Capítulo 5
La seguridad de los datos

1. Los riesgos de pérdida de datos

La protección de datos es esencial para una empresa, sea cual sea su tamaño, a partir del momento en que toda la información importante se almacena en la infraestructura de su red.

No es indispensable imaginar de forma sistemática el peor escenario, pero sin embargo nos permite tener en cuenta todas las contingencias que puedan conducir a la pérdida total o parcial, temporal o definitiva, de la información de la empresa. He aquí algunos ejemplos de riesgos que puedan afectar a los datos de un sistema de información:

– Fallos de la red eléctrica general que pueden conducir a cortes y por consiguiente corrupción de datos.
– Fallos del sistema operativo.
– Virus y programas informáticos malintencionados.
– Daños o averías del equipo (discos duros...).
– Eliminación de archivos (accidental o no).
– Alteración, modificación o supresión de información, de mala fe.
– Robo de materiales, programas informáticos; sabotajes.
– Errores de procesamiento de datos.

– Desastres naturales.

La posibilidad de pérdidas de datos importantes para la empresa implica la necesidad de realizar copias de los datos empleando copias de respaldo y archivos de toda la infraestructura informática (servidores de producción, desarrollo...).

Los principios generales

Debemos realizar copias de seguridad de todos los datos operativos para permitir la reconstrucción en caso de que sean destruidos o perdidos.

La aplicación de respaldo debe estar prevista para instalarse en servidores de forma que las transferencias de datos sean lo más eficaces posible y que el ancho de banda de la red no se vea afectado, en especial cuando las aplicaciones de negocio de la empresa se utilicen más.

Se recomienda encarecidamente guardar las copias de seguridad en un lugar seguro lejos de la ubicación de la mayoría de los sistemas críticos. En el caso de un incidente grave o de un siniestro que afecte totalmente a los sistemas, esta precaución permitirá poner en marcha equipos equivalentes en un lugar diferente.

Los soportes de salvaguardia utilizados para las operaciones de copia de seguridad deben probarse periódicamente para asegurarse de que los datos pueden restaurarse en un estado correcto cada vez que sea necesario.

Los principios generales presentados son válidos para la mayoría del software y aplicaciones de copia de seguridad. Pueden existir diferencias. Cada una de estas aplicaciones tiene especificaciones relativas al editor que los ha diseñado y el entorno para el que se ha previsto. Cada empresa escoge su aplicación de copia de seguridad en función de su entorno y de sus decisiones estratégicas.

En este capítulo, la información presentada puede variar en función de las aplicaciones y su editor. Sin embargo, los principios descritos siguen siendo válidos.

2. El respaldo y la restauración

2.1 Conceptos generales

Para empezar, es útil definir los conceptos principales que se utilizarán en los próximos capítulos.

2.1.1 Definiciones

El servidor de respaldo

Se trata de un servidor equipado con uno o varios dispositivos de almacenamiento, en general dedicados a esta función. Su papel principal consiste en realizar las fases de copia de seguridad, de archivo y restauración de datos (sistema operativo, archivos y bases de datos...).

El cliente de respaldo

El servidor también se almacena en la aplicación de respaldo, que es también cliente de la aplicación.

Las máquinas cliente son también servidores, representan los entornos que se han de respaldar.

El cliente incluye un conjunto de datos que se deben copiar en un equipo específico (servidor de archivos, de aplicación...).

Varios clientes pueden coexistir en una misma máquina física, cada cliente con sus propios atributos. Estos son:

- Un nombre: siempre el nombre del servidor conocido en la red de la empresa.
- Los conjuntos que se deben guardar o save-sets: los nombres de archivos, directorios o sistemas de archivos.
- La pertenencia a un grupo, un planning de copia de seguridad, una directiva, políticas...
- Un alias: otro nombre de la máquina en la red.

– Nodos de almacenamiento: lista prioritaria de los dispositivos locales o remotos a los que van a enviarse los flujos de datos.
– Nodos de almacenamiento de clonación: lista prioritaria para esta operación.
– Políticas de retención de datos y de búsqueda.

