Acronis

3 razones **por las que la copia de seguridad** es **estratégica**

Este documento técnico describe las tres razones por las que la copia de seguridad es un elemento estratégico del plan de IT y por qué es tan importante para su negocio que planifique y ejecute una estrategia que proteja el 100 por ciento de sus datos.

Tabla de contenido

Introducción

Usted es miembro de un pequeño equipo de IT que trabaja para una empresa de tamaño mediano y un incendio ha destruido sus instalaciones, incluido su centro de datos. Desgraciadamente, no ha dispuesto de tiempo ni de los recursos necesarios para desarrollar y ejecutar un plan de recuperación de desastres. De hecho, todavía no había desarrollado ni ejecutado una estrategia de copia de seguridad para proteger a la mayoría de sus sistemas.

La copia de seguridad es **estratégica** para su **negocio** ya que sus datos **lo son**

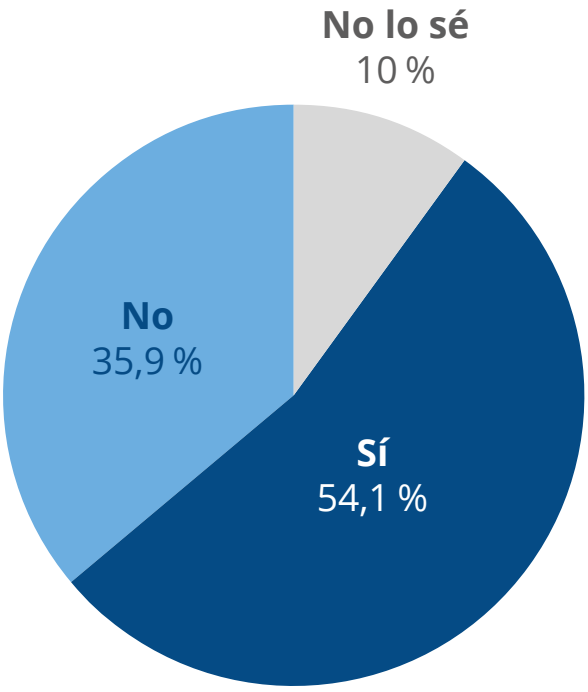
No está solo. Muchas organizaciones pequeñas y medianas carecen de operaciones de copia de seguridad y recuperación de desastres eficaces. Según la encuesta de recuperación de desastres de Acronis realizada por IDC en mayo de 2014, el 70 por ciento de los encuestados no estaban completamente seguros de esta afirmación: "Nuestras operaciones de copia de seguridad y recuperación de desastres están bien gestionadas y planificadas".

Sin embargo, ahora que su centro de datos ha sido destruido, se siente muy solo mientras medita cómo explicar a su equipo de gestión que una gran parte de los registros financieros, datos de facturación, pedidos en proceso, datos de clientes y contratos de la organización se han perdido... de forma permanente.

Teniendo en cuenta que la existencia de su organización depende de su estrategia de copia de seguridad, ¿por qué la copia de seguridad es una cuestión secundaria durante el proceso de planificación? Se planean, diseñan e implementan cuidadosamente los sistemas y la red, pero se demora la "discusión sobre la copia de seguridad" y su implementación:

- Gartner estima que solo el 35 por ciento de las pequeñas y medianas empresas (pymes) tienen un plan integral de recuperación de desastres en vigor.
- Solamente el 2 por ciento de las empresas encuestadas realizan copias de seguridad del 100 por ciento de sus datos. (Encuesta de recuperación de desastres de Acronis, IDC, mayo de 2014).
- El 36 por ciento de las empresas encuestadas admiten que no realizan copias de seguridad de los servidores virtuales con la misma frecuencia con que hace copias de seguridad de sus servidores físicos. (Encuesta de recuperación de desastres de Acronis, IDC, mayo de 2014).

¿Realiza su organización una copia de seguridad de servidores virtuales con la misma frecuencia con que hace copias de seguridad de servidores físicos?



Fuente: Encuesta de recuperación de desastres de Acronis, IDC, mayo de 2014

La copia de seguridad es estratégica para su negocio, ya que sus datos lo son. Sin copias de seguridad, su negocio va a fracasar. La copia de seguridad es su póliza de seguro y ninguna otra tecnología ni proceso manual puede reemplazarla. Perderla es semejante a que un comerciante o fabricante pierda un inventario que la empresa no había tenido tiempo de asegurar.

