**Gestores de Arranque**

Es un programa que administra el arranque del ssoo. En el caso de que haya varios ssoo, es cuando tiene utilidad, ya que permite elegir al usuario entre un ssoo u otro, mostrando un menú para realizar la elección. Está situado en el MBR, al igual que la tabla de particiones. Hay varios gestores de arranque:

* **NTLDR (NT loader**), perteneciente a los ssoo desde w NT, w2000, wxp, ws2003. Generalmente se ubica en el directorio raíz del sistema pero también puede estar en dispositivos portátiles. El arranque con este gestor requiere que en el sector de arranque estén presentes los siguientes archivos: NTLDR, Boot.ini (contiene las opciones de configuración para el menú de inicio).
* **Bootmgr**: gestiona el arranque de w7, vista y ws2008; también se encuentra en el directorio raíz del sistema. Cuando arranca el sistema este llama al winload.exe (sustituye al NTLDR) que es el cargador del sistema operativo, a su vez este ejecuta al Ntoskrnl.exe que es el núcleo del sistema operativo responsable de la carga de los controladores de los dispositivos. Finalmente se ejecuta el BCDedit que es el que reemplaza al boot.ini.
* **Lilo**: para sistemas basados en Linux, permitiendo el arranque multisistema y multiplataforma.
* **GRUB**: más moderno que lilo. Viene en Debian y Ubuntiu.

**TEMA 5: GESTION DE LA INFORMACION**

**5.1. Almacenamiento secundario**

Sirve para almacenar grandes cantidades de información, tendrá mayor capacidad que la RAM, pero con un gran inconveniente, el tiempo de acceso es mucho mayor. El tipo de almacenamiento barato, no volátil, y de gran capacidad.

Existen dos tipos:

1. Acceso directo: es aleatorio y también secuencial, P.J: un HD.
2. Acceso secuencial: solo es secuencial, como una cinta magnética.

***5.1.1. Los discos magnéticos.***

La superficie de estos discos están cubiertas con partículas de un material magnetizable, como óxido de hierro. Cuando se les aplica un campo magnético se van a orientar en una posición o en otra, es decir, en 0 y 1. Las cabezas de lectura o escritura, o el cabezal, es el encargado de magnetizar estas partículas.

***¿Cómo se organizan los datos en un disco?***

Antes de poder utilizar un disco magnético hay que formatearlos, es decir, a bajo nivel. En este formateo se crea la estructura del disco duro.

* Creación de las pistas.
* Numeración de las pistas.
* Creación de los sectores.
* Numeración de los sectores.

Después se haría un formateo de alto nivel que es el que hace el usuario, creando particiones.

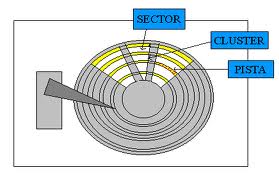
***Discos duros.***

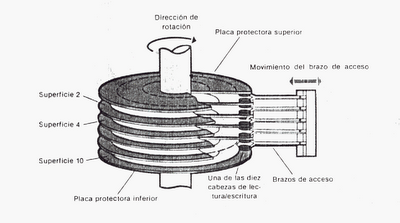
Son dispositivos electro-mecánico. Permiten el almacenamiento y la recuperación de grandes cantidades de información. Físicamente es una caja cerrada que contiene, por un lado, la unidad de lectura y escritura y, por otro, el disco en sí.

Unidad de lectura y escritura: es el conjunto de componentes electrónicos y mecánicos. Posee dos motores, uno mueve las cabezas y, el otro, hace girar los discos.

Disco: es una pila de platos que van girando y donde se almacena la información. Su estructura es:

Cara, cada cara en pistas, cada pista en sectores, y cada sector en clústeres. Tanto las cabezas y pistas se empiezan a numerar desde 0, pero los sectores desde 1.





