UD 04_01 – Administración de un sistema operativo cliente tipo Windows.

Instalación. Usuarios y grupos. Contraseñas. ACLs.

Contenido

1 INTRODUCCIÓN

Entendemos como sistema operativo cliente el sistema que no está diseñado para actuar como servidor en un sistema informático, sino que desempeña el papel de sistema cliente conectado a un servidor. Estos sistemas operativos permiten trabajar tanto de forma separada sin conectarse a un servidor, como de forma conjunta uniéndose a un sistema informático mayor que cuente con un servidor.

Como sistemas operativos clientes típicos podemos citar, entre otros muchos, los siguientes:

- Windows 10
- Windows Vista
- Windows 7
- Windows 8
- GNU/Linux (Ubuntu, LinuxMint, etc.)
- Mac OS

De momento, en este tema vamos a ver cómo instalar y administrar someramente el sistema operativo Windows 7 en su versión Professional. Muchos de los conceptos que veremos son compatibles con cualquier otro sistema operativo de Microsoft, y algunos otros conceptos son incluso universales. No vamos a estudiar Windows 10 ya que en el terreno empresarial Windows 7 es el más usado con mucha diferencia.

2 VERSIONES DE WINDOWS 7

Para comprobar nuestra versión actual de Windows 7 tenemos que acceder al panel de sistema. Podemos acceder a esta pantalla desde Panel de Control y dentro elegir Sistema, o bien pulsando botón derecho del ratón sobre Mi PC (o equipo) y eligiendo la opción Propiedades, o bien pulsando la combinación de teclas Windows + Pausa.

Las tres versiones principales de Windows 7 son las siguientes:

- **Windows 7 Home Premium** es la versión que se suele montar en los sistemas dirigidos al usuario medio y no incluye algunas características como el escritorio remoto.
- **Windows 7 Professional** es la versión que se suele instalar en los sistemas dirigidos al sector profesional y excluye algunas características multimedia, como el servidor de contenidos multimedia.
- **Windows 7 Ultimate** tiene todas las características posibles.

Aparte de estas tres versiones principales, Microsoft también ha lanzado algunas versiones un tanto extrañas, como:

- Windows 7 Starter: no tiene interfaz Aero (efectos gráficos) y solo puede ejecutar 3 programas en multitarea como máximo.
- Windows Home Basic: no tiene interfaz Aero aunque la multitarea es total.

3 LA INTERFAZ DE WINDOWS 7

Windows 7 presenta una interfaz con algunas modificaciones importantes sobre versiones anteriores de Windows.

La **barra inferior** de Windows es muy parecida a la antigua, con el botón de inicio a la izquierda, un reloj y algunos iconos de programa a la derecha, y espacio libre en medio para alojar los iconos que representan programas. Estos iconos son algo más grandes en Windows 7 y permiten realizar dos funciones, ejecutar programas y cambiar entre los programas en ejecución. Podemos llevar cualquier icono de programa a la barra, de modo que este siempre disponible, aunque el programa no esté en ejecución, y podemos arrastrar los iconos de la barra para ordenarlos como mejor veamos.

Cuando movemos el cursor del ratón sobre un botón de la barra que representa a un programa en ejecución, el interfaz Aero nos muestra una previsualización en pequeño de cada ventana asociada a dicho botón. Si movemos el cursor a una de dichas visualizaciones se ocultarán todas las ventanas del escritorio para mostrarnos únicamente la ventana seleccionada.

Haciendo clic con el botón derecho sobre estos botones obtendremos un menú que nos permite realizar varias cosas, como abrir un documento cerrado anteriormente, abrir una nueva ventana, crear un nuevo documento, etc.

La interfaz general de Windows 7 es muy configurable, permitiéndonos establecer comportamientos para multitud de componentes. Podemos acceder a estas opciones desde Panel de Control – Apariencia y personalización.

Dos opciones que merece la pena destacar sobre la interfaz de Windows 7 son:

- **Búsqueda de ficheros**. Podemos escribir en cualquier ventana del explorador de archivos el nombre de cualquier fichero que deseemos, y Windows 7 localizará dicho fichero. Podemos refinar estas búsquedas para buscar por contenido, indexar localizaciones, almacenar búsquedas, etc.

- **El botón de inicio**. Podemos simplemente pulsar en el teclado la tecla Windows y a continuación escribir el nombre de cualquier programa que queramos ejecutar, veremos cómo Windows localiza dicho programa (muchas veces basta con introducir algunos caracteres) y nos permite lanzarlo directamente con la tecla Intro. Esta opción también nos permite buscar documentos y no está limitada a buscar por cadenas literales desde el inicio, sino que podemos buscar por cualquier parte del nombre, e incluso buscar dentro de los documentos el texto deseado.

4 INSTALANDO Y CONFIGURANDO WINDOWS 7

4.1 Requisitos de hardware

Antes de instalar cualquier sistema operativo, es conveniente asegurarnos de que los componentes de nuestro hardware cumplen los requisitos mínimos de dicho sistema. Si lo instalamos en un sistema moderno, no debería haber muchos problemas, pero en sistemas más antiguos si podemos encontrarnos con incompatibilidades.

En concreto, los requisitos de hardware de Windows 7 son los siguientes:

https://support.microsoft.com/es-es/help/10737/windows-7-system-requirements

- Procesador de 32 bits (x86) o 64 bits (x64) a 1 GHz o más.
- Memoria RAM de 1 gigabyte (GB) (32 bits) o memoria RAM de 2 GB (64 bits).
- Espacio disponible en disco duro de 16 GB (32 bits) o 20 GB (64 bits).
- Dispositivo gráfico DirectX 9 con controlador WDDM 1.0 o superior.

4.2 Revisión de la compatibilidad hardware y software

Una vez hemos determinado que los componentes del equipo cumplen los requisitos mínimos necesarios para la instalación, debemos asegurarnos de que el hardware del equipo es compatible con Windows 7 antes de lanzar la instalación. Podemos encontrar un asistente de compatibilidad en el propio disco de instalación de Windows 7.

4.3 Posibilidades de la instalación

Hay una serie de decisiones que debemos tomar antes de la instalación de Windows 7:

Edición de Windows 7 a instalar. Ya explicamos anteriormente las diferencias entre versiones. Si no introducimos la información de registro a la hora de instalar Windows 7, Microsoft nos permitirá usar durante 30 días el sistema sin ningún tipo de limitación. Esto puede servirnos para probar varias versiones y escoger la que más nos convenga.

Instalación nueva o actualización. Una instalación nueva comienza desde cero, deberemos reinstalar todos nuestros programas y configuraciones. Una actualización a Windows 7 necesita que en la maquina tengamos ya instalada una versión anterior de Windows. Es altamente recomendable instalar siempre un sistema desde cero, ya que si actualizamos el sistema resultante no será 100% estable en la mayoría de las ocasiones. (Ejemplo de actualizaciones: http://www.youtube.com/watch?v=vPnehDhGa14)

Particionado del disco duro. Durante la instalación podremos crear y borrar particiones de cualquiera de nuestros discos duros. Debemos escoger dónde vamos a instalar Windows 7. Por defecto, veremos cómo Windows 7 intenta crear una partición primaria inicial en el disco para instalar todos sus archivos de arranque.

Cómo invocar el proceso de instalación. Podemos iniciar el sistema directamente desde nuestro disco de instalación, modificando la BIOS si es necesario para que arranque el sistema desde allí. También es posible introducir el disco de instalación en nuestro Windows anterior sin tener que reiniciar la máquina y escoger la opción de instalar Windows 7.

Entre ambas opciones existen diferencias importantes:

Si ejecutamos la instalación desde un Windows anterior, introduciendo el DVD de Windows 7.	**Si ejecutamos la instalación arrancando el sistema desde el DVD de Windows 7.**
Podemos actualizar una versión anterior de Windows a Windows 7.	No podemos actualizar una versión anterior de Windows.
Podemos reinstalar Windows 7.	No podemos reinstalar Windows 7.
Podemos ejecutar un asistente que nos permite comprobar la compatibilidad con Windows 7 el hardware y el software actual.	No podemos acceder al asistente.
Podemos instalar Windows 7 en la misma unidad que otro Windows.	Podemos instalar Windows 7 en la misma unidad que otro Windows.
No podemos modificar las particiones el disco duro.	Podemos crear y borrar particiones de cualquier disco duro.

4.3.1 Instalación limpia

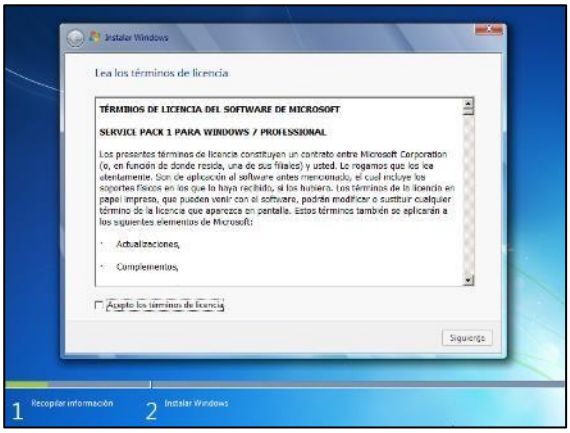
Este tipo de instalación es el más simple y el comúnmente recomendado. Debemos conseguir que el ordenador arranque y cargue directamente desde el DVD de Windows 7, impidiendo que arranque desde el disco duro por si acaso en este hay algún otro sistema operativo.

Debemos estar atentos en el inicio del sistema, ya que normalmente deberemos pulsar una tecla para que el equipo arranque desde el DVD.

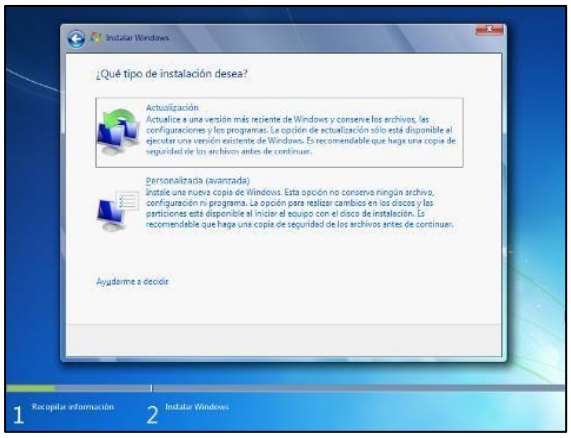
Si el equipo no arranca desde el DVD, deberemos acceder a la BIOS y modificar el orden de arranque del sistema. Si nos encontramos con un equipo que no cuente con una unidad óptica (netbooks por ejemplo) intentaremos arrancar bien con una lectora de DVD externa, o bien desde una memoria USB donde habremos copiado antes el DVD de Windows 7. (Buscando en google podremos encontrar bastante tutoriales que nos indican cómo conseguir transferir el arranque desde el DVD hasta la memoria USB).

Una vez conseguido arrancar el sistema desde el DVD, veremos un par de pantallas que nos permiten indicar nuestras preferencias en cuanto al idioma.

Posteriormente veremos el EULA (End User License Agreement) o lo que es lo mismo, la licencia de uso del sistema operativo Windows 7. Debemos indicar que estamos de acuerdo con la misma para proseguir con la instalación.

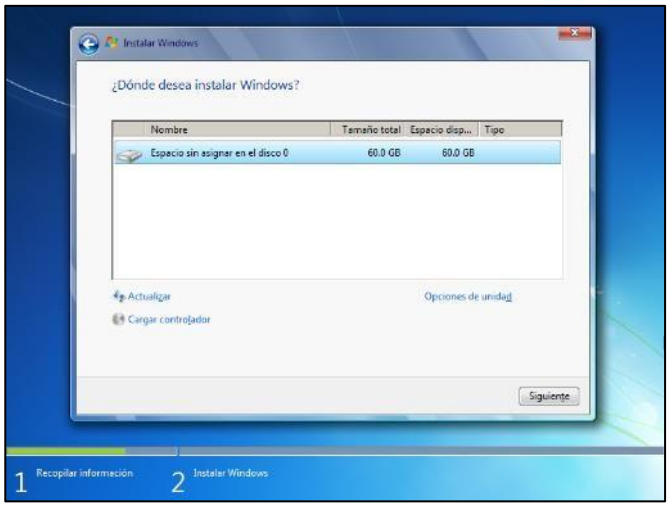


Accederemos entonces a una pantalla donde podremos elegir el tipo de instalación que deseamos realizar.

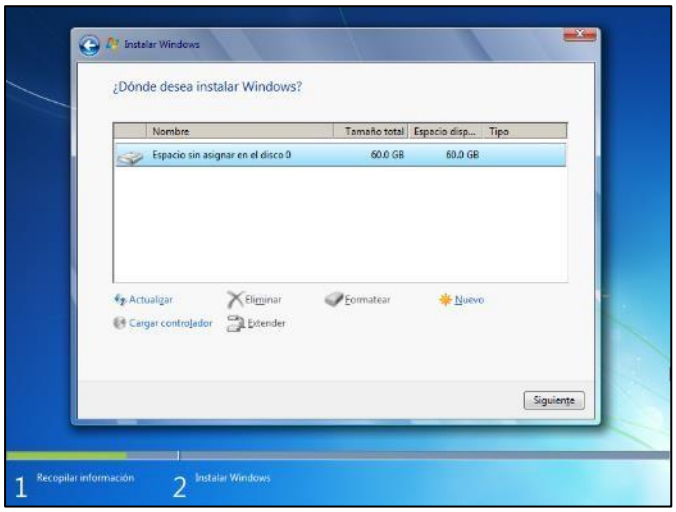


Como hemos iniciado el sistema desde el DVD la opción para actualizar el sistema no funcionará, y si intentamos seleccionarla obtendremos un error. Debemos seleccionar la opción Personalizada (avanzada) para continuar con nuestra instalación desde cero.

A continuación, el sistema nos preguntará dónde queremos instalar Windows 7.

