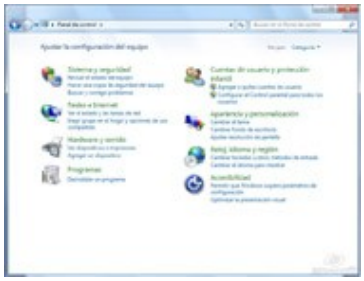
Administración básica del sistema (WINDOWS II).

Caso práctico
Carlos *acaba de instalar Windows 7 Enterprise en su ordenador y tras las configuraciones básicas se le plantea la duda de cómo mantener su equipo en óptimas condiciones de rendimiento y seguridad, por lo que le pregunta a* ***Ana****: -¿Dónde puedo descargarme herramientas que sirvan para controlar y mantener el funcionamiento del ordenador en buenas condiciones?*
Ana *le responde: -Windows 7 cuenta con un gran número de programas que te permitirán actualizar, proteger, administrar y monitorizar el funcionamiento de tu equipo.*

1.- Herramientas administrativas y del sistema.

Caso práctico
Carlos *pide ayuda a Ana: -¿Podrías echarme una mano y decirme cuáles son las herramientas para administrar Windows 7? ¿y cómo puedo utilizarlas?*
Ana *responde: -Claro, comencemos a ver las herramientas administrativas del sistema.*



Herramientas administrativas es una carpeta del Panel de Control que contiene herramientas para los administradores del sistema y para usuarios avanzados. Las herramientas de la carpeta pueden variar dependiendo de la versión de Windows que se use.
Las Herramientas administrativas se encuentran dentro del Panel de control. Éste es el centro neurálgico desde donde podemos acceder a cualquier configuración de Windows.

Para acceder a él tenemos dos opciones, mediante mi PC y Panel de Control, o mediante la barra de inicio

En el **Panel de Control** nos encontramos los siguientes **grupos de primer nivel**:

- ✓ **Sistema y seguridad**
- ✓ **Redes e Internet**
- ✓ **Hardware y sonido**
- ✓ **Programas**
- ✓ **Cuentas de usuario y protección infantil**
- ✓ **Apariencia y Personalización**
- ✓ **Reloj, idioma y región**
- ✓ **Accesibilidad**

1.1.- Herramientas administrativas.

Dentro del grupo de primer nivel `Sistema y seguridad` se hallan las `Herramientas administrativas`. Otra forma de acceder a éstas es a través de `Inicio > Todos los programas > Herramientas administrativas`.

Las herramientas administrativas principales son:

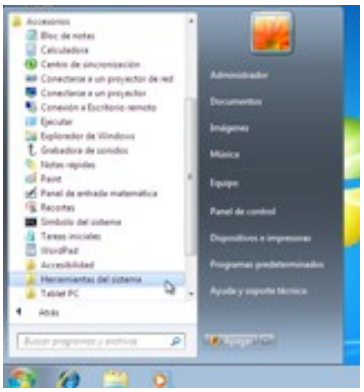
- ✓ `Administración de equipos`**:** Permite administrar equipos locales o remotos con una sola herramienta de escritorio consolidada. Mediante Administración de equipos se pueden realizar

numerosas tareas, como supervisar eventos del sistema, configurar discos duros y administrar el rendimiento del sistema.

- ✓ **`Administración de impresión`**: Permite administrar impresoras y servidores de impresión en una red y realizar otras tareas administrativas.
- ✓ **`Configuración del sistema`**: Permite identificar problemas que puedan estar impidiendo la correcta ejecución de Windows.
- ✓ **`Diagnostico de memoria de Windows`**: Permite comprobar si la memoria funciona correctamente.
- ✓ **`Directiva de seguridad local`**: Permite consultar y editar la configuración de seguridad de directiva de grupo.
- ✓ **`Firewalls de Windows con seguridad avanzada`**: Permite configurar opciones avanzadas del firewall en el equipo propio y en otros equipos remotos de la misma red.
- ✓ **`Iniciador iSCSI`**: Permite configurar conexiones avanzadas entre dispositivos de almacenamiento en una red.
- ✓ **`Monitor de rendimiento`**: Permite consultar información avanzada del sistema acerca de la unidad central de procesamiento (CPU), la memoria, el disco duro y el rendimiento de la red.
- ✓ **`Orígenes de datos (ODBC)`**: Permite usar la conectividad abierta de bases de datos (OBDC) para mover datos de un tipo de base de datos (un origen de datos) a otro.
- ✓ **`Programador de tareas`**: Permite programar la ejecución automática de aplicaciones u otras tareas.
- ✓ **`Servicios de componentes`**: Permite configurar y administrar los componentes del Modelo de objetos de componentes (COM). Los Servicios de Componentes están diseñados para ser usados por programadores y administradores.
- ✓ **`Servicios`**: Permite administrar los diversos servicios que se ejecutan en segundo plano en el equipo.
- ✓ **`Visor de eventos`**: Permite consultar información sobre eventos importantes (por ejemplo, cuando se inicia o se cierra una aplicación, o un error de seguridad), que se guardan en los registros de los eventos.

En esta unidad estudiaremos con más detalle algunas de estas herramientas, como por ejemplo, el Administrador de equipos, las Directivas de seguridad local, el Monitor de rendimiento, el Programador de tareas, la herramienta Servicios, etc.

1.2.- Herramientas del sistema.



Existen unas determinadas herramientas del sistema a las que también se accede mediante **`Inicio > Todos los programas > Accesorios > Herramientas del Sistema`**.

