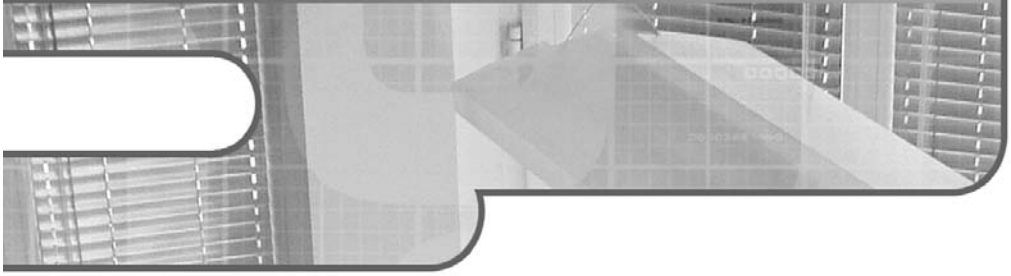


Capítulo 15
Copia de seguridad y restauración

1. Presentación de la recuperación de desastres

Hoy en día, cada vez más empresas trabajan empleando diariamente herramientas informáticas (servidores, puestos de trabajo, terminales fijos o móviles, e-mail, etc.). Los datos manipulados están disponibles en diferentes soportes, accesibles por uno o varios usuarios y más o menos confidenciales. Para muchas empresas, su actividad principal está basada en datos digitales (contratos, facturas, pedidos, gestión de inventario, productos, servicios en línea, sitios web, proyectos, etc.). Por este motivo, la pérdida de datos informáticos durante un siniestro puede resultar vital para una empresa (incendio, eliminación accidental, caídas de sistema, piratería, robo, etc.). Según las estadísticas, una empresa que pierde una parte fundamental de sus datos informáticos tras una caída del sistema o una manipulación incorrecta tiene un porcentaje muy alto de cesar toda actividad en las semanas siguientes al siniestro, si no se ha implemantado previamente un plan de recuperación de desastres. Por este motivo, la copia de seguridad es un aspecto esencial, común a casi todas las empresas. Implementar una solución informática significa, también, planificar e implementar soluciones de restauración en caso de siniestro.

1.1 Recuperación de desastres

La recuperación de desastres consiste en restaurar el servicio que se haya visto impactado tras un siniestro. Para ello, una empresa puede implementar un plan de recuperación de desastres (PRD) que consiste en definir las tareas y acciones a realizar para restaurar, en un tiempo récord, el servicio ofrecido a los usuarios. Un PRD contiene principalmente un plan de respaldo que consiste en definir una política relativa al almacenamiento del conjunto de datos de la empresa para poder restaurarlo en caso de necesidad. Antes de implementar una política de respaldo, una empresa debe realizar un estudio preliminar que ayudará a definir claramente las necesidades y orientar la manera más adecuada de implementar el plan de respaldo. Para satisfacer mejor las exigencias requeridas por un sistema informático, es necesario respetar y seguir las mejores prácticas definidas en las normas ITIL (*Information Technology Infrastructure Library*).

Las mejores prácticas contenidas en las publicaciones ITIL abogan por dar respuesta a las siguientes preguntas antes de implementar un plan de recuperación de desastres:

- **Definir los elementos a securizar y/o respaldar**: securizar o respaldar el conjunto del perímetro informático conlleva costes (software, hardware, espacio de almacenamiento en disco o cinta, redundancia de equipos, etc.). Por este motivo, conviene evaluar previamente el volumen de datos a almacenar realizando la selección de los elementos a conservar.
- **Evaluar los costes del respaldo**: a mayor cantidad de datos a respaldar, mayor será el coste del plan de respaldo (equipo de copia de seguridad, espacio en disco, etc.). Para controlar su presupuesto, es importante no descuidar los costes vinculados al respaldo. Todos los elementos de la infraestructura de copia de seguridad deben ser evaluados, como el hardware, software, volumen de datos, costes de retención, costes de almacenamiento al igual que los costes humanos (administrador, operador, etc.).

