

# ¿Por qué los centros de datos son importantes en su estrategia de backups?

¿Por qué los centros de datos son importantes en su estrategia de backups? ¿Razones? ¿Motivos?. Este tema lo amarán, estoy seguro. Sin más preámbulos entremos en materia. A medida que los datos se han vuelto más importantes para las empresas actuales, el desarrollo de estrategias para respaldarlos de manera efectiva se ha convertido en una gran preocupación para las organizaciones de todos los tamaños. Si bien las empresas solían almacenar simplemente todos sus datos críticos en el sitio, recurren cada vez más a los centros de datos para proporcionar servicios de respaldo.

Cuando se usan de manera efectiva, los centros de datos convencionales y definidos por software pueden proporcionar una tranquilidad incomparable para las organizaciones que simplemente no pueden permitirse el lujo de que algo suceda con sus datos.

## Falla del disco duro

La mayoría de las organizaciones entienden la importancia de hacer una copia de seguridad de los datos, ya sea a través de un centro de datos definido por software u otras opciones DCaaS, pero un número sorprendente también se aferra a enfoques obsoletos. Simplemente hacer una copia de seguridad de los datos en discos duros externos no solo es inconveniente de administrar, sino que también puede resultar en un desastre. Ya sea que los datos se almacenen en dispositivos mecánicos HDD o dispositivos SSD más nuevos, el riesgo de perderlos debido a fallas mecánicas o accidentes es significativo. Cerca de 140,000 discos duros fallan en los

Estados Unidos cada semana, con casi el 30 por ciento de ellos fallando debido a un error humano.

Simplemente hacer una copia de seguridad de los datos en un disco duro local no es suficiente protección incluso para una pequeña empresa. Si bien los discos duros pueden parecer una solución económica, simple y segura, a menudo es imposible recuperar datos de un dispositivo fallido. Además, los discos duros generalmente no se respaldan en tiempo real, lo que resulta en datos incompletos cuando se usan para la recuperación después de una situación de pérdida de datos. Los centros de datos pueden realizar copias de seguridad de los datos instantáneamente en un entorno de nube como parte de sus ofertas de centro de datos como servicio (DCaaS), y también proporcionan múltiples redundancias de energía y computación para garantizar que los datos estén siempre disponibles incluso en caso de falla del hardware.

## Desastres naturales

Cuando ocurren desastres naturales, las personas  generalmente piensan en la amenaza de daño físico. Las inundaciones y el viento pueden destruir oficinas o causar estragos en la logística de la flota de almacenes. Sin embargo, para muchas organizaciones, los desastres naturales representan una amenaza mucho más grave a largo plazo: la pérdida de datos. Según los datos de FEMA, 40-60 por ciento de las empresas nunca vuelven a abrir después de sufrir daños por un desastre natural. Si bien parte de esto se debe al costo absoluto de reconstruir la infraestructura comercial crítica, la pérdida de datos es otro factor importante en estas fallas.

Sin las copias de seguridad del centro de datos, las empresas pueden perder datos críticos del negocio para siempre cuando un desastre natural destruye una parte de su infraestructura de TI. Reconstruir una oficina es una cosa, pero reconstruir una base de datos de clientes cuidadosamente segmentada que se

ensambló durante muchos años es casi imposible. Privadas de los datos que su negocio necesita para funcionar, estas compañías no tienen más remedio que cerrar sus puertas o comenzar de cero. Al hacer una copia de seguridad de la información con los centros de datos DCaaS creados para resistir los desastres naturales más intensos, las empresas pueden estar tranquilas sabiendo que sus datos aún estarán disponibles después.

## Seguridad física

Desde el punto de vista de la seguridad, la oficina típica no es muy intimidante. Incluso si un edificio tiene un sistema de seguridad o un guardia, a menudo no hay nada que impida que alguien entre a una oficina y robe un disco duro o descargue datos vitales en una tarjeta de memoria. Más importante aún, ¿qué es lo que impide que un empleado interno haga lo mismo?

Incluso las oficinas más seguras no se acercan a las medidas de seguridad física de un centro de datos convencional o definido por software. Con múltiples capas de seguridad, autenticación de dos factores que incorpora datos biométricos y listas de acceso restrictivas, los centros de datos DCaaS ofrecen los niveles más altos de seguridad física que una organización podría pedir. Esto garantiza que incluso en el improbable caso de que los datos críticos salgan por la puerta principal de la oficina, siempre habrá una copia de seguridad de forma segura detrás de las paredes de un centro de datos seguro.

## Protección contra ransomware

Los ciberataques se han vuelto cada vez más sofisticados en los últimos años. Una de las estrategias más exitosas que se utilizan hoy en día es el ransomware, que utiliza malware incrustado en un sistema para encriptar datos para que los propietarios de los datos y otros usuarios autorizados no

puedan acceder a ellos. Una vez que los datos están encriptados, los hackers contactan a las víctimas y ofrecen desbloquearlos a cambio de un pago monetario. Sin embargo, no debería sorprendernos que incluso en los casos en que se paga el rescate, los datos generalmente permanecen cifrados.

Mantener una copia de seguridad por separado en un entorno de centro de datos seguro garantiza que las empresas aún podrán acceder a ella y mantener su negocio en funcionamiento, incluso si sus sistemas principales son víctimas de ransomware. Con estos ataques cada vez más ambiciosos en los últimos años, las organizaciones de todos los tamaños deben pensar en estrategias de respaldo para mitigar su impacto.

## Disponibilidad de datos

Los clientes de hoy quieren acceder a productos y servicios de inmediato. Esto ejerce una enorme presión sobre las organizaciones para construir infraestructuras de red que brinden altos niveles de tiempo de actividad para satisfacer las demandas de los clientes. Cuando los sistemas se caen y los servicios dejan de estar disponibles, los clientes pierden la fe en una empresa y recurren a otras alternativas. Restaurar la confianza del cliente en una marca puede llevar años, si es posible.

Hacer una copia de seguridad de los datos en una instalación DCaaS segura que ofrece un alto tiempo de actividad puede ayudar a las empresas a protegerse contra las posibles fallas de su propia infraestructura de TI. También asegura que los datos seguirán estando disponibles en caso de incumplimiento o falla que cause una pérdida significativa de datos. Esta redundancia permitirá a las empresas recuperarse rápidamente de los contratiempos para que puedan volver a satisfacer las necesidades de los clientes con una interrupción mínima del servicio.

Los centros de datos tienen un papel fundamental que

desempeñar en la estrategia de respaldo de cada organización, ya sea una empresa de nivel empresarial o una pequeña startup con solo un puñado de clientes. Pensar en el futuro para formar planes de contingencia para lidiar con la pérdida de datos puede brindar tranquilidad tanto a las empresas como a los clientes a medida que los datos se vuelven más importantes para entregar los productos y servicios de hoy y del futuro.

Ver así mismo: [Data center, edge cloud, nube híbrida y atada](#) ; [Cómo los centros de datos híbridos pueden ayudar a optimizar DCIM](#) ; [Cómo hacer un backup de un cloud server](#)