Las funcionalidades de las herramientas del sistema más importantes son:

- ✓ **`Desfragmentador de disco`**: Se utiliza para volver a organizar los datos fragmentados de forma que los discos y las unidades puedan funcionar de manera más eficaz. Se ejecuta por defecto según una programación (que puede adaptarse a medida), pero también puede analizar y desfragmentar los discos y unidades manualmente.
- ✓ **`Liberador de espacio en disco`**: Permite reducir el número de archivos innecesarios en el disco duro liberando espacio en el disco y ayudando a que el equipo funcione de manera más rápida. Esta herramienta del sistema quita archivos temporales, vacía la Papelera de reciclaje y elimina varios archivos del sistema y otros elementos que ya no se necesitan.
- ✓ **`Mapa de caracteres`**: Se usa para insertar en los documentos caracteres especiales que no aparecen en el teclado, por ejemplo, caracteres matemáticos, notaciones científicas, símbolos de moneda y caracteres de otros idiomas.

- ✓ `Editor de caracteres privados`: Permite crear caracteres, modificar caracteres existentes, guardar caracteres y ver y examinar la biblioteca de caracteres.
- ✓ `Equipo`: Permite ver las unidades de disco y otro hardware conectado al equipo.
- ✓ `Información del sistema`: Permite ver información detallada del equipo, como el sistema operativo, su versión, el nombre del sistema, tipo de sistema (arquitectura 32 ó 64 bits), procesador, etc.

El Desfragmentador de disco y el Administrador de dispositivos son herramientas ...

- ○ El desfragmentador pertenece a las herramientas administrativas y el Administrador de equipos a las herramientas del sistema.
- ◉ **El desfragmentador pertenece a las herramientas del sistema y el Administrador de equipos a las herramientas administrativas.**
- ○ Ambos pertenecen a las herramientas del sistema.
- ○ Ambos pertenecen a las herramientas administrativas.

2.- Administración de grupos y cuentas de usuario locales.

Caso práctico

Carlos *le comenta a* ***Ana*** *que en su casa varios miembros de su familia utilizan el mismo ordenador por lo que le interesa que cada persona tenga su usuario independiente. En ese momento Ana ve oportuno comentarle cómo puede gestionar distintas cuentas de usuario, los privilegios de cada una y la posibilidad de crear grupos de usuarios.*

Ana *le explica a Carlos que en la mayoría de los sistemas operativos actuales, aparecen dos* ***conceptos relacionados con la seguridad del sistema****: Autentificación y Autorización.*

Autentificación: Para usar el sistema es necesario abrir una sesión de trabajo (login) para lo cual tendremos que autentificarnos, proporcionando al sistema un nombre de usuario y una contraseña. En caso de no tener una cuenta de usuario abierta en el sistema, será imposible entrar en el mismo.

Autorización: Una vez que el usuario se ha autentificado y abierto sesión, cada vez que quiera usar un recurso (un fichero, una carpeta, una impresora, etc) el sistema comprobará si está autorizado o no para realizar esa acción. Los administradores del sistema pueden modificar estas autorizaciones mediante unas listas de acceso.

Carlos toma buena nota de las explicaciones de Ana para posteriormente ponerlas en práctica.

En este apartado vamos a aprender a configurar la seguridad y el acceso de usuarios al propio equipo (autentificación). Para ello, explicaremos cómo administrar los usuarios locales y, por tanto, el acceso al sistema local. El proceso de autorización lo veremos en el apartado de Administración de seguridad de recursos a nivel local.

2.1.- Tipos de cuentas de usuario y grupos locales (I).

Las cuentas de usuario están pensadas para uso individual, mientras que los grupos sirven para facilitar la administración de varios usuarios. Los equipos con Windows 7 se pueden configurar como parte de un grupo doméstico o de trabajo o como parte de un dominio. En esta unidad partimos de la base de que nuestro equipo no está conectado aún a una red, por lo que los usuarios y grupos que utilizaremos serán a nivel local. En la siguiente unidad de trabajo veremos cómo conectar un equipo a la red y veremos la diferencia entre su configuración dentro de un grupo de trabajo o de un dominio.

En Windows 7 existen varios tipos de cuentas de usuario: Estándar, Administrador e Invitado. Según el tipo, se tiene un nivel diferente de control sobre el equipo.

- ✓ `Cuenta de usuario estándar`: Tiene privilegios limitados, se puede usar la mayoría de los programas instalados en el equipo, pero no se puede instalar o desinstalar software ni hardware, eliminar archivos que son necesarios para que el equipo funcione, o cambiar opciones de configuración en el equipo que afecten a otros usuarios.
- ✓ `Cuenta de administrador`: Tiene el máximo control sobre el equipo y sólo se debe utilizar cuando se lleven a cabo tareas de administración que requieran los privilegios del administrador. Este tipo de cuenta permite realizar cambios que afectan a otros usuarios. Son tareas fundamentales de los administradores las relativas a la configuración de seguridad, a la instalación de software y hardware, y a la obtención de acceso a todos los archivos en un equipo.
- ✓ `Cuenta de Invitado`: Suele ser utilizada por usuarios temporales del equipo. Aunque tiene derechos muy limitados, hay que tener cuidado al utilizarla porque se expone al equipo a problemas de seguridad potenciales. El riesgo es tan alto que la cuenta de invitado viene deshabilitada con la instalación de Windows 7.

Las cuentas de usuario se identifican con un **SID** (Security Identifier - Identificador de Seguridad) se trata de un número de identificación único para cada usuario. Es como el DNI de cada

usuario,Windows identifica los usuarios a través de su SID y no por su nombre como hacemos nosotros. Un SID está formado de la siguiente manera:

```
S-1-5-21-448539723-413027322-839522115-1003
```

2.1.1.- Tipos de cuentas de usuario y grupos locales (II).

Los grupos en Windows 7 proporcionan la posibilidad de otorgar permisos a tipos de usuarios con características similares, simplificando así la administración de cuentas de usuario. Si un usuario es miembro de un grupo de usuarios con acceso a un recurso, ese usuario en particular puede acceder al mismo recurso. Los grupos de usuarios locales se nombran como Equipo\Nombre_grupo (donde Equipo es el nombre del ordenador).