**Nº SECTORES = Nº CARAS \* Nº PISTAS(de cada cara) \* Nº SECTORES (de cada pista)**

**512 bytes \* Nº SECTORES = CAPACIDAD**

Características:

**Tiempos**

* Tiempo de búsqueda: tiempo que tarda la cabeza desde la posición en donde esta hasta la pista donde este localizada la información deseada.
* Tiempo de latencia: es el tiempo de espera de la cabeza en la pista hasta que se coloca el sector deseado.
* Tempo medio de acceso: es el tiempo que tarda en llegar al sector, es la suma del tiempo de búsqueda y el tiempo de latencia.
* Tiempo pista a pista: tiempo que tarda en cambiar de una pista a otra adyacente.
* Tasa de transferencia: velocidad de lectura/escritura.

**Interfaces**

IDE, SATA, SCASI, SAS, etc. (trabajo de clase).

**Velocidad de rotación**

En r.p.m

**Tamaño del disco**

En pulgadas

**Capacidad**

Tb, Gb, Mb.

### *Discos Flexibles*

* Se les conocía con Floppy o Disquete
* La superficie era un plástico, pero cubierto por un material magnetizable (Óxido de hierro)
* Inconvenientes:
* Capacidad baja (1,44 Mb).
* Tiempo de acceso (x10 veces más lento que los HD porque no pueden girar a tanta velocidad como los estos).
* Poco fiables por pérdida de información.

### *Cintas Magnéticas*

* Almacenamiento masivo de la información.
* Acceso secuencial.
* Su principal uso sigue siendo las copias de seguridad (backup).

## *Discos Ópticos*

* Superficie circular de policarbonato.
* La información se guarda realizando surcos microscópicos.
* La información es almacenada en espiral desde el círculo más interno hasta el más interno.
* La técnica de escritura perfora el disco. Estas micro perforaciones se denominan “Pits”
* Los Pits tienen longitud variable 🡪 Se mide en micrones.
* El espacio entre Pits se denomina “Land”.
* Cada Pit está delimitado por unos y su longitud depende del número de ceros
  + 1000000001000000010000000010000000100000001
* La unidad óptica que está formada por:
  + - Por un motor que hace girar el disco.
    - Por un cabezal con una lente láser.
* El láser al pasar por la superficie del disco se refleja de forma distinta si pasa por un Pit o por un Land.
* La intensidad de la luz reflejada cuando pasa por un Pit es menor que por un Land.

### *Blu-Ray*

* Disco óptico de nueva generación.
* Para almacenar video de alta definición.
* Estándar de una serie de empresas 🡪 Asociación Blu-Ray (BDA) la cual dirigen Sony y Philips.
* Almacenamiento de 25Gb por capa.
* Utiliza un láser azul que es de menor longitud de onda el cual permite almacenar más datos.

## *Discos de Estado Sólido (SSD-Solid State Drive)*

* Son discos que utilizan tecnología Flash.
* No precisan parte mecánica para trabajar.
* La información es leída o escrita mediante impulsos electrónicos.
* Ventajas:
  + - No produce ruido 🡪 No tienen parte mecánica.
    - El consumo de energía es menor 🡪 No se necesita motor que haga girar los platos.
    - Se calientas menos.
    - Pesan mucho menos que los HD.
    - El acceso (L/E) es mucho más rápido.

## *Dispositivos Removibles*

* Graban la información en soportes (discos o cartuchos) que se pueden extraer. Existen varios tipos:
* Zip Iomega 🡪 100Mb-750Mb.
* SuperDisk ls 120🡪 120Mb.
* Jaz Iomega 🡪 1Gb-2Gb(Cartuchos caros).

## *Tarjetas de memoria*

* Son memorias Flash derivadas de las EEPROM.
* Funcionan mediante impulsos.
* Características:
* Memoria no volátil.
* Velocidad de acceso alta.
* No producen ruido porque carecen de parte mecánica.
* Capacidad de almacenamiento alta.
* Precio barato.

## Sistemas Raid

Redundant Array of Independet Disk (Conjunto redundante de discos independientes).

Grupo de discos que actúan como un único sistema de almacenamiento.

