Tema 8°: SEGURIDAD EN UNA LAN

1. *Conceptos generales*
2. *Seguridad física del servidor*
3. *La seguridad de los datos*
4. *La protección de acceso al ordenador*
5. *La protección de acceso a los datos*
6. *La protección de los datos*
7. *Las auditorías*

8.1.- Conceptos generales.-

La seguridad en una red local debe contemplar la problemática relacionada con el acceso indebido de recursos y aplicaciones de los usuarios, así como la debida a fallos del sistema, y también, simplemente, la alimentación del mismo.

Para garantizar la seguridad de la red local, el administrador de la misma debe aplicar distintas medidas de seguridad, que se engloban en el concepto de ***seguridad del servidor,*** del que pueden distinguirse cuatro apartados:

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

Por otro lado, los problemas de seguridad en redes, en relación con el exterior a una red determinada, pueden dividirse, en términos generales, en cuatro áreas interrelacionadas:

- *Secreto*
- *Validación de identificación*
- *No repudio*
- *Control de integridad*

El ***secreto*** tiene que ver con mantener la información fuera de las manos de usuarios no autorizados, es decir, es lo que normalmente se piensa cuando se afronta el tema de seguridad en las redes. La ***validación de identificación*** se encarga de determinar con quien se está hablando antes de revelar una información delicada. El ***no repudio*** se encarga de validar las *firmas*. Por último, el ***control de integridad*** se corresponde con la necesidad de asegurarse de que un de que un mensaje recibido realmente fue el enviado y que no ha sufrido ninguna modificación en el camino.

A lo largo de este capítulo se afrontará, de forma separada, las dos vertientes: seguridad en el ámbito de redes de área local y la protección de dicha red en su conexión con el exterior.

8.2.-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.

8.2.1.-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 moqueta con productos antiestáticos, utilizar fundas protectoras para ambas e instalar el servidor a 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 entre 18°C y 26°C y asegurar una buena aireación.

8.2.2.-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 eléctrica del ordenador. Para proteger al servidor contra los ruidos eléctricos, puede recurrirse a una línea dedicada de suministro eléctrico. No deben entonces conectarse otros dispositivos a este suministro de corriente dado que pueden generar ruidos que anulen las ventajas de la protección ofrecida por la fuente dedicada. La conexión a la fuente de energía ha de hacerse siempre con un cable estándar de tres hilos conectando a tierra el hilo correspondiente.

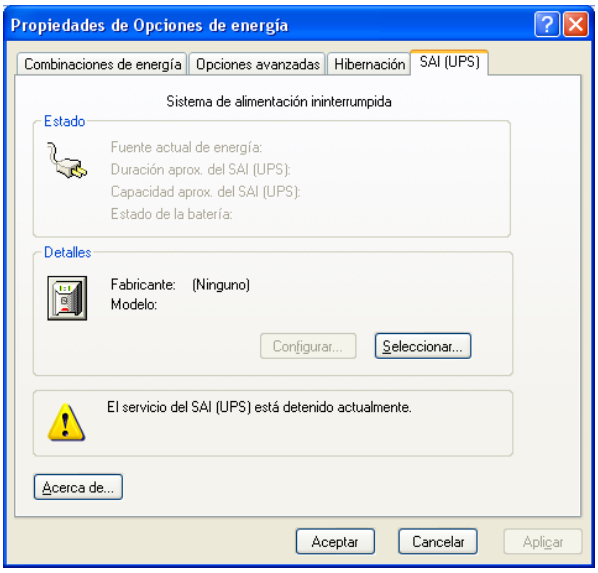
La prevención contra altibajos de tensión y cortes de corriente suele reealizarse mejorando la instalación con ***Sistemas de alimentación ininterrumpida*** (SAI) o en***UPS (Uninterrumpible Power Suply)*** que permiten al servidor continuar activo durante un cierto tiempo ante un eventual corte de la corriente.

Clientes con aplicaciones críticas deberían, asimismo, disponer de SAI para evitar pérdidas de datos durante un corte de energía.

Por último cada dispositivo de red debería disponer de un filtro o ***estabilizador de corriente*** como protección a las sobretensiones.

Si se dispone de un Sistema de Alimentación Ininterrumpida, éste puede configurarse, para su uso en Windows 2000, ejecutando el icono ***Opciones de Energía*** del ***Panel de control*** obteniéndose la pantalla adjunta al seleccionar la pestaña SAI (UPS).

Otros factores externos que, por obvios no se comentan son la ***suciedad,*** la posibilidad de ***incendios o inundaciones*** y el ***robo*** o la ***destrucción intencionada***.



8.3.- La seguridad de los datos

Es importante que los datos que están ubicados en el servidor de la red se encuentren bien protegidos. Para ello deben considerarse los siguientes apartados:

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

8.3.1.- La seguridad del almacenamiento en el disco duro

La unidad básica de almacenamiento de la información es el disco duro. La forma mas común de organizar el almacenamiento de la información es a través de un único disco duro, aunque, dependiendo del tamaño de la empresa, debe considerarse la posibilidad de trabajar con mas de un disco duro asociado.

