S. INFORMÁTICOS

UNIDAD 6

Administración básica del sistema (WINDOWS II)

Javier Díaz Garrido

INDICE

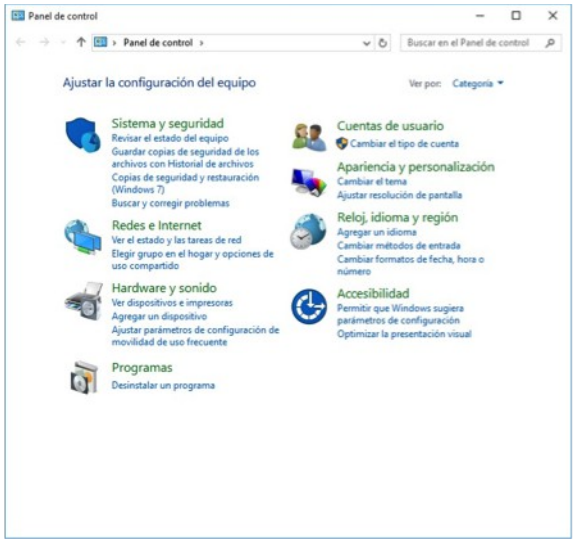
Administración básica del sistema (WINDOWS II)

1.- Herramientas administrativas y 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**:

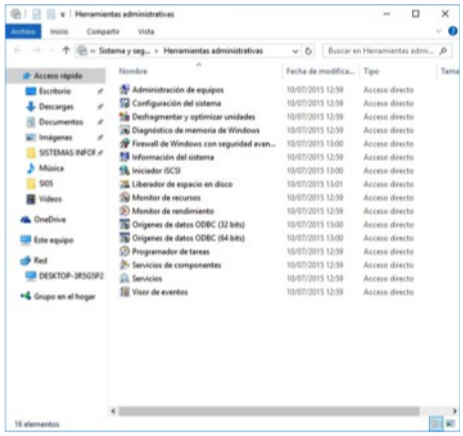
- **Sistema y seguridad**
- **Redes e Internet**
- **Hardware y sonido**
- **Programas**
- **Cuentas de usuario y protección infantil**
- **Apariencia y Personalización**
- **Reloj, idioma y región**
- **Accesibilidad**

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.



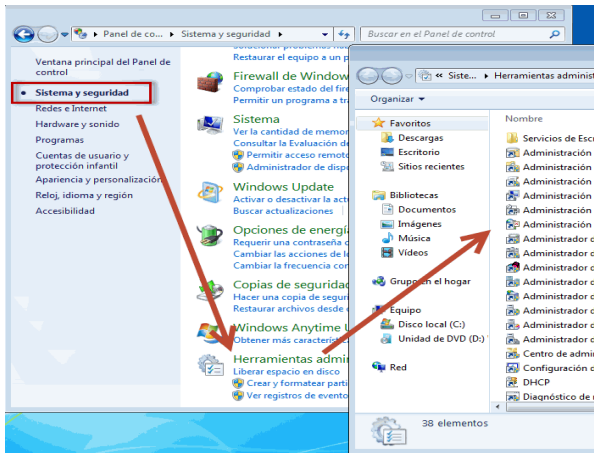
- **Diagnostico de memoria de Windows:** Permite comprobar si la memoria funciona correctamente.
- **Directiva de seguridad local:** Permite consultar y editar la configuración de seguridad de directiva de grupo.
- **Firewalls de Windows con seguridad avanzada:** Permite configurar opciones avanzadas 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. En windows 10 lo encontramos en Inicio > Aplicaciones > Herrramientas administrativas 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.

Autoevaluación

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 7/8 hay varios tipos de cuentas de usuario: Estándar, Administrador e Invitado.

En windows 10 además aparece el concepto de **cuenta para la familia,** las cuales se podrán controlar por el administrador para gestionar los recursos que tengan a su disposición. Además tambien disponemos de “Otros Usuarios”, que permite que las personas que no formen parte de la familia puedan iniciar sesión con sus propias cuentas, siempre y cuando usen las credenciales de una cuenta de Microsoft.

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
```

Para saber más

Puedes ver en este video cómo se habilita la cuenta de invitado:

http://www.cursosenhd.com/tutorial/activar-desactivar-la-cuenta-de-invitado/

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

Los grupos en Windows 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 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 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 una único equipo Windows. 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.

Descripción de grupos de usuarios: https://msdn.microsoft.com/es-es/windows/desktop/cc785098

Autoevaluación

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 (I).

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

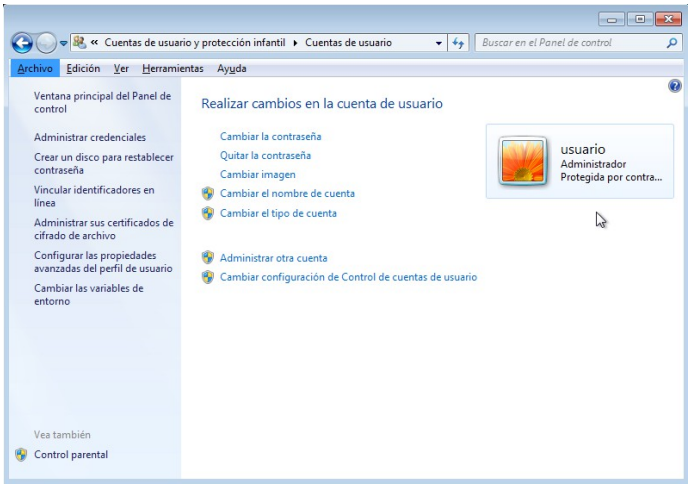
- **Asistente para cuentas de usuario desde Panel de Control**
- **Gestión de cuentas de usuario desde Herramientas Administrativas - Administración de equipos**

- **Asistente para cuentas de usuario desde Panel de Control**

  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**:

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

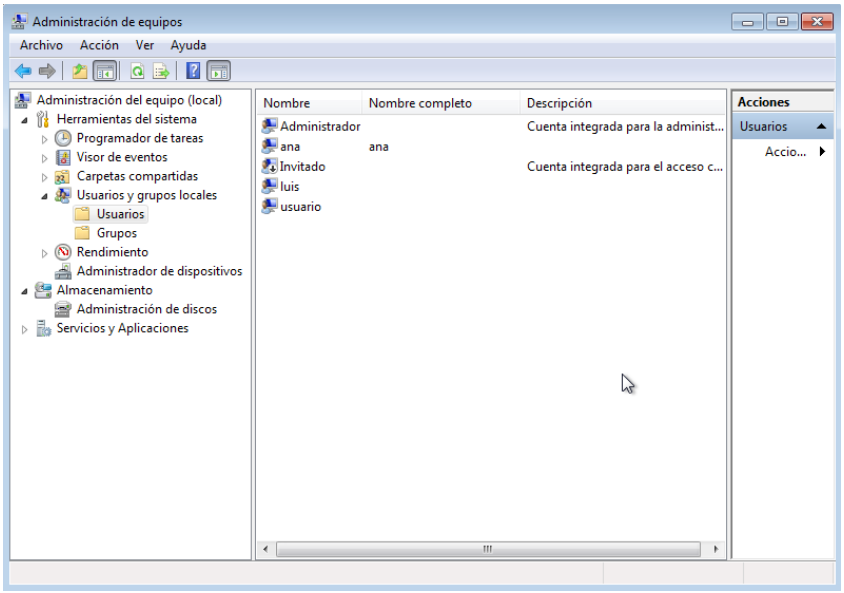
  Cuando **eliminamos una cuenta de usuario**, ésta se borra definitivamente del sistema. No podemos recuperarla creando otra con el mismo nombre con el objeto de conseguir los mismos permisos de la cuenta antigua. Esto es debido a que cuando creamos otra cuenta nueva el sistema asigna un nuevo SID distinto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

  En Windows 10 es en **Configuración > Cuentas > Familia y otros usuarios > Agregar otra persona a este equipo.** Apartir de aquí, se inciará un asistente que nos pedirá las credenciales de dicha persona con una cuenta de Microsoft, o si lo deseamos podemos hacer click en “la persona que quiero agregar no tiene dirección de correo electrónico. A continuación, nos aparecerá otra pantalla en la cual nos invitan a crear una cuenta de Microsoft, sino deseamos hacerlo basta con pulsar en el enlace inferior que dice “ Agregar un usuario sin cuenta Microsoft”. En la siguiente pantalla aparecerá un menú donde podemos introducir el nombre de usuario y la clave para finalizar el proceso.

