

Pasos de preparación para una recuperación ante desastres

Pasos de preparación para una recuperación ante desastres, es el tema de nuestro blog de tecnología y cuentos de datos. Un tema, como siempre, muy interesante y que hemos tocado tangencialmente en otros post de este sitio: [Qué es DRP](#); [Configure su plan de recuperación de desastre](#); [Prueba de recuperación ante desastres...etc etc.](#)

Introducción

Desarrollar un plan de recuperación ante desastres y construir una infraestructura es una tarea para los administradores de TI. Los servicios en la nube ofrecen costos más bajos y mayor flexibilidad, pero no están exentos de riesgos.

La recuperación ante desastres como servicio significa más implementación y pruebas de resiliencia, pero también significa más incertidumbre.

Este proceso, seguramente causará muchos problemas espinosos: suele ser costoso, es difícil y la mayoría de las veces, solo se puede probar fuera del horario comercial.

El servicio de recuperación ante desastres ([DRaaS](#)) es un método de recuperación ante desastres en la nube, que tiene un costo más bajo, es más fácil de implementar, tiene la capacidad de proporcionar planes de prueba regularmente y puede seguir el ritmo de los cambios en la empresa.

Va
le
la
pe
na
se
ña
la
r
qu
e
la
s
op
ci
on
es
de
re
cu
pe
ra
ci
ón
an
te
de
sa
st
re
s
en
la
nu
be
pu
ed

DRaaS

Servicio de Recuperación ante Desastres

Tiene un costo
más bajo

Es más fácil de
implementar

Puede seguir el ritmo de los
cambios de la empresa



en
no
es
ta
r
di
sp
on
ib
le
s
de
sp
ué
s
de
un
de
sa
st
re
de
va
st
ad
or
.
Es
to
si
gn
if
ic
a
re
cu
rs

os
y
da
to
s
de
TI
va
ra
do
s,
pa
ra
li
za
nd
o
el
ne
go
ci
o.

Cómo crear un plan de recuperación ante desastres

El personal del centro de datos y las partes interesadas del negocio dedican mucho tiempo y esfuerzo a desarrollar y probar scripts de recuperación ante desastres.

1. Primero, anticipe posibles desastres en el centro de datos: el clima severo, los cortes de energía, los sistemas del proveedor se desconectan, el sabotaje interno o los ataques externos son posibles.
2. Asegúrese de que las aplicaciones de recuperación ante desastres de su empresa estén en línea inmediatamente.

Listas de verificación de auditoría y procedimientos clave que priorizan las operaciones diarias.

3. A continuación, obtenga e instale una infraestructura de centro de datos redundante: servidores, software, conexiones de red, operadores que admitan aplicaciones y más.
4. Los planes de recuperación ante desastres no pueden evitar las consideraciones de costos; un centro de datos fuera de línea es costoso.

Por lo general, los planes de recuperación ante desastres requieren la replicación de los componentes de infraestructura de cada aplicación. Además, esto requiere una conexión de red al sitio de copia de seguridad principal, para proporcionar al sistema la información de software actual.

Los trabajadores apropiados deben saber cómo invocar el proceso de copia de seguridad. Ellos decidirán qué sistemas usar y qué empleados deben reemplazar las copias de seguridad del sistema.

Las responsabilidades de recuperación ante desastres incluyen notificar a sus proveedores de redes y sistemas sobre los datos modificados y asegurarse de que los empleados sepan cómo restaurar los sistemas. Idealmente, los usuarios comerciales solo se ven ligeramente afectados.

El equipo de TI debe proporcionar los últimos procedimientos de respaldo de datos al personal durante la recuperación de datos ante desastres.

Con demasiada frecuencia, los departamentos de TI dedican mucho tiempo a diseñar y analizar entornos informáticos físicos de recuperación ante desastres, en lugar de dedicar tiempo a agregar valor a la codificación y las pruebas.

Para probar un plan de este estilo, el equipo del centro de datos debe probar, recibir, enmarcar, apilar e instalar el

hardware junto con el sistema operativo correspondiente y todos los parches más recientes. Crean cuentas de usuario exclusivamente para este propósito; implementar entornos de servidores de aplicaciones o marcos e instalar herramientas de prueba. Los programadores pueden dedicar la mitad de su tiempo a problemas comunes de infraestructura para estos instantes críticos, en lugar de probar programas.

