



- ◆ Trabajo realizado por el equipo de la Biblioteca Digital de la Fundación Universitaria San Pablo-CEU
- ◆ Me comprometo a utilizar esta copia privada sin finalidad lucrativa, para fines de investigación y docencia, de acuerdo con el art. 37 del T.R.L.P.I. (Texto Refundido de la Ley de Propiedad Intelectual del 12 abril 1996)



## **SEGURIDAD DEL SERVIDOR**

Dentro del concepto de seguridad del servidor se pueden distinguir cuatro apartados:

- La seguridad física.
- La seguridad de los datos.
- La protección de acceso al ordenador.
- La protección de acceso a los datos.

### **LA SEGURIDAD FÍSICA DEL SERVIDOR**

El lugar donde esté colocado el servidor es sumamente importante para su estabilidad. El servidor necesita estar protegido contra distintos factores externos que pueden alterar el funcionamiento de la red.

Estos factores externos son: la electricidad estática, el calor, los ruidos eléctricos, los altibajos de tensión y los cortes de corriente.

#### **La protección contra la electricidad estática y el calor**

Se han de tomar algunas precauciones para proteger al servidor de las cargas estáticas, ya que el rendimiento de éste afecta a toda la red.



## **SEGURIDAD DEL SERVIDOR**

Dentro del concepto de seguridad del servidor se pueden distinguir cuatro apartados:

- La seguridad física.
- La seguridad de los datos.
- La protección de acceso al ordenador.
- La protección de acceso a los datos.

### **LA SEGURIDAD FÍSICA DEL SERVIDOR**

El lugar donde esté colocado el servidor es sumamente importante para su estabilidad. El servidor necesita estar protegido contra distintos factores externos que pueden alterar el funcionamiento de la red.

Estos factores externos son: la electricidad estática, el calor, los ruidos eléctricos, los altibajos de tensión y los cortes de corriente.

#### **La protección contra la electricidad estática y el calor**

Se han de tomar algunas precauciones para proteger al servidor de las cargas estáticas, ya que el rendimiento de éste afecta a toda la red.

Entre las precauciones que se han de tomar está la de tratar regularmente las alfombras y moquetas con productos antiestáticos, utilizar fundas protectoras para ambas e instalar el servidor sobre una superficie conectada a una toma de tierra.

No utilizar plásticos ni material sintético, ya que generan electricidad estática.

El calor y el frío excesivos son riesgos potenciales para el buen funcionamiento del servidor. Se ha de mantener la temperatura de la habitación del servidor entre 18° y 26° C, y asegurar una buena aireación.

## La protección contra los ruidos eléctricos, los altibajos de tensión y los cortes de corriente

Los ruidos eléctricos son causados por las inconsistencias del suministro de la corriente del ordenador. Para proteger al servidor contra los ruidos eléctricos, puede recurrirse a la instalación de una línea dedicada de suministro eléctrico.

No hay que conectar otros dispositivos a este suministro de corriente, porque pueden generar ruidos que anulen las ventajas de la protección ofrecida por la fuente de corriente dedicada.

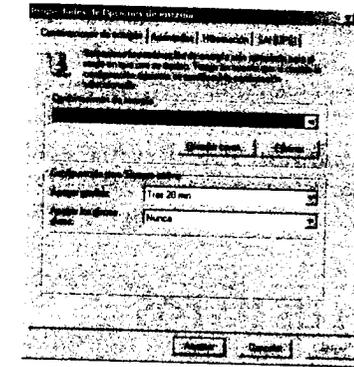
La conexión a la fuente de energía se ha de hacer con cable estándar de tres hilos, con el hilo de masa conectado a tierra.

Debe prevenirse contra los altibajos de tensión y contra el corte de la corriente. Para esto lo mejor es completar la instalación con un *sistema de alimentación ininterrumpida* o SAI (*UPS, Uninterruptible Power Supply*). El SAI permite al servidor continuar activo durante cierto tiempo ante un eventual corte de la corriente.

Puede también tomarse la precaución de instalar un SAI en cada una de las estaciones que trabajen con aplicaciones críticas, para protegerse de los daños producidos por la pérdida de datos durante un corte de energía.

Además, cada dispositivo de la red podría tener un filtro de energía eléctrica como protección de las sobretensiones.

Si se dispone de un **sistema de alimentación ininterrumpida (SAI)** podrá configurarse, para su uso con *Windows 2000*, ejecutando el icono **Opciones de energía** del **Panel de control** y verá la pantalla siguiente:



## La suciedad

Aquí interviene tanto la suciedad de la sala donde se encuentra el servidor como la suciedad que pueden generar los propios usuarios.

Hay que mantener la sala en un estado de perfecta limpieza para evitar que el polvo pueda concentrarse dentro del servidor y altere su correcto funcionamiento.

Referente a los usuarios y administradores se ha de tener en cuenta que cualquier vertido de líquidos o de restos de alimentos sobre la pantalla y/o el teclado del servidor pueden producir distintos daños potenciales en el servidor. También, se ha de tener precaución con la ceniza de los cigarrillos tanto dentro del teclado como en la pantalla y la CPU porque pueden producir daños importantes.

## La seguridad contra incendios y agua

De qué vale tener bien protegido el servidor si no se cuenta con una buena protección contra incendios. En la sala donde se encuentre instalado el servidor debe haber detectores de humo de alta sensibilidad y un sistema contra incendios a base de gas halón a presión. Este sistema debe producir un aviso previo a su utilización porque provoca el apagado del incendio de forma inmediata por consumo del oxígeno de la sala y, por tanto, todas las personas deberán salir de dicha sala porque podrían correr riesgo de asfixia.

También deberá estar protegido el servidor contra peligros de inundaciones y goteras que podrían provocar cortocircuitos eléctricos.

## La protección contra robo y destrucción

Es muy importante que en la sala donde se encuentra el servidor haya una protección efectiva que imposibilite tanto el robo del equipo o de alguno de sus componentes como la posibilidad de algún atentado que provoque la destrucción de todo, o de alguna parte importante, del servidor (tanto a nivel de *hardware* como de *software*).

La sala deberá estar protegida con sistemas antirrobo (tanto a nivel de las puertas como de las ventanas), las puertas que conducen a la sala deberán permanecer cerradas y se deberá identificar a cualquier persona que tenga acceso al servidor.

La información y el *software* han de estar guardados en otras habitaciones cerradas y los disquetes se han de encontrar cerrados con llave en los cajones de los archivos o de las mesas.

## LA SEGURIDAD DE LOS DATOS

Es importante que los datos que están ubicados en el servidor de la red se encuentren bien protegidos.

Para que los datos se encuentren perfectamente protegidos, hay que considerar tres apartados:

- La seguridad del almacenamiento en el disco duro.
- La configuración de seguridad.
- La copia de seguridad de los datos.