Windows 7 emplea los siguientes tipos de grupo:

- ✓ **`Grupos locales`**: Definidos en un equipo local y utilizados sólo en dicho equipo local.
- ✓ **`Grupos de seguridad`**: Pueden tener descriptores de seguridad asociados. Se utiliza un servidor Windows para definir grupos de seguridad en dominios.
- ✓ **`Grupos de distribución`**: Se utilizan como lista de distribución de correo electrónico. No pueden tener descriptores de seguridad asociados.

Cuando se instala Windows 7 se crean por defecto varios grupos de usuarios predefinidos en el sistema:

- ✓ Administradores.
- ✓ Operadores de copia de seguridad.
- ✓ Operadores criptográficos.
- ✓ Lectores del registro de eventos.
- ✓ Invitados.
- ✓ Operadores de configuración de red.
- ✓ Usuarios del registro de rendimiento.
- ✓ Usuarios del monitor del sistema.
- ✓ Usuarios avanzados*.
- ✓ Usuarios autenticados.
- ✓ Usuarios de escritorio remoto.
- ✓ Duplicadores.
- ✓ Usuarios*.

Los usuarios miembros del grupo de Usuarios son los que realizan la mayor parte de su trabajo en un único equipo Windows 7. Estos usuarios tienen más restricciones que privilegios. Pueden conectarse a un equipo de manera local, mantener un perfil local, bloquear el equipo y cerrar la sesión del equipo de trabajo.

Por otra parte, los usuarios pertenecientes al grupo de Usuarios avanzados, tienen derechos adicionales a los del grupo Usuarios. Algunos de estos derechos extra son la capacidad de modificar configuraciones del equipo e instalar programas.
http://technet.microsoft.com/es-es/library/cc785098%28WS.10%29.aspx

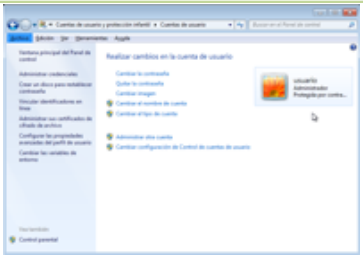
La cuenta de Invitado ...

- ○ Viene habilitada por defecto.
- ○ Viene deshabilitada por defecto.
- ○ Permite el acceso a usuarios esporádicos o temporales del sistema.
- ◉ **Segunda y tercera son ciertas.**

2.2.- Gestión de cuentas de usuario y grupos locales.

Podemos crear, borrar y modificar cuentas de usuario en Windows 7 utilizando varios programas distintos:

- ✓ **Asistente para cuentas de usuario desde Panel de Control**
- ✓ **Gestión de cuentas de usuario desde** `Herramientas Administrativas - Administración de equipos`



Para abrir la herramienta Cuentas de usuarios, hay que abrir el Panel de control desde el menú Inicio y, a continuación, hacer doble click en Cuentas de usuario.

Para crear una cuenta de usuario nueva, hay que seguir estos pasos:

1. Hacer click en Administrar otra cuenta y
2. Crear una nueva cuenta.
3. Escribir el nombre que deseamos utilizar para la cuenta y, después, hacer click en Siguiente.
4. Seleccionar el tipo de cuenta que deseamos y después hacer click en Crear cuenta.

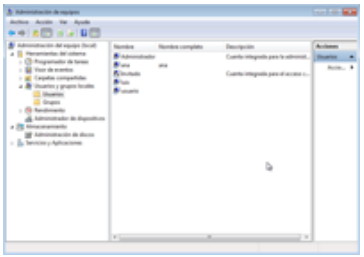
Para **realizar cambios en una cuenta**, hay que seguir estos **pasos**:

1. Hacer click en la cuenta que desea cambiar.
2. Seleccionar el elemento que desea cambiar: (nombre, imagen, tipo, contraseña, borrado).

Cuando **eliminamos una cuenta de usuario**, ésta se borra definitivamente del sistema. No podemos recuperarla creando otra con el mismo nombre con el objeto de conseguir los mismos permisos de la cuenta antigua. Esto es debido a que cuando creamos otra cuenta nueva el sistema asigna un nuevo SID distinto de la cuenta antigua.

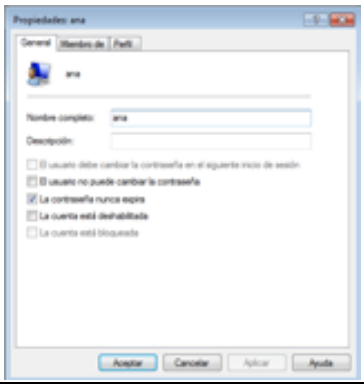
Nota: No se puede borrar una cuenta de un usuario si tiene sesión abierta en el sistema.

La tercera opción que tenemos para gestionar cuentas de usuario, es la opción más interesante de todas las que nos ofrece Windows 7. Es la **consola de usuarios locales y grupos**. Podemos llegar a dicha consola de varias formas.



Podemos ejecutar desde **Inicio - Ejecutar** y escribir LUSRMGR.MSC.
O desde `Panel de Control - Sistema y seguridad - Herramientas Administrativas - Administración de equipos` y en ella escogemos la carpeta de usuarios locales y grupos.

Lleguemos desde donde lleguemos, veremos que tenemos dos carpetas, una para los usuarios y otra para los grupos. Podemos crear usuarios nuevos accediendo a las propiedades de la carpeta usuarios (botón derecho sobre ella) y seleccionando la opción de `Usuario Nuevo`. Podemos modificar un usuario accediendo a sus propiedades. Del mismo modo podemos crear nuevos grupos y modificar los ya existentes. Podemos tanto asignar a un usuario varios grupos, como asignar a un grupo varios usuarios.