Cada disco duro del sistema tiene asignado un número (comenzando desde 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 de un total de 28 unidades).

- **IDE y ESDI.** En una controladora primaria de estos dos tipos, los números van de cero al uno. Cuando esta controladora se completa puede recurrirse a una segunda controladora (lo que permitiría un total de hasta 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 utilizado 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 son reconocidas 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 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 sistemas operativos para su arranque (cada uno deberá estar en su propia partición primaria).

- **Particiones secundarias o extendidas** 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 este caso, el disco duro no podrá tener mas de tres particiones primarias).

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

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 pueden dividirse 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.

Sistemas de archivos

Puede escogerse entre varios sistemas de archivos distintos para el disco duro, por ejemplo:

- **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 inferiores a 2 GB y no soporta dominios.

- **FAT32**. Se puede acceder a este sistema de archivos desde Windows 95, 98, 2000 y XP y OS/2. Permite trabajar con particiones mayores de 2 GB, el tamaño máximo de un archivo es 4 GB, los volúmenes pueden tener 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 archivos 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 de disco para cada usuario, compresión y encriptación de archivos, almacenamiento remoto, una herramienta de defragmentación y el sistema de archivos distribuidos (DFS). Sus volúmenes pueden sobrepasar los 2 TB y el tamaño de un archivo sólo está limitado por el tamaño del volumen.

Se define como **Integridad de los datos** a la capacidad que tiene un disco de evitar un error de grabación, de corrupción o de pérdida de datos.

Se llama **Paridad** a la 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.

8.3.2.-Sistemas RAID

RAID es un conjunto de dos o mas 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 de 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 los datos se hace desde el software, aunque se pueden utilizar controladoras RAID que sí regenerarían automáticamente los datos).
- La capacidad global del disco aumentará, ya que se suman las capacidades de los diferentes discos que componen el conjunto.

Se suelen considerar hasta siete niveles RAID, los cuales ofrecen grandes diferencias entre rendimiento e integridad de los datos, dependiendo de las especificaciones de cada nivel:

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 se define normalmente como *striping*. Sus ventajas son:

- Alto rendimiento
- No tiene coste adicional
- Emplea toda la capacidad del disco

Sus inconvenientes son:

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

RAID 1: Conjunto de discos en espejo

Este nivel se conoce 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.

Sus ventajas son:

- Mayor rendimiento en las lecturas de datos respecto a un disco convencional
- Recuperación de los datos en caso de error en uno de los discos

Sus inconvenientes son:

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

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

Emplea múltiples discos como el RAID 0 pero alguno de estos discos son empleados para códigos de error, que los emplea para referencia de los datos en el caso de que falle uno de los discos. Este nivel tiene un coste bastante elevado ya que se necesitan muchos discos para mantener los códigos de error. Al estar distribuidos los datos en varios discos se consigue mejorar la velocidad de transferencia, principalmente en la lectura, ya que se pueden emplear todos los discos en paralelo.

Sus ventajas son:

- 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

Sus inconvenientes son:

- Es una solución cara ya que se requieren muchos discos para guardar los códigos de error
- El tiempo de escritura de 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 de 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.

Sus ventajas son:

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

Sus inconvenientes son:

- 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

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

Sus ventajas son:

- Buen rendimiento en las escrituras de datos
- Tiene integridad de datos

Sus inconvenientes son:

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

Sus ventajas son:

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

Sus inconvenientes son:

- 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.

Sus ventajas son:

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

Sus inconvenientes son:

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

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, FATS2 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-S. 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 RAID1. 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 falta una banda, se perderán todos los datos. Corresponde a RAID O. 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 dejara de funcionar. Cuando falta 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**.

8.3.3.- Copias de seguridad de los datos

Se entiende por ***copia de seguridad*** (Back Up) de los datos introducidos en el sistema de almacenamiento masivo de un servidor a la copia fiel, obtenida en un medio de almacenamiento externo (cintas magnéticas , discos ópticos, disquetes, etc.) con el fin de prevenir cualquier incidencia ocurrida en el servidor.

En general, el responsable de la realización de copias de seguridad es el administrador de la red, la cual puede delegar en alguien te tenga los permisos adecuados para ello (por

ejemplo, los operadores de copia) no siendo una buena política la de permitir que usuarios individuales realicen la salvaguarda de sus propios archivos.

Tipos de protección de datos

Hay dos tipos diferentes de protección de datos:

- Las copias de seguridad
- El copiado de archivos

La diferencia básica entre ambas 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 útilies cuando se borran, por descuido, los archivos de datos o los programas.

El *copiado de 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 de una gran ayuda para gestionar el espacio del disco duro, ya que hay archivos que no se necesitan de forma continuada y, sin embargo est{an ocupando espacio en el disco.