### La seguridad del almacenamiento en el disco duro

La unidad básica de almacenamiento de la información es el disco duro. Su capacidad está en constante incremento (de 8 GB en adelante).

La forma más común de organizar el almacenamiento de la información es a través de un único disco duro (cuenta con la ventaja de la simplicidad de su configuración) aunque, dependiendo del tamaño de la empresa, se debe considerar la posibilidad de trabajar con más de un disco duro asociado.

Cada disco duro del sistema tiene asignado un número (comenzando en el cero) y se asignan de forma diferente en función del tipo de disco:

- **SCSI.** En una controladora primaria de este tipo, los números van del cero al seis (aunque posee otra dirección que suele estar reservada para el adaptador del bus). Cuando esta controladora se completa puede recurrirse a una controladora secundaria y así sucesivamente hasta un total de cuatro (lo que permitiría disponer hasta de un total de 28 unidades).
- **IDE y ESDI.** En una controladora primaria de estos dos tipos, los números van del cero al uno. Cuando esta controladora se completa puede recurrirse a una segunda controladora (lo que permitiría disponer hasta de un total de cuatro discos).

Todos los discos duros deben estar formateados a bajo nivel para poder utilizarse con *Windows 2000*.

## PARTICIONES

En un disco básico, la partición hace que un disco duro (o una parte de él) pueda ser utilizada como medio de almacenamiento.

Por medio de las particiones, el disco duro se puede dividir en *unidades lógicas* que cada una dará acceso a una parte del disco duro.

Las particiones pueden ser de dos tipos:

- **Particiones primarias** que es reconocida por la **BIOS** del ordenador como capaz de iniciar el sistema operativo desde ella. Para ello, dispone de un sector de arranque (**BOOT SECTOR**).

Pueden existir hasta un máximo de cuatro particiones primarias, de las cuales únicamente una puede estar activa en cada momento.

Con un programa de inicialización adecuado se podrá seleccionar entre los diferentes sistema operativos para su arranque (cada uno deberá estar en su propia partición primaria).

- **Particiones secundarias** que se forman en las áreas del disco duro que no tienen particiones primarias y que están contiguas.

Puede haber, como máximo, una partición extendida (en ese caso, el disco duro no podría tener más de tres particiones primarias).

Las particiones extendidas deben estar configuradas en unidades lógicas para poder ser utilizadas para almacenar información.

- **Partición de NetWare o partición tradicional de NetWare.** Es una partición en la que se pueden crear volúmenes tradicionales de *NetWare*. Los volúmenes *NSS* no se pueden crear en este tipo de partición.
- **Partición *NSS* de NetWare.** Es una partición en la que se pueden crear volúmenes *NSS*. Los volúmenes tradicionales de *NetWare* no se pueden crear en este tipo de partición.

Las particiones deben estar formateadas para establecer letras de unidades que van desde la **C:** en adelante.

La partición primaria corresponde a la unidad **C:**.

Las particiones secundarias se pueden dividir en una o varias *unidades lógicas*.

## VOLÚMENES

Un volumen es una parte de un disco físico (o de varios discos) que funciona igual que una unidad separada.

## ESPACIO LIBRE DE ALMACENAMIENTO

Con este término se designa el espacio del disco duro que no pertenece a ninguna partición o volumen, y puede utilizarse para crearlos.

## SISTEMAS DE ARCHIVOS

Es posible escoger entre varios sistemas de archivos distintos para el disco duro. Entre ellos se encuentran:

- **FAT (File Allocation System).** Se puede acceder a este sistema de archivos desde *MS-DOS* y todas las versiones de *Windows*. Permite trabajar con particiones menores de 2 GB y no soporta dominios.
- **FAT32.** Se puede acceder a este sistema de archivos desde *Windows 95 OSR2*, *Windows 98* y *Windows 2000*. Permite trabajar con particiones mayores de 2 GB, el tamaño máximo de un archivo es de 4 GB, los volúmenes pueden llegar hasta 2 TB (en *Windows 2000* sólo hasta 32 GB) y no soporta dominios.
- **NTFS (NT File System).** Es el sistema desarrollado para *Windows NT 4* que permite nombres de archivo de hasta 256 caracteres, ordenación de directorios, atributos de acceso a archivos, reparto de unidades en varios discos duros, reflexión de discos duros y registro de actividades. *Windows 2000 Server* incluye mejoras para este sistema de archivos: permite utilizar el *Directorio Activo*, dominios, cuotas en disco para cada usuario, compresión y encriptación de archivos, almacenamiento remoto, una herramienta de desfragmentación y el sistema de archivos distribuidos (*DFS*). Sus volúmenes pueden sobrepasar los 2 TB y el tamaño máximo de un archivo sólo está limitado por el tamaño del volumen.
- **Sistema de archivos de NetWare tradicional** basado en particiones *NetWare*, volúmenes, directorios y archivos. Requiere cantidades de memoria RAM específicas en función del espacio en disco total que admita el servidor y el tiempo de montaje del volumen está en función de su tamaño. El volumen *SYS* ha de ser un volumen tradicional obligatoriamente (por las características no soportadas en volúmenes *NSS*). Se pueden actualizar los volúmenes *NetWare* tradicionales a *NSS* en cualquier momento.
- **Servicios de almacenamiento de Novell (NSS).** Constituyen un nuevo servicio de almacenamiento modular de alto rendimiento que se ejecuta en *NetWare 5* y que es totalmente compatible con el tradicional *Sistema de*

*archivos de NetWare*. Reúnen todo el espacio libre sin particionar existente en todas las unidades de disco duro conectadas al servidor, junto con el espacio no utilizado de los volúmenes *NetWare*, y lo incluye en una agrupación de almacenamiento.

Las características de los *NSS* son las siguientes:

Característica	Capacidad de los NSS
Número de archivos por servidor	8 billones
Tamaño máximo de los archivos	8 terabytes
Número máximo de archivos	1 millón por servidor abiertos simultáneamente
Tiempo de apertura de archivos	Independientemente del tamaño del archivo, se abre inmediatamente
Tamaño máximo del volumen	8 terabytes
Número máximo de volúmenes en un único servidor	255 (montados)
Segmentos de volumen	Ilimitados
Extensión del árbol de directorios	Limitado por el administrador
Tiempo de montaje de volúmenes	Está en función del tamaño del volumen (por lo general, menos de un minuto)
Memoria RAM necesaria	4 MB como mínimo; se puede añadir memoria RAM para aumentar el rendimiento del caché

## SISTEMAS RAID

**RAID** es un conjunto de dos o más discos que funcionan de forma conjunta, para poder aumentar el rendimiento y el nivel de protección de los datos.