Si compruebas el nombre de esta última consola, verás que aparece la palabra local en el mismo. Esto es así por que se distinguen dos ámbitos al hablar de usuarios: Los usuarios locales y los usuarios de

dominio. Mientras no tengamos instalado un dominio (para lo cual necesitaremos algún servidor Windows de la familia Server) siempre estaremos trabajando con cuentas locales.

Si accedemos a las **propiedades de un usuario**, veremos que tenemos tres pestañas con las que trabajar:

- ✓ **General**: Podemos indicar el nombre completo de la cuenta, una descripción, e indicar algunas opciones de la cuenta.
  El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.
  El usuario no puede cambiar la contraseña. Prohibimos que el usuario pueda cambiar su contraseña.
  La contraseña nunca caduca. Ya veremos como en Windows 7 las contraseñas se consideran material fungible, es decir, que tras un cierto tiempo de uso el sistema obligará a cambiar dichas contraseñas. Mediante esta opción indicamos que la contraseña podrá usarse sin que caduque nunca.
- ✓ **Cuenta deshabilitada**: No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.
- ✓ **La cuenta está bloqueada**: Por determinados mecanismos de seguridad se puede llegar a bloquear una cuenta, que implicará que dicha cuenta estará deshabilitada. Desde esta opción podemos volver a desbloquearla, simplemente desmarcando la casilla.

Además de la pestaña General, tenemos la referida a **Miembro de**, desde esta pestaña podemos introducir al usuario en grupos. Los grupos se usan para dar permisos y derechos a los usuarios más fácilmente, sin tener que ir usuario por usuario. Así por ejemplo, si introducimos a un usuario como miembro del grupo Administradores, le estaremos dando todos los permisos del grupo Administradores.

En la pestaña Miembro de, veremos **todos los grupos a los que el usuario pertenece** actualmente. Si le damos al botón agregar podremos escribir directamente el nombre de un grupo donde agregarlo. Si queremos escoger dicho grupo de una lista de los grupos posibles, hay que escoger la opción Avanzada y luego Buscar ahora, que nos mostrará una lista de todos los grupos del sistema. Basta con seleccionar el que queramos (o los que queramos) y pulsar aceptar.

La última pestaña es de **Perfil**. Ésta nos permite indicar **la ruta del perfil**, los **archivos de inicio de sesión** y las **carpetas personales del usuario**. Como en un apunte posterior veremos el tema de perfiles, de momento lo dejamos pendiente.

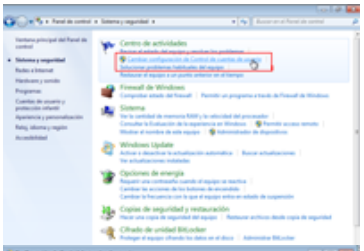
Relacionado con la seguridad de cuentas de usuario nos encontramos el UAC, ¿sabes a qué hacen referencia estas siglas? Descubre una de las características de seguridad perfeccionada por Windows7 y que crearon cierta controversia en Windows Vista:

UAC (User Account Control, Control de Cuentas de Usuario)

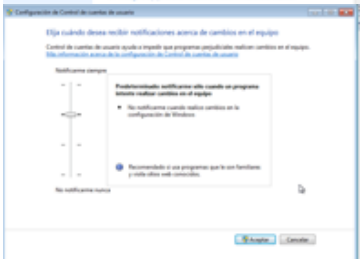
El **UAC (User Account Control, Control de Cuentas de Usuario)** es una característica de seguridad que se encarga de **notificar alertas de seguridad del sistema** al usuario. Lanza mensajes de alerta cuando se quiere realizar alguna acción que influya en el sistema, tal como la instalación de determinados programas, la modificación el registro de Windows, la creación de servicios, etc. User Account Control (UAC) es el responsable de mensajes como "Un programa no identificado desea

tener acceso a este equipo" o "Necesita confirmar esta operación", y aunque, en ocasiones, estos mensajes pueden llegar a ser algo molestos, evita básicamente que se instale software sin el consentimiento del usuario.

Esta función de seguridad ya se encontraba en Windows Vista y Windows 7 la mejora, permitiendo al usuario una mayor configuración para reducir el número de alertas que aparecen.



Para **acceder al UAC** nos dirigimos al `Panel de Control – Sistema y seguridad – Centro de Actividades – Cambiar configuración de Control de cuentas de usuario`. En la siguiente imagen podemos ver su localización dentro de Sistema y seguridad.



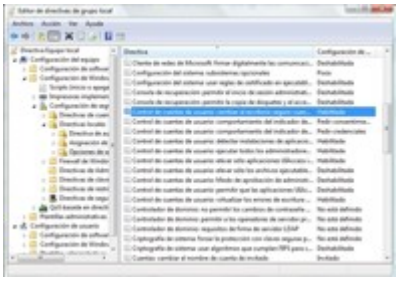
Para configurar el **UAC** contamos con cuatro **opciones**:

1. `Notificarme siempre` **cuando**:
   - ✓ Un programa intente instalar software o realizar cambios en el equipo.
   - ✓ Realice cambios en la configuración de Windows.
2. **Predeterminado:** `notificarme sólo cuando un programa intente realizar cambios en el equipo`
   - ✓ No notificarme cuando realice cambios en la configuración de Windows.
3. `Notificarme sólo cuando un programa intente realizar cambios en el equipo (no atenuar el escritorio)`
   - ✓ No notificarme cuando realice cambios en la configuración de Windows.
4. `No notificarme nunca` **cuando**:
   - ✓ Un programa intente instalar software o realizar cambios en el equipo.
   - ✓ Realice cambios en la configuración de Windows.