Este documento técnico presenta las tres razones por las que la copia de seguridad es un elemento estratégico del plan de IT y por qué es tan importante diseñar y ejecutar inmediatamente una estrategia de copia de seguridad que garantice la protección del 100 por ciento de sus datos.

N.º 1: La copia de seguridad es la única manera de proteger los datos empresariales

La vida está llena de incertidumbres y su empresa no está exenta de ellas. Un desastre natural como un terremoto o una inundación, o un incidente causado por el hombre como un virus o una vulneración de la seguridad, o incluso un error de software o hardware, puede causar pérdida de datos. Una pérdida de datos se produce con más frecuencia de lo que la gente cree o está dispuesta a admitir. De hecho, NO es una cuestión de SI su empresa sufrirá una pérdida de datos, sino CUÁNDO va a suceder esto, dada la variedad de factores internos y externos que pueden afectar a sus sistemas y datos.

La razón principal de que la copia de seguridad sea un elemento estratégico es que se trata de la única manera de proteger los datos esenciales. Piense en las implicaciones que tendría para su negocio si pierde los datos contenidos en POS, CRM, fabricación, I+D y sistemas financieros. Como mínimo, la pérdida de datos irremplazables causaría la pérdida de ventas e ingresos, sanciones contractuales, posibles litigios, incumplimiento de normativas y pérdida de valor de las acciones. En el peor de los casos, la pérdida de datos causaría la quiebra.

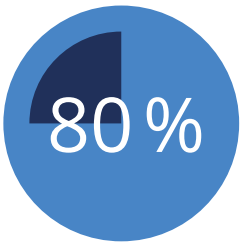
Según el Institute for Business and Home Safety, se estima que 25 por ciento de las empresas no vuelve a abrir después de un desastre de grandes proporciones. Incluso si no se produce ningún desastre, estas son algunas maneras adicionales de perder datos:

- Cada semana, 140 000 unidades de disco duro fallan en Estados Unidos. (Según los Archivos Nacionales y la Administración de registros de Washington)
- El 6 por ciento de todos los PC van a sufrir un episodio de pérdida de datos en cualquier momento. (The Cost of Lost Data, David. M. Smith)
- El 31 por ciento de los usuarios de PC han perdido todos sus archivos a causa de eventos que estaban fuera de su control.

Con el fin de determinar el mejor método de copia de seguridad para su organización, es necesario comprender las necesidades de valor y disponibilidad de sus diversos activos de datos e incorporar los resultados de ese análisis en su plan de IT.

No todos los datos son iguales en su entorno. Algunos datos cambian rápidamente y son muy importantes para su negocio. De estos datos, debe realizar copias de seguridad frecuentes para asegurarse de limitar la cantidad de datos que se pueden perder. Debido a que estos datos son más valiosos para su negocio, deberá gastar más dinero, dedicar más recursos y asegurarse de que puede proteger y recuperar el 100 por ciento de estos datos o poco menos. Debe estudiar la implementación de un plan de copia de seguridad complejo, tal vez realizar copias de seguridad cada pocas horas y preparar esas copias de seguridad para que pueda recuperar sus sistemas como una máquina virtual en su ubicación principal o en una ubicación remota.

Otros datos, aunque son importantes, no cambian con tanta frecuencia y su organización no necesita acceder a ellos inmediatamente. Para estos datos, estudie la implementación de un plan de copia de seguridad más simple; haga una copia una vez al día y guárdela en medios más económicos, como cintas o una opción de almacenamiento en la nube a largo plazo de bajo costo.



Casi el 80 % de las empresas estiman que el costo por tiempo de inactividad les cuesta **al menos 20 000 dólares** por hora o más

Fuente: Encuesta de recuperación de desastres de Acronis, IDC, mayo de 2014

Esta es una de las razones fundamentales por las que es necesario incorporar la copia de seguridad como un elemento estratégico de su plan de IT. Si lo hace, puede coordinar mejor la arquitectura y los sistemas de IT a fin de garantizar la optimización de los requisitos de copia de seguridad según el valor de los datos, la velocidad a la que cambian y el tiempo necesario para que el negocio recupere los datos.

N.º 2: Ningún plan de recuperación ante desastres funciona sin copia de seguridad

La recuperación ante desastres proporciona continuidad del negocio en caso de desastre u otro evento imprevisto y se compone de un sitio primario y secundario, mantenido de forma continua o desarrollado rápidamente como un sistema de reserva. Los datos, sistemas operativos, aplicaciones, archivos y carpetas se replican y se realiza una copia de seguridad de los mismos entre los sitios con el objetivo de restaurar sus sistemas a un estado operativo y reducir al mínimo la pérdida de datos y el tiempo de inactividad. La copia de seguridad es el elemento esencial de una estrategia efectiva de recuperación ante desastres.