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

2.2.1.- Gestión de cuentas de usuario y grupos locales (II).

•Gestión de cuentas de usuarios locales y grupo mediante Herramientas administrativas - Administración de equipos



La tercera opción que tenemos para gestionar cuentas de usuario. Es la **consola de usuarios locales y grupos**. Podemos llegar a dicha consola de varias formas.

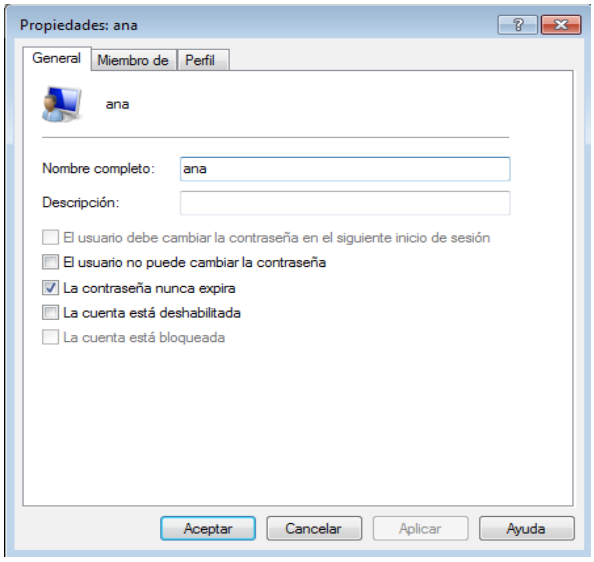
Podemos ejecutar desde **Inicio - Ejecutar** y escribir `LUSRMGR.MSC`.

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.

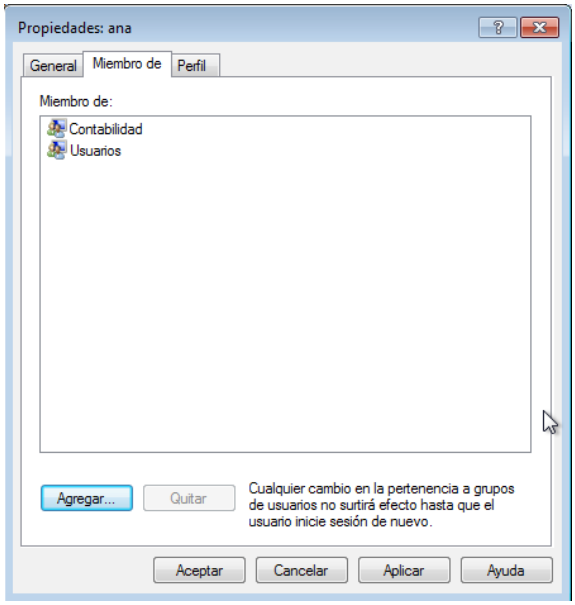
  El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.

  El usuario no puede cambiar la contraseña. Prohibimos que el usuario pueda cambiar su contraseña.

La contraseña nunca caduca. Ya veremos como en Windows 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.

2.2.2.- Gestión de cuentas de usuario y grupos locales (III).



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.

Debes conocer

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 Windows 7 y que crearon cierta controversia en Windows Vista.

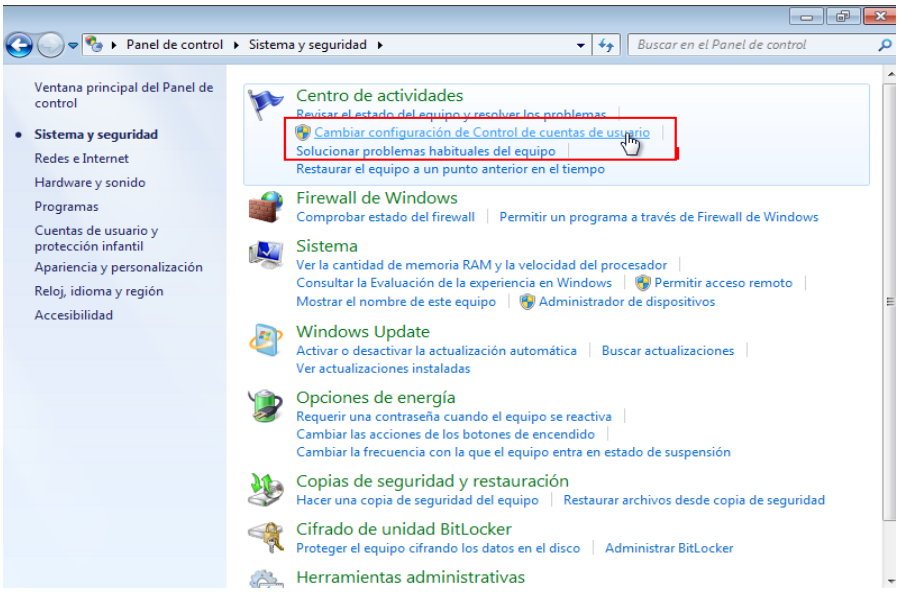
Anexo I.- UAC Control de Cuentas de Usuario.