En función de nuestras necesidades escogeremos una u otra opción.

Editor de directivas de grupo local y el UAC

También podemos editar el UAC desde el Editor de directivas de grupo local. Para ello, desde el campo de búsqueda del menú de Inicio, escribimos gpedit.msc y pulsamos Enter, se nos abrirá el editor de directivas. Dentro de éste buscamos la cadena `Configuración del equipo – Configuración de Windows - Configuración de seguridad - Directivas locales - Opciones de seguridad` y encontraremos varias entradas referentes al UAC.



Cada entrada indica su utilidad en su nombre, tendremos que decidir si se activan o se desactivan. En cualquier caso, es posible que los cambios requieran de un reinicio para funcionar. En la imagen podemos ver una de estas entradas del editor de directivas relativa al UAC.

3.- Administración de seguridad de recursos a nivel local.

Caso práctico

__Carlos__ le comenta a Ana que hay información en su ordenador de casa que quiere que esté accesible para toda su familia y otra que no. __Ana__ le propone estructurar la información en diferentes directorios o carpetas para que sólo los usuarios que quiera __Carlos__ accedan a los archivos. Carlos comenta: -Me parece buena idea. ¿Cómo tendría que hacerlo?
__Ana__ responde: -Debes conocer cómo se gestiona la seguridad de los recursos a nivel local. Pongámonos manos a la obra.

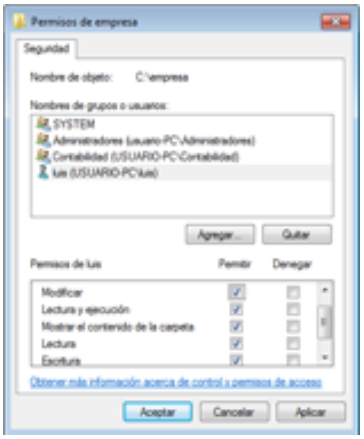
Los recursos de un sistema son los distintos elementos con los que ese sistema cuenta para que sean usados por los usuarios. Así, una impresora, una carpeta, un fichero, una conexión de red, son ejemplos de recursos.

Así pues, cada recurso cuenta con una lista donde aparecen los usuarios que pueden usar dicho recurso y de qué forma pueden usarlo. Hemos visto que el sistema no ve usuarios y grupos, realmente ve Identificadores de Seguridad (SID), de modo que dicha lista realmente tendrá en su interior una serie de SID y los permisos que cada uno de esos SID tiene sobre el recurso.

Ya sabemos que los usuarios y grupos permiten limitar la capacidad de estos para llevar a cabo determinadas acciones, mediante la asignación de derechos y permisos. Un **derecho** autoriza a un usuario a realizar ciertas acciones en un equipo, como hacer copias de seguridad de archivos y carpetas, o apagar el equipo. Por otro lado, un **permiso** es una regla asociada a un recurso que regula los usuarios/grupos que pueden tener acceso al recurso y la forma en la que acceden.

Los permisos de un recurso se guardan en una lista especial, que se conoce como ACL (Access Control List o Lista de Control de Acceso). En este apartado vamos a ver cómo podemos modificar las ACLs de los recursos para que sean usadas por los usuarios y grupos locales, es decir, aquellos que residen en nuestro propio equipo.

3.1.- Permisos de archivos y carpetas.



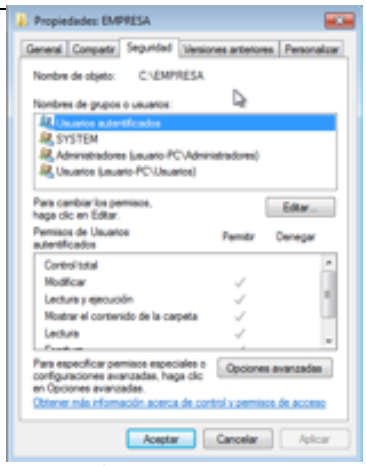
Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. El recurso comprobará entonces si en su ACL aparece el SID del usuario, y en caso contrario, comprobará si en su ACL aparece el SID de algún grupo al que pertenezca el usuario.

Si no aparece en la ACL ningún SID del usuario, el recurso niega el acceso al usuario.

Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc.) está permitida para ese SID en su ACL, si lo está, le autoriza para hacerlo, en caso contrario se lo impide.

Puede ocurrir que un usuario tenga permisos contradictorios. Imagínate que en el ACL de una carpeta llamada EMPRESA aparece que el SID del usuario LUIS puede escribir en la carpeta, pero LUIS pertenece al grupo CONTABILIDAD que aparece en el ACL de empresa como que no tiene derecho a escribir. Bien, en este caso se aplica la siguiente regla:

1. Lo que más pesa en cualquier ACL es la **denegación** implícita de permisos. Si un permiso esta denegado, no se sigue mirando, se deniega inmediatamente.
2. Es suficiente con que un permiso esté concedido en cualquier SID para que se considere concedido. (A excepción de la regla 1, es decir, que no esté denegado implícitamente en ningún sitio).



Esto se entiende mejor gestionando el ACL de algún recurso.

Pongamos un ejemplo, creemos en la raíz de nuestro volumen (con sistema de archivos NTFS) una carpeta con nombre EMPRESA. Una vez creada, accedemos a sus propiedades y en ellas a la `pestaña Seguridad`:

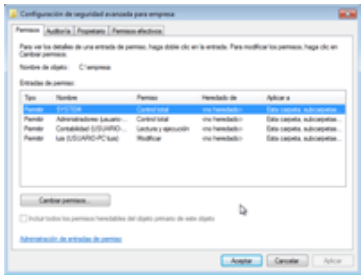
Podemos ver como en la parte superior tenemos las SID a las que concedemos permisos (usuarios y grupos) y en la parte inferior tenemos los permisos concretos que le concedemos a dicha SID. Si ves las dos columnas por cada permiso, podemos tanto **Permitir** como **Denegar un permiso**. La denegación de un permiso es la que más pesa, y se aplica inmediatamente. De hecho, se aconseja no denegar permisos, a menos que sea absolutamente necesario.