Las organizaciones utilizan muchos enfoques para recuperarse de un error del sistema o un desastre y cada uno de ellos se basa en la copia de seguridad. Por ejemplo, cuando un servidor falla sin previo aviso, una solución de conmutación por error cambia la carga de trabajo de un servidor a través de un servidor de reserva, sistema o red sin intervención humana. Con la conmutación por error, es necesario replicar los datos en el segundo servidor y hacer también una copia de seguridad de los mismos.

La alta disponibilidad proporciona redundancia para que pueda minimizar o eliminar el tiempo de inactividad y asegurar que los sistemas críticos estén siempre disponibles: no instantáneamente, sino normalmente al cabo de unos minutos. La alta disponibilidad es un único sistema y contiene un solo conjunto de datos. Puede replicar los datos o no, aunque sí que debe realizar una copia de seguridad de ellos.

Cuando ocurra un desastre, puede recuperar un sistema mediante la reconstrucción de un nuevo sistema. Para lograr esto, es necesario reinstalar todo el software o copiar una imagen del sistema antiguo al nuevo sistema. En cualquier caso, se necesita como mínimo una copia de seguridad de los datos.

La migración es el proceso de mover sistemas operativos, aplicaciones, datos, archivos, carpetas, etc. a un sistema nuevo (y potencialmente diferente). Hay muchas razones por las que se desea migrar un sistema que incluye la necesidad de realizar tareas de mantenimiento o de actualización de sus servidores, optimizar los recursos del sistema, mover las máquinas físicas a un entorno virtual, replicar servidores, recuperarse de un desastre, o modificar su infraestructura de IT debido a una fusión o adquisición o al crecimiento espectacular de la empresa.

Hay varios tipos diferentes de migración, incluyendo la migración de datos, migración de aplicaciones y migración a la nube. Para migrar un sistema, es necesario tener una copia de seguridad de los datos y aplicaciones como mínimo.

La conmutación por error, alta disponibilidad, sistemas tolerantes a fallos, recuperación del sistema y migración son elementos potenciales de un plan de recuperación de desastres cuando ocurren eventos muy específicos y cada método se basa en un enfoque bien pensado para hacer copias de seguridad: un enfoque que es necesario para planear por adelantado, no después de los hechos.

Otro componente importante de su plan de recuperación de desastres es determinar el número de copias de seguridad que necesita y dónde residirán estas copias. Acronis intenta simplificar esta tarea y recomienda una metodología de copia de seguridad 3-2-1:

- Mantener todos los datos en tres (3) lugares: las opciones incluyen sistemas de producción, copia de seguridad de NAS y copia de seguridad en la nube.
- Mantener copias de seguridad en dos (2) tipos de soporte (disco y en la nube).
- Mantener una (1) copia de datos de copia de seguridad en una ubicación externa.

Tener una copia de seguridad de sus datos in situ es efectiva en el caso de que un sistema principal experimente un error de hardware o software, tal vez incluso una vulneración de seguridad o un virus. Si se producen estos tipos de eventos, la copia de seguridad in situ suele ser la forma más rápida de hacer que los sistemas de la organización vuelvan a funcionar cuando se compara con las demás opciones.

El 59 %

de las empresas
reconocen los peligros
de mantener una sola forma
de copia de seguridad

Fuente: Encuesta realizada por Redmond Magazine

Mantener copias de seguridad en dos tipos de soporte diferentes es importante en caso de un error del soporte. Según Boston Network Computing, el 34 por ciento de las empresas no logran probar sus copias de seguridad en cinta, y de los que lo hacen, el 77 por ciento han encontrado errores de copia de seguridad en cinta.

Mantener una copia de seguridad externa cuando un desastre destruya tanto sus sistemas como las copias de seguridad in situ. Cuando tenga que activar un sitio secundario, puede utilizar la copia de seguridad externa. El almacenamiento de una copia de seguridad en la nube es eficaz para cualquier evento imprevisto, especialmente un desastre. Las organizaciones más grandes almacenan copias de seguridad, ya sea en una nube privada o pública, mientras que las pymes tienden a almacenar las copias en una nube pública.

Si no puede garantizar la continuidad del negocio sin un plan de recuperación de desastres y copia de seguridad, no puede permitirse el lujo de posponer la planificación de recuperación ante desastres. Junto con su estrategia de copia de seguridad, debe ser un elemento estratégico de su plan de IT.