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

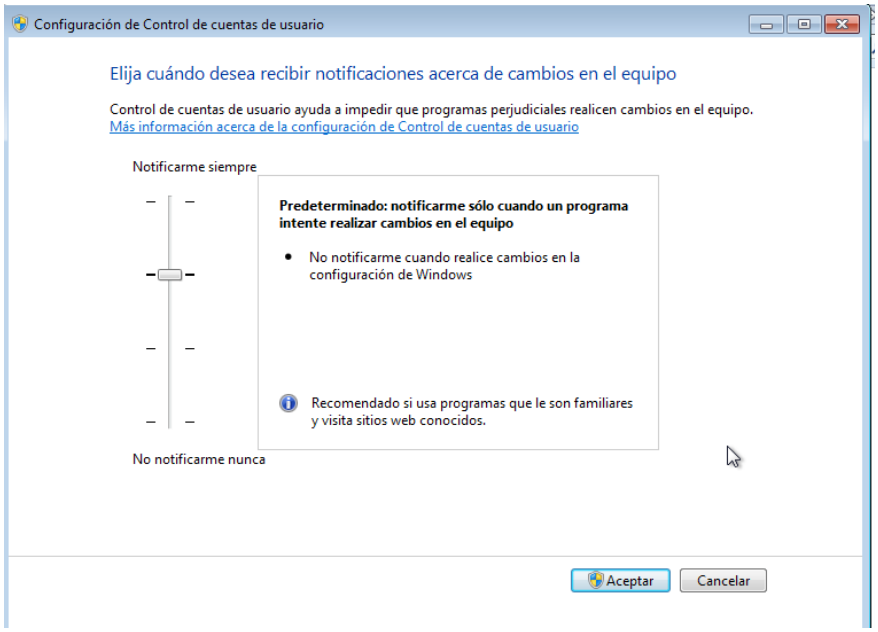
de servicios, etc. User Account Control (UAC) es el responsable de mensajes como "Un programa no identificado desea tener acceso a este equipo" o "Necesita confirmar esta operación", y aunque, en ocasiones, estos mensajes pueden llegar a ser algo molestos, evita básicamente que se instale software sin 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**:



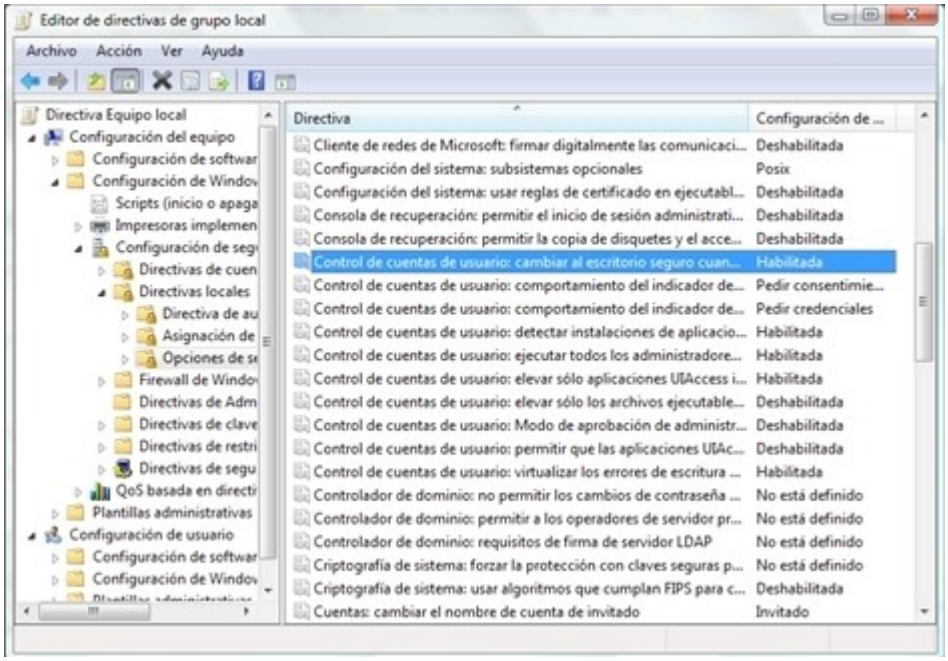
1. **Notificarme siempre cuando**:
   - Un programa intente instalar software o realizar cambios en el equipo.
   - Realice cambios en la configuración de Windows.
2. **Predeterminado: notificarme sólo cuando un programa intente realizar cambios en el equipo**
   - No notificarme cuando realice cambios 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.

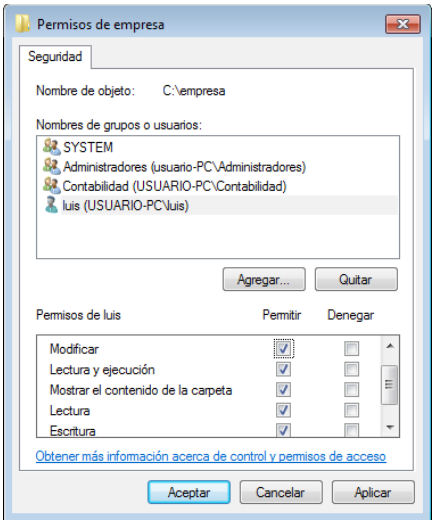
Los recursos de un sistema son los distintos elementos con los que ese sistema cuenta para que sean usados por los usuarios. Así, una impresora, una carpeta, un fichero, una conexión de red, son ejemplos de recursos.

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 (I).



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.

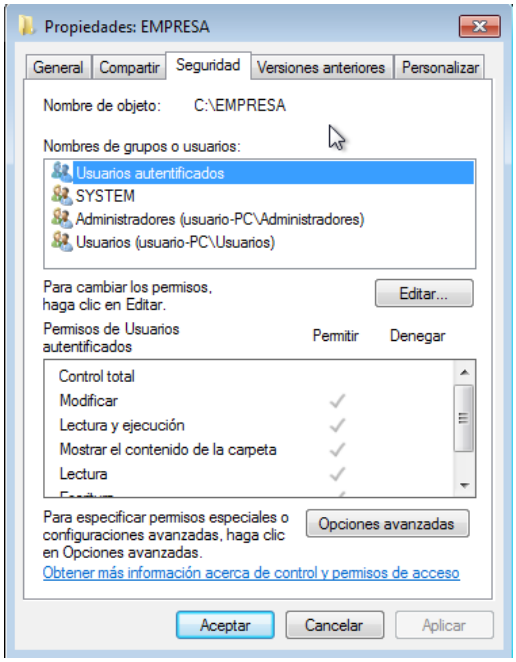
3.1.1.- Permisos de archivos y carpetas (II).

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**.



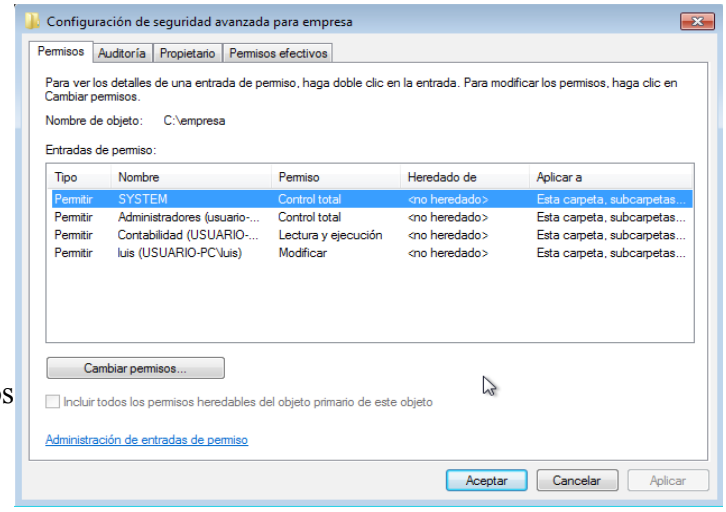
Tomamos de referencia, de nuevo, a la carpeta llamada EMPRESA, vamos a prepararla para que pueden leer y escribir en ella los usuarios que sean miembros del grupo EMPLEADOS, para que sólo puedan leer los del grupo JEFES pero no escribir, y que los demás usuarios no puedan ni leer en ella ni escribir. 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 se hace desde 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.