Métodos de realizar copias de seguridad

Para realizar copias de seguridad pueden utilizarse varios métodos:

- **Copia de seguridad diaria:** Se realiza con los archivos seleccionados que se haya modificado en el día en que se realiza la copia de seguridad. Los archivos no se marcan como copiados para que puedan volver a ser respaldados 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 ser respaldados 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 para que no puedan volver a ser respaldados 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 ser respaldados cuando se desee.

- **Copia de seguridad normal:** Se realiza con todos los archivos seleccionados. Los archivos se marcan como copiados para que no puedan volver a ser respaldados hasta que se modifiquen

En general son normas que se aconseja seguir:

- Respaldar diariamente los archivos modificados
- Respaldar semanalmente el sistema entero
- Copiar mensualmente los ficheros de datos

8.4.- Protección de acceso al ordenador

Para la protección de acceso al ordenador existen varias posibilidades:

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

Protección por contraseña CMOS

La protección por contraseña en la CMOS (pequeña memoria RAM en la que se encuentra almacenada la configuración del ordenador y se mantiene mediante la energía de una pila recargable, por lo que no se pierde cuando se apaga el ordenador) 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 disco duro ni desde disquete ni desde CD-ROM) y el ordenador quedará bloqueado.. Para indicar la contraseña ha de hacerse 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 realiza mediante el software y únicamente debe utilizarse 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.

8.5.- La protección de acceso a los datos

Dentro de la protección de acceso a los datos se centra fundamentalmente en la autentificación del usuario.

La autentificación 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:

- **Autentificación:** 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 autentificación 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 mas 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 una 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 reconozcan y confíen el uno en el otro, pueden sencillamente intercambiar claves públicas y establecer una transmisión de datos segura, con autentificación 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: autentificación de usuarios Web, autentificación de servidores web, correo electrónico seguro (S/MIME), seguridad IP (IPSec), seguridad de 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 de certificado.** El emisor firmante del certificado se conoce 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 (período en 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 del 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 autentificado 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 autentificarse 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 que 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 un emisor como una entidad raíz de confianza, un equipo coloca un 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 válidas 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, la **firma digital** demuestra la autenticidad de los datos electrónicos.

Para crear la 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 la **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 la 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 pueden asumirse sin riesgo alguno que ni los datos ni la firma han sido modificados durante la transmisión.

8.6.- La protección de los datos

La protección de los datos se fundamenta en las siguientes opciones:

- *Protección de directorios y/o archivos*
- *Encriptación de los datos*
- *Auditorías*

Protección de directorios y/o archivos

Cuando un usuario crea un directorio, un archivo o un objeto se convierte automáticamente en su propietario.

Un propietario puede asignar permisos a sus directorios, archivos u objetos aunque no puede transferir la 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 quien ha infringido los permisos asignados el administrador puede comprobar la información de posesión (auditoría).

La encriptación de los datos

El **Sistema de archivos de cifrado** (EFS) dc 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.

8.7.- Las auditorías

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

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

- El acceso a objetos como archivos y carpetas
- La administración de cuentas de usuario y de grupos.
- El inicio y finalización de sesión de 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 y Windowes 2000* se ha de hacer con el **visor de sucesos**).

A continuación se describen 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:

- Activar las categorías de los sucesos que se desean auditar.
- Habilitar la auditoría.
- Definir el tamaño y el comportamiento del registro de seguridad.
- 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	**Tipos de acceso a archivos**
Recorrer carpeta.	Ejecutar archivo
Listar carpeta.	Leer datos.
Atributos de lectura.	Atributos de lectura.
Atributos extendidos de lectura.	Atributos extendidos de lectura.
Crear archivos	Escribir datos.
Crear carpetas	Anexar datos
Atributos de escritura.	Atributos de escritura.
Atributos extendidos de escritura.	Atributos extendidos de escritura.
Eliminar subcarpetas y archivos.	Eliminar archivos.
Eliminar.	Eliminar.
Permisos de lectura.	Permisos de lectura.
Cambiar permisos.	Cambiar permisos.
Tomar posesión.	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 autentificación dentro de un dominio. Comprueba la identidad del usuario y los servicios de red. Esta comprobación dual se denomina **autentificación mutua**.

El mecanismo de autentificación 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 autentificación 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 autentificación Kerberos VS funciona de la manera siguiente:

- Un usuario de un sistema cliente se autentifica en el KDC mediante una contraseña o tarjeta inteligente.
- 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 autentificación Kerberos V5 en el controlador de dominio.
- El TGS emitirá al cliente un **vale de servicio**.
- 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 autentificación 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 autentificación.

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 autentificar en un dominio del *Directorio Activo* para tener acceso a los cursos de red del dominio).
- En un dominio, los clientes y los servidores UNIX pueden tener cuentas del Directorio Activo y, por tanto, pueden ser autentificados desde un controlador de

dominio.