N.º 3: La copia de seguridad es un requisito para mantener su estado de cumplimiento

La mayoría de los requisitos de cumplimiento regulatorio dicta que las organizaciones deben proteger y asegurar sus datos. Estos son algunos ejemplos de las regulaciones de cumplimiento más destacadas que requieren que una organización realice copias de seguridad de los datos con el fin de seguir cumpliendo las normativas.

HIPAA (EE. UU.) - Si su organización mantiene registros electrónicos de pacientes, la Health Information Portability & Accountability Act (HIPAA) requiere que su organización cuente con controles para gestionar la integridad de datos, autenticación, seguridad, planes de contingencia y controles de acceso y auditoría. La copia de seguridad de los datos del paciente es un elemento importante en el cumplimiento de estos requisitos.

Data Protection Act 1998 (Reino Unido) – La Data Protection Act rige la protección de datos personales en personas vivas identificables en el Reino Unido. Uno de los principios de protección de datos dicta que las organizaciones deben tomar medidas para asegurar que no haya pérdida accidental, destrucción o daños a datos personales. Solo la copia de seguridad puede garantizar que los datos no se pierdan o destruyan accidentalmente.

SOX (EE. UU.) - Todas las organizaciones que cotizan en bolsa en los EE. UU. están sujetas a la Sarbanes-Oxley Act de 2002, que cuenta con estrictos requisitos relacionados con la retención, alteración y destrucción de registros. La copia de seguridad de los registros financieros y empresariales es un elemento importante en el cumplimiento de estos requisitos.

Basilea II y Basilea III (Global) – Entre otros requisitos, Basilea II y III ordenan que las instituciones financieras deben tener los datos bajo control en todo momento y que debe haber planes de copia de seguridad del sistema en vigor.

FINRA (EE. UU.) – La Financial Industry Regulatory Authority es una organización no gubernamental que regula las empresas de intermediación miembros y los mercados de intercambio en nombre del SEC. Las reglas 17a-3 y 17a-4 del SEC describen los requisitos del mantenimiento de registros. De acuerdo con dichas reglas, estas organizaciones deben mantener registros de numerosos tipos de transacciones financieras por un período de tres o seis años, dos de ellos en un lugar de fácil acceso.

PCI (Global) – El Payment Card Industry's Data Security Standard (PCI 3.0 DSS) 12.10.1 requiere que los minoristas creen un plan de respuesta a incidencias que se implementará en caso de infracción. El plan debe abordar un proceso de copia de seguridad de datos.

GLBA (EE. UU.) - Las agencias federales del Federal Financial Institutions Examination Council (FFIEC) y la Federal Trade Commission (FTC) supervisan las instituciones financieras afectadas por la Gramm-Leach-Bliley Act (GLBA). Ambas organizaciones exigen a las instituciones financieras que pongan en marcha planes de contingencia que les permita recuperarse de una emergencia o desastre. Las regulaciones requieren un plan de copia de seguridad de datos, un plan de recuperación de desastres y un plan de operaciones en modo de emergencia.

Por qué Acronis es la única solución de copia de seguridad estratégica para pymes

Hay tres tipos principales de soluciones de copia de seguridad disponibles en el mercado hoy en día:

- La plataforma tradicional de uso general, que ofrece un servidor, célula o núcleo de copia de seguridad inteligente, y que realiza y gestiona la protección de datos unificada completa para todo el entorno, ya sea físico, virtual, o ambos.
- Productos o herramientas independientes que protegen sus diferentes tipos de datos, plataformas de sistemas operativos y aplicaciones.
- Un conjunto integrado de productos que proporciona control, gestión y presentación de informes para todo su entorno de manera unificada, independientemente del tamaño de su organización, el número de tipos de datos y el número y tipos de plataformas de sistemas operativos y aplicaciones.

Una plataforma tradicional dará soporte a un gran número de elementos de datos, plataformas de sistemas operativos y aplicaciones de muchos tipos. Una única plataforma implica tratar con un solo proveedor y la eliminación de las complejidades de la negociación y la gestión de múltiples proveedores. La compra de una plataforma tradicional es una decisión estratégica.

Por desgracia, para las organizaciones pequeñas y medianas, una plataforma tradicional de protección de datos suele ser demasiado cara. Hay costos significativos por adelantado al adquirir una plataforma tradicional, incluyendo la licencia, hardware dedicado, componentes de red de soporte del núcleo central y costos de mantenimiento. Una plataforma tradicional de protección de datos también requiere uno o más administradores a tiempo completo, capacitados y certificados: un recurso que muchas pequeñas y medianas empresas no pueden permitirse.

