# Desastres del centro de datos: cómo prepararse para lo peor

Desastres del centro de datos: cómo prepararse para lo peor. hay un adagio popular que dice que hombre prevenido valo por dos.Los centros de datos albergan de forma segura equipos informáticos esenciales e información importante. Sus racks de servidores pueden contener equipos y valor por valor de muchos millones de dólares en los datos que contienen.

Las empresas hacen todo lo posible para hacer una copia de seguridad de los datos de manera segura y prevenir / reparar cualquier falla de hardware para minimizar el tiempo de inactividad. Aún así, una de las amenazas más olvidadas para los clientes y las empresas no está preparada para los desastres del centro de datos.

Cuando una empresa está construyendo un nuevo centro de datos, la prevención y recuperación de desastres es un tema importante de preocupación. Los grandes centros de datos a menudo se encuentran en lugares donde existe un bajo riesgo de eventos naturales devastadores. Aun así, los gerentes de los centros de datos necesitan saber cómo prepararse para lo peor y qué hacer después de un desastre.

## Tipos de desastres

El primer paso en cualquier plan para evitar y recuperar desastres es identificar los posibles tipos de desastres que pueden ocurrir. Los siguientes son todos ejemplos de desastres importantes para los que una instalación debe prepararse.


## Incendio

Un incendio es uno de los tipos de desastres más comunes que puede enfrentar un centro de datos. Las instalaciones tienen que prepararse para el riesgo de que se les acerque un incendio forestal protegiendo sus propiedades y, por supuesto, prepararse para un incendio que comienza desde el interior.

## Inundaciones

Las inundaciones pueden ser causadas por lluvia excesiva, nieve derretida, condenas rotas u otros eventos naturales. Otro tipo de inundación a tener en cuenta proviene de tuberías rotas dentro del centro de datos.

### Terremoto

Los terremotos pueden ser absolutamente devastadores y a menudo golpeados con muy poca advertencia. Incluso pequeños terremotos pueden causar daños graves a equipos sin protección.

### Tornado

El poderoso viento de un tornado puede dejar sin electricidad, cortar circuitos de datos, empujar árboles hacia un edificio y mucho más.

### Huracán

Todo el mundo sabe que los dispositivos informáticos no funcionan bien con el agua, pero además de eso, los huracanes pueden causar daños por el viento, incendios, cortes de energía y mucho más.

### Ataque terrorista

Los centros de datos son responsables de apoyar a una gran parte de la economía, lo que los convierte en un objetivo potencial para los ataques cibernéticos .

Los gerentes de los centros de datos deberán evaluar la probabilidad de cada uno de estos desastres. Comprender que los terremotos, por ejemplo, son mucho más probables en áreas construidas sobre y alrededor de fallas puede ayudar a comprender dónde invertir los recursos de recuperación ante desastres.

## Tipos de impactos que un desastre puede tener en los centros de datos

Cuando ocurre un desastre, puede tener un impacto inmediato y duradero en un centro de datos. Prepararse para el riesgo de

un desastre es importante, pero los riesgos que siguen al evento merecen el mismo enfoque.

Por ejemplo, si hay un incendio, el impacto obvio es que el equipo podría quemarse y quedar inutilizable. En un incendio extremo que está fuera de control, toda la instalación podría ser destruida. Sin embargo, un buen centro de datos responderá rápidamente incluso a un pequeño incendio para minimizar el daño adicional. Si el centro de datos no tiene un sistema de extinción de incendios seguro para la electrónica, el daño del agua podría ser extenso.

Cada tipo de desastre tendrá impactos 'primarios' (como el incendio mismo) y luego impactos 'secundarios' que deben planificarse. Cuando se hace correctamente, un centro de datos puede minimizar el daño, el tiempo de inactividad y el impacto que un desastre tiene en la instalación.

## Cómo prepararse para un desastre

La preparación para un desastre comienza desde el comienzo de cualquier diseño de centro de datos. Ya sea que esté construyendo una nueva instalación desde cero o simplemente convirtiendo un espacio actual, esto tomará un poco de reflexión. Las siguientes son soluciones clave de planificación de desastres que pueden ayudar a reducir drásticamente el riesgo para cualquier centro de datos:

1. Supresión de incendios adecuada : se requieren sistemas de extinción de incendios en casi todos los edificios. Es importante elegir un sistema que no dañe el equipo informático dentro del centro de datos. En la actualidad, existen muchas soluciones en el mercado para proteger los servidores de incendios, como un fluido de protección contra incendios de fluorocetona .
2. Seguridad física avanzada : la seguridad física ayudará a minimizar el riesgo de ataques terroristas, ayudará a evitar que un empleado descontento cause daños y

mejorará la seguridad general.

3. Estantes de rack de servidor sísmico : en áreas donde son posibles terremotos, los estantes de rack de servidor especialmente diseñados ayudan a mantener los servidores, enrutadores, conmutadores y otros equipos en su lugar. También ayudarán a reducir la vibración que llega a este equipo, lo que puede minimizar el riesgo de daños.
4. Sistema de gestión de inundaciones : los centros de datos a menudo tienen pisos elevados que ayudarán a evitar que el agua llegue al equipo. Este sistema también incluirá bombas que pueden eliminar rápidamente el agua y drenarla fuera de las instalaciones.
5. Múltiples circuitos de datos : múltiples circuitos de datos en una instalación proporcionarán redundancia en caso de que uno de ellos se corte o se dañe debido a un desastre.
6. Fuente de energía redundante : tener un sistema de suministro de energía ininterrumpido mantendrá un centro de datos en funcionamiento incluso cuando no haya energía comercial durante un período prolongado de tiempo.
7. Ubicación de recuperación ante desastres : en situaciones donde el tiempo de inactividad es absolutamente inaceptable, una empresa puede operar múltiples centros de datos en ubicaciones geográficamente distantes.

## Reaccionar ante un desastre en un centro de datos

Cuando ocurre un desastre, todos los centros de datos deben tener un plan de recuperación ante desastres bien ensayado que sea fácil de seguir. Este plan guiará a los empleados sobre qué hacer durante el desastre, así como los días y horas posteriores. Un buen plan de recuperación tiene instrucciones

para evaluar los sistemas dañados, cómo restaurar todos los sistemas esenciales y mucho más.

Los empleados también deben saber qué sistemas restaurar primero y cuáles pueden esperar. En la mayoría de los casos, la restauración de la conectividad a Internet será una prioridad porque es esencial para todas las demás funciones del sistema.

Las empresas que priorizan el tiempo de actividad y la confiabilidad tendrán un plan detallado de recuperación ante desastres que actualizarán periódicamente. También realizarán simulacros de desastres para garantizar que todos sepan cómo responder a situaciones que esperan que nunca ocurran.

Otros recursos útiles:Pruebas de recuperación ante desastres: garantizar que su plan de recuperación ante desastres funcione ; ¿Qué es es DRP (Disaster Recovery Plan o Plan de recuperación de Desastres)?; ¿Qué debe incorporar su plan de recuperación de desastres? Cloud y Colocation