Los discos que forman el array se pueden configurar de distintas formas. A cada forma se le denomina niveles.

Cuando trabajamos con ellos, para el usuario y para el SO todos los discos forman una única unidad lógica.

* Beneficios:

-Tolerancia a errores de datos

-Rendimiento

-Capacidad

-Integridad de los datos

-La patente del RAID se realizó en el año1978 por IBM

-Formas de implementar un sistema Raid 🡪 Por Hardware o por Software

-Por Hardware:

- Ventajas:

-Más rápido 🡪 La controladora RAID es la que atiende y hace las operaciones en los discos (No el SO)

-Fácil de configurar 🡪 Mediante la consola de configuración RAID de la controladora

-En caso de error un disco, se sustituye el disco y la controladora se encarga del proceso de réplica

-Inconvenientes:

-Es de elevado precio

-Le añade al sistema un punto más de fallo 🡪 La controladora

-Por Software:

-Ventajas:

-Más barato que por hardware

-Más flexible 🡪 Se pueden construir Raid de particiones en lugar de discos completos

Inconvenientes:

-Más lento que por hardware

-Consume recursos del procesador

### Raid 0

* Conjunto dividido, Striping o distribución por bandas.
* Los datos se dividen en Striped y se escriben alternativamente en los discos que forman el array.
* Son necesarios 2HD o más
* Como resultado obtengo una unidad de mayor tamaño.
* No es redundante ni tolerante a fallos. Por este motivo no es recomendable en sistemas que necesitan seguridad.
* Ejemplo:

Array Size = 4Tb

Data Space = 4Tb

### Raid 1

* Mirror o espejo.
* En Raid 1 los discos se agrupan en discos de dos.
* Los datos se dividen en bloques y son duplicados en ambos discos en tiempo real.
* Son necesarios 2HD.
* Es redundante y tolerante a fallos 🡪 Si un disco falla, la información se recupera gracias al segundo.
* La capacidad del array se ve mermada porque un disco es utilizado exclusivamente para almacenar una copia de los datos .
* Ejemplo:

Array Size = 4Tb

Data Space = 2Tb

### Raid 5

* Conjunto dividido con paridad distribuida (Paridad par o Paridad impar).
* Utiliza los bits de paridad para reconstruir la información en caso de fallo en un disco.
* El bit de paridad ocupa mucho menos que duplicar un disco entero.
* Son necesarios 3HD o más.
* Ejemplo:

Array Size = 8Tb

Data Space = (4-1)\*2Tb = 6Tb

### Raid 0+1

* Conocido como Raid01.
* Utilizado para replicar y compartir datos entre varios discos.
* Primero se crea el Raid 0 dividiendo los datos en los discos y luego se crea el Raid 1 realizando un espejo de los anteriores.
* Dos Raid 0 unidos por un Raid 1.

### Raid 1+0 (10)

-Dos Raid 1 unidos por un Raid 0

**TEMA 6: ADMINISTRACION DE USUARIOS**

**6.1. ¿DÓNDE VAMOS A DEFINIR LAS CUENTAS DE USUARIO?**

* En la máquina local.

Sólo podrán utilizarse en esa máquina.

* En el Dominio. (tercer trimestre).

Se podrán utilizar en cualquier máquina que pertenezca a ese dominio o a uno de confianza.

**6.1.2. Las cuentas de usuarios.**

Son una colección de información que indican al SO:

* + Los archivos y carpetas que tiene el usuario.
  + Cambios que puede realizar en el equipo.
  + Las preferencias personales del usuario.

Todo esto va a permitir que un solo equipo lo puedan utilizar distintos usuarios.

**6.1.3. Tipos de cuentas de usuario.**

* Administrador. Lo importante es la contraseña.
* Invitado. No debería de usarse, y es para usuarios ocasionales.
* Usuarios estándar. Tendrán una serie de privilegios y características según correspondan.