Con el botón `Editar` se nos abre una nueva pantalla donde aparecen los botones `Agregar` y `Quitar`. Con ellos podemos añadir o quitar usuarios o grupos de la ACL. En la parte inferior podemos pulsar en las casillas de `Permitir` **y** `Denegar` para dar y quitar **permisos**.

¿Te has fijado que la columna de Permitir está en gris y no nos deja cambiarla? Pero, ... ¿por qué razón ocurre esto? Bien, en este momento, nos toca hablar de la **herencia**.

Tomamos de referencia, de nuevo, a la carpeta llamada EMPRESA, vamos a prepararla para que pueden leer y escribir en ella los usuarios que sean miembros del grupo EMPLEADOS, para que sólo puedan leer los del grupo JEFES pero no escribir, y que los demás usuarios no puedan ni leer en ella ni escribir. Bien, si ahora dentro de la carpeta EMPRESA creamos una nueva carpeta INFORMES, ¿no sería lógico que esta carpeta INFORMES "heredará" la ACL de su carpeta superior EMPRESA para que no tuviera que configurarla nuevamente?

Pues precisamente eso es lo que hace Windows 7, cualquier recurso que creemos, heredará automáticamente la ACL de su recurso padre si es que existe. En nuestro caso, la carpeta EMPRESA ha heredado la ACL de la raíz de nuestro volumen. De modo que no podremos quitar usuarios, quitar permisos, etc.

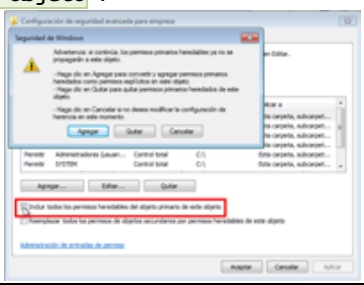


Para realizar cambios en la ACL de nuestra carpeta EMPRESA, debemos indicarle que "rompa" la herencia, es decir, que deseamos retocar manualmente su ACL.

Para ello, accedemos al botón de Opciones Avanzadas que está en la pestaña Seguridad.

Podemos ver en estas opciones avanzadas 4 pestañas, de momento nos quedamos en la primera, permisos.

Vemos como en la parte inferior de esta ventana, podemos ver como esta marcada la opción de: "`Incluir todos los permisos heredables del objeto primario de este objeto`".



Esto implica: "Heredar del objeto principal las entradas de permiso relativas a los objetos secundarios e incluirlas junto con las entradas indicadas aquí de forma explícita". Si desmarcamos dicha opción mataremos la relación de herencia de nuestro recurso, y podremos gestionar su ACL "directamente". Vamos a ello.

Hay que tener cuidado, una vez quitada la herencia, el sistema nos da a elegir entre dos opciones: Si escogemos la opción Agregar, la herencia se interrumpirá, y podremos retocar la ACL como nos plazca, pero dicha ACL será la que ahora mismo tiene el recurso, heredada de su objeto principal.

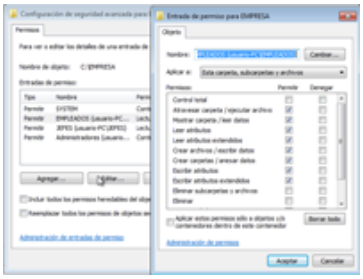
Si escogemos la opción Quitar, la ACL se borrará totalmente, se interrumpirá la herencia y la podremos crear desde cero.

Si elegimos quitar y empezar desde cero, hay que tener en cuenta que en las ACL no sólo deben aparecer nuestras SID normales, sino que grupos como Creator Owner o System son necesarios para que el sistema pueda trabajar sin problemas con dichas carpetas. Si quitamos estos SID tendremos problemas en el futuro (copias de seguridad, auditorías, etc.).

Vemos que debajo de la opción de **Heredar del objeto principal**, tenemos otra opción que nos permite activar que los objetos por debajo del nuestro hereden las modificaciones que hagamos en nuestra ACL. Esto es importante tenerlo en cuenta si queremos que los cambios que hagamos en la ACL se repliquen en los objetos hijos del nuestro, ya que hemos roto la herencia y a veces tendremos que forzar dichos cambios.

Agregaremos en este momento a los grupos EMPLEADOS y JEFES y les asignaremos los permisos antes citados. Una vez eliminada herencia de permisos podremos **quitar los grupos**predeterminados de Windows que no nos hacen falta en nuestro ejemplo, estos son, **Usuarios y Usuarios autenticados**. El motivo principal para eliminarlos de la ACL de la carpeta EMPRESA es que si los dejáramos cualquier usuario del sistema podría acceder y ver el contenido de la carpeta. Esto es así, porque cuando creamos un usuario en Windows, éste lo hace miembro automáticamente de estos grupos. La ACL de la carpeta EMPRESA quedaría como vemos en la imagen. Resumiendo, los grupos de usuarios que deben tener acceso a la carpeta EMPRESA serán el grupo de Administradores (con Control total - todos los permisos), el grupo SYSTEM (creados estos dos grupos de forma automática por Windows) y los grupos EMPLEADOS y JEFES.

Los distintos **permisos** que se pueden aplicar para cada SID en la ACL no son únicamente los que vemos en las propiedades de la carpeta, si entramos desde la pestaña de Seguridad en `Opciones avanzadas` veremos un cuadro llamado `Entradas de permisos` para los distintos usuarios y grupos de la ACL. Tras esto, hacemos click en el botón `Cambiar permisos` y después en el botón `Editar`. De esta manera, veremos cómo podemos indicar otro tipo de permisos.