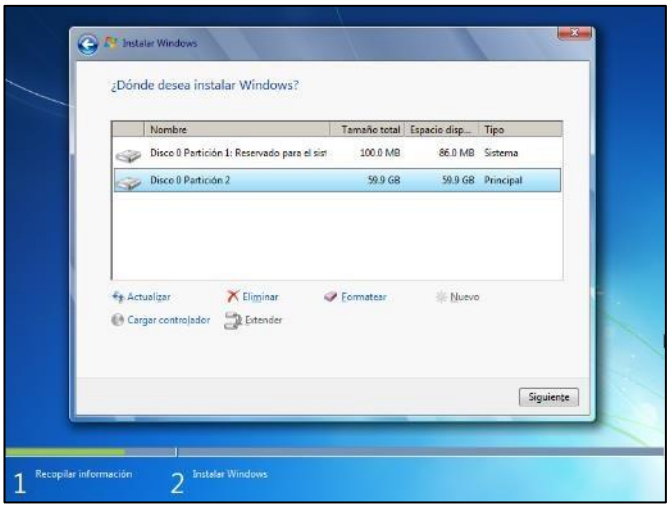


En este ejemplo vemos como el sistema sólo cuenta con un único disco duro (disco 0) de 60 GB y que está totalmente limpio (60 GB de espacio disponible). Si quisiéramos elegir una partición en concreto, crearla, modificarla o eliminarla debemos escoger Opciones de unidad.



Vemos cómo ahora sí nos permite seleccionar las opciones para Eliminar, Formatear, crear una partición Nueva e incluso Extender una partición. Una vez creada la partición y seleccionada, pulsamos Siguiente.

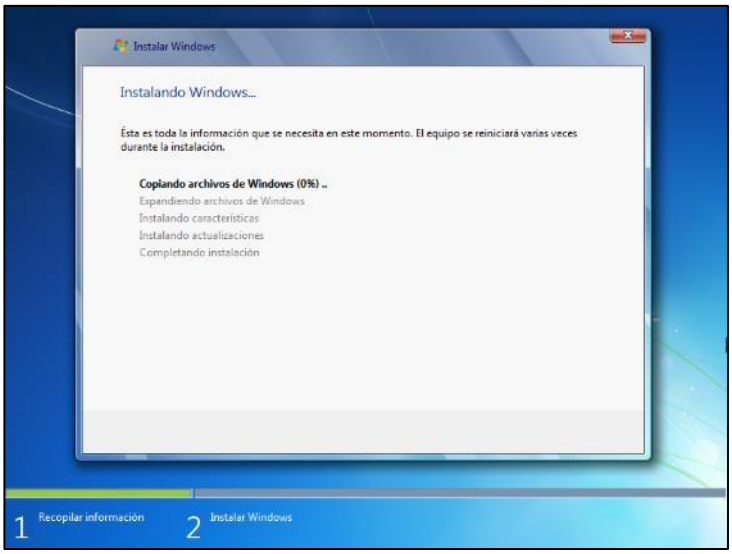
Windows 7 intenta crear siempre una partición inicial para arranque del sistema de 100 MB. Esta partición le sirve para almacenar los ficheros necesarios para iniciar el sistema. En caso de que sea imposible crear esta partición, Windows 7 instalará dichos ficheros en la propia partición donde se instala.



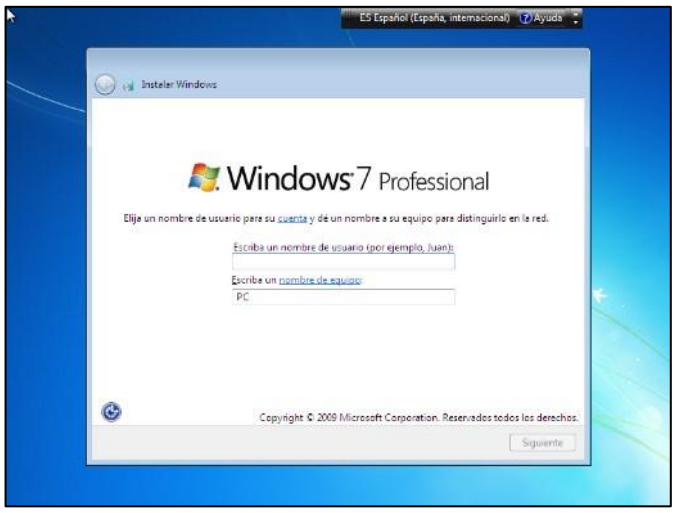
El DVD de Windows 7 contiene drivers (controladores) para las controladoras de disco duro más usadas, pero podría darse la circunstancia de que el driver que utilizamos no esté incluido entre ellos. Esto hará que W7 no pueda reconocer nuestro disco duro, y por lo tanto no aparecerá en la lista de unidades. Si se diera este caso, vemos cómo hay una opción que nos permite solucionar esto: Cargar controlador. Esto nos permite guardar el driver de la controladora en una unidad USB (normalmente lo descargaremos desde Internet o bien lo sacaremos del CD de instalación de la placa base).

Una vez que hemos seleccionado el disco duro y la partición del mismo donde queremos instalar Windows 7, el programa de instalación comenzará a copiar los ficheros del DVD a la partición y

descomprimirlos. Una vez realizado esto configurará nuestro hardware y realizará todas las tareas necesarias para instalar Windows 7. Es el proceso que más tiempo ocupa y no necesita de la intervención del usuario en ningún momento.

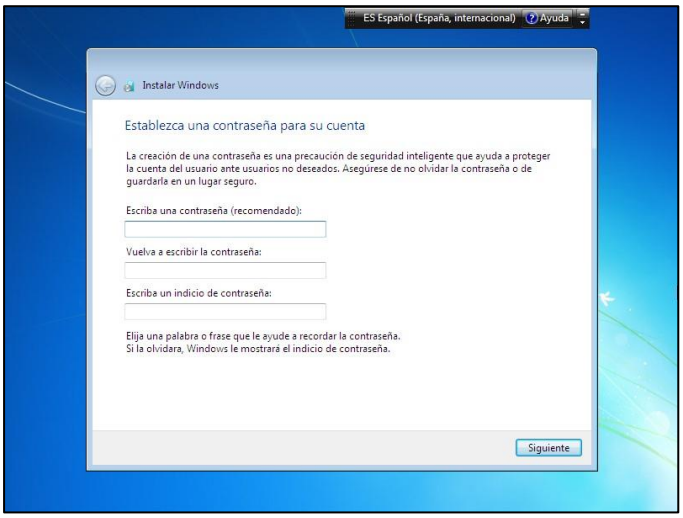


Una vez terminado el proceso anterior, Windows 7 solicitará al usuario algunos datos muy importantes.



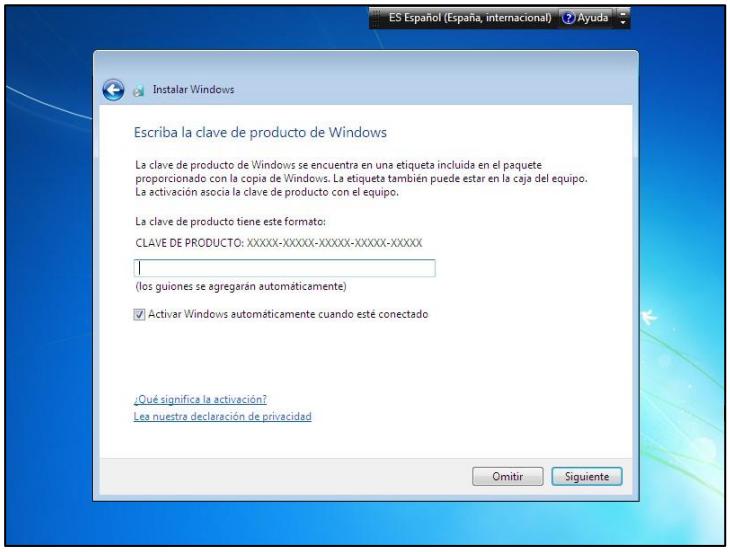
El **nombre de usuario** que nos pide en este momento será el nombre de la primera cuenta creada en el sistema. Dicha cuenta contará con permisos de administración del sistema, ya que será miembro del grupo Administradores. El **nombre de equipo** se recomienda que sea conciso. Hay que evitar que el nombre del equipo sea también el nombre de una cuenta de usuario.

A continuación, podremos introducir una **contraseña** para el usuario creado. Aunque no es obligatorio es muy recomendable. (Punto importante: Un Administrador de Sistemas NUNCA debe olvidar una contraseña, así que mucho cuidado en este punto).

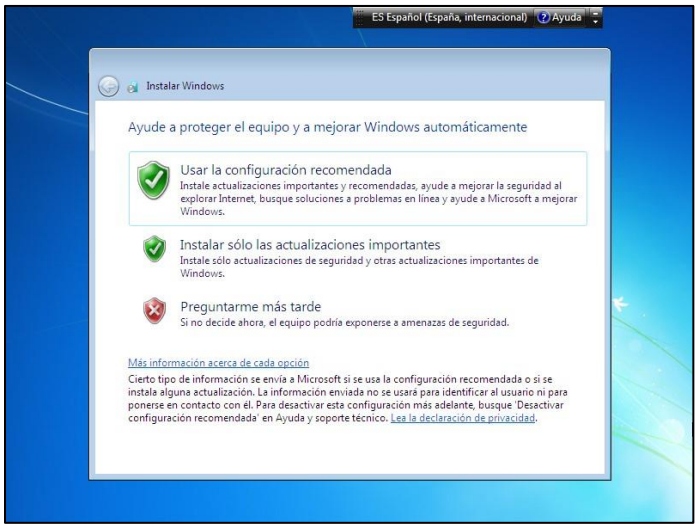


Al igual que es muy recomendable utilizar contraseñas, no es nada recomendable utilizar el campo que nos permite indicar un **indicio** de la contraseña, ya que este campo es público y puede ser visto por cualquier usuario, que en un momento dado podría llegar a adivinar nuestra contraseña a partir de la información que escribamos aquí como indicio. Dado que Windows 7 no nos permite dejar este campo en blanco se aconseja escribir algún o algunos caracteres al azar.

Ahora Windows 7 nos pedirá que introduzcamos una **clave de producto** (Product Key). Esta clave será validada por un servidor de Microsoft una vez que tengamos activa la conexión a Internet de nuestro ordenador. No es un campo obligatorio en este punto de la instalación, y podemos dejar dicho campo en blanco y desactivar la casilla Activar Windows automáticamente cuando esté conectado. Esto nos permitirá usar Windows 7 durante unos 30 días sin tener que introducir ninguna clave. Pasados estos días de prueba, o bien introducimos una clave valida o será imposible seguir usando Windows 7.



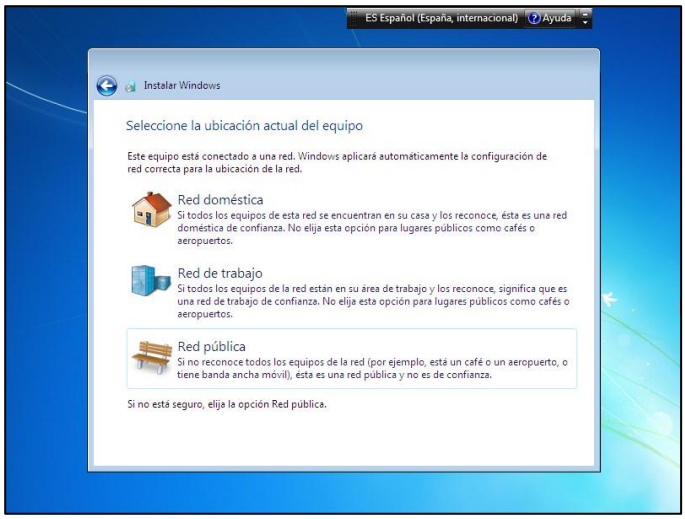
A continuación, W7 nos permite configurar las **actualizaciones automáticas**. (Muy recomendable escoger la primera opción por motivos de seguridad).



Si no activamos estas actualizaciones automáticas, nuestra máquina no descargará los parches de seguridad que vayan siendo lanzados por Microsoft, de modo que nuestro sistema será vulnerable a todos los exploits o agujeros de seguridad que vayan siendo descubiertos en el software de nuestra máquina.

En la siguiente pantalla W7 nos permite elegir nuestra zona horaria y la hora y fecha actuales.

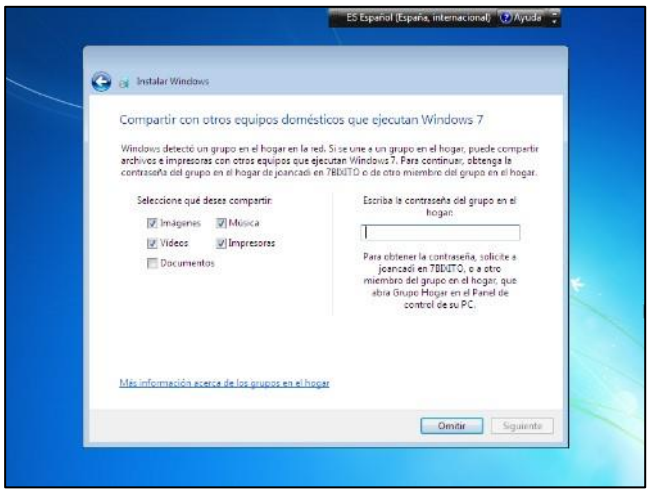
Ahora Windows 7 puede presentarnos diversas pantallas, según sea capaz de reconocer nuestra red y conectarse automáticamente a Internet o no. Es posible por ejemplo que en este punto nos pregunte la clave de nuestra red WiFi para poder conectarse, o que nos muestre un mensaje indicando que no está disponible ninguna conexión a Internet.



Si vemos la anterior pantalla, es que la conexión ha podido ser realizada sin problemas. Las dos primeras opciones nos permiten conectarnos a la red sin ningún tipo de problemas.