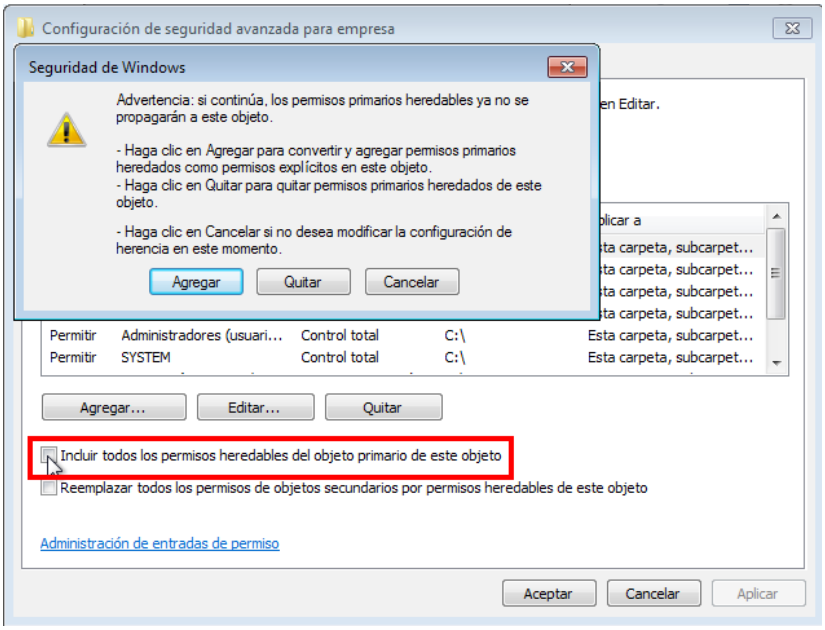
Para ello, accedemos al botón de Opciones Avanzadas que está en la pestaña Seguridad.

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:

"**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.

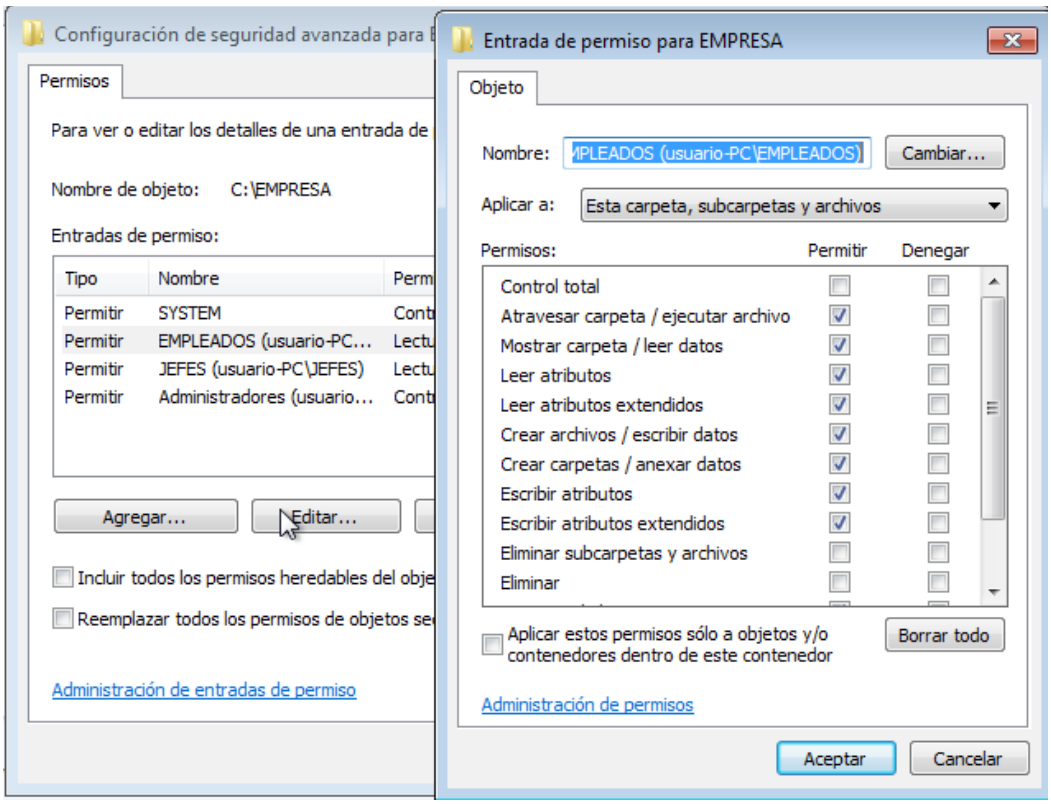
Si elegimos quitar y empezar desde cero, hay que tener en cuenta que en las ACL no sólo deben aparecer nuestras SID normales, sino que grupos como Creator Owner o System son necesarios para que el sistema pueda trabajar sin problemas con dichas carpetas. Si quitamos estos SID tendremos problemas en el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

3.1.2.- Permisos de archivos y carpetas (III).

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 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.

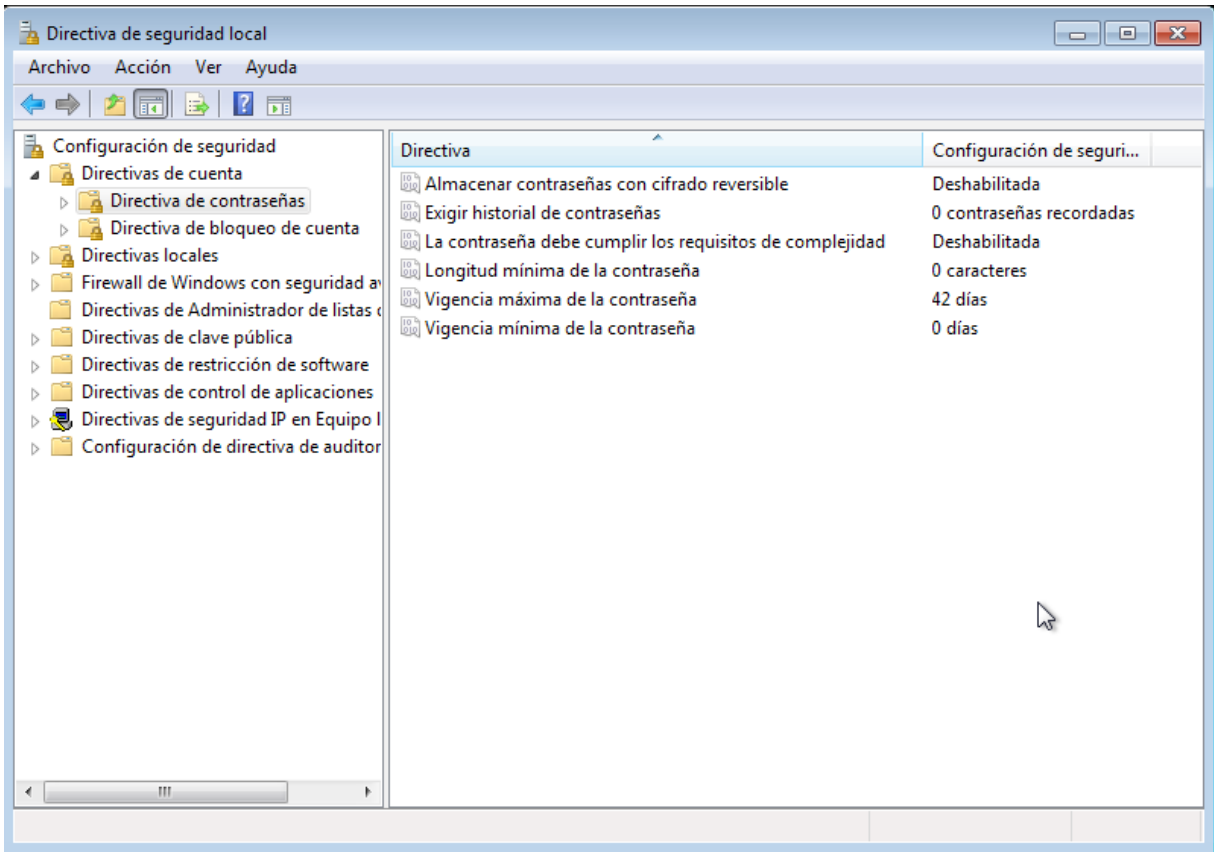
Con las **Directivas de seguridad local** veremos cómo aplicar distintas restricciones de seguridad sobre las cuentas de usuario y contraseñas. Por otro lado, las **Directivas de grupo local** nos permiten configurar equipos de forma local o remota, instalar o eliminar aplicaciones, restringir los derechos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

3.2.1.- Directivas de seguridad local.