El permiso `Atravesar carpeta` permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas).

El permiso `Leer atributos` permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

El permiso `Escribir atributos` permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

El permiso `Tomar posesión` permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

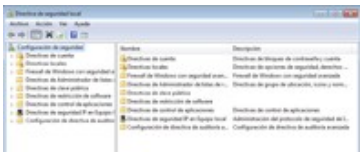
Un permiso muy especial es el de **Control Total**. Si este permiso se lo otorgamos a un usuario en una carpeta, este usuario podrá eliminar cualquier cosa que haya en esa carpeta, incluso si le denegamos el permiso de eliminación en esos recursos. Hay que tener mucho cuidado al conceder este permiso.

3.2.- Directivas de seguridad local y Directivas de grupo local.

Siempre desde una cuenta con privilegios de administrador Windows 7 nos proporciona la posibilidad de gestionar de forma centralizada la configuración de la seguridad de nuestro sistema, a través de las **Directivas de seguridad local** y las **Directivas de grupo local**. Ambas opciones cuentan con consolas para facilitar la configuración de las directivas. Una directiva es un conjunto de reglas de seguridad que se pueden implementar en un sistema.

Con las **Directivas de seguridad local** veremos cómo aplicar distintas restricciones de seguridad sobre las cuentas de usuario y contraseñas. Por otro lado, las **Directivas de grupo local** nos permiten configurar equipos de forma local o remota, instalar o eliminar aplicaciones, restringir los derechos de los usuarios, entre otras acciones.

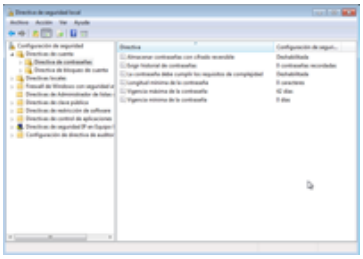
3.2.1.- Directivas de seguridad local.



Windows 7 es un sistema operativo muy configurable por parte del usuario. Aunque estas configuraciones suelen estar algo ocultas para que no sean accesibles por los usuarios normales, y sólo pueden ser modificadas desde las consolas del sistema.

En concreto, desde la consola de Directiva de Seguridad Local, podemos gestionar varios aspectos sobre las cuentas y contraseñas. (Para acceder a la consola Directivas de Seguridad haremos: `Inicio - Ejecutar - SecPol.msc`

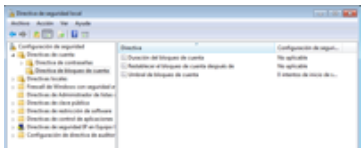
Una vez dentro podemos acceder a: `Configuración de Seguridad - Directivas de Cuenta - Directivas de Contraseñas)` o también se puede acceder a través de `Inicio - Panel de Control - Sistema y Seguridad - Herramientas administrativas - Directiva de seguridad local`.



Las **configuraciones** más útiles que podemos gestionar desde aquí son:

- ✓ **Forzar el historial de contraseñas**. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuantas contraseñas recordaráWindows 7.
- ✓ **Las contraseñas deben cumplir los requerimientos de complejidad.** Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.
- ✓ **Longitud minina de la contraseña.** Indica cuantos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.
- ✓ **Vigencia máxima de la contraseña.** Las contraseñas de los usuarios caducan y dejan de ser validas después del número de días indicados en esta configuración, y el sistema obligará al usuario a cambiarlas. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
- ✓ **Vigencia minina de la contraseña.** Indica cuanto tiempo debe transcurrir desde que un usuario se cambia la contraseña, hasta que puede volver a cambiarla. Esta configuración de seguridad local se usa para evitar que un usuario cambie continuamente su contraseña a fin de volver a quedarse con su contraseña original caducada.

Bloqueo de las cuentas:



Desde secpol.msc también podemos gestionar un comportamiento de las cuentas de usuario relacionado con las contraseñas, y es el de bloquear las cuentas si se intenta acceder al sistema con las mismas pero usando contraseñas incorrectas. Esta configuración la encontramos en (`Inicio - Ejecutar - SecPol.msc - Configuración de Seguridad - Directivas de Cuenta - Directivas de Bloqueo de Cuentas`)

Aquí podemos **configurar**:

- ✓ **Duración del bloqueo de cuenta**. (Durante cuanto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee).
- ✓ **Restablecer la cuenta de bloqueos después de**. (Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero).
- ✓ **Umbral de bloqueo de la cuenta.** (Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta).

3.2.2. Directivas de grupo local.

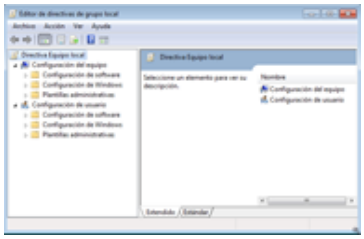
Las directivas de grupo forman parte de la estructura de Windows XP, Windows Vista y Windows 7. En estos sistemas, las políticas de grupo son una herramienta muy poderosa que permite a los administradores configurar equipos de forma local o remota, instalando aplicaciones, restringiendo los derechos de los usuarios, eliminando aplicaciones, instalando y ejecutando scripts, y redirigiendo carpetas del sistema a red o viceversa. Pero también tienen utilidad las políticas de grupo en entornos pequeños, incluso en una sola maquina.

Usando las políticas de grupo en una maquina corriendo Windows 7, podemos:

- ✓ Modificar políticas que se encuentran en el registro del sistema. El registro del sistema es una gran base de datos en la que se configuran cientos de comportamientos de Windows 7. Desde las políticas de grupo podemos acceder a estas características y modificarlas, de una forma mucho más simple que mediante la edición pura del registro.
- ✓ Asignar scripts que se ejecutaran automáticamente cuando el sistema se encienda, se apague, un usuario inicie sesión o cierre sesión.
- ✓ Especificar opciones especiales de seguridad.