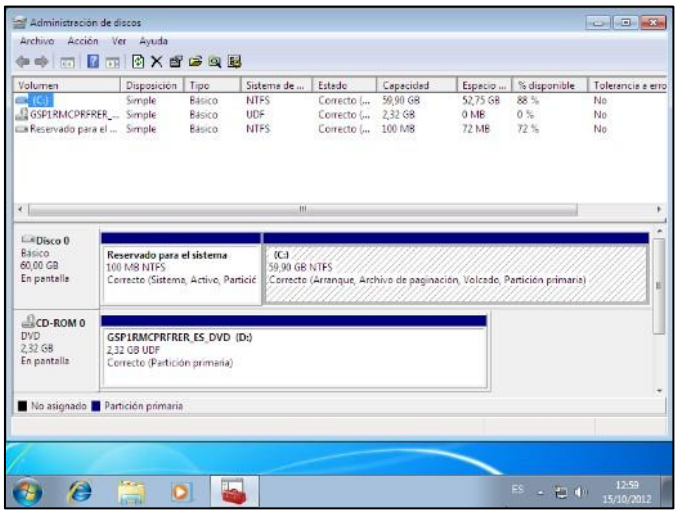
- La opción **Red doméstica** permite además configurar un grupo de trabajo para compartir nuestros documentos.
- La opción **Red de trabajo** no configura automáticamente dicho grupo de trabajo.
- La opción **Red pública** le indica a Windows 7 que estamos conectados en un entorno inseguro (una WiFi pública en la calle, por ejemplo) y activa un sistema de seguridad mayor que no permite compartir documentos y nos protege de posibles ataques.

Vemos aquí la pantalla que nos muestra Windows 7 si le indicamos que queremos pertenecer a una Red doméstica. Podemos seleccionar los tipos de documentos que queremos compartir automáticamente y definir una contraseña para proteger la conexión. Si ponemos esta misma contraseña en varios equipos de Windows 7 tendremos montada una red doméstica bastante funcional y sin tener que configurar nada en los equipos. (Todos los equipos deben ejecutar Windows 7).



4.4 La partición de 100MB

Si instalamos Windows 7 en un disco duro sin particiones, veremos que crea una partición de 100MB y la reserva para el sistema. A esta pequeña partición no se le asigna ninguna letra de unidad así que el usuario normalmente ni siquiera se da cuenta de que está creada a menos que usemos el gestor de discos (DISKMGMT.MSC).



Esta partición sirve para dos funciones. En primer lugar, almacena los ficheros de inicio del sistema y la base de datos de configuración del inicio (BCD). En segundo lugar, almacena la información requerida para usar la encriptación de volúmenes BitLocker (se explicará posteriormente).

Si decidimos que nunca vamos a usar la encriptación de volúmenes podemos evitar que Windows 7 cree esta partición, pero para ellos deberemos crear las particiones con un programa distinto al que viene incluido en el DVD de instalación de W7. Si al instalar le indicamos que use una partición ya creada anteriormente, Windows 7 no creará la partición de 100 MB.

4.5 Instalar Windows 7 en una partición donde ya hay otro Windows

Una opción muy interesante que Microsoft añadió a Windows Vista y que sigue presente en Windows 7 es la de permitir instalar Windows en una partición donde ya existe una versión de Windows, pero sin actualizarla, sino desde la instalación limpia.

El programa de instalación de Windows 7 moverá automáticamente los directorios **Windows**, **Archivos de programa** y **Usuarios** a una carpeta nueva con el nombre de **Windows.old**.

Esto nos permitirá tener nuestro nuevo sistema Windows 7 instalado desde cero, pero sin tener que sacar copias de seguridad de los datos del Windows anterior. Simplemente tendremos que acceder a esta carpeta Windows.old e ir copiando los archivos que nos interesen a sus nuevas ubicaciones.

Es importante hacer constar que ese Windows antiguo no podrá volver a ser usado para arrancar el sistema, sólo se guarda para asegurarnos de no perder nada y no tener que sacar copias de seguridad a un medio externo normalmente muy lento.

Una vez que hemos recuperado todos los archivos deseados, podemos borrar esa carpeta Windows.old sin ningún tipo de problemas.

4.6 Activación y validación de Windows 7.

Vimos que la instalación de Windows 7 nos pedía una clave de producto (Product Key). Estas PK son cadenas de 25 caracteres alfanuméricos que son únicas para cada equipo en todas las versiones de las claves menos en las de licencias por volumen.

Esta clave de producto viene ya introducida en cualquier copia de Windows que venga preinstalada al comprar un ordenador nuevo. Si usamos el DVD de Windows 7 suministrado por el fabricante comprobaremos que no nos pide de nuevo la clave.

Cada clave es dependiente de la edición de Windows adquirida. Es decir, al introducir la clave el propio sistema sabe si dicha clave es para un Windows 7 Professional, Home, etc. Si introducimos una clave que no pertenece a la versión de Windows 7 que estamos instalando, el sistema nos indicara que dicha clave es incorrecta.

Vimos en el punto anterior referente a la instalación de Windows 7 cómo no era obligatorio introducir la clave en el momento de la instalación. Podremos usar la copia instalada de Windows 7 sin ningún tipo de restricciones durante 30 días. Antes del fin de este periodo de prueba debemos entrar una PK valida y activar nuestra copia de Windows en Internet. Si no activamos Windows 7, el sistema nos pedirá que lo activemos (cada vez de forma más vehemente) hasta que nos impida utilizarlo por completo.

4.6.1 Ampliación del período de evaluación

Existe una forma de ampliar el periodo de prueba de 30 a 60 días, llegando incluso a ampliarlo hasta 120 días. Para hacer esto debemos abrir el prompt del sistema **(cmd) con permisos de administrador** y escribir el siguiente comando:

```
slmgr -rearm
```

Cuando completemos este comando debemos reiniciar el sistema y veremos como el sistema nos permite seguir usándolo 30 días más. Este "truco" podemos utilizarlo hasta un total de 3 veces, con lo que conseguimos un periodo de prueba de 120 días.

4.6.2 Licencias OEM

Las licencias OEM no permiten borrar Windows de un equipo e instalarlo en otro. Si el servidor de activaciones detecta una licencia OEM que ha cambiado de equipo directamente la considerará inválida.

4.6.3 Activando una copia retail de Windows

Desde Windows XP, Windows obliga a que activemos online cualquier copia de Windows, ya sea conectándonos por Internet al servidor de activaciones de Microsoft (proceso transparente para el usuario) o bien mediante una llamada telefónica gratuita a una centralita automatizada de Microsoft.

Cada licencia de Windows 7 normalmente admite ser activada en un único equipo, y al activarlo online en el servidor de activación de Microsoft queda almacenado un registro con la clave de licencia introducida y un código que identifica a nuestro ordenador. Si intentamos activar

Windows en otro equipo con esa misma licencia, se detectará en el servidor de activaciones que ya existe un registro con esa clave y que está asignada a un equipo distinto al que estamos usando.

Existen licencias especiales de Microsoft que permiten ser activadas en más de un equipo al mismo tiempo. Unas son las conocidas como licencias para la familia, que permiten ser activadas en 3 ordenadores distintos con un coste inferior al que representaría comprar 3 licencias retail.

Otras licencias que permiten ser activadas varias veces son las licencias por volúmenes, normalmente usadas por las empresas.

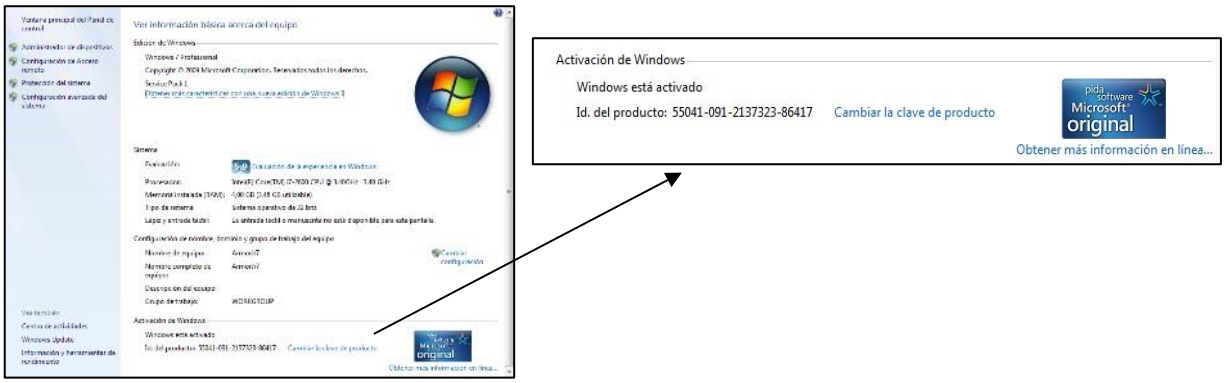
Hemos comentado que en los servidores de activación de Microsoft queda almacenado un registro donde se almacenan la clave de la licencia y un código que identifica nuestro ordenador. Si cambiamos alguna pieza importante de nuestro ordenador, cuando lo iniciemos y el sistema se conecte online detectará que el código del ordenador ha cambiado. Normalmente no tendremos ningún problema con esto, pero si el servidor de activaciones entiende que hemos cambiado varias veces de equipo, nos pedirá que reactivemos nuestra copia de Windows rellenado un simple formulario y, si las anomalías continúan, poniéndonos en contacto telefónico con un operador mediante un número de teléfono gratuito.

La licencia retail nos permite borrar Windows de un equipo e instalar Windows en un equipo nuevo, esto será tratado por el servidor de activaciones de Microsoft y no nos mostrará ningún mensaje, siempre y cuando el antiguo equipo nunca intente activarse con la clave de Windows que estamos usando en nuestro nuevo equipo. Es por esto que si usamos una clave de W7 para activar más de un equipo, será rápidamente detectada por Microsoft, y normalmente dicha clave pasará a la lista negra de claves y quedará inutilizada.

Nuestros equipos se ponen en contacto habitualmente con estos servidores de activación de Microsoft, es decir, que no se limitan a conectarse en el proceso de activación, sino que la comunicación es bastante frecuente.

Si nuestra clave se desactiva en alguna de estas comprobaciones, comprobaremos que el fondo de pantalla se queda en negro, un mensaje recordándonos que tenemos que activar el sistema ya que éste no es una copia genuina de Windows aparecerá en el escritorio, y un formulario pidiéndonos que activemos el software aparecerá de vez en cuando en primer plano. Al mismo tiempo, las actualizaciones automáticas quedaran restringidas, permitiendo únicamente descargar los parches de seguridad. A pesar de todo esto, la copia de Windows podrá seguir siendo usada durante un tiempo, y en algunas ocasiones Microsoft puede permitir que estas copias puedan ser usadas indefinidamente.

Para comprobar si nuestro Windows 7 es original y está activado, podemos acceder a las propiedades del Sistema (Windows + Pausa).



5 El proceso de arranque de Windows 7

En un tema anterior ya vimos cómo era el proceso de arranque de Windows 7, pero sin incluir todas las opciones del mismo. Vamos a ver ahora dicho proceso añadiendo estas opciones:

1. BOOTSTRAP – POST – MBR. (Todo este sistema ya lo hemos estudiado ampliamente).
2. El MBR lee el sector de arranque de la primera partición activa. Este sector de arranque carga el programa Bootmgr.
3. Bootmgr lee el contenido de la base de datos BCD, que contiene información sobre la configuración de todos los sistemas operativos instalados en el equipo. Si es necesario muestra un menú por pantalla para que el usuario pueda escoger el SO a cargar.
4. Cuando escojamos una opción de este menú (o el sistema lance automáticamente la entrada del menú por defecto) el sistema realizara una de las siguientes acciones:
    a. Si escogemos un SO Windows 7 o Vista, Bootmgr ejecuta Winload.exe desde el directorio %SystemRoot%\System32.
    b. Si el sistema comprueba que hemos hibernado Windows 7 o Vista, Bootmgr ejecuta el programa Winresume.exe y restaura la sesión hibernada.
    c. Si escogemos una versión anterior de Windows, Bootmgr le cede el control al programa Ntldr.exe, que a su vez leerá el fichero boot.ini y puede mostrarnos por pantalla un menú para elegir entre distintos Windows (todos anteriores a Vista).

El programa Winload.exe que se encarga de ejecutar Windows 7, comienza ejecutando los programas que se encargan de cargar el núcleo (Ntoskrnl.exe y Hal.dll), leyendo las configuraciones del registro de Windows, y cargando los drivers necesarios para inicializar el hardware. A continuación, inicia la aplicación que se encarga de iniciar nuestro propio Windows 7 (Wininit.exe) que a su vez inicia un programa que se encarga de gestionar toda la seguridad local (Lsass.exe) y también inicia un programa que se encarga de iniciar los servicios (Services.exe). Una vez ejecutados todos estos procesos, el sistema ya está preparado para que iniciemos sesión en el sistema (o lo que es lo mismo, que hagamos login en el sistema).

6 SEGURIDAD EN WINDOWS 7

Windows 7 es el sistema operativo más utilizado en la actualidad, esto conlleva que es el sistema operativo más atacado. En un entorno doméstico no tenemos por qué preocuparnos excesivamente de la seguridad del sistema, pero en un entorno empresarial la seguridad cobra un papel importantísimo.

Windows 7 es un sistema mucho más seguro que versiones anteriores de Windows como XP. El sistema ha sido diseñado y su arquitectura modificada para conseguir esto.

6.1 Amenazas a la seguridad del sistema

Cuando hablamos de amenazas a la seguridad de nuestro sistema, normalmente nos estamos refiriendo a virus, gusanos, troyanos y spyware (software espía).