Cuentan con las siguientes ventajas:

- El rendimiento general del sistema aumenta ya que pueden funcionar de forma paralela con los diferentes discos del conjunto.
- Dependiendo del nivel *RAID* que se escoja, si uno de los discos del conjunto falla, la unidad continúa funcionando, sin pérdida de tiempo ni de datos. La reconstrucción de los datos del disco que ha fallado se hace de forma automática sin intervención del usuario (en el caso de algunos sistemas operativos, la regeneración de datos se hace desde el *software*, aunque se pueden utilizar controladoras *RAID* que sí regenerarían los datos automáticamente).
- La capacidad global del disco aumentará, ya que se suman las capacidades de los diferentes discos que componen el conjunto.

## Niveles Raid

La primera definición de *RAID*, fue en 1987 y se describieron 5 niveles, aunque posteriormente se desarrollaron 2 más. Los niveles *RAID* ofrecen grandes diferencias entre rendimiento e integridad de los datos, dependiendo de las especificaciones de cada nivel. No hay un nivel *RAID* perfecto para todos los usuarios, ya que cada uno de ellos cumplen distintos propósitos:

**RAID 0:** Datos en bandas de discos sin paridad y sin corrección de errores.

En este nivel, los datos están repartidos entre los diferentes discos. Este nivel será relacionado en muchas ocasiones como *striping*.

Cuenta con las siguientes ventajas:

- Proporciona un alto rendimiento.
- No tiene costo adicional.
- Se emplea toda la capacidad del disco.

Cuenta con los siguientes inconvenientes:

- No es verdaderamente un disco *RAID* ya que no tiene integridad de datos.
- Un error en uno de los discos implica la pérdida total de los datos.

**RAID 1:** Conjunto de discos en espejo.

Este nivel es también conocido como *mirroring* ya que los datos son escritos al mismo tiempo en dos discos diferentes y se dispone de dos copias exactas del total de la información. Este nivel es una solución cara, ya que desaprovecha la mitad de la capacidad total del conjunto de discos.

Cuenta con las siguientes ventajas:

- Mayor rendimiento en las lecturas de datos respecto a un disco convencional.
- Se pueden recuperar todos los datos en caso de error en uno de los discos.

Cuenta con los siguientes inconvenientes:

- Es más caro, ya que se necesita el doble de discos.
- Moderada lentitud en la escritura de datos, ya que se han de escribir en dos localizaciones distintas.

**RAID 2:** Con código de correcciones de error utilizando la generación Hamming de códigos de error.

Emplea múltiples discos (como en el nivel *RAID 0*) pero algunos de estos discos son empleados para códigos de error, que los emplean para referencia de los datos en caso de que falle uno de los discos. Este nivel tiene un costo bastante elevado ya que se necesitan muchos discos para mantener los códigos de error.

Gracias a cómo están distribuidos los datos en los discos se consigue mejorar la velocidad de transferencia principalmente en la lectura, ya que se pueden emplear todos los discos en paralelo.

Cuenta con las siguientes ventajas:

- Se emplea para mejorar la velocidad de demanda y también la velocidad de transferencia.
- Se pueden recuperar los datos gracias a los discos de códigos de error.

Cuenta con los siguientes inconvenientes:

- Es una solución cara, ya que se requieren muchos discos para guardar los códigos de error.
- El tiempo de escritura de los datos es bastante lento, incluso aunque los datos se separen en los diferentes discos.

**RAID 3:** Sistema de discos en paralelo con disco de paridad para la corrección de errores.

Emplea múltiples discos para hacer el *striping* (como en el nivel *RAID 2*) pero sólo hace falta un disco para mantener la paridad.

Es una buena alternativa para aplicaciones de velocidad de transferencia alta, ya que, gracias a la distribución de los datos, se pueden emplear todos los discos en paralelo.

Cuenta con las siguientes ventajas:

- Buen rendimiento para aplicaciones de velocidad de transferencia alta.
- Gracias al disco de paridad, se pueden recuperar los datos.

Cuenta con los siguientes inconvenientes:

- Si se pierde el disco de paridad, se pierde toda la información redundante disponible.
- El tiempo de escritura de los datos es bastante lento.

**RAID 4:** Sistema de discos independientes con disco de control de errores.

Este nivel es parecido al *RAID 3*. Los bloques de datos se distribuyen en los diferentes discos por lo que se consigue un rendimiento superior en las escrituras.

Cuenta con las siguientes ventajas:

- Buen rendimiento en los escrituras de datos.
- Tiene integridad de datos.

Cuenta con los siguientes inconvenientes:

- Si se pierde el disco de paridad, se pierde toda la información redundante disponible.
- Menor rendimiento en las lecturas de datos.

**RAID 5:** Sistema de discos independiente con integración de códigos de error mediante una paridad.

En este nivel los datos y la paridad son guardados en los mismos discos, por lo que se consigue aumentar la velocidad de demanda, ya que cada disco puede satisfacer una demanda independientemente de los demás. A diferencia de *RAID 3*, guarda la paridad del dato dentro de los discos y no hace falta un disco para guardar dichas paridades.

Cuenta con las siguientes ventajas:

- La velocidad de transferencia de datos es alta
- No se desaprovecha un disco exclusivamente para paridad.
- Se pueden recuperar los datos.

Cuenta con los siguientes inconvenientes:

- El rendimiento en las escrituras de datos es bajo.
- No aumenta el rendimiento en las aplicaciones.

**RAID 6:** Sistema independiente de disco con integración de códigos de error mediante una doble paridad.

Es esencialmente una extensión del nivel *RAID 5* pero, además, guarda una segunda paridad. Este nivel proporciona muy buena integridad de los datos y repara diversos errores en los discos.

Cuenta con las siguientes ventajas:

- Se pueden recuperar diversos errores simultáneamente.
- El nivel de integridad es muy elevado. Es la solución idónea para aplicaciones críticas.

Cuenta con los siguientes inconvenientes:

- El rendimiento en escrituras de datos es bastante lento.
- No se dispone de muchas implementaciones comerciales de este nivel.

Términos RAID.