Si estamos trabajando bajo un dominio (con un servidor en la red administrando dicho dominio) las políticas de grupo cobran mayor protagonismo. En un ambiente de grupo de trabajo, las políticas de grupo de cada máquina controlan los aspectos únicamente de dicha maquina, y en algunos casos es imposible sacarles el rendimiento esperado.

La consola desde donde podemos gestionar las directivas de grupo es el gpedit.msc. (`Inicio - Ejecutar - gpedit.msc`).



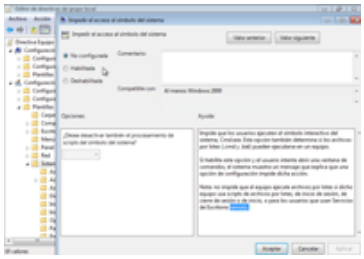
Para poder trabajar con el gpedit.msc necesitamos estar usando una cuenta de usuario que pertenezca al grupo Administradores. Esta consola es muy configurable, permitiéndonos añadir y quitar opciones según deseemos. De momento, vamos a trabajar con las opciones que aparecen por defecto.

Si nuestro equipo está unido a un dominio, podemos configurar directivas del dominio completo, que afectaran a varias maquinas. Sin embargo, nos vamos a centrar aquí en las directivas locales, ya que no estamos trabajando en un dominio, de momento.

Principalmente veremos que dentro de las **directivas de grupo locales** tenemos dos **opciones**: **Configuración del equipo** y **Configuración del usuario**. En el caso de estar trabajando en grupo de trabajo es prácticamente indistinto trabajar con una opción u otra.

Para aprender más de una directiva en concreto, simplemente tendremos que seleccionarla con el ratón, y veremos una descripción detallada de dicha directiva en el panel central.

Algunas directivas aparecen tanto en la configuración del equipo como en la configuración del usuario. En caso de conflicto, la configuración del equipo siempre tiene preferencia.



Para modificar el estado o configuración de una directiva, simplemente tenemos que realizar doble click sobre dicha directiva para que nos aparezca el cuadro de dialogo que nos permite modificar dicha directiva. En dicho cuadro de dialogo nos mostrará una explicación de la funcionalidad de dicha directiva.

Respecto a la configuración, veremos que podemos:

- ✓ **No configurar la directiva**, con lo que se comportará según el criterio por defecto para dicha directiva.
- ✓ **Habilitarla**, con lo que la pondremos en marcha en el sistema.
- ✓ **Deshabilitarla**, con lo que impediremos que se ponga en marcha dicha directiva.

Algunas directivas especiales permiten especificar otras informaciones.

Se recomienda leer cuidadosamente la explicación de cada directiva para entender sus efectos sobre el sistema y decidir habilitarla o no.

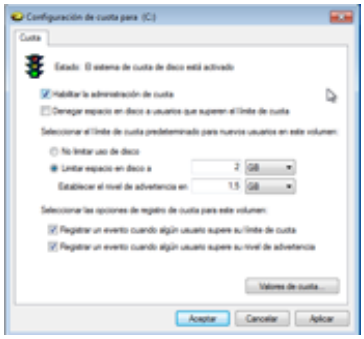
Probad a deshabilitar la directiva que hemos tomado como ejemplo (gpedit.msc - Configuración de Usuario - Plantillas Administrativas - Sistema - Impedir el acceso al símbolo del sistema) e intentad ejecutar una ventana de símbolo de comandos (cmd.exe)

Vemos como desde las directivas de grupo podemos modificar el comportamiento de Windows, dándonos una gran potencia en la administración del equipo.

3.3.- Cuotas de disco.

Uno de los recursos más importantes del ordenador es su capacidad de almacenamiento. Cuando un equipo es utilizado por varios usuarios, es preciso hacer una gestión del espacio de almacenamiento para que todos tengan el necesario.

Siguiendo esta idea podemos limitar para cada usuario el espacio del disco que puede emplear. Esta característica se conoce como **cuotas de disco**. Se pueden habilitar cuotas de disco al tener acceso a las propiedades del volumen de disco en el Explorador de Windows o mediante el objeto de directiva de grupo. Veamos cada uno de estos métodos:



A través del Explorador de Windows:

1. Haz click con el botón secundario en el volumen de disco para el que se desea habilitar cuotas de disco y, a continuación, haz click en `Propiedades`.
2. En la ficha `cuota`, haz click para seleccionar la casilla de verificación `Habilitar la administración de cuota` .

A través de directivas de grupo:

1. Establecer una directiva de grupo:

1. Haz click en `Inicio` , haz click en `Ejecutar`, escribe mmc y, a continuación, haz click en `Aceptar`.
2. En el menú `consola`, haz click en `Agregar o quitar complemento` .
3. Haz click en `Agregar`, haz click en `Directiva de grupo` bajo `Complementos independientes disponibles` y, a continuación, haz click en `Agregar` .
4. En el Asistente de seleccionar un objeto de directiva de grupo, bajo `Objeto de directiva de grupo`, deja la ubicación predeterminada del equipo local y a continuación, haz click en`Finalizar.`
5. Haz click en `Cerrar` y, a continuación, haz click en `Aceptar`.

2. Habilitar cuotas de disco en el objeto de directiva de grupo:
   1. En la `Raíz de consola`, expande `Directiva de equipo local`, expande `Configuración del equipo`, expanda `Plantillas administrativas` , expanda `sistema` y, a continuación, haz doble click en `Cuotas de disco` .
   2. Haz doble click en `Habilitar cuotas de disco` y selecciona `habilitado`
3. Reinicia el equipo.