Windows 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`

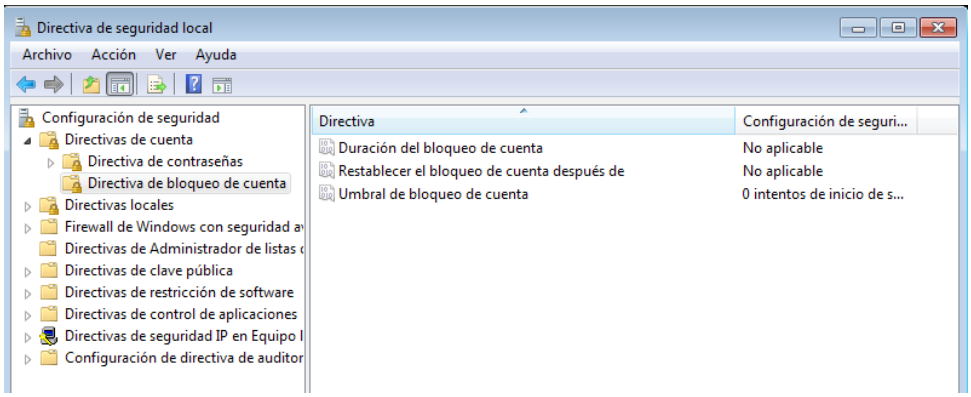
Una vez dentro podemos acceder a: **Configuración de Seguridad - Directivas de Cuenta - Directivas de Contraseñas**) o también se puede acceder a través de **Inicio - Panel de Control - Sistema y Seguridad - Herramientas administrativas - Directiva de seguridad local.**



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 recordará Windows.
- **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).

Para saber más

En estas páginas de Microsoft Windows puedes ver cómo cambiar la configuración de la directiva de contraseñas en Windows 10

Acerca de la configuración de sincronización en Windows 10:

https://support.microsoft.com/es-es/help/4026102/windows-10-about-sync-settings

Cambiar contraseña:

https://support.microsoft.com/es-es/help/14087/windows-7-change-your-windows-password#1TC=windows-7

3.2.2. Directivas de grupo local.

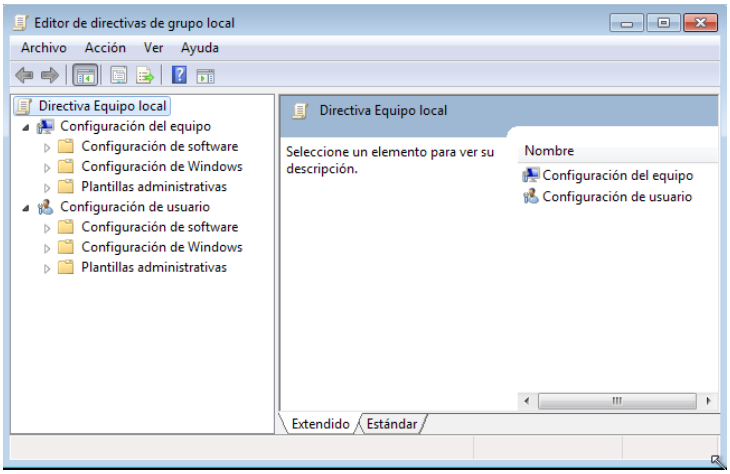
Las directivas de grupo es una característica de Windows XP, familia de sistemas operativos. Directiva de grupo es un conjunto de reglas que controlan el medio ambiente de trabajo de cuentas de usuario y cuentas de equipo. Las políticas de grupo son una herramienta muy poderosa que permite a los administradores 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, 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`**).**



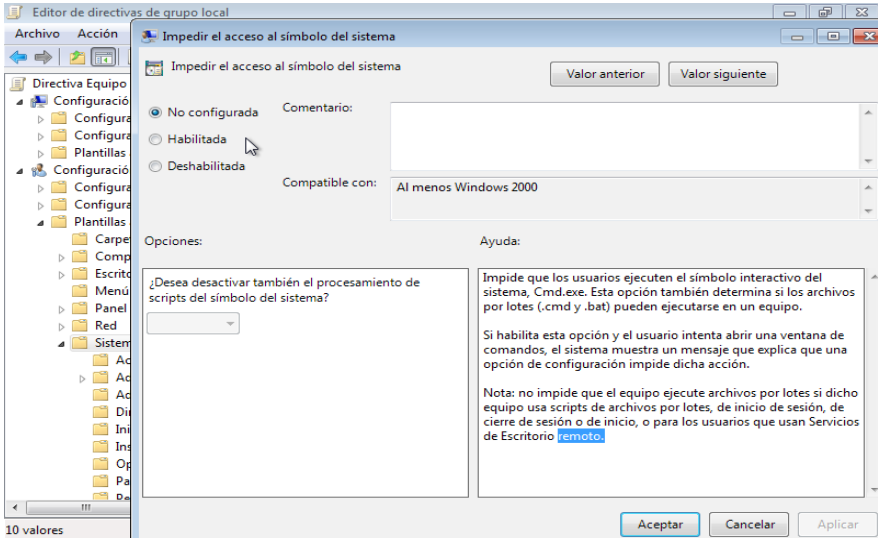
Para poder trabajar con el `gpedit.msc` necesitamos estar usando una cuenta de usuario que pertenezca al grupo Administradores. Esta consola es muy configurable, permitiéndonos añadir y quitar opciones según deseemos. De momento, vamos a trabajar con las opciones que aparecen por defecto.

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.

Para saber más

Cómo personalizar las directivas de grupo local en Windows 8:

Personalizar directivas de grupo local en Windows 8: http://soportedi.uc.cl/2013/07/personalizar-windows-8-en-sus.html

3.3.- Cuotas de disco.