Cuando damos de alta un usuario en el sistema creamos una cuenta, pero sobre todo se crea “Perfil de usuario local”. Se crea la 1º vez que el usuario inicia sesión. Se almacena en el disco sura. Permite que varios usuarios utilicen el mismo equipo. Se crea el fichero Ntuser.DAT (oculto). Este archivo se ubica en: c:\usuarios\%username%\Ntuser.DAT.

**6.1.4. Las cuentas de grupos.**

Nos van a permitir definir características comunes a varias cuentas de usuario. Hay muchos grupos predefinidos. Una cuenta de usuario puede pertenecer a varios grupos. En el momento que asociamos un usuario a un grupo adquiere las características de este automáticamente. Hay una pestaña de miembro de para introducir un usuario en un grupo, o quitarle.

**6.1.5. Dar de alta usuarios y/o grupos.**

* Desde el administrador del servidor.
* Desde el administrador de equipos.
* La consola de usuarios y grupos locales.
* Línea de comandos.

Cuando vamos a dar de alta un usuario con el nombre nos vale.

**6.2. DIRECTIVAS DE GRUPO Y DIRECTIVAS DE SEGURIDAD LOCAL**

**6.2.1. Directivas de grupo:**

Son el conjunto de reglas y configuraciones que ayudan a administrar usuarios y equipos. Nos dicen las acciones que pueden realizar los usuarios sobre un objeto determinado (impresora). Se utilizan para definir configuraciones automatizadas para grupos de usuarios y equipos.

***¿Qué permiten las directivas de grupo?***

* Controlar el acceso a los componentes de windows, a los recursos del sistema, a los recursos de la red, a las utilidades del panel de control, al escritorio y al menú de inicio.
* Nos permiten configurar as directivas para el bloqueo de cuentas y contraseñas, asignación de derechos a los usuarios.

**¿Dónde se aplican?**

* En el directorio activo.
* En un equipo local, que no pertenece a un dominio. Se van a definir las directivas de grupo local y se guardan en el propio equipo.

**6.2.2. Directivas de equipo local.**

Va a haber tres niveles de directivas:

1. Directivas de grupo local: se van a aplicar a todos los usuarios del sistema las mismas opciones de configuración tanto de usuarios como de equipo.
2. Directivas de grupo local para administradores y no administradores. Solo tienen configuración de usuario, en la parte de equipo no van a aparecer.
3. Directivas de grupo local para un usuario. Solo contienen la configuración de usuarios. Se definen para un usuario o grupo concreto.

**6.2.3. Componentes y estructura de las Directivas de grupo.**

La consola de directivas de grupo 🡪gpedit.msc

**Configuración de equipo**: aquí se agrupan todos los parámetros de configuración que pueden establecerse a nivel de equipo. Se aplican durante del inicio del sistema, con independencia del usuario que vaya a iniciar la sesión.

**Configuración de usuario**: aquí se agrupan todos los parámetros de configuración que pueden establecerse a nivel de usuario. Se aplican durante el inicio de la sesión.

*Configuración de software*: se aplica con las directivas de dominio. Configura las directivas para la instalación y actualización del software. Existe un objeto denominado “Instalación de Software” que es usado para distribuir SW y actualizaciones. Se puede asociar al equipo (entonces se ejecuta cuando se inicia el equipo); o asociar al usuario (entonces se ejecuta cuando inicia sesión el usuario pidiéndole a este que realice la instalación, es decir, no es automática).

*Configuración de Windows*: dentro tenemos los scripts (Ficheros de comandos) y la configuración de seguridad.

* Los ficheros de comandos los voy a utilizar tanto para usuarios y equipos. Va a haber archivos de comando para el inicio y apagado de equipos. Se almacenan en System32/GroupPolicy/Machine/scripts (aquí dos directorios: startup y shutdown).
* Archivos de comandos para el inicio y cierre de sesión de usuarios, Se almacenan en la misma ruta System32/GroupPolicy/Users/scripts (aquí dos directorios: logon y logoff).

Configuración de seguridad: ver Las directivas de seguridad local.