- **Virus**. Es un programa que se autoreplica, normalmente incrustándose en otros ejecutables. La infección se extiende cuando un usuario lanza un ejecutable que ha sido infectado, momento en el que el virus aprovecha para incrustarse en más ejecutables del sistema atacado. Hoy en día no son una gran amenaza, ya que son fácilmente detectados por los antivirus.
- **Gusanos**. Son programas que se replican de un ordenador a otro utilizando la red. Son mucho más peligrosos que los virus ya que los antivirus no son demasiado efectivos contra ellos, sin embargo, necesitan para su funcionamiento que tengamos abierto un puerto en nuestro sistema y que ese posea un fallo de seguridad importante para que el gusano pueda introducirse. Si nuestro sistema esta actualizado es bastante improbable que seamos atacados por un gusano.
- **Troyanos**. Son programas que se introducen en nuestro sistema con permiso del usuario. Suelen hacerse pasar por programas inofensivos y son los más peligrosos hoy en día, ya que existen muchas formas de ejecutar uno de estos troyanos desde una página web, ya sea haciéndose pasar por un visor de vídeos o programa parecido, o incluso aprovechando fallos de seguridad de los navegadores web para ejecutarse directamente sin que el usuario pueda hacer nada para evitarlo una vez que ha visitado una página preparada a tal fin.
- **Spyware**. Son programas que no deseamos en nuestro sistema, que se suelen encargar de mostrarnos publicidad, de rastrear las páginas que visitamos en internet, mostrarnos ventanas emergentes (pop-ups) de anuncios, ponernos barras en los exploradores de internet, modificar las configuraciones de Windows para que no podamos eliminarlos, etc. Normalmente se suelen introducir con permiso del usuario, por lo que muchos antivirus no los eliminan, ya que se comportan como programas legales.

A todas estas amenazas se las suele conocer con el nombre genérico de malware. En el peor de los casos, son capaces de instalar en nuestro equipo un servidor que servirá como puerta trasera, permitiendo que el atacante ejecute código en nuestro sistema siempre que quiera. Estos sistemas afectados de esta manera se conocen como equipos zombis o bots (de robot) y los que controlan dichos sistemas montan lo que se conoce como botnets, redes de miles de estos ordenadores zombis, controlados para realizar ataques sobre distintos servidores de Internet.

6.2 Características de Windows 7 para la seguridad

Las principales características que se han añadido o mejorado en Windows 7 (y algunas en Vista) referentes a la seguridad son:

- **Firewall de Windows**. El firewall o cortafuegos de Windows ha sido mejorado ampliamente sobre el cortafuego que se utilizaba en XP. Es un firewall de dos sentidos, monitorizando tanto el tráfico de entrada como el de salida de nuestra red, y soporta en su totalidad el protocolo IP en su versión 6 (IPv6). Se añaden en Windows 7 múltiples perfiles lo que permite que tengamos distintas configuraciones para distintas redes. Dispone además de una consola de configuración avanzada, lo que nos permite establecer nuestras propias reglas para el cortafuego, y a un nivel muy bajo, además.

- **Control de Cuentas de Usuario (UAC)**. Nos permite usar una cuenta de usuario normal para utilizar Windows, ya que cuando el usuario desee realizar una acción que necesite permisos de administración UAC se encargará de pedirnos dichas credenciales mediante un pop-up en pantalla. En Windows 7 se ha mejorado el sistema de modo que veremos menos veces estos avisos, que eran excesivamente frecuentes en Windows. No es nada recomendable desactivar UAC como hacen algunos usuarios, ya que es una barrera bastante útil contra el malware. Podemos configurar el nivel de alerta de esta herramienta escribiendo UAC directamente desde el Inicio.

- **Windows Defender**. Es un antispyware gratuito de Microsoft, que monitoriza el sistema para prevenir la instalación de los spyware más famosos, y de avisarnos si algún programa se comporta como un spyware.

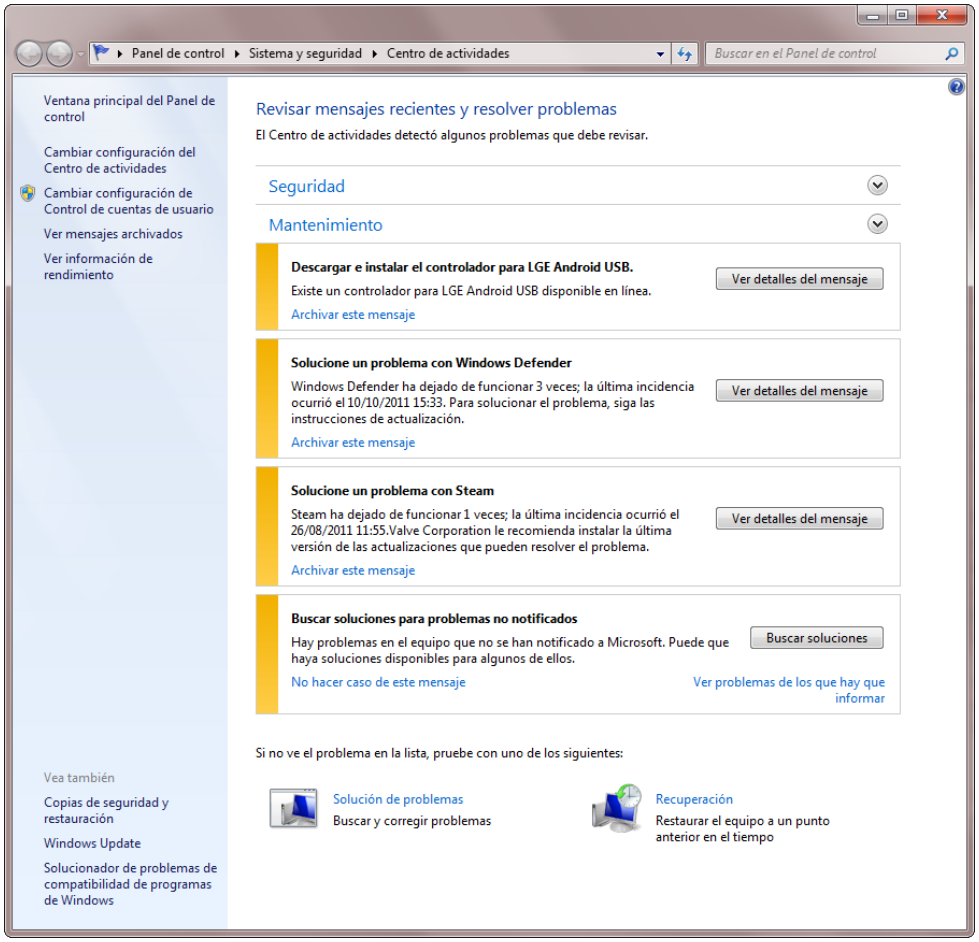
- **Internet Explorer**. IE se ejecuta en modo protegido, que limita la capacidad de cualquier código malicioso para instalarse en el sistema.

- **Encriptación**. Windows 7 incluye en sus versiones Enterprise y Ultimate la posibilidad de cifrar volúmenes completos de datos NTFS mediante el "Bitlocker Drive Encryption". Podemos cifrar particiones del disco duro, memorias USB, discos externos, etc.

- **Windows Security Essentials**. Aunque no es una característica de Windows 7 debemos reseñarla aquí, ya que es un antivirus de Microsoft totalmente gratuito (para versiones originales de Windows) y bastante funcional. Este programa también realiza las funciones de Windows Defender, por lo que no funcionarán ambos juntos.

En Windows 7 podemos acceder al Centro de Actividades, que nos da un vistazo rápido sobre la seguridad del sistema. Nos informa de las posibles amenazas detectadas en el equipo. Este centro de actividades no sólo funciona con software de Microsoft, sino que también reconocerá los principales programas de seguridad de otras compañías.

Un apartado tremendamente importante para la seguridad de nuestro sistema es activar las actualizaciones automáticas, ya que si nuestro equipo no está actualizado será mucho más vulnerable al no tener corregidos todos los agujeros de seguridad que se vayan descubriendo.



7 SEGURIDAD, AUTENTIFICACIÓN Y AUTORIZACIÓN

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. Veremos cómo gestionar las **cuentas de usuario** en el siguiente punto.

- **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**.

8 GESTIÓN DE CUENTAS DE USUARIOS Y GRUPOS

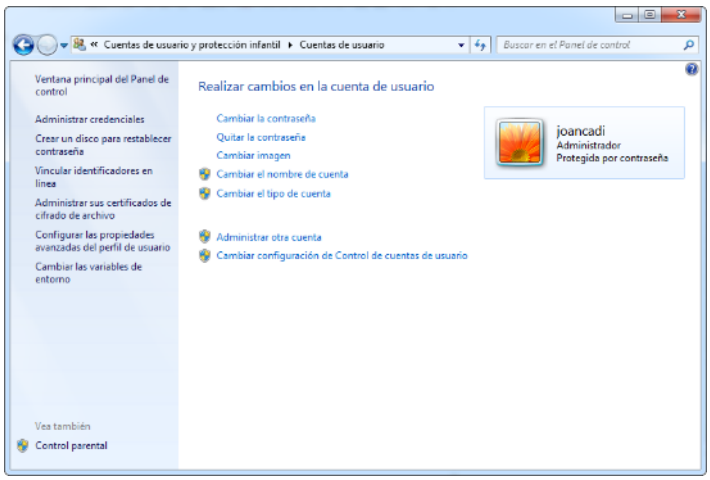
Podemos crear, borrar y modificar cuentas de usuario en Windows usando varias técnicas distintas.

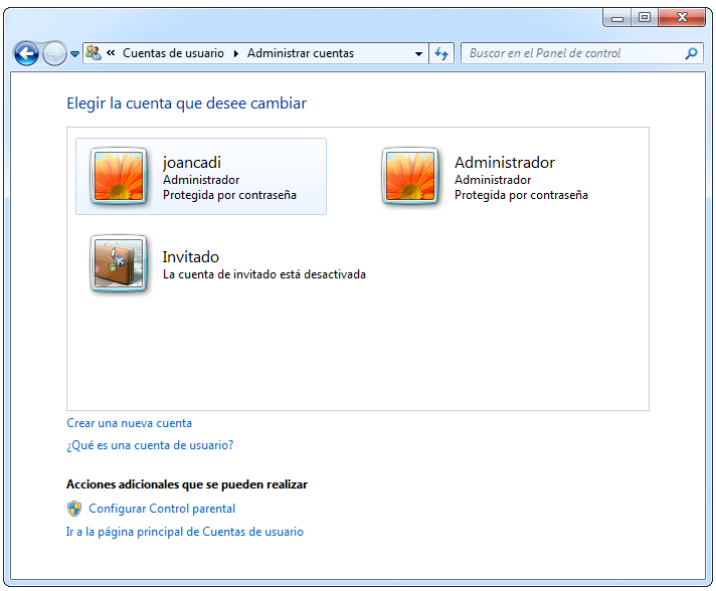
1. Asistente para cuentas de usuario desde Panel de Control.
2. Gestión de cuentas de usuario y grupo locales mediante consola.
3. Gestión de cuentas de usuario mediante consola especial.
4. Gestión de cuentas de usuario desde el interfaz de línea de comandos de Windows (CLI).

8.1 Asistente para cuentas de usuario desde el panel de control

Para abrir la herramienta Cuentas de usuarios, hay que abrir el Panel de control desde el menú Inicio - Cuentas de usuario.

Desde aquí podemos crear cuentas, modificarlas, cambiar contraseñas, gráficos asociados a la cuenta, etc.





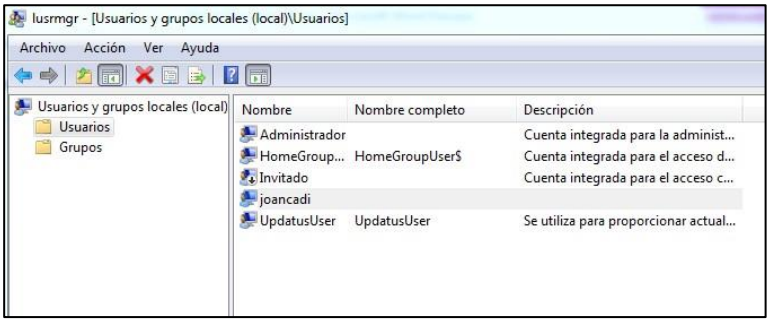
Esta es la opción más simple para crear cuentas de usuario, es fácil de usar, pero muy poco potente. Aunque con distintas prestaciones, básicamente esta aplicación es igual entre XP, 2008, Vista y 7. En Windows 10 es similar, aunque la versión Home intenta crear las nuevas cuentas a partir de datos como cuentas de correo, teléfono o o una cuenta de Microsoft de los nuevos usuarios que se van a crear, en cualquier caso, nos podemos saltar esto y finalmente crear la cuenta como en los sistemas operativos anteriores.

8.2 Gestión de cuentas de usuarios y grupos locales mediante consola

Otra opción que tenemos para gestionar cuentas de usuario, es la consola de usuarios locales y grupos. Podemos llegar a dicha consola de varias formas, aunque la más rápida es invocándola directamente desde Inicio – Ejecutar y escribir **LUSRMGR.MSC**

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 (botón derecho sobre el usuario y escogiendo Propiedades, o directamente realizando doble clic sobre el usuario).



8.2.1 Grupos

Del mismo modo que trabajamos con usuarios, podemos hacerlo con los grupos, creando grupos nuevos o modificando los ya existentes.

Un usuario puede pertenecer a todos los grupos que deseemos, y un grupo puede contener tantos usuarios como necesitemos.

Podemos crear todas las cuentas de usuarios que queramos, pero aparte de estas cuentas normales, existen dos cuentas de usuario especiales en Windows, ya creadas y que no pueden (no deben) ser modificadas o eliminadas.

