Acronis

#CyberFit

El atajo secreto a la recuperación ante desastres

Índice

Introducción

Es posible que piense que es suficiente con la copia de seguridad. Es posible que no comprenda el valor de sus datos, sistemas y aplicaciones hasta el día en que son objeto de un ataque. La recuperación ante desastres es ese paso más que garantiza la pronta reanudación de la actividad empresarial después de una interrupción. Ya sabemos que nunca le va a pasar a usted, sino que es solo algo que merece la pena tener.

¿Qué es la recuperación ante desastres?

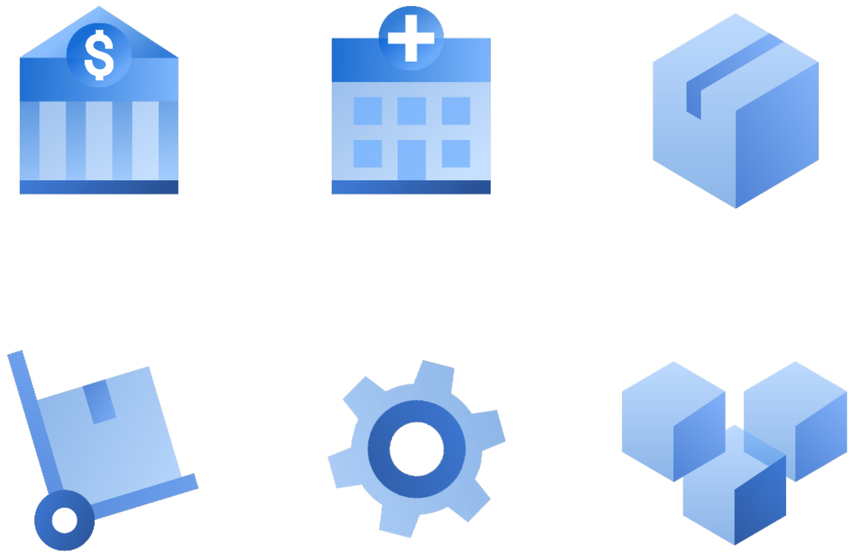
La recuperación ante desastres (DR) no puede funcionar sin copia de seguridad. Incluye las copias más recientes de los datos y las funciones de proceso en una plataforma que ofrece disponibilidad automatizada de sus datos, aplicaciones y sistemas más críticos.

Garantiza que los procesos de interdependencia se recuperan en el orden correcto, se restauran al punto de recuperación preciso y en el momento adecuado.

¿Está en riesgo su empresa?

¿Quién necesita DRaaS? Todo el mundo. Cualquier empresa puede ser víctima de algún tipo de desastre. Es posible que su empresa esté ubicada en zonas propensas a sufrir desastres o que carezca de recursos técnicos o de la experiencia necesaria para implementar un programa de recuperación ante desastres.

Sectores como los que se incluyen a continuación dependen de aplicaciones y datos críticos o se enfrentan a fuertes sanciones en caso de infracciones de normativas y de cumplimiento:



- Servicios financieros
- Atención sanitaria
- Sector legal
- Transporte
- Telecomunicaciones
- Fabricación
- Construcción
- Energía
- Comercio electrónico
- Servicios públicos
- Cadena de suministro y logística

No se trata solamente de TI

Recuperar la actividad rápidamente no es solo un problema del departamento informático (TI). Cuando las interrupciones afectan a los departamentos de Recursos Humanos, financiero, legal y otros, es problema de todos.

TI

- Copia de seguridad y recuperación
- Acuerdos de nivel de servicio (SLA), internos y externos
- Satisfacción de los empleados
- Auditorías
- Cumplimiento y normativas

Alta dirección

- Plan de continuidad de la actividad empresarial
- Percepción del mercado
- Productividad de los empleados
- Cumplimiento y normativas
- Seguros

Finanzas

- Cumplimiento y normativas
- Protección de datos sensibles
- Mantenimiento de las operaciones empresariales
- Confianza económica y del mercado
- Auditorías

Recursos Humanos

- Contratación y planificación de la plantilla
- Formación
- Productividad de los empleados
- Protección de datos sensibles

Legal

- Cumplimiento y normativas
- Protección de datos sensibles
- Seguros

La realidad

Los desastres pueden ocurrir en cualquier momento, y de muchas maneras.

Estamos aquí para impedir que pase a engrosar las estadísticas.