*Plantillas administrativas*: contienen todas las configuraciones de políticas basadas en el registro de windows 20087 server. Se pueden modificar cada plantilla, para habilitar o deshabilitar sus directivas. Las configuraciones se van a guardar en el registro, HKEY.LOCAL.MACHINE, las referentes al equipo; y en HKEY.CURRENT.USER. Las plantillas son distintas en configuración de equipo y de las de usuario.

**6.2.4. Actualización de las directivas**.

Las de grupo, cada vez que se arranca el sistemas para las de equipo y las de usuario cada vez que inicia sesión. Se puede forzar la actualización ejecutando GPUPDATE.EXE.

**Directivas de seguridad local (pertenece al apartado anterior)**

Ejecutamos SECPOL.MSC, para la consola de seguridad local. Vamos a ver:

Las directivas de cuenta.: que a su vez tiene:

Directivas de contraseña, nos va a permitir indicar como es la contraseña de los usuarios. Hay cinco:

* Almacenar contraseñas con cifrado reversible.

Directivas de bloqueo de cuenta, son tres:

* Duración de bloqueo de cuenta.
* Restablecer el bloqueo de cuenta después de.
* Umbral de bloqueo de cuenta.

**6.3. ADMINISTRADOR DE DISCOS**

Posee discos básicos y dinámicos (o almacenamiento básico y dinámico).

En el server hay que decidir qué tipo de disco se va a tener.

Un disco básico está compuesto por particiones primarias o extendidas. Dentro de las extendidas creamos lógicas. Hay un total de 4 primarias o 3 primarias y 1 extendida (como máximo). Si convertimos un básico en dinámico no se pierden los datos.

Un disco dinámico, es un tipo de disco mejorado que aparece a partir de windows 2000, no son soportados por Linux ni UNIX. La palabra partición desaparece y se llaman volúmenes. Estos discos permites volúmenes repartidos entre varios discos (distribuidos y seccionados), también permite volúmenes tolerantes a fallo (Rad 1 y Raid 5). Al crearlo no hace falta reiniciar el sistema.

**6.3.1. Tipos de discos dinámicos.**

1 Volumen simple 🡪 equivale a una partición primaria. No es tolerante a fallos, pero que se pueden reflejar o crear volúmenes reflejados. 🡪 si el volumen no es de inicio o de sistema se puede distribuir a otros volúmenes.

2 Volumen distribuido 🡪 se distribuye como mínimo en dos discos duros. Como máximo se podría extender a 32 discos. No son tolerantes a fallos y no se pueden reflejar.

3 Volumen seccionado o RAID 0 🡪 los datos se almacenan en bandas en un mínimo de dos discos. De forma alterna y equitativa. No tolerante a fallos y no se puede reflejar.

4 Volumen reflejado o RAID 1 🡪es tolerante a fallos y duplica los fallos. No se pueden extender. Los dos volúmenes deben de ser del mismo tamaño y en discos diferentes.

5 Volumen RAID 5 🡪 es tolerante a fallos con datos y paridades distribuidas en bandas, en mínimo tres discos. No se pueden ampliar, extender ni reflejar. Los volúmenes de inicio y de sistema no pueden ser RAID 5.

**6.3.2. Cuotas de disco**

Nos van a permitir realizar un seguimiento y control del uso del espacio de disco de los distintos volúmenes. Se puede hacer de dos formas distintas:

1. Cuando un usuario sobrepasa el límite de espacio en disco especificado (la cantidad de espacio de disco que se puede usar) no puede utilizar más espacio y registre un suceso.
2. Cuando un usuario sobrepase el límite de advertencia de espacio especificado, se registra un suceso

Se pueden habilitar mediante las directivas de grupo correspondiente 🡪 configuración de equipo 🡪 plantillas administrativas 🡪sistema 🡪 Cuotas de disco 🡪Con seis directivas. Una vez habilitadas vamos a ver como se configuran 🡪 propiedades de volumen 🡪 pestaña cuotas 🡪botón valores de cuota 🡪 aquí asignamos los valores de advertencia o espacio máximo, a un usuario o a varios o usuarios. Una vez creada la cuota se puede exportar para otros volúmenes.