– **Definir las cláusulas del contrato de nivel de servicio**: las publicaciones que describen las mejores prácticas informáticas mencionan la gran importancia de definir previamente el nivel de servicio ofrecido a los usuarios. Estas cláusulas deben registrarse en un documento que indique con claridad la calidad que se espera de los servicios (contrato entre cliente y proveedor también llamado SLA: *Service Level Agreement*), así como los tiempos de interrupción de servicio máximos en caso de avería o siniestro. La duración máxima de interrupción del servicio aceptable antes del reinicio de la actividad, también llamada RTO (*Recovery Time Objective*) de acuerdo a las publicaciones ITIL.
– **Definir la pérdida de datos aceptable en caso de siniestro**: tras un desastre, es posible restaurar los datos perdidos o dañados de un servidor en un momento T, si la aplicación de las políticas de copia de seguridad está en funcionamiento. Sin embargo, los datos introducidos por los usuarios varios minutos antes del siniestro pueden no haber sido respaldados. Esto quiere decir, implícitamente, que no es posible restaurar los elementos que no hayan sido respaldados. Por este motivo, es importante definir la tolerancia relativa a la pérdida de datos en caso de siniestro en un documento específico, también llamado RPO (*Recovery Point Objective*) en las publicaciones ITIL.
– **Definir la política de retención de los respaldos**: cuando los respaldos se realizan en cinta, online o en disco, se consume espacio de almacenamiento. La política de retención de respaldos define el tiempo durante el que es necesario conservar los archivos almacenados antes de sobrescribirlos con una nueva copia de seguridad o, simplemente, destruirlos. Cuanto mayor sea el período de conservación de los respaldos, más fácil será para un administrador restaurar datos eliminados hace varios días. El caso se presenta sobre todo para las situaciones de eliminación accidental de datos. Por ejemplo, si un usuario elimina accidentalmente una carpeta importante y ningún usuario se da cuenta de ello en dos semanas... será entonces imposible para un administrador restaurar los datos eliminados si la política de retención de copias de seguridad impone una rotación para la sobrescritura de los archivos de una semana. Para poder restaurar en diferentes situaciones, es posible implementar dos planes de respaldo simultáneamente. Por ejemplo, un plan de respaldo semanal en disco podría realizar copias de seguridad con un período de retención de cuatro semanas, mientras que otro plan de respaldo mensual en cinta podría realizar copias de seguridad con un plazo de retención de un año.

– **Definir una política de restauración de datos**: existen diferentes métodos para restaurar los datos en función de los métodos de copia de seguridad o recuperación implementados para securizar la infraestructura informática. Durante un siniestro, conviene determinar previamente los métodos de recuperación de los datos en función del tipo de situación. Una política de restauración debe estar definida de acuerdo a las cláusulas definidas en los contratos de calidad de servicio. Por ejemplo, si un usuario pierde un archivo, será más rápido intentar restaurar los datos mirando en la caché de instantáneas que recuperar una cinta del centro de respaldo de archivos. Esto permite restaurar los datos más rápidamente y aumentar el porcentaje de disponibilidad para respetar las cláusulas de calidad de servicio por parte de los administradores, así como reducir el tiempo de interrupción máximo admisible por los usuarios. Resulta básico validar y probar regularmente cualquier plan de respaldo que se implemente, con el objetivo de garantizar que la política de restauración es operativa y que los datos almacenados son explotables. Sucede con demasiada frecuencia que una empresa respalda sus datos en cinta y que el día que se requiere una restauración los administradores se encuentran impotentes, con una cinta en blanco o datos inutilizables. Conviene probar, sistemáticamente, que el proceso de restauración funciona y que los archivos restaurados son accesibles por los usuarios. Esto garantiza la integridad de los datos restaurados así como la calidad del servicio proporcionado.

1.2 Presentación de la copia de seguridad

Existen varias tecnologías de copia de seguridad de datos, varios soportes de destino y varios fabricantes; las soluciones utilizan componentes hardware o software.