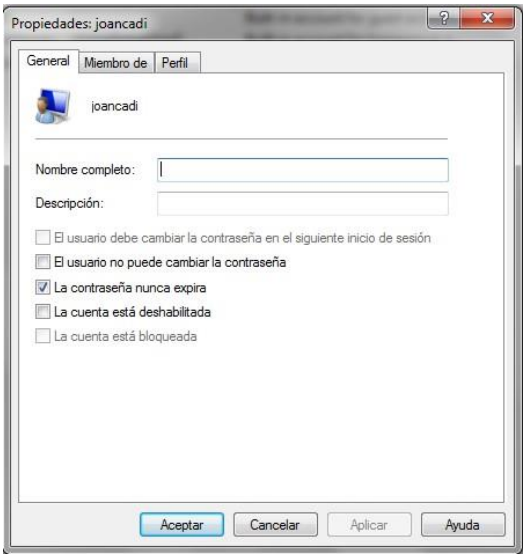
- La cuenta del **Administrador** del sistema (Administrador). Todos los sistemas Windows tienen una cuenta especial conocida como Administrador. Esta cuenta tiene todos los derechos sobre todo el equipo. Puede crear otras cuentas de usuario y es el responsable de gestionar el sistema. Muchas funciones del sistema están limitadas para que solo puedan ser ejecutadas por el Administrador, y si bien es posible crear cuentas de usuario y darles los mismos derechos que la cuenta Administrador (integrándolas como miembros del grupo Administradores), Administrador sólo puede haber uno. Esta cuenta siempre debe contar con contraseña y se crea en el momento de la instalación del sistema (aunque se crea normalmente sin contraseña). En Windows 7 esta cuenta Administrador no dispone de contraseña por defecto y esta deshabilitada para que no pueda ser usada.

- La cuenta de **Invitado** (Guest). Es la contraria a la cuenta de Administrador, está totalmente limitada, no cuenta apenas con ningún permiso o derecho, pero permite que cualquier usuario pueda entrar en nuestro sistema sin contraseña (lo que se denomina acceso anónimo) y darse un "paseo" por el mismo. Por defecto, en Windows 7 esta cuenta esta desactivada. Es altamente recomendable nunca activar dicha cuenta a menos que sea indispensable, ya que representa un riesgo altísimo de seguridad.

Si comprobáis el título de esta consola con la que estamos trabajando, veréis que aparece la palabra local en el mismo (Usuarios y grupos locales). Esto es así porque se distinguen dos ámbitos al hablar de usuarios: Los usuarios y grupos locales y los usuarios y grupos de dominio. Mientras no tengamos instalado un dominio (para lo cual necesitaremos algún servidor Windows como NT, 2000, 2003, 2008 o 2016) 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. En Windows 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: Mediante determinados mecanismos de seguridad que ya veremos, se puede llegar a bloquear una cuenta, impidiendo su uso. Desde esta opción podemos volver a desbloquearla, simplemente desmarcando la casilla.

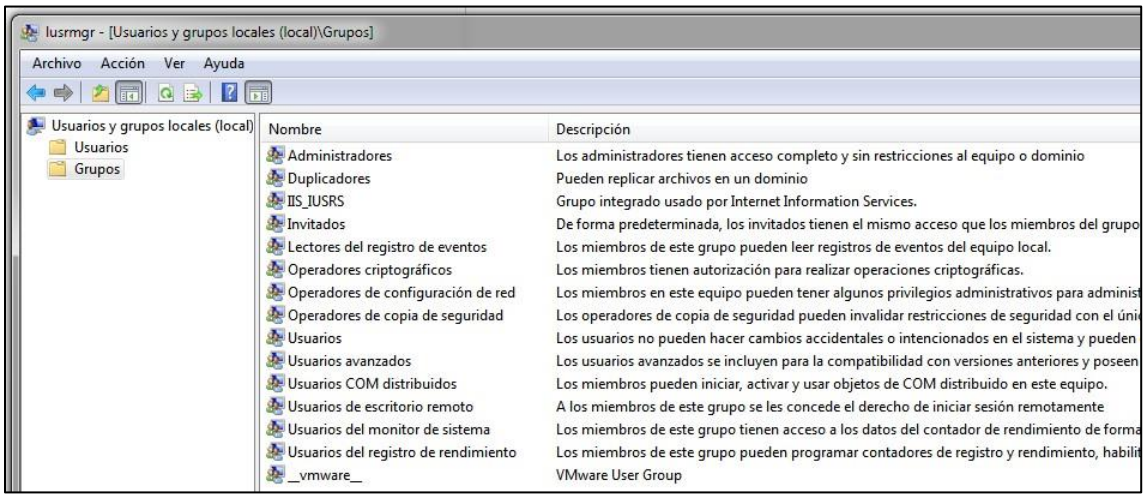
- **Miembro de**: Desde esta pestaña podemos introducir al usuario en grupos. Los grupos se usan para dar permisos y derechos a los usuarios fácilmente, sin tener que ir usuario por usuario. Así, por ejemplo, si introducimos a un usuario como miembro del grupo Administradores, le estaremos dando todos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

- **Perfil**: Nos permite indicar la ruta del perfil, los archivos de inicio de sesión y las carpetas personales del usuario. Como en un apunte posterior (Windows 2008) veremos el tema de los perfiles, de momento lo dejamos pendiente.

Esta consola LUSRMGR.MSC es la forma típica de gestionar usuarios y grupos en Windows. También podemos llegar a ella realizando botón derecho sobre Mi PC (o Equipo) y seleccionado Administrar.

Si nos vamos a la gestión de grupos, veremos cómo Windows 7 ya incluye por defecto unos cuantos grupos creados:



El grupo más importante es el de **Administradores**, ya que cualquier usuario al que hagamos miembro de dicho grupo pasará a tener los privilegios de un Administrador.

Otro grupo interesante es **Invitados**, ya que cualquier usuario al que hagamos miembro de dicho grupo pasará a tener todas las limitaciones del grupo Invitados.

Podemos crear todos los grupos que queramos, sin ningún tipo de limitación y hacer miembros de los mismos a los usuarios que deseemos. Esto suele ser muy cómodo a la hora de asignar permisos, ya que nos evita tener que ir asignándolos usuario a usuario.

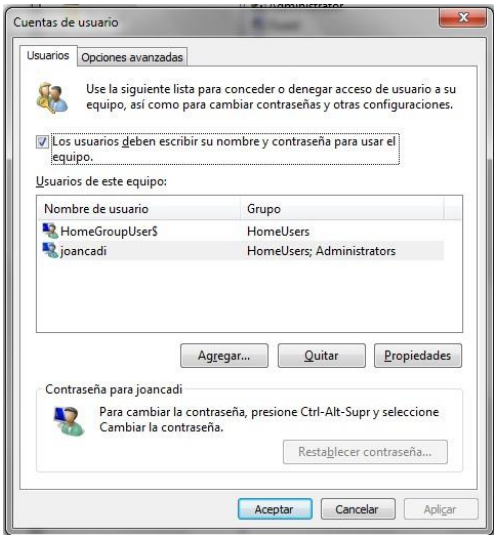
8.3 Gestión de cuentas de usuario mediante consola especial

Podemos también gestionar las cuentas de usuario mediante una consola especial, normalmente oculta. Para acceder a dicha consola, hay que ejecutar la siguiente orden desde una ventana del intérprete de comandos:

```
CONTROL USERPASSWORDS2
```

o también se puede ejecutar

```
NETPLWIZ
```



Con este gestor de cuentas de usuario, tenemos un control especial sobre los usuarios, permitiéndonos realizar algunas acciones que no son accesibles desde ningún otro sitio.

La primera opción que vemos en pantalla, "Los usuarios deben escribir su nombre y contraseña para usar el equipo" nos permite indicar si queremos usar la autentificación o no. Si lo desactivamos, obtendremos un Windows que se iniciará automáticamente con la cuenta que indiquemos sin mostrarnos siquiera la pantalla de bienvenida. Si tenemos varios usuarios, en el momento en que desactivemos dicha casilla y pulsemos aceptar o aplicar, nos preguntará el sistema por el usuario a cargar automáticamente.

Obviamente, esta opción solo debería usarse en ambientes domésticos donde sólo un usuario usa el ordenador.

Para agregar cuentas de usuario usamos el botón agregar, para eliminar cuentas el botón quitar, etc. Si seleccionamos una cuenta de usuario y pulsamos el botón propiedades, pasamos a sus propiedades.

Desde esta pantalla de propiedades, podemos observar cómo podemos incluir al usuario en algún grupo de usuarios, bien uno de los dos incluidos en el gestor (usuarios estándar y usuarios restringidos) o bien seleccionando otro grupo como puede ser el de administradores, etc.

En la pestaña **Opciones avanzadas** de este gestor, podemos ver opciones muy interesantes como la administración de nuestras contraseñas, un botón que nos lleva a LUSRMGR.MSC, obligar a utilizar el inicio de sesión seguro, etc.

Una opción muy interesante, (y muy peligrosa y poco segura) que nos podemos encontrar en la primera pantalla es la posibilidad de cambiar la contraseña de cualquier usuario, incluido el usuario administrador. Para hacerlo, basta con que nos hayamos autentificado con una cuenta de

usuario que pertenezca al grupo Administradores. Esta opción ha sido incluida ya que a veces los usuarios olvidan con el tiempo la contraseña que le asignaron a la cuenta de Administrador en el momento de la instalación del equipo, y es a su vez la causante de que Microsoft oculte esta consola para que no sea ejecutada por los usuarios normales.

8.4 Gestión de cuentas de usuario desde la interfaz de línea de comandos (CLI) de Windows

La última opción para gestionar las cuentas de usuario, es hacerlo directamente desde el shell de texto o interfaz de línea de comandos (CLI). Esta opción puede parecer la más engorrosa, pero resulta ser la más práctica y potente en muchísimas ocasiones, sobre todo si conocemos como hacer scripts de sistema.

Para ello disponemos de una orden que nos permiten gestionar las cuentas de usuario:

```
net user
```

Este comando nos permite consultar, agregar o modificar cuentas de usuario.

Su sintaxis es la siguiente:

```
net user [nombredeusuario [contraseña | *] [opciones]] [/domain]

net user nombredeusuario [contraseña | *] /add [opciones] [/domain]]

net user [nombredeusuario [/delete] [/domain]]
```

Expliquemos los parámetros de la orden que hemos visto en la sintaxis:

nombredeusuario → Específica el nombre de la cuenta de usuario que se desea agregar, eliminar, modificar o consultar. El nombre de la cuenta de usuario puede tener hasta 20 caracteres.

contraseña → Asigna o cambia una contraseña para la cuenta de usuario. Escribimos un asterisco (*) si deseamos que se nos pida la contraseña. Los caracteres de la contraseña no se muestran en la pantalla a medida que los escribimos, así que hay que tener cuidado.

/domain →Realiza la operación en el controlador principal del dominio del equipo. (Esta opción no la utilizaremos de momento ya que no hemos creado ningún dominio).

/add → Agrega el usuario al sistema.

/delete → Borra el usuario del sistema.

Si al ejecutar la orden desde la línea de comandos (CMD) obtenemos el **error de sistema 5 (acceso denegado)** es porque estamos ejecutando una línea de comandos sin ser administrador. Para evitar esto, haced un acceso directo a CMD en el escritorio, y lanzadlo con botón derecho – Ejecutar como Administrador. (Truco: También podemos escribir CMD en el botón inicio (Windows – escribir CMD) y en lugar de pulsar INTRO pulsamos CONTROL – MAYUSCULAS – INTRO con lo que conseguiremos que lo que ejecutemos se ejecute como Administrador).

Ejemplo:

```
NET USER PAQUITO /ADD
```

Vemos en la sintaxis cómo además de los elementos anteriores podemos escribir algunas opciones. Las opciones más utilizadas son las siguientes:

Opción	Descripción
/active:{no | yes}	Habilita o deshabilita la cuenta de usuario. Si no está activa, el usuario no puede tener acceso a los recursos del equipo. La opción predeterminada es **yes** (activa).
/comment:"texto"	Proporciona un comentario descriptivo acerca de la cuenta de usuario. Puede tener hasta 48 caracteres. Escribimos el texto entre comillas.
/expires:{{mm/dd/aaaa | dd/mm/aaaa | mmm,dd ,aaaa} | never}	Provoca que la cuenta de usuario caduque en la fecha especificada. Las fechas de caducidad pueden tener el formato [*mm***/***dd***/***aaaa*], [*dd***/***mm***/***aaaa*] o [*mmm***,**dd **,***aaaa*], según el código de país o región.
/fullname:"nombre"	Especifica un nombre de usuario completo en lugar de un nombre de usuario normal. Escribimos dicho nombre entre comillas.
/passwordchg:{yes | no}	Especifica si los usuarios pueden cambiar su contraseña. La opción predeterminada es **yes**.
/times:{día[-día][,día[-día]] ,hora[hora][,hora[-hora]] [;...] | all}	Específica las horas en las que se permite al usuario el uso del equipo. El parámetro *Hora* está limitado a incrementos de 1 hora. Para los valores de *día*, se puede escribir el día o usar abreviaturas. Para las horas se puede usar la notación de 12 horas o de 24 horas. Para el formato de 12 horas, usamos am, pm, a.m. o p.m. El valor **all** significa que un usuario puede iniciar una sesión en cualquier momento. Un valor nulo (en blanco) significa que un usuario nunca puede iniciar la sesión. Separamos el día de la hora mediante comas y las unidades de día y hora con punto y coma.

Obviamente la mayor potencia de la interfaz de línea de comandos (shell de texto o CLI) aparece cuando usamos scripts. Estos scripts son pequeños programas que podemos realizar con un editor de texto y que se ejecutan directamente en nuestro sistema operativo.

Imaginemos el siguiente ejemplo: decido crear una cuenta de usuario en mi equipo por cada uno de los alumnos a los que doy clase. Quiero indicar que sólo puedan abrir sesión de lunes a viernes entre las 16 y las 22 horas. Quiero usar como contraseña de cada usuario "caballo" pero obligando a cambiar dicha contraseña en el primer inicio de sesión del alumno.

Si tengo unos 90 alumnos entre varios grupos, está claro que el tiempo que voy a usar en crear dichas cuentas va a ser importante. (Imaginad que ocurriría si quisiera hacer algo parecido, pero en una empresa con 900 empleados). Todo este proceso podría automatizarse y realizarse casi instantáneamente utilizando el CLI y un script. Podría solucionar todo el problema de la siguiente forma (más abajo se explica cómo hacerlo paso a paso):

Creo un fichero de texto (alumnos.txt) donde en cada línea aparece el nombre del alumno (sin espacios en blanco). Dicho fichero naturalmente podría obtenerlo de la lista de clase, de un programa de horario, etc.