**6.4. PERMISOS NTFS.**

Todos los archivos y carpetas de un volumen formateado con este sistema de archivos tienen asociado un objeto, este objeto se llama ACL (lista de control de acceso). Esta determina el nivel de acceso de un usuario o de un grupo que quiera acceder a esta carpeta o archivo.

**6.4.1. Permisos básicos para un fichero:**

1. *Lectura:* permite ver y tener acceso a su contenido.
2. *Escritura*: permite escribir en el fichero.
3. *Lectura y ejecución*: permite ver y tener acceso al contenido del fichero y además ejecutarlo.
4. *Modificar*: permite leer y escribir en el fichero, pero además también permite eliminarlo.
5. *Control total*: leer, escribir, modificar, eliminar y también puede cambiar los permisos y tomar posesión del mismo.

**6.4.2. Permisos básicos para un directorio:**

1. *Lectura*: permite ver y listar ficheros y subdirectorios.
2. *Escritura*: permite agregar fichero y subdirectorios.
3. *Lectura y ejecución*: permite leer y listar ficheros y subdirectorios, y también ejecutar los ficheros.
4. *Modificar*: permite lectura, escritura, ejecución y también se puede eliminar.
5. *Control total*: permite todo lo anterior, y además, cambiar los permisos y tomar posesión.

Estos permisos son los básicos, se crean combinando un conjunto de permisos mas especifico denominados permisos especiales.

**6.4.3. ¿Cómo establecer permisos?**

Siempre en las propiedades del fichero 🡪pestaña seguridad 🡪opciones avanzadas…

**6.4.4. Herencia de permisos:**

Cuando creamos un archivo o carpeta en un volumen NTFS, el objeto va a heredar de forma automática los permisos de la carpeta contenedora. Los permisos se propagan haca abajo, de padres a hijos. Se puede interrumpir la herencia en tres niveles:

1. Eliminar la herencia del padre a todos sus hijos.
2. Eliminar la herencia a un objeto hijo.
3. Eliminar ciertos permisos de la herencia de un hijo.

Los permisos heredados aparecen en un gris claro.

**6.4.5. Propiedad y transferencia de objetos:**

El propietario de un objeto, es el que tiene el control directo sobre dicho objeto. No tiene por qué ser el creador. De manera predeterminada es el creador del recurso, pero esta propiedad se puede transferir. (Hay un permiso que se llama “tomar posesión“ y un comando “takeown” que sirven para esto). Cualquier administrador puede tomar posesión de los objetos, es decir, no se le puede bloquear el acceso.

**6.5. ADMINISTRADOR DE TAREAS**

Es una herramienta que sirve para controlar la actividad del sistema y su rendimiento en tiempo real. Visualiza información del estado del procesador, de la memoria, de los procesos, de la red y de los usuarios conectados. Está compuesto por:

1. **El administrador de aplicaciones.**
2. **El administrador de procesos.**
3. **El administrador de servicios.**
4. **El rendimiento del sistema.**
5. **El Administrados de las funciones de red.**
6. **El Administrador de Usuarios.**

*El Administrador de aplicaciones 🡪* Nos muestra el estado de los programas o aplicaciones que se están ejecutando en este momento en el sistema. Posee una columna que nos muestra el “estado” (activo, no responde) 🡪 Posee unos botones que nos va a permitir “finalizar”, terminar la aplicación; “cambiar a”, cambiar de la aplicación actual a la seleccionada; “Nueva tarea”, lanzar nueva aplicación.

*El administrador de procesos* 🡪 Nos va a dar información detallada de todos los procesos que están ejecutándose en ese momento en el sistema, incluidos los de sistema (servicios), los procesos locales, los procesos del usuarios que ha iniciado sesión y los procesos de los usuarios remotos. 🡪 Aparecen varias columnas: Nombre de imagen, nombre del usuario, % de CPU, cantidad de memoria, descripción del proceso (por defecto). En el menú ver podemos ampliar esas columnas. (Prioridad: a mayor prioridad mayor cantidad de memoria de CPU).

