Retrospect

# Planificando la recuperación ante desastres

*Un documento de buenas prácticas de los socios de Retrospect*

## Aspectos de la preparación ante desastres

Aún teniendo en cuenta lo que es una recuperación ante desastres y lo que significa para un sistema informático (por ejemplo, poder ejecutar una recuperación completa, "baremetal", tras un fallo en el disco duro), es de un alcance bastante menor si se compara con la preparación ante desastres para toda una empresa, lo que supone asegurar que una empresa pueda volver a la actividad en un corto período de timepo tras un incendio, inundación, robo o cualquier otra circunstancia. Cuestiones que incluyen "¿Dónde se reunirán y trabajarán los empleados" y "Cómo proporcionaremos ordenadores sin tener que esperar a que una compañía aseguradora extienda un cheque" son preocupaciones útiles a la hora de desarrollar un plan para salir airoso de una situación catastrófica.

## Incorporando a sus servicios la planificación de la preparación ante desastres

La preparación ante desastres es de hecho un tema tan amplio y complejo que se han creado empresas enteras que trabajan proveyendo tales servicios. Aunque definir las tareas necesarias para emular a tales empresas no es el objetivo de este documento, hay una cosa clara: los proveedores de servicios informáticos están en la mejor posición para conseguir que sus clientes piensen sobre qué se debe hacer para asegurar la supervivencia de sus empresas y para proporcionarles servicios que aseguren las funciones informáticas en curso.

Al menos, aunque solo sea para protegerse usted y su empresa de una pérdida de datos inesperada al trabajar con los sistemas de sus clientes, debería tener una copia de seguridad y un plan de recuperación completos para cada uno de ellos. Haga de ese plan un requisito, en detalle:

- Planificación e implementación inicial
- Gestión diaria (ejecutando copias de seguridad y recuperaciones, comprobación de notificaciones por correo electrónico)
- Mantenimiento y pruebas periódicas (archivando, verificación de recuperaciones parciales y completas)
- Reevaluación según sea necesario (capacidad, rendimiento, tecnología y metodología del sistema, etc.)

Las tareas mostradas arriba proveen significativos ingresos por servicios con el paso del tiempo y en torno a un 70-90% de un proceso de copia de seguridad y recuperación puede duplicarse desde el entorno de un cliente al de otro, haciendo de este proceso repetible la mayoría de las veces. Decida qué funciona y luego prepare a sus clientes (¡y también usted!) para el éxito.

## Las mejores prácticas para un plan de recuperación ante desastres y copia de seguridad

### Crear y formalizar un plan

Le recomendamos que formalice un plan de recuperación y copia de seguridad para cada uno de sus clientes. Debería incluir cosas tales como su acuerdo respecto al nivel del servicio proporcionado, que incluya los tiempos de respuesta que usted puede atender, cuáles son sus responsabilidades y cuáles las de sus clientes, medidas para el éxito y qué servicios en curso se proporcionarán.

### Recuperación y almacenamiento externo de copias de seguridad

Las copias de seguridad locales son las mejores primeras líneas de defensa contra la pérdida de datos, pero es fundamental mantener al menos una copia de los datos de la organización almacenada con

seguridad de forma externa, preferiblemente en un lugar retirado a bastantes kilómetros de distancia. Aquí tiene algunas cosas que debe considerar respecto a las copias de seguridad externas:

- ¿Qué datos deben respaldarse externamente? ¿Puede excluirse cualquier dato (como archivos de caché)?
- ¿Deberían estar codificados los datos?
- ¿Dónde se almacenarán los datos externos?
- ¿Cómo llegarán allí? (Opciones: copias de seguridad en la nube, transporte físico de los datos de respaldo)
- ¿Quién será responsable de transportar los datos físicos al exterior?
- ¿Cuándo tendremos acceso a los datos físicos si los necesitamos?
- ¿En qué intervalo será actualizado el almacenamiento externo?
- ¿Durante cuánto tiempo se archivarán los datos más antiguos?

### Construir su caja de herramientas de recuperación del Sistema

Cada proveedor de servicios informáticos debería mantener un arsenal de herramientas útiles. Como mínimo, tener lo siguiente preparado en todo momento:

- Grabe un Disco de Recuperación de Emergencia de Retrospect para los sistemas Windows.
    - Mejor cuando se licencia con el complemento Dissimilar Hardware Restore de Restrospect
    - Tenga en cuenta los requisitos de hardware específicos (como RAID y redes HBA)
- Cree un Disco de Herramientas de arranque para sistemas OS X.
    - Incluya la aplicación, motor y cliente Retrospect
    - Añada las utilidades favoritas de Mac (Disk Warrior, Tech Tool Pro, etc.)
- Si alguna copia de seguridad externa está almacenada en soportes, asegúrese de que podrá conseguir rápidamente una unidad para leer esos soportes, por si la unidad de respaldo principal se volviera inutilizable por alguna razón.
- ¡Asegúrese de tener acceso a cualquier contraseña y clave necesaria! Si el Post-it™ en el que tenía escrito su contraseña para la copia de seguridad estaba bajo el teclado* y se quemó con el resto de la oficina, estará en problemas si no tiene la contraseña almacenada de forma segura en cualquier otro lugar.

## Probar, probar, probar

Incluso los planes de recuperación ante desastres pensados cautelosamente necesitan ser probados. Hay pocas cosas más dolorosas que descubrir que las cosas no van como esperaríamos cuando se está ejecutando una recuperación crítica. El diseño de Retrospect incluye un método único de verificación de datos que utiliza las mismas rutinas que cuando se ejecuta una recuperación. Eso es perfecto para asegurarse de que los datos de respaldo son leíbles y concuerdan exactamente con los datos originales, pero probar con éxito una recuperación adecuada es siempre la mejor manera de mantener la confianza en el sistema.

Ponga en marcha un plan para testar, al menos trimestralmente, las recuperaciones de cada uno de sus clientes. Cuando ejecute dicho test, hay varias pruebas que no deben pasarse por alto:

- Buscar y recuperar un archivo
- Recuperar una carpeta a un punto anterior en el tiempo
- Recuperar un volumen entero y asegurarse de que arranca, las aplicaciones funcionan con normalidad, etc.
- Comprobar las funciones fundamentales de las aplicaciones de la empresa (contabilidad, correo electrónico, etc.) tras una recuperación

- Recuperar desde copias de seguridad externas

Además de garantizar la fiabilidad del sistema de respaldo, testar las recuperaciones le coloca en una inmejorable posición respecto a sus clientes en el día a día y mantiene *su confianza en usted.* Es un procedimiento en el que todos ganan.

## Comience inmediatamente, perfecto conforme avanza el tiempo

Haga lo que haga y aunque aún no haya diseñado el plan perfecto, no haga que sus clientes esperen para realizar las copias de seguridad externas. Realice alguna copia de seguridad externa AHORA. Por su propia naturaleza, los desastres, tanto los naturales como los provocados por el hombre son difíciles de predecir o prevenir. Es mejor tener al menos una copia de la copia de seguridad de sus clientes almacenada de forma segura externamente y de inmediato. Luego podrá reflexionar e implementar a lo largo del tiempo un sistema que proporcione un nivel de servicio que cumpla con las necesidades de sus clientes.

* Retrospect, Inc. no aprueba el almacenaje de contraseñas de ninguna otra forma que no sea segura y de confianza.