Creo un proceso por lotes que vaya leyendo dicho fichero de texto y vaya creando una cuenta de usuario por cada línea. Sería algo así (más abajo se explican los comandos y cómo ejecutar los scripts):

```
REM ------ crea.bat -------

@ECHO OFF

CLS

ECHO ------ Creando cuentas de alumnos --------

FOR /F  %%A  IN  (.\ALUMNOS.TXT)  DO  (

        NET USER %%A caballo /ADD /TIMES:L-V,16:00-22:00

        )

ECHO ------ Proceso Finalizado -----------------
```

Una vez ejecutado este simple script, tendría creadas todas las cuentas de usuario que necesito. Si un buen día quisiera borrar todas las cuentas de usuario creadas, simplemente tendría que utilizar otro script como el siguiente:

```
REM ------ borra.bat -------

@ECHO OFF

FOR  /F  %%A  IN  (.\ALUMNOS.TXT)  DO  (NET USER %%A /DELETE)
```

Más adelante veremos un tema dedicado a los comandos en los sistemas Windows, pero de momento explicaremos los utilizados en estos scripts y los necesarios para poder ejecutarlos:

REM → trata la línea como un comentario. A continuación del REM podemos escribir lo que queramos, un título, una explicación, etc.

CLS → limpia la pantalla.

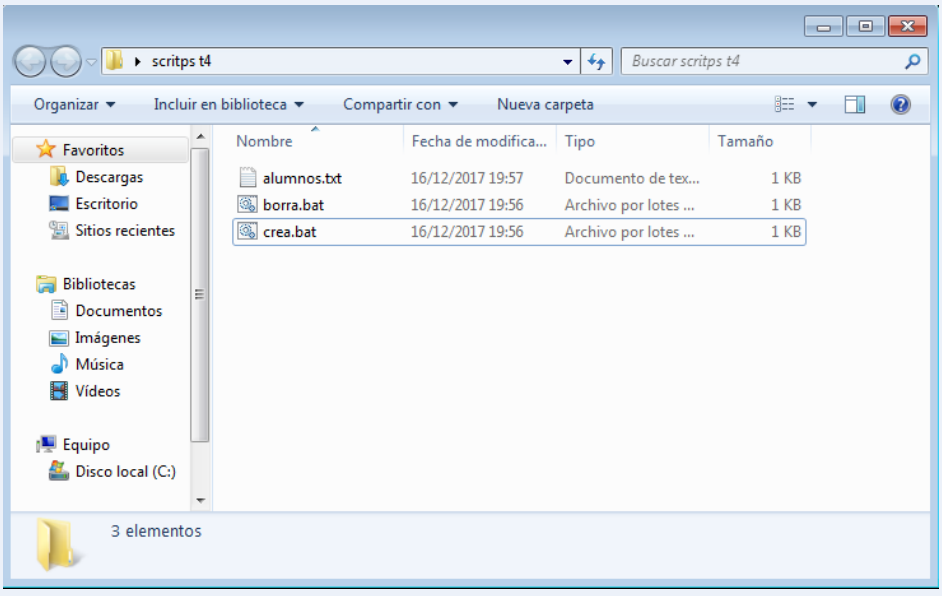
@ECHO OFF → desactiva el eco de los comandos, es decir, no se escribirá el comando en sí en la pantalla, aunque sí saldrán los posibles mensajes de aviso tras la ejecución de los comandos.

FOR → en la línea del FOR, tal como este bucle está escrito, se recorrerá todas las líneas del fichero ALUMNOS.TXT y tratará las líneas de ese fichero hasta el primer espacio que encuentre en cada una. El texto que se encuentra en cada línea hasta ese espacio, pasará a la variable **%%A**, que será el nombre de la cuenta de usuario.

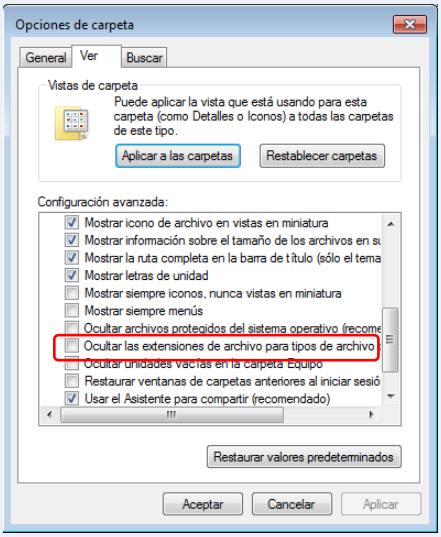
Para probar los scripts anteriores procede de la siguiente manera:

Utiliza la máquina virtual donde tienes instalado Windows 7.

Crea un directorio en el escritorio por ejemplo, con los siguientes ficheros de texto:



Para poder cambiar fácilmente las **extensiones** de los archivos, haz que estén visibles. Puedes hacerlo desde "Opciones de carpeta" (escríbelo en el buscador del inicio de Windows y te saldrá la ventana correspondiente) – pestaña Ver – desmarcar "Ocultar las extensiones de archivo para tipos de archivo conocidos":



En el fichero alumnos.txt, escribe un listado de nombres, cada uno en una línea. El contenido podría ser el siguiente (puedes hacer el listado tan largo como quieras):

```
ramon
ana
cristina
jose
```

En cada uno de los otros ficheros .bat, copia el contenido de cada uno de los scripts.

Abre CMD.EXE como Administrador.

Con el comando DIR se lista el contenido de un directorio, te puedes ayudar de él para ir viendo los nombres de los directorios y luego usarlos con el comando CD.

Con la tecla de tabulación se puede autocompletar el nombre de los directorios que empiezas a escribir.

Ve al directorio donde están los ficheros, necesitarás el comando CD:

- Con CD\ vas al directorio raíz (C:).
- Con CD.. vas al directorio del nivel anterior.
- Con CD nombre_directorio vas al directorio especificado a continuación de CD (puede ser una ruta o el nombre de un directorio si está en el nivel siguiente del directorio actual).

Una vez en el directorio donde están los tres ficheros anteriores, ejecuta el script crea.bat. Para ello, simplemente escribe en la línea de comandos

```
crea
```

Si lo has ejecutado como administrador se habrán creado los usuarios que hayas indicado en alumnos.txt. Puedes comprobarlo escribiendo en la línea de comandos:

```
net user
```

Puedes borrar los usuarios ejecutando el scritp borra.bat. Simplemente escribe en la línea de comandos:

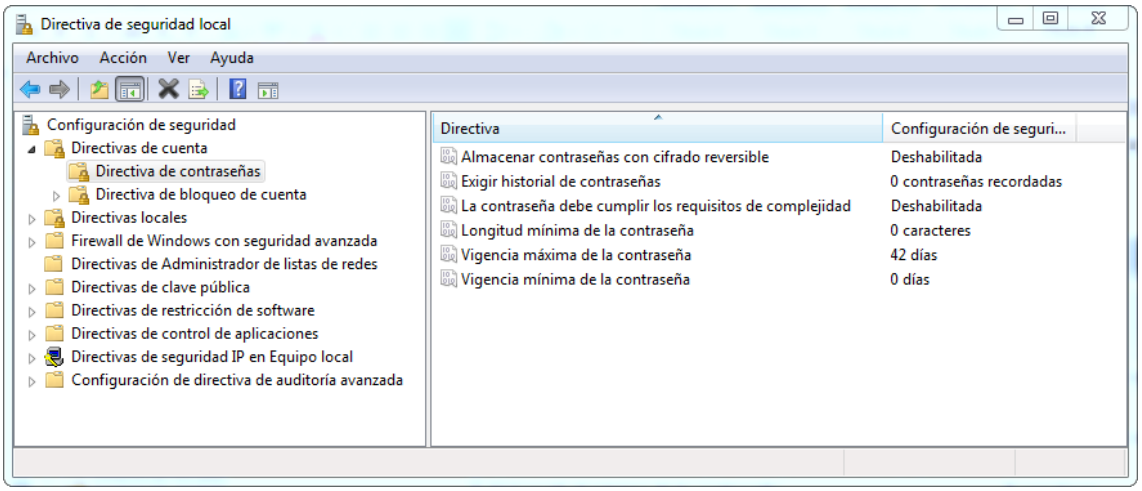
```
borra
```

Con net user, comprueba que ya no están los usuarios anteriores.

9 GESTIÓN DE LAS CONTRASEÑAS

Windows es un sistema operativo muy configurable por parte del usuario, aunque algunas de las configuraciones más potentes suelen estar algo ocultas para que no sean accesibles por los usuarios normales y sólo pueden ser modificadas por usuarios avanzados.

En concreto, desde la consola de Configuración de Directivas de Seguridad Local, podemos gestionar varios aspectos sobre las contraseñas. Esta consola se denomina **SECPOL.MSC**, y para gestionar las contraseñas, debemos entrar en Configuración de Seguridad, Directivas de Contraseña.



Las configuraciones más útiles que podemos gestionar desde aquí son:

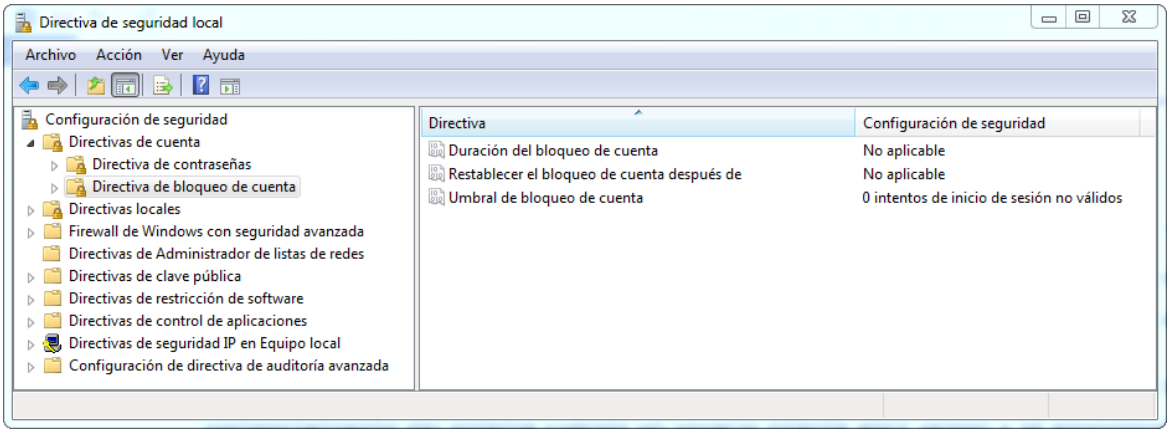
- **Historial de contraseñas**. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuántas contraseñas se recordarán.
- **Las contraseñas deben cumplir los requerimientos de complejidad**. Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas y minúsculas junto con números, no parecerse al nombre de la cuenta, etc.
- **Longitud minina de la contraseña**. Indica cuántos 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 válidas después del número de días indicados en esta configuración. El sistema obligará al usuario a cambiarla. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
- **Vigencia mínima de la contraseña**. Indica cuánto tiempo debe transcurrir desde que un usuario se cambia la contraseña hasta que puede volver a cambiarla.

Como ejercicio, estableced que el historial de contraseñas es de 5 y la longitud mínima es de 4 caracteres. Cread una cuenta de usuario EVARISTO34 desde la consola de usuarios locales

indicando que debe cambiar de contraseña en el primer inicio de sesión. Ponedle de contraseña CABALLO, e inmediatamente después intentad cambiar la contraseña a otra cualquiera.

Intentad poner de nuevo la contraseña CABALLO. Evidentemente, como queremos que la contraseña sea CABALLO, debemos deshabilitar la complejidad exigible en las contraseñas.

Desde la consola de configuración de seguridad local (secpol.msc) también podemos gestionar el comportamiento del sistema cuando un usuario intente abrir sesión y se equivoque repetidamente con la contraseña. Podemos indicar que una cuenta de usuario quede bloqueada si alguien intenta abrir sesión con dicha cuenta y se equivoca un número determinado de veces. Esta configuración la encontramos en Configuración de Seguridad – Directivas de Cuenta – Directivas de Bloqueo de Cuentas)



Aquí podemos configurar:

- **Duración del bloqueo de cuenta**. Durante cuánto 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 cuánto 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.

10 IDENTIFICADOR DE SEGURIDAD O SID

Imaginad que creamos una cuenta en nuestro equipo con nombre PACO y contraseña P1c4. Creamos varias carpetas que sólo le pertenecen a PACO, ciframos los archivos para que sólo los pueda leer PACO, etc. Un día por error borramos la cuenta PACO y todas esas informaciones quedan "huérfanas". Ni cortos ni perezosos decidimos crear otra vez la cuenta PACO con contraseña P1c4, para intentar acceder a dichos ficheros y carpetas. Pues bien, comprobaremos que nuestro sistema sabe perfectamente que ese nuevo PACO no tiene nada que ver con el antiguo PACO, y los considera usuarios totalmente distintos y no le deja acceder a los ficheros.

Esto es así porque el sistema operativo no usa para referirse a las cuentas su nombre y su contraseña, esos son campos que usamos nosotros, al igual que nos llamamos entre nosotros con nuestro nombre, pero la administración nos conoce por nuestro DNI. El DNI que usa el sistema para referirse a las cuentas de usuario se denomina SID (Security IDentifier o Identificador de Seguridad).

Un SID es algo parecido a lo siguiente:

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

El último número, en este caso 1003 se conoce como RID (identificador relativo del usuario) y todo lo que está delante del mismo identifica el dominio al que pertenece ese usuario. En concreto, esos tres grandes números que se observan (448539723-413027322-839522115) se generan automáticamente y al azar cada vez que instalamos un Windows, y aparecerán en todas las cuentas que creemos en dicho sistema. En Windows anteriores a XP no se podía clonar un equipo debido al SID, sin embargo, Windows desde la versión Vista no presenta problemas en repetir el SID en varias máquinas.