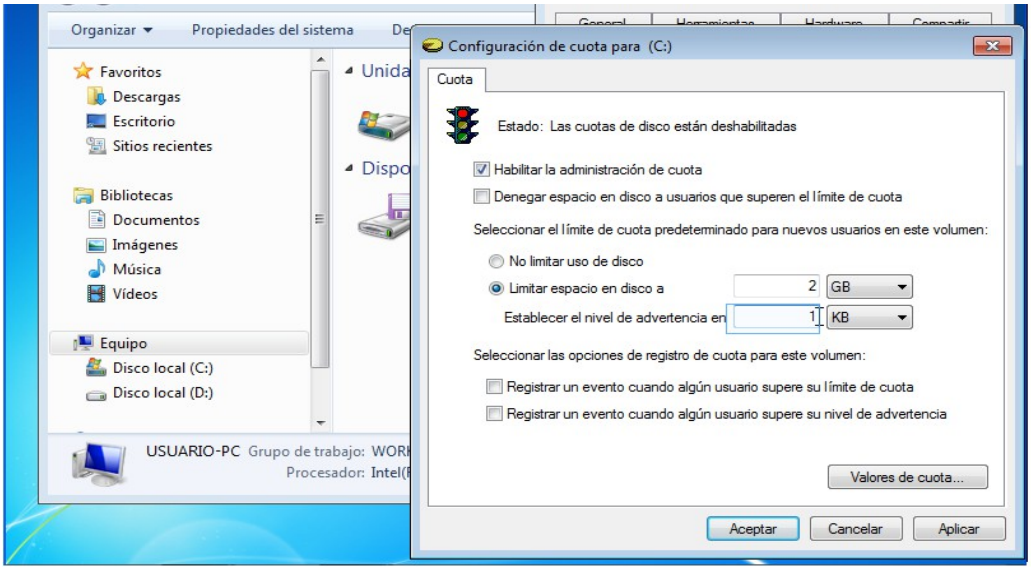
Uno de los recursos más importantes del ordenador es su capacidad de almacenamiento. Cuando un equipo es utilizado por varios usuarios, es preciso hacer una gestión del espacio de almacenamiento para que todos tengan el necesario.

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:

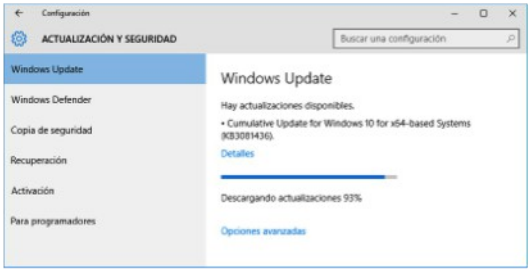


1. Establecer una directiva de grupo:
    1. Haz click en **Inicio** , haz click en **Ejecutar**, escribe mmc y, a continuación, haz click en **Aceptar**.
    2. En el menú **consola**, haz click en **Agregar o quitar complemento** .
    3. Haz click en **Agregar**, haz click en **Directiva de grupo** 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.

4.- Mantenimiento del sistema.

4.1.- Configuración de las actualizaciones automáticas.

Windows Update es la aplicación de Windows que nos permitirá buscar e instalar actualizaciones de Windows y otros productos de Microsoft.



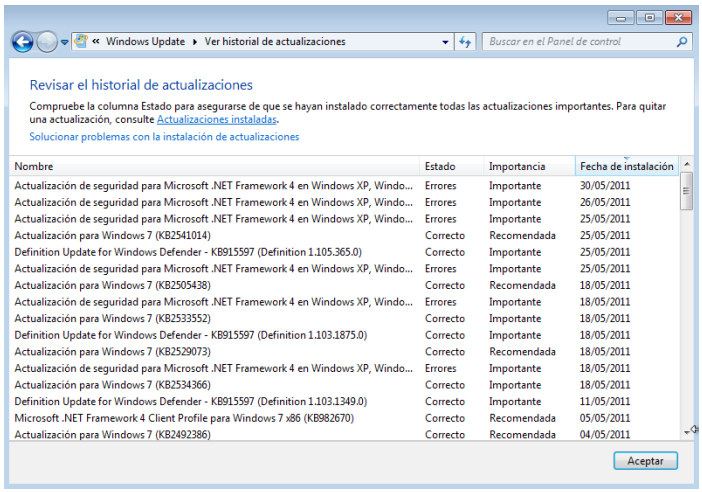
Es importante tener actualizado el sistema operativo, sobre todo cuando el sistema no lleva demasiado tiempo en el mercado, ya que con el tiempo aparecen errores (bugs) que Microsoft va resolviendo. Las actualizaciones nos permiten instalar directamente desde Internet las mejoras y soluciones que salen para nuestro sistema. Son especialmente importantes las actualizaciones que implican mejoras en la seguridad.

Podemos acceder a Windows Update a través del Panel de Control, Sistema y seguridad y pulsando en Windows Update en las versiones de windows 7 y 8. En windows 10 deberemos acceder a Configuración > Actualización y seguridad.

La zona principal, en las versiones de windows 7 y 8, nos muestra la configuración actual de Windows Update y en el panel izquierdo encontramos varias opciones relacionadas. Algunas de ellas son:

- **Buscar actualizaciones para iniciar la búsqueda manualmente**. Si existen actualizaciones disponibles, podremos elegir las que deseamos instalar.
- **Cambiar configuración.** Por defecto, Windows Update busca e instala las actualizaciones automáticamente, indicando su instalación a través de un icono en la barra de tareas. Puedes cambiar esta configuración como te explicamos en este avanzado.
- **Restaurar las actualizaciones ocultas**. Si una actualización no nos interesa, podremos ocultarla para que no nos vuelva a preguntar acerca de ella. Si cambiamos de idea, siempre podremos pulsar esta opción y volver a mostrarlas.
- **Ver historial de actualizaciones** muestra el listado incluyendo la fecha de instalación y su tipo (importante o recomendada).

Podemos ver las actualizaciones que ha ido instalando Windows Update en el equipo. Para, ello, en **Panel de control> Programas** disponemos del acceso **Ver actualizaciones instaladas** dentro de la **sección Programas y características**. También podemos **pulsar Ver historial de actualizaciones desde la ventana de Windows Update** y allí pulsar el enlace **Actualizaciones instaladas**.



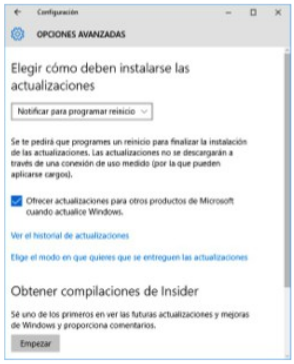
Accedemos a una ventana como la siguiente.

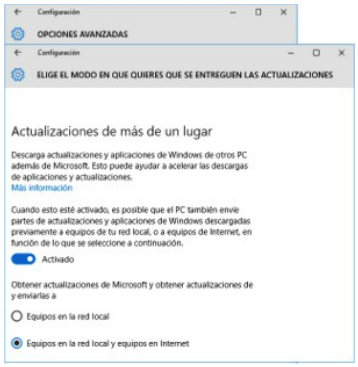
Si seleccionamos una actualización podremos pulsar el botón **Desinstalar**. En ocasiones también dispondremos de un botón **Cambiar**.

En las version de Windows 10 el las actualizaciones son obligatorias y no nos deja la opción de elegir si queremos o no queremos descargarlas. Como novedad podemos compartir las descargas con otros equipos en la red, de modo que se logrará acelerar la descarga de estas. Un equipo de la red lo descarga y luego lo comparte con el resto evitando la múltiple descarga de de internet de los mismos ficheros. Esto lo podemos gestionar en el apartado "Elige el modo en que quieres que se entreguen las actualizaciones".

En la versión profesional nos permite postponer la instalación de estas actualizaciones hasta que hayan sido probadas con garantías en los equipos con la versión Home.

Lo que si que podemos en esta versión es decidir cuando se produce el reinicio del sistema para finalizar con la instalación de la actualizaciones.





Normalmente no desinstalaremos actualizaciones, y no debemos hacerlo sólo para ganar espacio en disco. Sólo desinstalaremos una actualización, si ha habido algún problema durante el proceso de instalación de la misma o si el programa que actualiza ha dejado de funcionar correctamente a raíz de la misma.

4.2.- Monitorización del sistema y gestión de servicios (I): Monitor de rendimiento.