*El administrador de servicios* 🡪Los servicios van a proporcionar características del SO como registro de eventos, informe de errores, etc. De cada servicio vamos a tener la siguiente información: nombre, PID (Identificador del proceso), descripción, estado.

*El rendimiento del sistema* 🡪 Esta pestaña nos ofrece un resumen del uso de memoria y CPU mostrándonos una serie de gráficos (uso de la CPU, historial de uso, el uso de la memoria, historial del uso de la memoria en tiempo); y estadísticas (**Totales sistema** 🡪 nº de identificadores, subprocesos, procesos en ejecución, el tempo en uso desde que se arrancó el sistema y los archivos de paginación. **Memoria del núcleo** (Kernel) 🡪 Cantidad de memoria utilizada por el núcleo y cuanta esta paginada y cuanta no. **Memoria física** 🡪 Información sobre la RAM. **Carga de transacciones**).

*El Administrador de las funciones de red* 🡪 No muestra información sobre el funcionamiento y rendimiento de la red, mostrando el estado de las redes que están funcionando en el sistema, mediante una tabla descriptiva del dispositivo (Adaptador de red): velocidad, estado, bytes enviados/recibidos, etc.

*El Administrador de Usuarios* 🡪 No va a mostrar los usuarios que están conectados al equipo: su identificador, nombre, etc.

**6.6. VISOR DE EVENTOS**

Es una herramienta de supervisión que nos va ha permitir visualizar un conjunto de archivos de registro. Con esta herramienta vamos a poder visualizar y analizar los eventos (sucesos) que han ocurrido en le sistema. Para que esto suceda ha de estar inicializado un servicio concreto que es: “Registro de eventos”🡪 evenlog.

* + 1. **Eventos supervisables:**
* *Los sucesos de uso de los recursos del sistema, o registros de windows.*
  + - Registros de aplicación 🡪 Sucesos o eventos provenientes de las aplicaciones o programas.
    - Registros de seguridad 🡪 Eventos asociados a las directivas de auditoria establecidas en las directivas de grupo.
    - Registro del sistema 🡪 Contiene los sucesos o eventos que genera el SSOO y sus componentes.
    - Registro de instalación 🡪 Sucesos registrados en el proceso de instalación y configuración de las aplicaciones.
    - Registro de eventos reenviados 🡪 Siempre que este activo, nos va a permitir controlar los eventos reenviados a otros servidores.
* Las acciones de los usuarios, o registros de aplicaciones y servicios.
  + - Eventos de una única aplicación.
    1. **Tipos de sucesos/eventos**:

*Información:* Nos describe el funcionamiento correcto de una aplicación o controlador

*Auditoria correcta/aciertos*: intentos de acceso de seguridad auditada correcta. (inicio de sesión correcta)

*Auditoria de errores*: intento de acceso de seguridad auditada erróneo.

*Advertencia*: Muestra un suceso que inicialmente no es importante pero que hay que tenerlo en cuenta en un futuro. (poco espacio en c:.)

*Error*: indica un problema importante, perdida de datos o funcionalidad.

* + 1. **Información por defecto del sistema:**

Es la información que nos aparece por defecto en la pantalla (en las columnas). Esta es:

* Tipo de suceso.
* Fecha hora.
* El origen. (Si lo ha generado una aplicación, un componente , un servicio.
* El suceso. (Asignado con un número).
* El usuario. El que estaba conectado cuando ocurrió.
* La categoría. (Si es de seguridad, de aplicación,…)
* Y todas las columnas que nosotros queramos ver y seleccionar.
  + 1. **Configuración de las opciones del registro de sucesos:**

Cada uno de estos registro se van a almacenar en un fichero de extensión \*.evtx, almacenado en System32\Winevt\logs. Estos ficheros por defecto tienen un tamaño definido de 20480 kb, cuando el registro llega a este límite los eventos se sobrescriben empezando por el más antiguo. Esto se puede configurar.