La parte del SID S-1-5-21 nos da información sobre el objeto con el que estamos trabajando. Así por ejemplo si hablamos de algunos grupos o usuarios especiales tenemos:

- S-1-1-0 es el SID del grupo Todos (Everyone)
- S-1-2-0 es el SID del grupo Usuarios locales
- S-1-3-1 es el SID de Creator – Owner
- S-1-5 Este inicio de SID nos indica que estamos trabajando con un usuario o grupo normal.
- El RID del Administrador siempre es el 500.
- Los RID de usuarios suelen comenzar por el 1000.

Desde Windows es posible ver los SID que se le asignan a nuestros usuarios y grupos con la orden whoami.exe.

Abrid un shell, y ejecutad la siguiente orden:

```
whoami /USER
```

Que os responderá algo como lo siguiente:

```
SIS\Joancadi  S-1-5-21-448539723-413027322-839522115-1003
```

Podemos ver aquí como nos dice el nombre de nuestro usuario actual y además nos indica que SID le ha sido otorgado por el sistema.

Si queremos ver no sólo el SID que se le ha otorgado a nuestro usuario, sino el SID de todos los grupos a los que pertenece nuestro usuario, usad la orden con el parámetro /GROUPS.

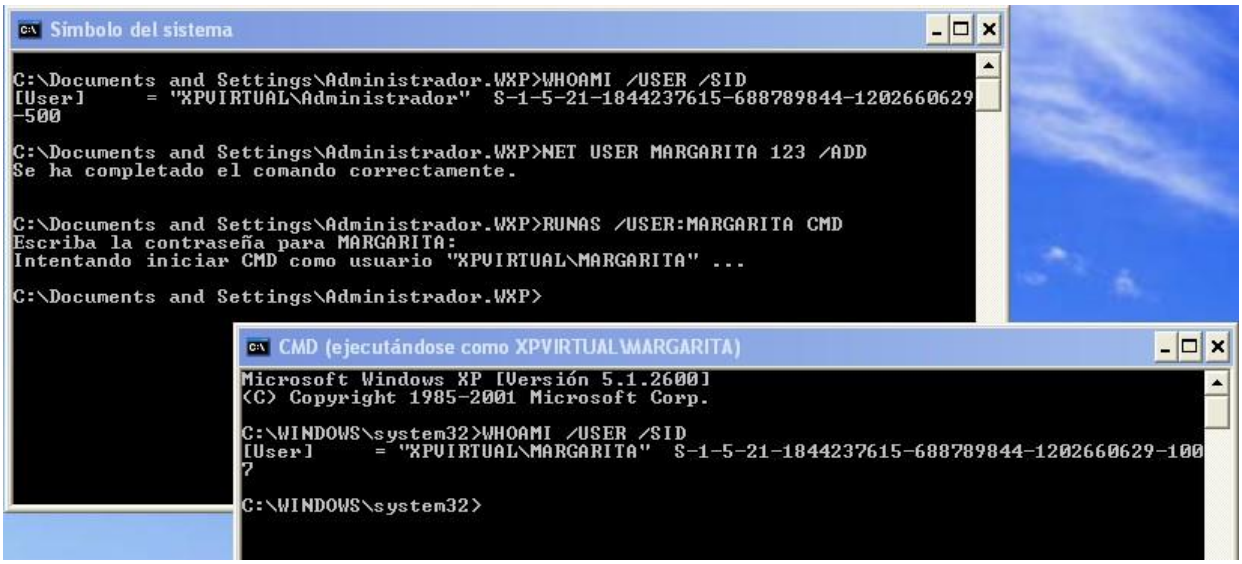
El comando whoami sólo nos muestra información sobre el usuario actual, así que, si queremos ver los SID de distintos usuarios, tendremos que ejecutar dicha orden como dichos usuarios. Aprovecho aquí para comentaros una orden que a veces es muy útil. En lugar de tener que ir cerrando y abriendo sesión con cada usuario, podemos "hacernos pasar" por dicho usuario sin tener que cerrar sesión, ni abrir sesión, ni nada. Para ello usaremos la orden **`runas`** (ejecutar como si fuera).

Para ellos, abrid un shell y ejecutad la orden:

```
runas /user:usuario_a_suplantar cmd
```

Con esto conseguiremos abrir una nueva shell en la que seremos el usuario que estamos suplantando, por lo que si ejecutamos en dicha ventana whoami nos responderá con el nuevo usuario.

Abrimos una nueva sesión de cmd ya que si ejecutamos directamente `runas  whoami` se ejecutaría la orden, pero no veríamos nada.



11 LISTAS DE CONTROL DE ACCESO (ACL)

Hasta aquí hemos visto algunos conceptos relacionados con la autentificación. Pasemos ahora a ver otros conceptos relacionados con la **autorización**.

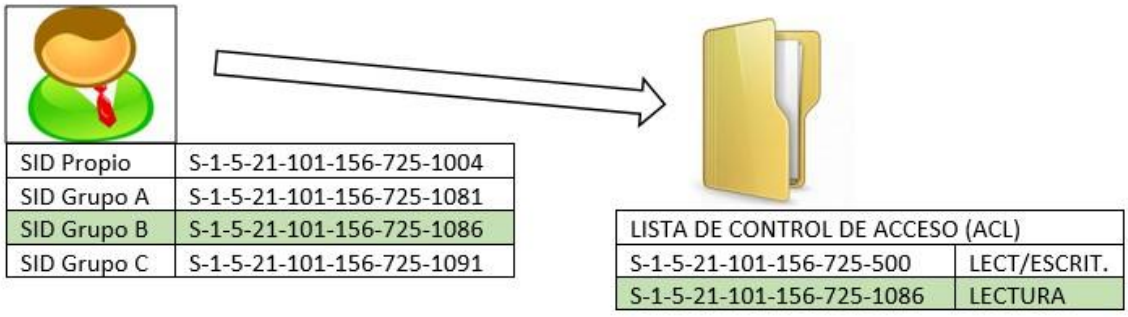
Un recurso local es cualquier elemento del sistema que permite ser usado por los usuarios. Así, una impresora, una carpeta, un fichero o una conexión de red son recursos. Por cada recurso, el sistema cuenta con una lista donde apunta los usuarios que pueden usar dicho recurso y de qué forma pueden usarlo. Si un usuario no está en esta lista, el sistema le impedirá usar el recurso.

Ya hemos visto que el sistema no ve usuarios y grupos, realmente ve Identificadores de Seguridad (SID), de modo que lo que dicha lista realmente tiene en su interior es una serie de SIDs y los permisos que cada uno de esos SIDs tiene sobre el recurso. Esta lista con la que cuenta cada recurso se conoce como **ACL** (Access Control List, o Lista de Control de Acceso).

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

Si no aparece en la ACL ningún SID del usuario o de algún grupo del que sea miembro, el sistema niega el acceso al usuario a dicho recurso.

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 la ACL, si lo está le autoriza para hacerlo, en caso contrario se lo impide.



SID Propio	S-1-5-21-101-156-725-1004
SID Grupo A	S-1-5-21-101-156-725-1081
SID Grupo B	S-1-5-21-101-156-725-1086
SID Grupo C	S-1-5-21-101-156-725-1091

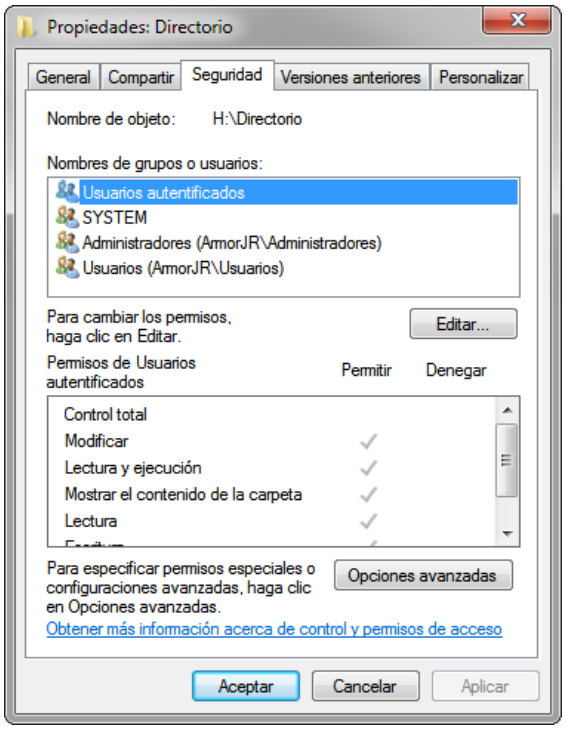
LISTA DE CONTROL DE ACCESO (ACL)	
S-1-5-21-101-156-725-500	LECT/ESCRIT.
S-1-5-21-101-156-725-1086	LECTURA

Puede ocurrir que un usuario tenga permisos contradictorios. Imaginemos que en el ACL de la carpeta FOTICOS aparece que el SID del usuario PACO puede escribir en la carpeta, pero PACO pertenece al grupo PROFESORES que aparece en el ACL de FOTICOS 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. Basta con que un permiso este 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.

Por ejemplo, creemos en la raíz de nuestro volumen (en NTFS) una carpeta con nombre DIRECTORIO. Una vez creada, accedemos a sus propiedades y en ellas a la pestaña Seguridad.



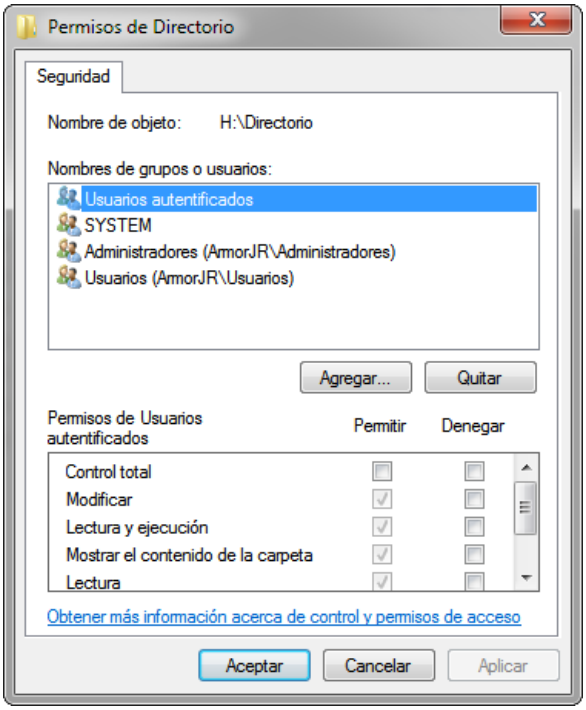
Podemos ver que en la parte superior tenemos las SID a las que concedemos permisos (usuarios y grupos) y en la parte inferior tenemos los permisos concretos que le concedemos a dicha SID.

Para cada permiso hay dos columnas: podemos tanto Permitir como Denegar un permiso.

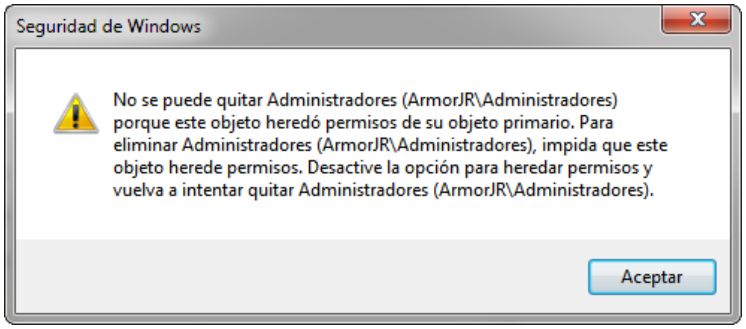
La denegación de un permiso es la que más pesa, y se aplica inmediatamente. De hecho, se aconseja no denegar permisos NUNCA, a menos que sea absolutamente necesario.

Si no vemos esta pestaña de seguridad puede ser porque estemos en un volumen de datos FAT, en lugar de NTFS. Las ACL necesitan ser almacenadas en el volumen de datos conjuntamente con el recurso al que pertenecen, y esto es algo que solamente se puede realizar con el sistema de ficheros NTFS.

Si hacemos clic en botón **Editar** pasaremos a la pantalla de la derecha. Con los botones Agregar y Quitar podemos añadir o quitar SID de la ACL. En la parte inferior podemos pulsar en las casillas de Permitir y Denegar para dar y quitar permisos.



Intentad quitar por ejemplo el grupo Administradores, y veréis como aparece un mensaje como el siguiente:



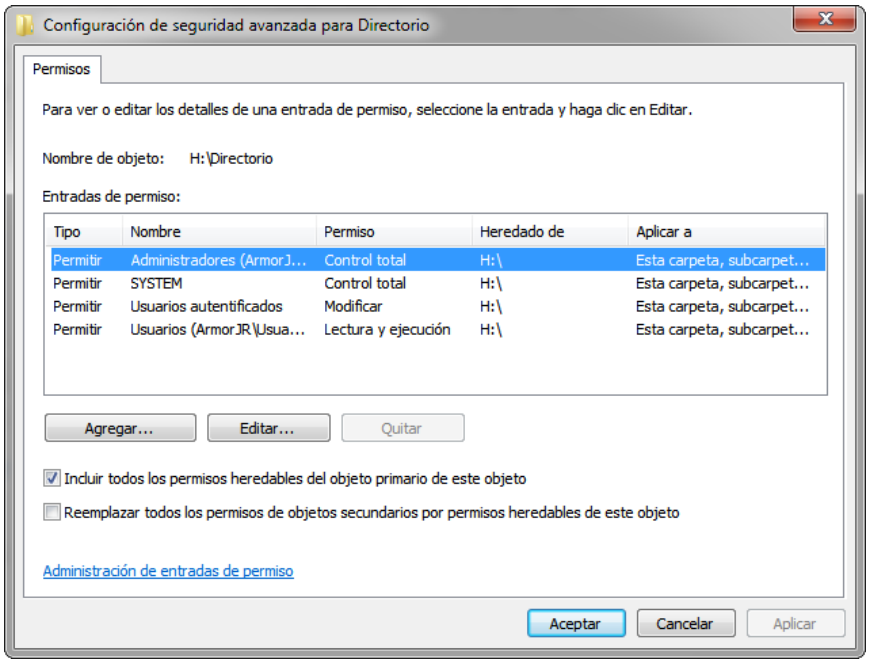
Veremos que no podemos realizar este tipo de acciones debido a que el objeto heredó permisos de su objeto primario. Veamos en profundidad este concepto de herencia.