Debido a la complejidad del proceso de recuperación ante desastres, las empresas suelen probar este, ante desastres accidentales una o dos veces al año. Cuanto más grande es la empresa, más complejo es el proceso de justificar un DRP.

Una vez que se planifican los procedimientos de recuperación ante desastres, rápidamente quedan obsoletos. Las aplicaciones cambian constantemente, por lo que los equipos deben revisar y actualizar los procedimientos de recuperación, con frecuencia. Las grandes corporaciones gastan incontables horas de empleados y más de 7 cifras en cada detalle de la planificación. Este presunto gasto se hace para asegurarse de que el plan siga siendo viable.

Muchas empresas solo hablan de boca para afuera sobre la recuperación ante desastres. Dedicar mucho tiempo a mitigar ese riesgo de recuperación ante desastres del 1 %, o incluso menor, no parece una buena inversión en inversiones de TI. Los administradores de TI tienen una lista larga y creciente de prioridades diarias, y cuando ocurre un desastre, la recuperación es lo único que importa.

Opciones de servicio de recuperación de desastres

Los servicios en la nube siguen ahorrando dinero en infraestructura compartida. Los avances en la virtualización y automatización de la nube permiten una mayor flexibilidad. Las empresas usan los recursos de la nube según sea necesario,

aunque solo para aplicaciones críticas. Los casos temporales en los que se realizan pruebas de recuperación ante desastres tienden a aumentar.

Con la recuperación ante desastres basada en la nube, los programadores no trabajan en bits y bytes, sino en interfaces de hardware y sistema operativo. Como resultado, se automatizan más tareas de [TI](#), aumenta la productividad y se reduce el tiempo de prueba de recuperación ante desastres. Se puede priorizar al personal del centro de datos con mayor frecuencia, asignando más recursos para probar toda la función del servicio de recuperación ante desastres.

Cuando la nube se convierte en tormenta

Como siempre, lo que se expresa aquí, siempre, corresponde al particular punto de vista de los redactores, no necesariamente de la empresa HostDime.

Los servicios de recuperación ante desastres tienen sus limitaciones, como pudiera ser, la incapacidad física de respaldar por completo la redundancia del sistema..

Los proveedores de este tipo de servicios no pueden justificar el costo de construir un centro de datos para imitar la configuración de la infraestructura de cada cliente, por lo que toman atajos. Los proveedores de servicios de recuperación ante desastres construirán sistemas para manejar una cantidad limitada de fallas.

En teoría, las empresas restaurarán sus sistemas ante catástrofes, como un corte de energía en un centro de datos. Sin embargo, en el caso de un gran desastre natural o provocado por el hombre, es posible que los sistemas colapsen. Téngalo en cuenta.

La recuperación ante desastres en la nube también aumenta la

demanda de ancho de banda de red empresarial. Coloque copias de aplicaciones e imágenes de máquinas virtuales (VM) en el servicio de recuperación de desastres basado en la nube del proveedor. Esas imágenes de aplicaciones y máquinas virtuales se actualizan constantemente, las transferencias de datos desde el sitio de producción de la empresa y el centro de datos del proveedor de servicios de recuperación ante desastres. Esta tensión de carga está disponible en ancho de banda.

Los servicios de recuperación ante desastres pueden manejar bien las aplicaciones simples, pero los sistemas de procesos intensivos que pueden degradar el rendimiento de la red, como la gestión de relaciones con los clientes, las aplicaciones de planificación de recursos empresariales.

A woman with long brown hair is seen from behind, sitting at a desk in a data center. She is looking at a laptop. In the background, there are several computer monitors displaying data. A futuristic digital overlay is superimposed on the scene, featuring a shield with a keyhole, a central glowing orb, and server racks. The HostDime Group logo is visible in the top right corner of the image.

HostDime Group
Premier Global Data Centers

Nuestros expertos en constante actualización, siempre tienen la mejor **solución** ante su necesidad específica.

HostDime

Nuestra empresa, Tiene el mejor [Plan de recuperación ante Desastres HostDime](#). Nuestros expertos, en constante actualización siempre tienen la mejor solución ante su

necesidad específica.

Usamos tecnología Veeam, Carbonite e inclusive Zerto. Anda, [Contacta](#) a uno de nuestros asesores expertos y plantéate tu caso.

HostDime, donde el futuro acontece.