Los clientes pueden agruparse y poseer atributos propios:

– Nombre.
– Hora de arranque.
– Tipo de arranque.
– Política de retención de datos y de búsqueda.

La aplicación de copia de seguridad

Es el software instalado en el servidor de copia de seguridad. Su función consiste en gestionar las operaciones en los soportes, las conexiones a los clientes y señalar los errores encontrados.

Los grupos de usuarios y los derechos de acceso

En la aplicación de copia de seguridad, podemos crear grupos de usuarios para las operaciones de copia y restauración o de archivo. Un usuario debe pertenecer a un grupo antes de poder asignarse los derechos de acceso especiales. En efecto, guardar y restaurar vuelve a copiar los datos; es conveniente limitar el acceso a los usuarios autorizados. Lo que implica un sistema de seguridad relativo a los usuarios del tipo:

– Toda persona que quiera utilizar el software de respaldo debe definirse como un usuario en la aplicación.
– Solo el propietario de la copia puede visualizar los datos que ha guardado.

Otras autorizaciones pueden definirse en función del contexto y las necesidades de los usuarios o del entorno.

La planificación de las copias de seguridad

La periodicidad se define en función de las necesidades y los niveles de protección: puede ser diaria, semanal o mensual.

Estas líneas de operación se definen como una combinación de períodos (día, semana, mes y año) y una frecuencia de respaldo.

2.1.2 La política de respaldo

Se define en función del volumen de datos que se han de copiar, de la cantidad de información que se debe retener o que pueda perderse, el entorno técnico y la duración legal de conservación de los datos.

Esta política consiste en definir:

- El entorno del sistema de información que hay que proteger (servicios, hardware, lugares, usuarios...) y la forma en que las operaciones se realizan.
- El tipo y la cantidad de datos que hay que almacenar (archivos de usuario o aplicaciones, cuentas de correo, bases de datos...). El número de archivos o el tamaño de las copias de seguridad puede evolucionar en el tiempo con la adición de nuevas aplicaciones y datos.
- La frecuencia y periodicidad de los respaldos.
- Los lugares y medios de almacenamiento de copias de seguridad.

Política de retención de datos respaldados

Existen dos tipos:

Política de búsqueda: período de mantenimiento de la información en los índices o la base de datos interna.

Política de retención: período de conservación de la información en la biblioteca de cintas o el conjunto de soportes de almacenamiento.

2.1.3 La copia de seguridad

Se trata de la operación que consiste en crear una copia de los datos sobre un medio de almacenamiento (cinta magnética, soporte óptico, disco duro...). Esta replicación de información se almacena y conserva para su posterior restauración en caso de que el original se suprima (involuntariamente o voluntariamente), sea destruido o dañado.

El software que copia los datos hacia un medio de comunicación se llama aplicación de copia de seguridad.

En la mayoría de los casos, la fuente corresponde a los datos almacenados en una unidad de disco; por ejemplo, archivos, directorios, bases de datos y aplicaciones.

El destino es un soporte de almacenamiento que utiliza un equipo de grabación y reproducción, como una unidad de cinta magnética, un robot, una unidad de almacenamiento compuesta de discos o de soportes ópticos (DVD-ROM...) o un almacenamiento basado en la red.

2.1.4 El archivado

Es una operación de copia idéntica a la salvaguardia, salvo que los datos copiados se almacenan y conservan para una duración más larga. Esta operación puede ser necesaria por razones legales o administrativas. También permitirá mantener el estado del sistema operativo de un servidor justo después de una instalación o una actualización importante.

El destino es un soporte que utiliza un dispositivo específico equivalente a los establecidos para el respaldo; el soporte WORM (*Write Once/Read Many*) puede utilizarse más específicamente en este caso.

2.1.5 La restauración

Esta operación realiza la reconstrucción de los datos originales a partir de una copia de seguridad o de un archivo.

Este concepto comprende la preparación y la recopia propiamente dicha de los datos; a veces son necesarias algunas acciones adicionales para que los datos sean explotables.