11.1 Herencia

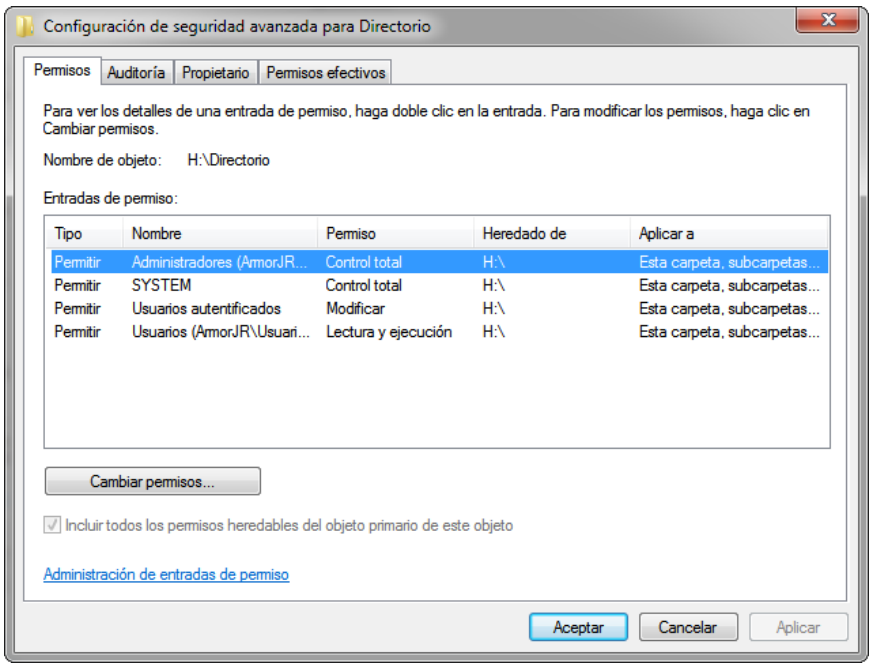
Imaginemos que creamos una carpeta por ejemplo CONTABLES, y la preparamos minuciosamente para que pueden leer y escribir en ella los usuarios que sean miembros del grupo CONTABLES, también la configuramos para que sólo puedan leer los del grupo JEFES, pero no escribir, y que los demás usuarios no puedan ni leer en ella ni escribir. Bien, si ahora dentro de la carpeta CONTABLES creamos una nueva carpeta INFORMES, ¿no sería lógico que esta carpeta INFORMES "heredara" la ACL de su carpeta madre CONTABLES para que no tuviéramos que configurarla nuevamente?

Pues precisamente eso es lo que hace Windows. Cualquier recurso que se crea hereda automáticamente la ACL de su recurso padre si es que existe. En nuestro caso, la carpeta DIRECTORIO ha heredado la ACL de su padre, es decir, la raíz de nuestro volumen H. De modo que no podremos ni agregar ni quitar usuarios, quitar permisos, etc.

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



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

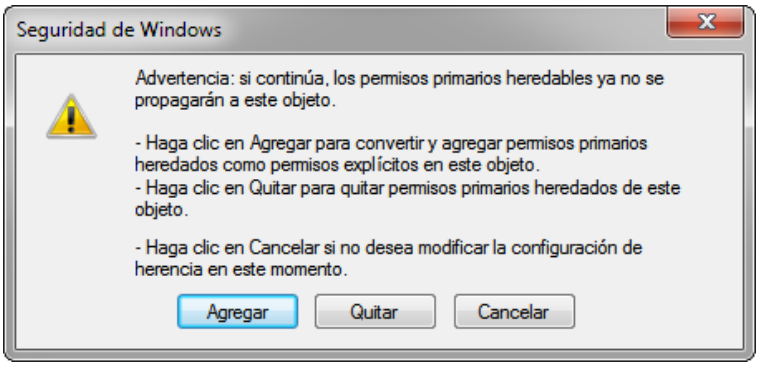


Podemos ver en estas opciones avanzadas cuatro pestañas (Permisos, Auditoria, Propietario, Permisos efectivos), de momento nos quedamos en la primera, **permisos**.

Para poder acceder a las opciones de Herencia, debemos hacer clic sobre el botón **Cambiar permisos** que vemos en la parte inferior de esta ventana.

Vemos que en la parte inferior de esta ventana está marcada la opción de "**Incluir todos los permisos heredables del objeto primario de este objeto**". Esta es la opción que hace que nuestra carpeta herede todos los permisos de su carpeta padre. Para desheredar esta carpeta, hemos de deseleccionar la casilla de verificación que aparece en esta opción.

Cuando lo hagamos, veremos que nos aparece una ventana donde Windows nos pide que elijamos entre dos opciones principales:



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. Es decir, seguiremos viendo los usuarios que veíamos antes con sus permisos tal como estaban, pero ahora ya podremos retocarlos como queramos.

Si escogemos la opción **Quitar**, la ACL se borrará totalmente, se interrumpirá la herencia y la podremos crear desde cero. Es decir, la lista de usuarios y permisos quedará en blanco y la tendremos que crear.

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 con el texto "**Reemplazar todos los permisos de objetos secundarios por permisos heredables de este objeto**" 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.

Realizad el siguiente **ejercicio**:

1. Cread 4 usuarios con nombre SARA, CLARA, IVAN y JUAN.
2. Introducid los 4 usuarios anteriores en el grupo DANZA, que también tendréis que crear.
3. Cread una carpeta en la raíz de vuestro volumen de datos con nombre BAILE, y dentro de ella crear una carpeta con nombre CLASICO. Modificad el ACL de BAILE para que sólo puedan leer y escribir en dicha carpeta los miembros del grupo BAILE. Quitad el grupo Administradores, Usuarios, etc.

Dejad los que aparecen en mayúsculas (Creator Owner y System) para que no tengamos problemas con la carpeta.

4. Comprobad abriendo sesión con los usuarios nuevos que efectivamente ellos pueden entrar y escribir en la carpeta BAILE y los demás usuarios del sistema no. (Podéis hacerlo bien cerrando y abriendo sesión, o con `runas`, lo que os resulte más cómodo).

Comprobaréis que para realizar el anterior ejercicio habréis tenido que romper la herencia de la carpeta BAILE.

Comprobad ahora el ACL de la carpeta CLASICO. Si cuando tocasteis los permisos de BAILE marcasteis la opción de "Reemplazar todos los permisos de objetos secundarios por permisos heredables de este objeto" la carpeta CLASICO habrá heredado todos los permisos de la carpeta BAILE.

11.2 Propiedad

En Windows, todo recurso que se cree tiene un propietario, normalmente el usuario que creó dicho recurso, ya sea este una carpeta, una impresora, etc. Este propietario lo solemos ver en las ACL como Creator Owner.

El propietario es el dueño absoluto del recurso, y tiene el derecho concedido de retocar la ACL como quiera. Aunque el usuario creador del objeto no esté presente en la pestaña de seguridad (no cuenta con entrada en la ACL del objeto), siempre podrá retocar la pestaña de seguridad para añadirse a sí mismo o borrar a los demás ya que es el propietario del objeto.

Si en el ejercicio anterior, por ejemplo, creamos la carpeta BAILE con nuestro usuario normal, este usuario será el propietario de la carpeta, de modo que incumpliríamos el enunciado del problema, que indicaba que los únicos con poderes sobre dicha carpeta deberían ser los usuarios del grupo DANZA.

Para solucionar esto, bastaría que creáramos la carpeta BAILE con la sesión iniciada de un usuario de dicho grupo, de modo que el propietario de la carpeta fuera por ejemplo SARA.

Como **ejercicio**, haced lo siguiente:

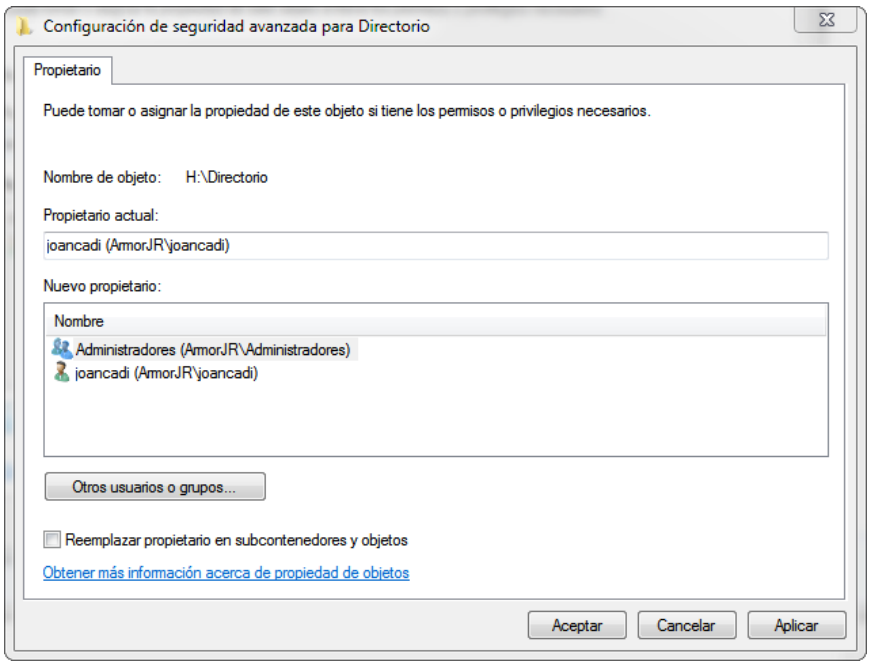
1. Cread un usuario EGOISTA.
2. Abrid sesión con dicho usuario.
3. Cread en la raíz de vuestro volumen de datos una carpeta con nombre MITESORO.
4. Modificad el ACL de dicha carpeta para que únicamente EGOISTA tenga permisos sobre ella.

Bien, ahora tendremos una carpeta creada en el sistema con nombre MITESORO, de la cual es propietario el usuario EGOISTA, y donde además sólo tiene permisos para acceder dicho usuario EGOISTA. Se supone entonces que ni el propio Administrador podría ser capaz de acceder a dicha carpeta.

En realidad, sí que el administrador podrá acceder a dicha carpeta, gracias que todos los miembros del grupo Administradores tienen un "poder" especial concedido en el sistema, que es el poder de tomar posesión de cualquier recurso.

Es imposible que un usuario en un sistema impida que el Administrador realice alguna función, (siempre que el Administrador sepa lo que es administrar un sistema, claro). En este caso como Administrador (o miembro del grupo Administradores) podemos hacer lo siguiente:

1. Accedemos a las propiedades de la carpeta "rebelde", en este caso MITESORO. Si bien en ella no podemos modificar nada, sí que podemos acceder a sus **propiedades avanzadas**, y dentro de dichas propiedades accedemos a **Propietario**.
2. Vemos desde aquí el propietario actual de la carpeta, pulsamos el botón **Editar** para cambiarlo.
3. Podéis ver que desde aquí podemos cambiar el propietario actual del objeto (owner), e indicar que el propietario actual es el grupo Administradores (o el usuario actual si es del grupo Administradores). Es recomendable siempre darle la propiedad al grupo Administradores, y no al usuario actual.



4. Basta con que seleccionemos el grupo Administradores y marquemos abajo Reemplazar propietario en sub contenedores y objetos y pulsemos Aplicar – Aceptar. Seremos propietarios de la carpeta.

Esto no nos permite acceder a la carpeta directamente, pero si nos permite modificar su ACL donde tendremos que introducir el SID del grupo Administradores para así poder acceder a la carpeta con los permisos que indiquemos. Es decir, deberemos salir de las propiedades de la carpeta, volver a entrar en las mismas y modificar seguridad para añadirnos como ya hemos visto anteriormente.

Otro **ejercicio** más para comprobar todo lo visto hasta ahora:

1. Abrid sesión con vuestro usuario, que debe ser miembro del grupo Administradores.
2. Cread 4 usuarios con nombre Alumno01, Alumno02, Alumno03 y Alumno04.
3. Cread un grupo Alumnos e introducid dentro los 4 usuarios anteriores.
4. Abrid sesión como Alumno01 y cread una carpeta en la raíz de vuestro volumen con nombre ALUMNADO.
5. Modificad sus permisos para que solo los miembros del grupo Alumnos puedan leer, escribir, etc., en dicha carpeta. Quitad todas las demás SID de su ACL, incluidas las SID especiales esta vez.
6. Comprobad que nadie fuera del grupo Alumnos puede acceder a la carpeta ALUMNADO.
7. Abrid sesión como Alumno02, cread dentro de ALUMNADO un subdirectorio con nombre PRIVADO. Modificad los permisos de dicha carpeta para que sólo pueda acceder Alumno02.
8. Dentro de Privado, cread un fichero de texto con nombre contraseñas.txt y escribid algún texto dentro de dicho fichero. Comprobad la ACL de dicho fichero, debería dejar únicamente a Alumno02 acceder al mismo.
9. Abrid sesión con vuestro usuario normal de siempre.
10. Cread un usuario con nombre CURIOSO y hacedlo miembro del grupo Administradores, pero no del grupo Alumnos.
11. Abrid sesión como el usuario CURIOSO y conseguid acceder a ALUMNADO. Comprobad que podéis leer el fichero contraseñas.txt.

11.3 Permisos

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 en **Opciones Avanzadas** y allí en **Permisos – Agregar** veremos cómo podemos indicar otro tipo de permisos.

- El permiso **Recorrer 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 **Atributos de lectura** 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 **Atributos de escritura** permite o impide que el usuario cambie los atributos de un archivo o de una carpeta.

- El permiso **Leer permisos** permite o impide que el usuario lea permisos del archivo o de la carpeta, como Control total, Leer y Escribir.

- 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.