Puede tomar la decisión de comprar productos y herramientas de copia de seguridad por separado a medida que los necesite, que es una táctica para hacer frente a sus necesidades de copia de seguridad sistema a sistema y aplicación a aplicación. Aunque esto puede simplificar la decisión inicial de compra, ya que cada una de estas aplicaciones es menos costosa que una plataforma tradicional, tendrá que tratar con diferentes proveedores de copia de seguridad para cada plataforma de sistema operativo y aplicaciones que tenga.

El inconveniente es que tener diversos productos y vendedores multiplica la formación, la complejidad de gestión, la instalación, la supervisión y la presentación de informes, ya que cada producto es diferente. A medida que crezca su organización, los costos de los productos y herramientas independientes adicionales comenzarán a acumularse. A medida que el número de sistemas operativos y aplicaciones se expande en su organización, tiene que contratar a más administradores de IT, aumentando las necesidades de formación del personal y del departamento de IT.

El 37 % de las empresas necesitan **proteger datos** de forma simultánea en entornos virtuales, físicos y en la nube

Fuente: Encuesta de recuperación de desastres de Acronis, IDC, mayo de 2014

Si tiene una pyme, la compra de un conjunto integrado de productos es una decisión estratégica, ya que tendrá una sola solución de copia de seguridad que responde a cada uno de sus sistemas operativos y aplicaciones, así como la capacidad de mezclar soluciones puntuales aisladas en una única solución integrada. Un conjunto integrado de productos significa que su organización está tratando con un solo proveedor y elimina la complejidad y el tiempo asociados con la gestión de múltiples proveedores. Además, dado que un conjunto integrado de productos utiliza una consola de instalación y gestión para todos sus productos, podrá simplificar sus necesidades de personal de IT y reducir los costos de formación de IT.

Resumen

Los profesionales de IT no deben retrasar la discusión de copia de seguridad. De hecho, la copia de seguridad y recuperación de desastres debe ser un punto de discusión en todo el proceso de planificación de IT. La copia de seguridad es un factor esencial (estratégico) para su organización, ya que:

Su negocio consiste en sus datos y la copia de seguridad es la única forma de protegerlos.
Sin copia de seguridad, no hay datos y el negocio no es viable.

La copia de seguridad es el componente más importante de cualquier plan de recuperación de desastres.
Sin copia de seguridad, no hay recuperación ante desastres y el negocio no es viable.

Todas las regulaciones de cumplimiento obligan a las empresas a realizar copias de seguridad de los datos.
Sin copia de seguridad, no hay cumplimiento normativo y existe la posibilidad de sufrir penalizaciones civiles o criminales.

Acronis ofrece a las pymes la única solución estratégica asequible para proteger los datos, en cualquier entorno y en cualquier lugar. Los productos de copia de seguridad de Acronis se basan en Acronis AnyData Engine, un conjunto de tecnologías de protección de datos de nueva generación, únicas, potentes y avanzadas que capturan, almacenan, recuperan y gestionan datos en entornos virtuales, físicos y en la nube. En función de sus necesidades empresariales, puede desplegar productos individuales de Acronis o mezclar de forma transparente lo que requiere hasta formar una solución unificada total que proteja los datos en cualquier entorno y en cualquier lugar.

Independientemente de su entorno, puede utilizar la misma consola unificada para configurar, instalar y mantener cada producto. Para varios sistemas empresariales, Acronis ofrece Acronis Management Server (AMS), un único panel que le permite gestionar fácilmente la copia de seguridad y recuperación de todos los datos en varios productos Acronis Backup Advanced. Desarrollado para organizaciones que requieren una solución completa, eficaz y fácil de usar, la tecnología de nueva generación de Acronis simplifica la copia de seguridad, la recuperación de desastres y el acceso seguro a sus datos esenciales, reduciendo la pérdida de datos, el tiempo de gestión de IT y el costo total de propiedad.

Acronis | ACRONIS AUTHORIZED PARTNER

Acerca de Codes

Somos profesionales de las tecnologías de la información.

Nuestras soluciones contribuyen con el cumplimiento de objetivos organizacionales de cada uno de nuestros clientes debido a que se alinean a las necesidades de las personas y negocios que las utilizan.

Más de 300 clientes han encontrado en nosotros una solución real a sus necesidades de TI, podemos decir con orgullo que cada uno de nuestros clientes son un Caso de Éxito ya que la excelencia va de la mano con nuestros productos y servicios.

Si desea información adicional, visite **www.codes.com.mx/acronis**