Windows 7 ya proporciona una herramienta para monitorizar el rendimiento de ciertos componentes del sistema. Hablamos del Monitor de rendimiento, con el que se puede visualizar la evolución del rendimiento en una gráfica actualizada en tiempo real. Además, con este monitor podemos realizar un seguimiento del comportamiento de elementos como el procesador, la memoria, el disco duro, el rendimiento de la red, o componentes del sistema más concretos como la función Readyboost y otros componentes de Windows.

Desde una única consola podemos supervisar el rendimiento de las aplicaciones y del hardware en tiempo real, personalizar qué datos desea recopilar en los registros, definir umbrales para alertas y acciones automáticas, generar informes y ver datos de rendimientos pasados en una gran variedad de formas.

El Monitor de rendimiento de Windows proporciona una interfaz gráfica para la personalización de conjuntos de recopiladores de datos y sesiones de seguimiento de eventos. La recopilación de datos y el registro se realiza mediante conjuntos de recopiladores de datos.

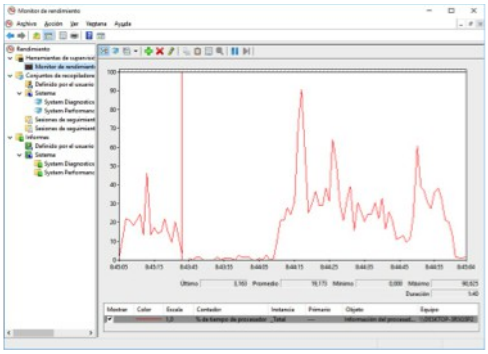
Veamos paso a paso cómo podemos configurar este monitor para que visualice el rendimiento en tiempo real de los aspectos que nos interesan con el objeto de localizar errores o componentes que están ralentizando nuestro PC.

1. **Abrir el Monitor de rendimiento**

   El primer paso será ejecutar el monitor de rendimiento del sistema. **Para iniciar el Monitor de rendimiento de Windows tenemos varias opciones:**

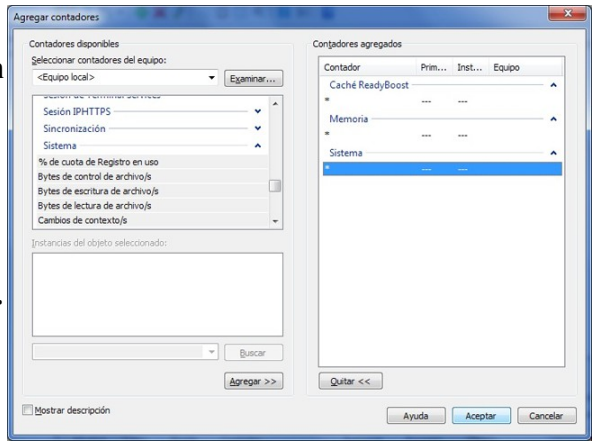
   - **Ir al Panel de Control - Sistema y Seguridad - Herramientas administrativas - Monitor de rendimiento.**
   - **O hacer click en Inicio**, después click en el cuadro **Iniciar búsqueda**, escribimos monitor y presionamos la tecla Enter.

2. **Acceder al monitor**

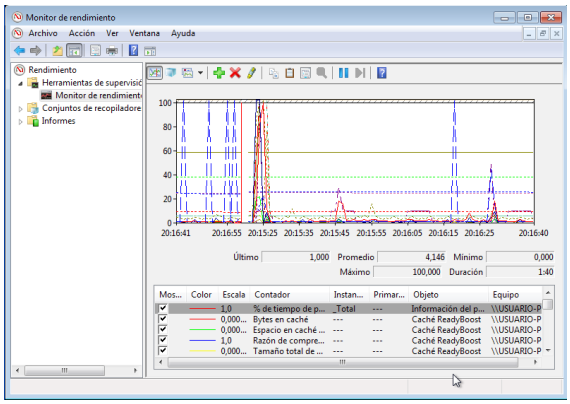


   En la ventana aparecerá un resumen del estado del sistema y una descripción de su funcionamiento. En la parte central en el apartado **Resumen del sistema** podremos ver en tiempo real el funcionamiento de algunos componentes del sistema. Para acceder a las gráficas de funcionamiento haremos click en la parte izquierda de la ventana en **Monitor de rendimiento** dentro de la carpeta **Herramientas de supervisión**. Veremos en pantalla una gráfica resumen de los elementos más importantes.

3. **Agregar componentes para monitorización**



   El siguiente paso será agregar componentes que van a ser monitorizados. Hay que tener en cuenta que cuantos más componentes agreguemos más confusa será la gráfica que se mostrará. Para conseguir agregarlos haremos click sobre **el símbolo más de color verde** que se encuentra sobre la gráfica junto con otros iconos. Aparecerá una ventana dividida en tres partes.



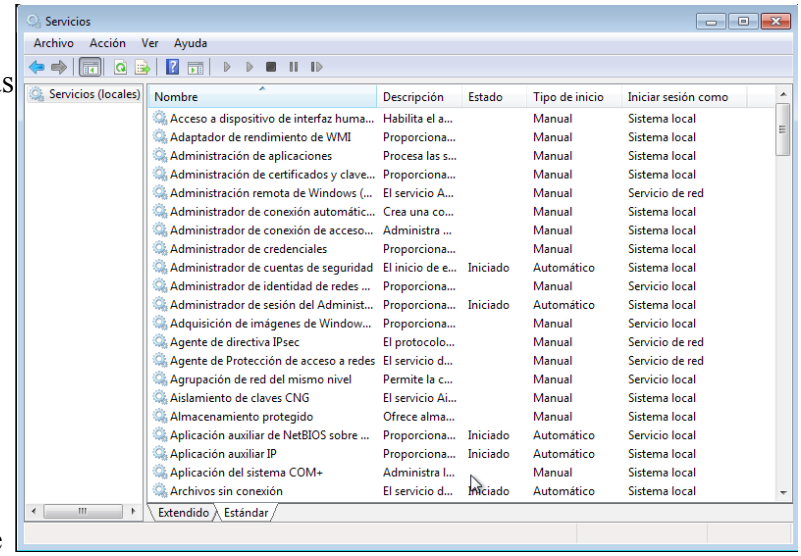
   En la parte superior izquierda seleccionaremos los componentes que vamos a monitorizar. Podemos ver desglosados los elementos analizados de cada componente si hacemos click en la flecha que apunta hacia abajo junto a cada uno de los contadores. En la parte llamada **Instancias del objeto seleccionado** podemos elegir que se controle una instancia concreta haciendo click sobre ella.

   También es posible controlar cada una de las instancias o que se contabilice el total. Si vamos a monitorizar varios componentes, es mejor elegir **Total** si es posible**.** Podemos ir agregando contadores pulsando sobre **Agregar**. De esta forma aparecerán en la parte llamada **Contadores agregados**. Para quitarlos los marcaremos en dicha zona y haremos click en **Quitar.** Al pulsar en **Aceptar** veremos en funcionamiento los contadores representados en la gráfica en tiempo real.

4.2.1.- Monitorización del sistema y gestión de servicios (II): Servicios.

Los servicios en Windows se ejecutan en segundo plano, y son transparentes para el usuario proporcionando muy variadas funcionalidades al sistema y consumiendo memoria, por supuesto, sin embargo algunos de ellos pueden no ser necesarios y pueden desactivarse sin que afecte al funcionamiento de nuestro equipo. Siempre antes de desactivar un servicio hay que informarse bien de su función.