A continuación se describen distintos términos que se utilizan con *RAID*:

- **Duplex controler.** Son controladoras de disco que pueden trabajar de modo simple o de forma doble para que la carga de la controladora sea distribuida y más eficaz.
- **Hot swap.** Son discos que se reemplazan en caliente. Esto quiere decir que si alguno de los discos *RAID* se estropeara físicamente, bastaría con quitarlo y poner otro sin tener que apagar el sistema.
- **Hot spare.** Es un disco que permanece siempre en el sistema esperando a que uno se estropee y él entre directamente en funcionamiento.
- **Integridad de los datos.** Es la capacidad que tiene un disco de evitar un error de grabación, de corrupción o pérdida de datos. Para tal efecto, se tiene que seleccionar un disco *RAID* o una alternativa.
- **Mirroring (Espejo).** Es el nivel *RAID 1* que pasa por hacer una copia íntegra de un disco en otro.
- **Paridad.** Es una información redundante que se guarda para regenerar los datos perdidos por un error en el disco. La paridad se genera haciendo un *XOR* sobre los datos de los discos.
- **RAID (Redundat Array of Inexpensive Disk).** Conjunto de discos con información redundante de bajo costo.
- **Reconstrucción o regeneración.** Cuando un disco falla, la información redundante en los discos y los datos en los discos buenos son usados para regenerar la información del disco averiado.
- **Redundat Power Supplies.** Indica un sistema que consta de dos fuentes de alimentación. Si una se estropea, se pone en marcha la otra, pudiéndose cambiar la estropeada en caliente.
- **Sistemas basados en velocidad de demanda.** Son aquellos en los que se requiere un gran número de demandas de Entrada/Salida en el menor tiempo posible. Una alta velocidad de demanda es típica en sistemas multiusuario o en aplicaciones de bases de datos en las que se generan un gran número de pequeñas demandas de Entrada/Salida.

- **Sistemas basados en velocidad de transferencia.** Son aquellos en los que se intenta satisfacer una sola demanda con la máxima velocidad. Un claro ejemplo son las aplicaciones de ingeniería, científicas, imágenes, etc.
- **Striping (bandas).** Es el hecho de unir dos o más discos físicos en un solo disco lógico con el fin de dividir los datos entre los diferentes discos para ofrecer una significativa mejora en el rendimiento del conjunto de los discos.

## DISCOS BÁSICOS Y DINÁMICOS

*Windows 2000* soporta dos tipos de discos: **básicos** y **dinámicos**.

Ambos pueden existir en un mismo sistema pero un volumen (formado por uno o más discos físicos) debe utilizar únicamente uno de ellos.

Un **disco básico** es un disco físico que contiene particiones primarias, particiones extendidas, unidades lógicas o volúmenes básicos. Puede contener conjuntos de volúmenes, conjunto de espejos, conjunto de bandas con o sin paridad creados con *Windows NT 4 o anterior* y se puede acceder a ellos desde *MS-DOS* (no es posible crear estos conjuntos desde *Windows 2000*, únicamente se pueden borrar. Es posible convertirlos a tipos de volúmenes de los discos dinámicos). Puede utilizar los sistema de archivos: *FAT*, *FAT32* y *NTFS*. Es tipo de disco que se establece por defecto en la instalación.

Un **disco dinámico** es un disco físico que contiene volúmenes dinámicos creados con *Windows 2000*. No puede contener particiones o discos lógicos y no se puede acceder a ellos desde *MS-DOS*. Puede contener volúmenes distribuidos, volúmenes seccionados, volúmenes reflejados y volúmenes *RAID-5*. Puede utilizar únicamente el sistema de archivos *NTFS*.

En los *discos básicos*, un **conjunto de volúmenes** es la unión de una o más áreas de espacio disponibles (que pueden estar en uno o varios discos duros) que, a su vez, puede dividirse en particiones y unidades lógicas (no es reconocido por *MS-DOS*, sólo funciona con *NTFS*). Habrá una letra de unidad que representará al conjunto de volúmenes. Cuando se amplían, los datos previamente existentes no se ven afectados. Sin embargo, no es posible reducirlos si no que se deberá eliminar el conjunto completo (con la pérdida de los datos). El equivalente en los *discos dinámicos*, es un **volumen distribuido**.

En los *discos básicos*, un **conjunto de espejos** indica dos particiones de dos discos duros distintos que se configuran para que una sea idéntica a la otra. La partición espejo no aparece en el **Administrador de discos** y sólo sirve para reflejar los datos de la otra partición (que entrará en funcionamiento cuando la primera partición falle). Este método hace que el nivel de seguridad sea alto (aunque no se evitan los virus ya que estarían grabados en ambas particiones). Corresponde a **RAID 1**. El equivalente en los *discos dinámicos*, es un **volumen reflejado**.

En los *discos básicos*, un **conjunto de bandas** es la unión de dos o más áreas de espacio disponibles (que pueden estar en dos o más discos duros) que, a su vez, se dividirán en bandas. En cada disco duro se creará una partición y todas ellas tendrán aproximadamente el mismo tamaño (no es reconocido por *MS-DOS*, sólo funciona con *NTFS*). Habrá una letra de unidad que representará al conjunto de bandas. Pueden ser:

- **Sin paridad.** Un conjunto de bandas sin paridad dividirá cada uno de los discos duros en partes pequeñas llamadas bandas (así, si tiene cuatro discos duros y cada uno tiene diez bandas, diremos que hay diez filas de cuatro bandas cada una). Al guardar un archivo no lo hará como se describió en el conjunto de volúmenes si no que lo distribuirá en las bandas de todos los discos duros (ocupando la primera fila de bandas disponible de cada disco duro antes de pasar a la segunda). De esa manera, el acceso será más rápido ya que se elimina parte del tiempo que tarda el cabezal en buscar los sectores y las pistas donde se encuentra el archivo pero tiene el inconveniente que si se estropea un disco duro se pierde toda la información del conjunto de bandas. Ofrece mayor velocidad en el almacenamiento de los datos, ya que los datos se copian al mismo tiempo en los diferentes discos pero el nivel de seguridad es menor ya que cuando falla una banda, se perderán todos los datos. Corresponde a **RAID 0**. El equivalente en los *discos dinámicos*, es un **volumen seccionado**.
- **Con paridad.** Un conjunto de bandas con paridad utilizará una banda de cada fila del disco duro para guardar información de paridad de todas las bandas de esa fila (así, si tiene cinco discos duros y cada uno tiene diez bandas, diremos que hay diez filas de cinco bandas cada una y en cada fila hay una banda denominada de paridad). La información se guarda igual que en el conjunto de bandas sin paridad pero guardando, en la banda de paridad de cada fila, información que permitirá recuperar los datos de cualquier banda de dicha fila si dejará de funcionar. Cuando falla una banda se pueden recuperar los datos defectuosos que contenía aunque pierde velocidad de almacenamiento. Otro inconveniente que tiene es la disminución del espacio libre para guardar información en un porcentaje igual al número de discos duros que forman parte del conjunto de bandas con paridad (así, si hay cinco discos duros se perderá un 20% y si hay cuatro discos duros se perderá un 25%) y, también, que necesita mayor cantidad de memoria *RAM* para no ver disminuir el rendimiento del equipo (aproximadamente, un 25% más de memoria). Corresponde a **RAID 5**. El equivalente en los *discos dinámicos*, es un **volumen RAID-5**.

## La copia de seguridad de los datos

¿Qué ocurriría si por error, distracción, etc., se produce una pérdida de datos importante? Pues no pasaría nada si se cuenta con un buen sistema de copias de seguridad de dichos datos que permita restaurar la información prácticamente al mismo nivel que se encontraba antes de su pérdida.