De las fugas de datos de 2019 fueron provocadas por la eliminación o sobrescritura no intencionada de archivos o carpetas[1]

de las fugas de datos de 2019 fueron provocadas por ataques delictivos o maliciosos[1]

de las organizaciones es probable que sufran interrupciones de la actividad para 2022 debido a la pérdida irrecuperable de datos[2]

de las empresas han sufrido ciberataques en los tres últimos años[3]

2,2 días

de tiempo medio de inactividad[2]

5600 $

de coste medio por minuto[2]

3,92 M$

de coste medio de una fuga de datos[2]

1) Ponemon Institute, 2019. 2) Gartner, 2019. 3) IDC, 2019.

Las amenazas

¿Qué amenazas debería tener en cuenta? Tal vez piense que solo los desastres naturales provocan inactividad con cortes de suministro eléctrico que afectan al hardware. Pero también hay que tener en cuenta el software y las personas. A medida que evoluciona la tecnología, también lo hacen las amenazas internas y externas.

Desastres naturales

Huracanes, tornados e incendios pueden provocar interrupciones serias debido a que afectan a instalaciones e infraestructuras.

Lo que la mayoría de las empresas es posible que no sepan es que solo el 6 % de las interrupciones son provocadas por desastres naturales.

Pandemias

Este tipo de amenazas afecta a los empleados de las empresas y, en el caso del teletrabajo, crea toda una variedad de escenarios de planificación que los departamentos de TI pueden no haber previsto.

Existe un riesgo mayor cuando los datos y los dispositivos residen fuera de la infraestructura habitual de TI.

Fallos de hardware y daños de software

Un fallo de hardware puede producirse por una corte del suministro eléctrico.
El software puede dañarse, entre otras razones, por fallos en la actualización y el formateo incorrecto de unidades, etc.

Error humano con o sin mala intención

Ocurre. Todos hemos borrado o sobrescrito accidentalmente algo.

Un empleado descontento también podría hacer estragos en datos y sistemas.

Ciberataques

Basta con comprometer la máquina de un empleado para que redes enteras queden a merced de ataques.

Los ataques pueden producirse rápidamente por el uso de contraseñas débiles, caer víctima de timos de phishing y hacer clic en enlaces maliciosos.

Evolución de la recuperación ante desastres

Década de 1990

Centros de datos de empresa o coubicación

- Hardware depreciado
- Redes
- Licencias
- Plataformas de replicación
- Cantidades masivas de almacenamiento

Década de 2000

Enfoque híbrido

- Licencias costosas
- Complicado
- Cobertura limitada

Década de 2010

Moderna recuperación ante desastres basada en la nube híbrida

- Rentable
- Facilidad de uso
- Lista para utilizar

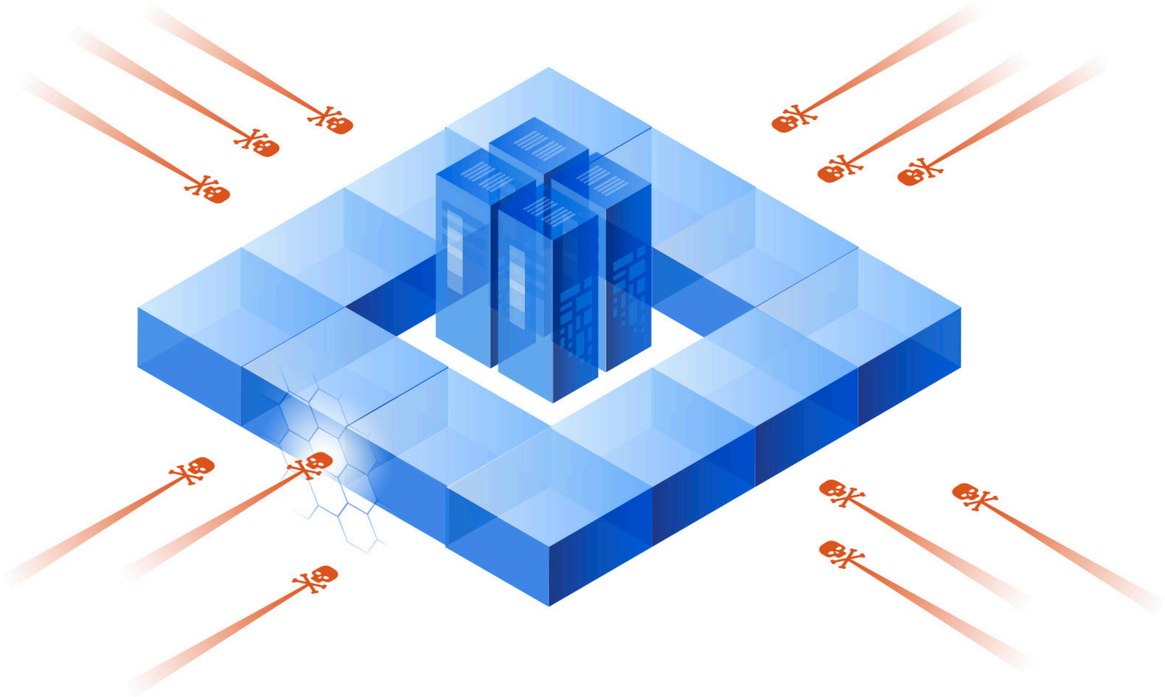
10 razones para invertir en recuperación ante desastres

Hay muchas razones para ir más allá de la copia de seguridad con recuperación ante desastres.