Encontramos en particular las copias de seguridad de datos en los soportes siguientes:

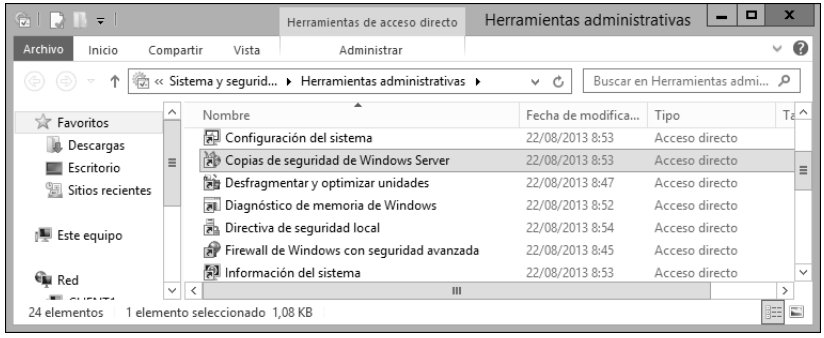
– **Cloud**
– **Discos duros internos/externos**
– **Soportes extraíbles**
– **CD/DVD ROM**
– **Ubicaciones de red**

- **Replicación de datos (en un equipo redundante o una ubicación geográfica diferente)**
- **Cintas de copia de seguridad**
- **Instantáneas**
- **RAID**
- **Snapshots (copia de seguridad del estado del sistema en un momento concreto)**

La mayoría de las soluciones software de terceros existentes utilizan componentes que necesitan un servidor sobre el que instalar la solución de copia de seguridad y agentes instalados en cada servidor para garantizar la comunicación y la transferencia de los datos a respaldar. En este libro se aborda, únicamente, la solución de copia de seguridad integrada en el sistema operativo Windows Server 2012 R2 (funcionalidad **Copias de seguridad de Windows Server**), las instantáneas (**Shadow Copy**), así como el sistema de copia de seguridad de tipo Cloud ofrecido por Microsoft llamado **Windows Azure Online Backup**.

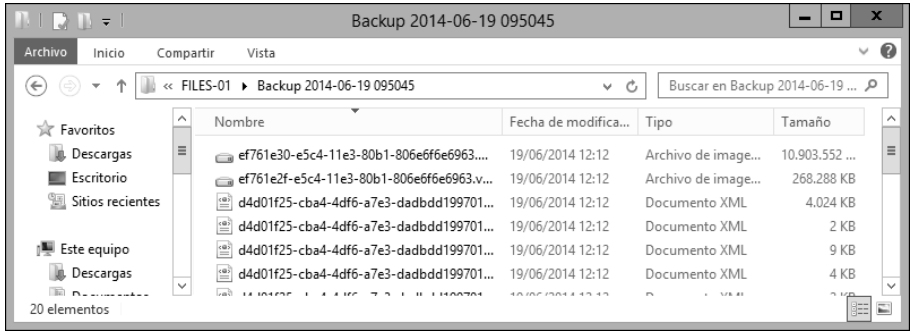
1.3 Copias de seguridad de Windows Server

El sistema operativo Microsoft Windows Server 2012 R2 integra de manera nativa la funcionalidad de servidor llamada **Copias de seguridad de Windows Server**. Una vez instalada, es posible acceder a esta herramienta como un complemento accesible desde la carpeta de sistema **%Windir%\system32\wbadmin.msc**, las herramientas administrativas del sistema operativo o mediante el Administrador del servidor.



Esta herramienta permite principalmente gestionar las copias de seguridad locales (ubicación de red, volumen en disco) o en línea (**Windows Azure Online Backup**).

Cuando ejecutamos una copia de seguridad con esta herramienta, el complemento *Copias de seguridad de Windows Server* crea un disco virtual del volumen a respaldar. Este disco virtual es un archivo imagen con formato *.vhdx, que es el nuevo formato de almacenamiento de las máquinas virtuales en Microsoft Hyper-V3. Los discos virtuales VHDX pueden soportar 64 TB de datos. El disco virtual dedicado para la copia de seguridad de los datos se crea en la ubicación siguiente: **[Unidad:\]\WindowsImageBackup\[Nombre de servidor]\Backup [Fecha de la copia de seguridad]**



Se puede navegar en cualquier momento por los archivos de imagen de disco duro empleando un complemento. La herramienta crea los archivos *BackupGlobalCatalog* y *GlobalCatalog* que registran la configuración de los volúmenes respaldados en la siguiente ubicación:
[Unidad:\]\WindowsImageBackup\[Nombre de servidor]\Catalog