de datos integral y a escala completa. Fundada en 1983, Arcserve es el proveedor más experimentado del mundo en soluciones de continuidad del negocio que permiten proteger infraestructuras de TI de varias generaciones, con aplicaciones y sistemas en cualquier ubicación, on-premise y en la nube. Organizaciones en más de 150 países confían en la experiencia y las tecnologías altamente eficientes e integradas de Arcserve para eliminar el riesgo de pérdida de datos y los largos períodos de inactividad, con hasta un 50% de ahorro en costos y complejidad en copias de seguridad y restauración de datos. Arcserve, con sede en Minneapolis (Minnesota), tiene presencia en todo el mundo.

Más información en **arcserve.com/la**

DISPONIBILIDAD DE LA DOCUMENTACIÓN PARA DR

Existe gran cantidad de información relacionada con la planificación de recuperación de desastres. Por ejemplo, los datos de contacto de sus proveedores, empleados, empresas de servicios públicos y demás organizaciones con las que podría necesitar comunicarse. También están los datos de los equipos de TI, como números de serie e información sobre garantías, ID de circuitos, planos, etc.

Asegúrese de contar con copias de esta información a las que pueda acceder incluso si no funcionan sus sistemas informáticos (y todo tipo de redes). Considere la opción de almacenar una copia en línea, además de una copia de seguridad en su smartphone, tablet o notebook, y en una unidad extraíble.