Antes de empezar con la explicación sobre las posibles técnicas de copias de seguridad, es necesario determinar quién va a ser el responsable de su realización.

Algunos administradores de red dejan los procesos de copias de seguridad a usuarios individuales, lo que significa que cada uno de ellos se responsabiliza de guardar sus propios archivos.

Esta forma de actuar no es buena, ya que, los usuarios no dedican el tiempo ni la periodicidad necesaria para hacer la copia de seguridad adecuada de sus archivos.

Por tanto, es mucho más positivo que sea un administrador, como responsable de mantener el funcionamiento y mantenimiento del sistema, el que se encargue de las tareas de copias de seguridad o delegue en alguien que tenga los permisos necesarios (por ejemplo, los Operadores de copia).

## MÉTODOS DE REALIZAR COPIAS DE SEGURIDAD

Para realizar copias de seguridad se disponen de varios métodos:

- **Copia de seguridad diaria.** Se realiza con los archivos seleccionados que se hayan modificado en el día en que se realiza la copia de seguridad. Los archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.
- **Copia de seguridad diferencial.** Se realiza con los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.
- **Copia de seguridad incremental.** Se realiza con los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos se marcan como copiados y ya no podrán volver a respaldarse hasta que se modifiquen.
- **Copia de seguridad intermedia.** Se realiza con todos los archivos seleccionados. Dichos archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.
- **Copia de seguridad normal.** Se realiza con todos los archivos seleccionados. Dichos archivos se marcan como copiados y ya no podrán volver a respaldarse hasta que se modifiquen.

## ELEGIR ENTRE COPIAS DE SEGURIDAD O COPIADO DE ARCHIVOS

Hay dos tipos diferentes de protección de los datos:

- Las copias de seguridad.
- El copiado de archivos.

La diferencia básica entre ambos sistemas está en el motivo de su realización.

Normalmente se realiza una copia de seguridad del sistema para proteger los datos de los errores mecánicos y humanos. Las copias de seguridad protegen de los problemas de *hardware* como, por ejemplo, fallos en algún disco duro. También son útiles cuando se borran, sin darse cuenta, los archivos de datos o los programas.

El copiado de los archivos se realiza, sin embargo, para guardar ciertos archivos a lo largo del tiempo, de la misma forma que se guardan copias en papel.

Un buen procedimiento de copiado es una gran ayuda para gestionar el espacio en el disco duro, ya que hay archivos que no se necesitan de forma continuada y, sin embargo, están ocupando espacio en el disco.

Hay algunas normas que es aconsejable seguir:

- Respalde diariamente los archivos modificados.
- Respalde semanalmente el sistema entero.
- Copie mensualmente los archivos.

## El respaldo diario de los archivos

El proceso del respaldo de los archivos casi siempre necesita bastante tiempo para su realización. Por tanto, es conveniente que sólo realice el respaldo diario de los archivos que hayan sido modificados.

Primero, deberá determinar cuáles son los archivos que deben respaldarse. Por lo general, los programas de aplicaciones y del sistema operativo no suelen sufrir variaciones y, por tanto, no necesitan respaldarse diariamente.

En cambio, los archivos de datos y de configuración de los programas o del sistema operativo son los que sufren variaciones, por tanto deberá respaldarlos diariamente.

Para poder localizar fácilmente la copia de seguridad realizada en último lugar, es muy recomendable poner en cada una de ellas la fecha y la hora en que se realizó.

## El respaldo semanal del sistema completo

Este método consiste en realizar una copia de seguridad normal de todo el contenido del ordenador y, al igual que el respaldo diario, es recomendable que se realice en unidades de cinta.

De este modo, en caso de tener que restaurar el contenido del ordenador se realizará de forma fácil y rápida.

Es el método más adecuado, porque permite tener pocas copias y, de esa forma, poder encontrar fácilmente la adecuada.

### El copiado mensual de los archivos

Por lo general, el copiado de los archivos es suficiente que se realice una vez al mes. Asegúrese de que tiene copiados los archivos en un medio o soporte diferente (cinta, disco, disquete) que las copias de seguridad, para que en caso de pérdida o deterioro de la cinta pueda recuperar la información.

El objetivo del copiado es distinto al del respaldo de los archivos, por lo que tendrá que seguir diferentes procedimientos, entre los cuales se encuentran:

- Determine qué directorios y archivos son los que van a copiarse.
- Determine si los archivos van a ser borrados después de ser copiados.
- Es recomendable que comprima los archivos antes de copiarlos, ya que reducirá el espacio de almacenamiento y el tiempo que tardará en realizarse el proceso.
- Saque un listado de los archivos que se han copiado.
- Guarde en lugar seguro las copias de los archivos.

### ELECCIÓN DEL HARDWARE DE COPIA DE SEGURIDAD

En ordenadores con discos duros de gran capacidad, el mejor dispositivo para el respaldo del sistema es una unidad de cinta.

Las unidades de cinta son más rápidas y producen mejores resultados que otros métodos, ya que no requieren discos duros ni disquetes.

Existen varios formatos de cinta que se pueden usar para hacer respaldos de una red. Entre ellos se encuentran:

#### El formato DC-6000

Este formato es el más antiguo de ellos (fue creado por **3M** en 1971), así como el de mayor tamaño.

Su capacidad se ha ido incrementando en función de tres valores: la longitud de la cinta (puede llegar hasta un máximo de 600 pies), la densidad (**bits por pulgada**) de la cinta y el número de pistas.

Con los últimos avances tecnológicos puede llegarse a **2 GB** (usando 30 pistas con una densidad de **68 kilobits** por pulgada).

Es fiable el resultado del respaldo pero lento (aproximadamente **5 MB** por minuto). Así mismo, la búsqueda de un fichero en la cinta es secuencial por lo que habrá que buscar en la cinta entera para conseguir encontrarlo.

El nombre de las cintas indica su capacidad. Por ejemplo, la cinta **DC-6525**, indica que tiene una capacidad de **525 MB**.

#### El formato DC-2000

Este formato, de tamaño algo más pequeño que el anterior, también fue diseñado por **3M**.

Se utiliza principalmente para hacer respaldos de discos duros de pequeño tamaño.

Su capacidad ha ido en aumento y puede llegar a guardar **420 MB** de datos sin comprimir (**850 MB** si están comprimidos).

#### El cartucho 8 mm

Este formato fue desarrollado por **Exabyte** y está basado en la tecnología desarrollada por **Sony** para sus cámaras de vídeo.

Usa el mismo cartucho que el de las cámaras de vídeo de 8 mm aunque su medio magnético es de mejor calidad.

Su capacidad ha ido en aumento y puede llegar a guardar **5 GB** de datos sin comprimir (**10 GB** si están comprimidos).

#### El cartucho 4 mm

Este formato está derivado del formato **DAT** desarrollado por **Sony**.