- Mucho más **rentable** que nunca
- **Minimice el impacto** de cualquier desastre
- Garantice una productividad de los empleados **permanente**
- Satisfaga sus requisitos **normativos y de** cumplimiento
- Acceda **a recuperación instantánea**
- **Reduzca la interrupción** de las operaciones
- **Reduzca las** pérdidas financieras **potenciales**
- **Reduzca las obligaciones** de responsabilidad
- **Minimice el riesgo** de exposición negativa
- **Facilite** la gestión de crisis

Dada la variedad de factores internos y externos que pueden afectar a sus sistemas y datos...

No se trata de si va a sufrir una pérdida de datos, sino de cuándo.



Cálculo del tiempo de inactividad

Estos factores pueden aplicarse a su empresa, utilizando costes y cifras de todos sus departamentos para calcular su coste por hora real de inactividad. ¿Conclusión? El tiempo de inactividad implica riesgo de perder mucho dinero.

Pérdida de ingresos + Pérdida de productividad + Coste de recuperación + Costes intangibles =
Coste de tiempo de inactividad (por hora)

Pérdida de ingresos

Esto resulta bastante fácil de comprender. Si su negocio está inactivo, no puede generar ingresos.

Utilice los ingresos anuales brutos para calcular el importe de ingresos por hora que se pierde durante el tiempo de inactividad para cada área de negocio.

Pérdida de productividad

El coste del tiempo de inactividad también aumenta cuando los empleados son incapaces de trabajar o se ven forzados a realizar actividades que no generan ingresos. Los salarios o sueldos por hora son un coste fijo y deben pagarse con independencia de su nivel de productividad.

Coste de recuperación

Generalmente, no piensa en los costes asociados a la recuperación y la reanudación de las operaciones empresariales.

Los costes típicos son los siguientes:

- Los servicios y el tiempo de empleados necesarios para recuperar la pérdida de datos
- Los dispositivos/herramientas físicas que puede necesitar reparar o sustituir
- El coste de la pérdida de datos

Costes intangibles

Cualquier daño a la reputación o a la marca supone la pérdida de dinero. El más mínimo tiempo de inactividad puede ensombrecer de manera insalvable su actividad empresarial, y cómo se gestiona ese tiempo puede marcar la diferencia entre recuperarse o desaparecer.

Opciones para crear un programa de recuperación antes desastres

Si gestiona su propio programa de recuperación ante desastres, necesitará:

- **Personal para:**
  - Evaluaciones
  - Diseño
  - Pruebas
  - Implementación
  - Administración
- **Formación**
- **Documentación**
- **Generación de informes**
- **Infraestructura de recuperación**

Si elige un partner certificado de Acronis obtendrá:

- **Nuestros años de experiencia en recuperación ante desastres**
- **Servicios de recuperación ante desastres activos de forma rápida y sencilla**
- **Modelo de prestación de servicio permanente y eficaz**
- **Soporte 24/7**
- **Funciones de prueba simplificadas**
- **Supervisión y administración**
- **Recursos informáticos y almacenamiento en la nube integrados**
- **Gastos operativos asequibles**

Mantener el negocio abierto nunca ha sido tan fácil

Imagine un único agente. Una única consola. Una única nube.

Protección de datos

\+

Ciberseguridad

\+

Recuperación ante desastres

Copia de seguridad y restauración

Prioridad principal:

- Impedir la pérdida de datos valiosos
- Datos ubicados en servidores, estaciones de trabajo y dispositivos móviles

Administración y protección de endpoints

Prioridad principal:

- Detección y neutralización de ataques de malware
- Evaluación de vulnerabilidades y administración de configuraciones
- Filtrado de URL
- Administración de parches

Recuperación ante desastres

Prioridad principal:

- Alta disponibilidad de las aplicaciones críticas
- Recuperación rápida para evitar costosos tiempos de inactividad

Acronis

#CyberFit

¡Gracias!

Póngase en contacto con nosotros hoy mismo para ver cómo podemos ayudarle a acelerar su capacidad para recuperarse de un desastre.

www.acronis.com | dr@acronis.com