La densidad de la cinta es muy alta y su velocidad de transferencia de datos puede llegar hasta **30 MB** por segundo.

Su capacidad de datos es muy grande y puede duplicarse si están comprimidos los datos.

La búsqueda de datos es muy rápida y el coste del **hardware** es relativamente bajo.

Por todo ello, este formato es, actualmente, el más usado para realizar respaldos en discos duros de gran tamaño.

1° SISTEMA	DIARIO	ARCHIVOS MODIFICADOS	CINTA
2° SISTEMA	SEMANAL	SISTEMA COMPLETO	CINTA
3° SISTEMA	MENSUAL	ARCHIVOS NO MODIFICADOS EN EL ÚLTIMO MES	DISCO O DISQUETES

## LA PROTECCIÓN DE ACCESO AL ORDENADOR

Para la protección de acceso al ordenador existen varias posibilidades:

- Protección por contraseña en la CMOS.
- Protección por contraseña en el sector de arranque.
- Protección por contraseña en archivos de arranque.

### Protección por contraseña en la CMOS

La protección por contraseña en la CMOS (es una pequeña memoria RAM en la que se encuentra almacenada la configuración del ordenador y se mantiene por una pila recargable por lo que no se pierde cuando el ordenador se apaga) se ejecuta cuando se arranca el ordenador y se ha realizado el chequeo correspondiente. Si no se conoce esta contraseña, no se cargará el sistema operativo (ni desde el disco duro ni desde un disco flexible) y el ordenador quedará bloqueado. Para indicar la contraseña se ha de hacer desde el SETUP correspondiente.

### Protección por contraseña en el sector de arranque

La protección por contraseña en el sector de arranque permite que el ordenador solicite una contraseña del mismo modo que la opción descrita en el apartado anterior. Esta opción se ha de realizar por software y únicamente se ha de utilizar cuando el ordenador no incorpore una opción para hacerlo desde el SETUP correspondiente.

### Protección por contraseña en archivos de arranque

La protección por contraseña en archivos de arranque se ha de hacer con programas instalados y que se ejecuten al procesar los archivos CONFIG.SYS o AUTOEXEC.BAT.

Este método prácticamente no sirve para nada ya que la ejecución de estos archivos puede ser bloqueada fácilmente por cualquier usuario.

## LA PROTECCIÓN DE ACCESO A LOS DATOS

Dentro de la protección de acceso a los datos se encuentran cuatro opciones:

- Autenticación del usuario.
- Protección de directorios y/o archivos.
- Encriptación de los datos.
- Auditorías.

### La autenticación del usuario

El contenido de la mayoría de las comunicaciones de una *Intranet*, como son la navegación por las páginas *Web* o los foros públicos de charlas, puede ser seguido por cualquiera que tenga el equipo necesario para ello. El contenido de otras transmisiones de datos como, por ejemplo, el intercambio de información relativa a las tarjetas de crédito utilizadas en las compras en línea, debe ser privado.

Las transmisiones de datos se consideran privadas y seguras siempre que se cumplan dos condiciones:

- Autenticación. El receptor de los datos sabe que el remitente es exactamente quién dice ser o lo que dice ser.
- Cifrado. Los datos enviados están cifrados de modo que sólo puede leerlos el destinatario interesado.

La criptografía de clave pública es un método muy utilizado para mantener la privacidad y seguridad de las transmisiones de datos por *Internet*.

### PARES DE CLAVES

La autenticación y el cifrado se facilitan mediante pares matemáticamente relacionados de códigos digitales o **claves**. Una de las claves de cada par se divulga públicamente, mientras que la otra se mantiene en el más estricto secreto.

A todos los transmisores de datos, ya se trate de una persona, un programa de *software* u otra entidad, se les distribuye un par de claves mediante un sistema de criptografía de clave pública.

Las claves son generadas por el sistema de criptografía y se utilizan combinadas.

### Clave pública

El sistema de criptografía comunica la **clave pública** a cualquier parte que necesite validar la firma de un propietario de un par de claves o establecer comunicación privada con él.

Las partes que soliciten comunicación privada con el propietario del par de claves utilizan programas de *software* con criptografía habilitada y su clave pública para:

- Validar (descifrar) la firma del propietario del par de claves.
- Cifrar datos para transmitirlos al propietario del par de claves.

### Clave privada

El propietario del par de claves, o un sistema de criptografía que esté actuando en su nombre, vigila estrechamente esta clave.

El propietario del par de claves utiliza programas de *software* con criptografía habilitada y su **clave privada** para:

- Firmar (cifrar) datos.
- Descifrar datos cifrados con su clave pública.

### ESTABLECIMIENTO DE UNA RELACIÓN DE CONFIANZA

En caso de que el remitente y el receptor se conozcan y confíen el uno en el otro, pueden sencillamente intercambiar claves públicas y establecer una transmisión de datos segura, con autenticación y cifrado. Para ello, utilizarían sus respectivas claves públicas y sus propias claves privadas.

No obstante, en circunstancias normales, lo habitual es que las partes que necesiten efectuar transmisiones de datos de forma segura no tengan en qué basarse para confiar en sus respectivas identidades. Para comprobar sus respectivas identidades, cada una de las partes necesita una tercera parte que demuestre su identidad.

### AUTORIDADES CERTIFICADORAS

Aquella parte que necesite probar su identidad en la criptografía de clave pública debe obtener los servicios de una tercera parte fiable, denominada **Autoridad certificadora (CA)**.

La principal finalidad de la CA es comprobar que el usuario es quién o lo que dice ser y emitir a continuación un **certificado de clave pública** para que pueda utilizarlo. El certificado de clave pública demuestra que la clave pública que incluye pertenece al usuario cuyo nombre figura en el certificado.

Una vez que se ha establecido la identidad de la parte solicitante a través de la CA, ésta emite un certificado electrónico y le aplica su **firma digital**.

### CERTIFICADO DE CLAVE PÚBLICA

Los **certificados de clave pública** se pueden emitir para una gran variedad de funciones: la autenticación de usuarios *Web*, autenticación de servidores *Web*, correo electrónico seguro (*S/MIME*), Seguridad de IP (*IPSec*), Seguridad del nivel de transacción (*TLS*) y firma de código.

Los certificados también son emitidos de una entidad emisora de certificados a otra con el fin de establecer una **jerarquía de certificados**. La entidad que recibe el certificado se denomina como **sujeto del certificado**. El emisor y firmante del certificado se conocen como **entidad emisora de certificados**. La mayor parte de los certificados utilizados en la actualidad se basan en el estándar *X.509* que constituye la tecnología básica utilizada en la **infraestructura de claves públicas (PKI)**.

Normalmente, los certificados contienen la información siguiente:

- Valor de la clave pública del sujeto.
- Información del identificador del sujeto, como su nombre y dirección de correo electrónico.
- Período de validez (el período durante el que se considera válido el certificado).
- Información del identificador del emisor.
- La firma digital del emisor, que da fe de la validez del enlace entre la clave pública del sujeto y la información del identificador de sujeto.

Un certificado es válido sólo para el período especificado en éste; cada certificado contiene las fechas de expedición y caducidad, que marcan el límite del período de validez. Una vez que el período de validez del certificado ha transcurrido, el sujeto del certificado caducado debe solicitar un certificado nuevo.

En los casos en que sea necesario deshacer el enlace autenticado en un certificado, el emisor puede revocarlo. Cada emisor mantiene una **lista de certificados revocados (CRL)** que los programas pueden utilizar al comprobar la validez de un certificado determinado.

Una de las ventajas principales de los certificados es que los equipos ya no tienen que mantener ningún conjunto de contraseñas para sujetos individuales que necesiten como requisito previo autenticarse para tener acceso. Por el contrario, el equipo, simplemente, establece la confianza en un emisor de certificados.

Cuando un equipo, como un servidor *Web* seguro, designa a otro equipo como **entidad emisora raíz de confianza**, es porque confía de forma implícita en las directivas que el emisor utiliza para establecer los enlaces de los certificados que emite (por ejemplo, confía en que el emisor ha comprobado la identidad del sujeto del

certificado). Para designar a un emisor como entidad raíz de confianza, un equipo coloca el certificado firmado por el propio emisor que contiene la clave pública del emisor en el **almacén de certificados** de la entidad emisora de certificados raíz del equipo. Se confía en las **entidades emisoras subordinadas** o intermedias únicamente si disponen de una ruta de acceso de certificados válida de una entidad emisora de certificados raíz de confianza.

## FIRMA DIGITAL

Del mismo modo que una firma personal aplicada a un documento en papel demuestra la autenticidad de dicho documento, una **firma digital** demuestra la autenticidad de los datos electrónicos.

Para crear una firma digital, el *software* utilizado asocia los datos que se firman a la clave privada del firmante.

Una firma digital está vinculada de forma exclusiva al firmante y a los datos. Nadie puede duplicar la firma ya que nadie más conoce la clave privada del firmante. Además, el firmante no puede negar haber firmado los datos. Esto se denomina **imposibilidad de repudio**.

Cuando una **Autoridad certificadora** firma un certificado de clave pública, garantiza que se ha verificado la identidad del propietario de la clave pública conforme a las directivas establecidas y difundidas por la CA.

Una vez recibidos los datos firmados (como el certificado de clave pública) el *software* comprueba su autenticidad aplicando a los datos el mismo cálculo que el *software* utilizó en un principio. Si los datos no han sufrido modificaciones, los dos cálculos darán idénticos resultados. A partir de ese momento puede asumirse sin riesgo alguno que ni los datos ni la firma han sido modificados durante la transmisión.

## La protección de directorios y/o archivos

Cuando un usuario crea un directorio, un archivo o un objeto, se convierte automáticamente en su propietario (también durante el proceso de instalación se adjudicaron propietarios a todos los directorios y archivos que se crearon).

Un propietario puede asignar permisos a sus directorios, archivos u objetos aunque no puede transferir su propiedad a otros usuarios (en algunos sistemas operativos, se puede conceder el permiso **Tomar posesión** que permitirá, a los usuarios que se les conceda, tomar posesión en cualquier momento. También, pueden tomar posesión los **administradores** pero no pueden transferirla a otros usuarios. De esta manera, un administrador que tome posesión y cambie los permisos podrá acceder a los archivos que no tienen concedido ningún permiso).

Para ver quién ha infringido los permisos asignados, puede comprobar la información de posesión (auditoría).

## La encriptación de los datos

El **Sistema de archivos de cifrado (EFS)** de *Windows 2000* permite a los usuarios almacenar sus datos en el disco de forma cifrada.

El **Cifrado** es el proceso de conversión de los datos a un formato que no lo puede ser leído por otro usuario (cuando un usuario cifra un archivo, éste permanece automáticamente cifrado mientras esté almacenado en un disco).

El **Descifrado** es el proceso de reconversión de los datos de un formato cifrado a su formato original (cuando un usuario descifra un archivo, éste permanece descifrado mientras esté almacenado en un disco).

Los administradores pueden recuperar datos cifrados por otro usuario (de esta forma, se asegura la accesibilidad a los datos si el usuario que los cifró ya no está disponible o ha perdido su clave privada).

Sólo se pueden cifrar archivos y directorios en volúmenes de unidades formateadas para ser usadas por el sistema NTFS.

No se pueden cifrar las carpetas ni los archivos que estén comprimidos ni los archivos del sistema.

Cuando se cifra un directorio, el sistema preguntará si se desea que se cifren también todos los archivos y subcarpetas de la carpeta seleccionada. Si se decide hacerlo, se cifrarán todos los archivos y subcarpetas que se encuentren en dicha carpeta, así como los archivos y subcarpetas que se agregue posteriormente a ella (si se cifra sólo la carpeta, no se cifrarán los archivos ni las subcarpetas que contenga pero se cifrarán todos los archivos y subcarpetas que se agreguen posteriormente a ella).

Cuando se cifra un archivo, el sistema preguntará si se desea que se cifre también el directorio que lo contiene. Si decide hacerlo así, se cifrarán todos los archivos y subcarpetas que se agreguen posteriormente a la carpeta.

**NOTA.** Los programas que crean archivos de trabajo temporales pueden comprometer la seguridad del cifrado de archivos. Si utiliza algún programa de ese tipo, aplique el cifrado en las carpetas y no en los archivos individuales.

## Las auditorías

Las **auditorías** permiten supervisar los sucesos relacionados con la seguridad del equipo.

Los tipos de sucesos más comunes que se pueden auditar son:

- El acceso a objetos, como archivos y carpetas.
- La administración de cuentas de usuarios y de grupos.

- El inicio y finalización de sesión de los usuarios.
- Los servicios de impresión.

En cada uno de los sucesos auditados se genera un registro de seguridad que se puede visualizar (en *Windows NT 4* y *Windows 2000* se ha de hacer con el *Visor de sucesos*).

Ahora se describirán brevemente las distintas auditorías en *Windows 2000*.

## AUDITAR SUCESOS DE SEGURIDAD

El establecimiento de auditorías es un aspecto importante en la seguridad del equipo, ya que permite controlar la creación o la modificación de objetos, hacer un seguimiento de los problemas de seguridad potenciales, ayuda a asegurar la responsabilidad del usuario y proporciona pruebas en caso de una infracción en la seguridad.

Los pasos principales para implementar la auditoría de seguridad en un equipo son:

1. Activar las categorías de los sucesos que se desean auditar.
2. Habilitar la auditoría.
3. Definir el tamaño y el comportamiento del registro de seguridad.
4. Si se ha seleccionado la categoría de auditoría de acceso a servicios de directorios o la categoría de acceso a objetos, se deben determinar los objetos a los que se desean controlar el acceso y modificar los descriptores de seguridad correspondientes.

## DIRECTIVA DE AUDITORÍA

Una **directiva de auditoría** especifica las categorías de sucesos relacionados con la seguridad que se desean auditar.

Las categorías de sucesos que pueden auditar son:

- Auditar el acceso a objetos.
- Auditar el acceso a servicio de directorio.
- Auditar el cambio de directivas.
- Auditar el seguimiento de procesos.
- Auditar el uso de privilegios.
- Auditar la administración de cuentas.
- Auditar los sucesos de inicio de sesión.
- Auditar los sucesos de inicio de sesión de cuenta.
- Auditar los sucesos del sistema.

Si se activa **Auditar el acceso a objetos** y es un servidor controlador de dominio, se debe activar también **Auditar el acceso del servicio de directorio**.

## AUDITAR EL ACCESO A OBJETOS

Cada objeto dispone de un conjunto de información de seguridad (**descriptor de seguridad**). Una parte del descriptor de seguridad indica los grupos o usuarios que tienen acceso a un objeto, así como los permisos concedidos (o denegados) a dichos grupos o usuarios. Esta parte de los descriptores de seguridad se conoce como **lista de control de acceso discrecional (DACL)**.

Sin embargo, además de contener información de permisos, un descriptor de seguridad para un objeto también contiene información de auditoría. A esta información de auditoría se le conoce como **lista de control de acceso de sistema (SACL)** e indica:

- Las cuentas de grupo o usuario que se van a auditar al tener acceso a un objeto.
- Los sucesos de acceso que se van a auditar para cada grupo o usuario.
- Un atributo **Éxito** o **Error** para cada suceso de acceso, en función de los permisos concedidos a cada grupo y usuario de la *DACL* del objeto.

En general, los tipos de acceso que se pueden auditar dependen de si se audita el acceso a archivos y carpetas o a objetos del *Directorio Activo*.

Para establecer la auditoría del acceso a objetos, se ha de habilitar desde la **Directiva de grupo** correspondiente.

## ARCHIVOS Y CARPETAS

Se puede auditar el acceso a archivos y carpetas en volúmenes *NTFS* para identificar quién ha realizado varios tipos de acciones con los archivos y carpetas.

Se han de especificar los archivos y carpetas que se van a auditar, el usuario cuyas acciones se van a auditar y los tipos de acciones que se van a auditar (se puede aplicar la auditoría a un objeto y, a través de herencia, aplicarse a cualquier objeto secundario).

### Tipos de acceso a carpetas

Recorrer carpeta.  
Listar carpeta.  
Atributos de lectura.  
Atributos extendidos de lectura.  
Crear archivos.  
Crear carpetas.

### Tipos de acceso a archivos

Ejecutar archivo  
Leer datos.  
Atributos de lectura.  
Atributos extendidos de lectura.  
Escribir datos.  
Anexar datos.

**Tipos de acceso a carpetas**

Atributos de escritura.  
 Atributos extendidos de escritura.  
 Eliminar subcarpetas y archivos.  
 Eliminar.  
 Permisos de lectura.  
 Cambiar permisos.  
 Tomar posesión.

**Tipos de acceso a archivos**

Atributos de escritura.  
 Atributos extendidos de escritura.  
 Eliminar archivos.  
 Eliminar.  
 Permisos de lectura.  
 Cambiar permisos.  
 Tomar posesión.

Para especificar los archivos y los tipos de acceso a archivos que van a auditarse, se ha de utilizar el **Explorador de Windows**.

**OBJETOS DEL DIRECTORIO ACTIVO**

Para auditar objetos del *Directorio Activo*, también puede auditar las siguientes acciones:

- Leer y escribir todas las propiedades.
- Leer y escribir propiedades individuales (hay varias propiedades individuales).

**Kerberos V5**

**Kerberos V5** es el protocolo de seguridad principal para la autenticación dentro de un dominio. Comprueba la identidad del usuario y los servicios de red. Esta comprobación dual se denomina **autenticación mutua**.

El mecanismo de autenticación de *Kerberos V5* emite vales para tener acceso a los servicios de red. Estos vales contienen datos cifrados que incluyen una contraseña cifrada para confirmar la identidad del usuario al servicio solicitado. Exceptuando la escritura de una contraseña o las credenciales de tarjeta inteligente, todo el proceso de autenticación es transparente para el usuario.

El **Centro de distribución de claves (KDC)** que se ejecuta en cada controlador de dominio como parte del *Directorio Activo*, se utiliza para almacenar todas las contraseñas del cliente y otros datos de su cuenta.

El proceso de autenticación *Kerberos V5* funciona de la manera siguiente:

1. Un usuario de un sistema cliente se autentifica en el *KDC* mediante una contraseña o tarjeta inteligente.
2. El *KDC* emite al cliente un **vale especial que concede vales (TGT)**. El sistema de cliente utiliza este *TGT* para tener acceso al **servicio de concesión de vales (TGS)** que forma parte del mecanismo de autenticación *Kerberos V5* en el controlador de dominio.

3. El *TGS* emitirá al cliente un **vale de servicio**.
4. El cliente presenta este vale de servicio al servicio de red solicitado. El vale de servicio prueba la identidad del usuario al servicio y la identidad del servicio al usuario.

*Kerberos V5* se utiliza como el método de autenticación predeterminado de *IPSec (Windows 2000)*.

**KERBEROS V5 Y LOS CONTROLADORES DE DOMINIO**

Los servicios de *Kerberos V5* en *Windows 2000* se instalan en cada controlador de dominio y, también, se instala un cliente de *Kerberos* en cada estación de trabajo o servidor de *Windows 2000*.

Cada controlador de dominio funciona como un *KDC*. Un sistema con *Windows 2000* utiliza *DNS* para localizar el controlador de dominio disponible más cercano. Este controlador de dominio funcionará como el *KDC* preferido para ese usuario durante el inicio de sesión del usuario. Si el *KDC* preferido deja de estar disponible, *Windows 2000* localizará un *KDC* alternativo para proporcionar la autenticación.

**INTEROPERABILIDAD DE KERBEROS V5**

*Windows 2000* admite dos tipos de interoperabilidad de *Kerberos V5*.

- Se puede establecer una relación de confianza entre un dominio y un dominio de *Kerberos* basado en *MIT* (de esta manera, un cliente de un dominio de *Kerberos* se puede autenticar en un dominio del *Directorio Activo* para tener acceso a los recursos de red del dominio).
- En un dominio, los clientes y los servidores *UNIX* pueden tener cuentas del *Directorio Activo* y, por tanto, pueden ser autenticados desde un controlador de dominio.