Pero, ¿cómo podemos acceder a los servicios? Windows 7 y 8 nos proporciona la herramienta **Servicios**, a la que podemos acceder desde Inicio -> Panel de Control -> Sistema y seguridad -> Herramientas administrativas - Servicios o desde el cuadro de búsqueda introduciendo `services.msc`.



En Windows 10 accedemos a la herramienta **Servicios** desde Todas las aplicaciones -> Herramientas administrativas de Windows -> Servicios

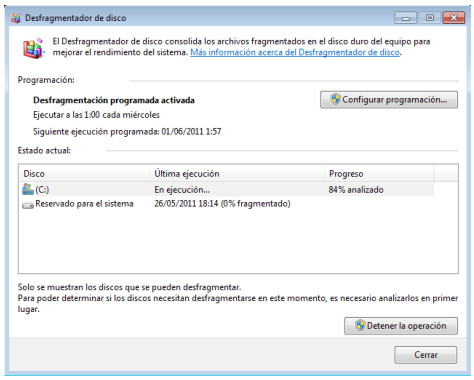
Esta herramienta te muestra un listado de los procesos junto con su descripción, el tipo de inicio y otras características. Además de permitir la consulta, también se pueden iniciar o desactivar los servicios que se ejecutan en Windows. A continuación, ponemos un listado de ejemplo de algunos servicios y su función que podemos encontrarnos en la herramienta Servicios:

- Servicios de Escritorio remoto - `TermService`, - `SessionEnv`, - `UmRdpService`
- Tarjeta inteligente - `SCardSvr`: Administra el acceso a tarjetas inteligentes.
- Registro remoto - `RemoteRegistry`: Modificar registro a usuarios remotos.
- Ubicador de llamada a procedimiento remoto - `RpcLocator`
- Windows Search - `WSearch`: Indexa los archivos, el correo electrónico y otros contenidos para hacer búsquedas con más rapidez.
- Servicio del Reproductor de Windows Media - `WMPNetworkSvc`: Comparte las bibliotecas del Reproductor de Windows Media con otros dispositivos.
- Tarjetas inteligentes - `SCPolicySvc`: Permite configurar el sistema para bloquear el escritorio al extraer la tarjeta inteligente.
- Parental Controls - `WPCSvc`: Control parental.
- Archivos sin conexión - `CscService`: Realiza actividades de mantenimiento en la caché de archivos sin conexión.
- Agente de Protección de acceso a redes - `napagent`: Administra información de los equipos de una red.
- Net Logon - `Netlogon`: Autentica usuarios y servicios.

- Servicio del iniciador iSCSI de Microsoft - `MSiSCSI`
- Aplicación auxiliar IP - `iphlpsvc`
- Cliente de seguimiento de vínculos distribuidos - `TrkWks`: Mantiene los vínculos entre archivos NTFS dentro de un equipo o entre equipos de una red.
- Propagación de certificados - `CertPropSvc`
- BranchCache - `PeerDistSvc`: Caché del contenido de la red en red local.
- Servicio de compatibilidad con Bluetooth - `bthserv`: Permite la detección y asociación de dispositivos Bluetooth remotos.
- Servicio de detección automática de proxy web WinHTTP - `WinHttpAutoProxySvc`
- Servicio Informe de errores de Windows - `WerSvc`, Envío de informes sobre los errores a Microsoft.
- Servicio Cifrado de unidad BitLocker - `BDESVC`
- Sistema de cifrado de archivos - `EFS`, para almacenar archivos cifrados en particiones NTFS.
- Fax - `Fax`
- Acceso a dispositivo de interfaz humana - `hidserv`

4.3.- Desfragmentación y chequeo de discos (I).

La **fragmentación de un disco** se produce cuando numerosos archivos se encuentran divididos a lo largo de la partición. El hecho de que un archivo se encuentre disperso reduce el rendimiento de la unidad, por que el cabezal tendrá que saltar por varias partes del disco para obtener la información y eso aumenta el tiempo de acceso al contenido del archivo.



Un programa desfragmentador de disco nos ayuda a que todas las porciones de un archivo queden contiguas y que la parte del disco duro que tiene información esté al principio y el espacio de la partición quede al final.

Es muy recomendable desfragmentar el disco duro cuando notes que el rendimiento del disco duro esté decayendo, es decir, que el sistema operativo tarde mucho en encontrar la información en el disco duro porque ésta se encuentra muy dispersa.

Windows 7 y 8 proporciona una herramienta para ello, el **Desfragmentador de disco**, podemos acceder a ella desde **Inicio - Todos los programas - Accesorios - Herramientas del sistema**. En Windows 10 basta con escribir desfragmentar en el cuadro de búsqueda de la barra de tareas. El Desfragmentador de disco vuelve a organizar los datos fragmentados de manera que los discos y las unidades puedan funcionar de manera más eficaz. Se ejecuta por defecto según una programación (que puede definirse a medida), pero también puede analizar y desfragmentar los discos y las unidades manualmente.

Para saber más

Puedes encontrar más información sobre la desfragmentación en este post:

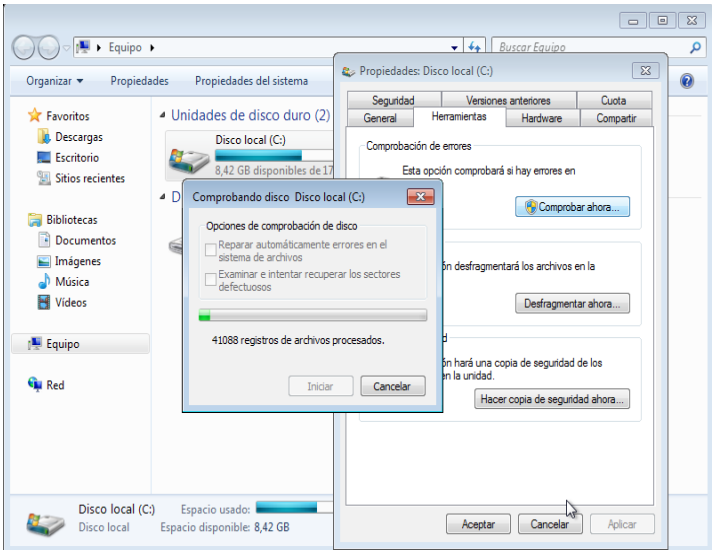
Cinco razones para desfragmentar tu disco duro: https://hipertextual.com/archivo/2013/09/desfragmentar-un-disco/

4.3.1.- Desfragmentación y chequeo de discos (II).

Por otra parte, podemos **comprobar o chequear los discos**, para comprobar si existen problemas en los mismos. Windows proporciona una herramienta para ello, si existen problemas, la herramienta intentará reparar los que encuentre. Por ejemplo, puede reparar los problemas relacionados con sectores defectuosos, clústeres perdidos, archivos con vínculos cruzados y errores de directorio. Para poder usar la herramienta se debe iniciar sesión como administrador o como miembro del grupo Administradores.

Tenemos dos opciones para ejecutar la herramienta de Chequeo de discos de Windows, con el comando `chkdsk.exe` (Check disk) o desde el **Equipo** o **Explorador de Windows** en la ficha **Propiedades del disco**. A continuación describimos ambos procesos:

Para ejecutar `Chkdsk` en el símbolo del sistema:



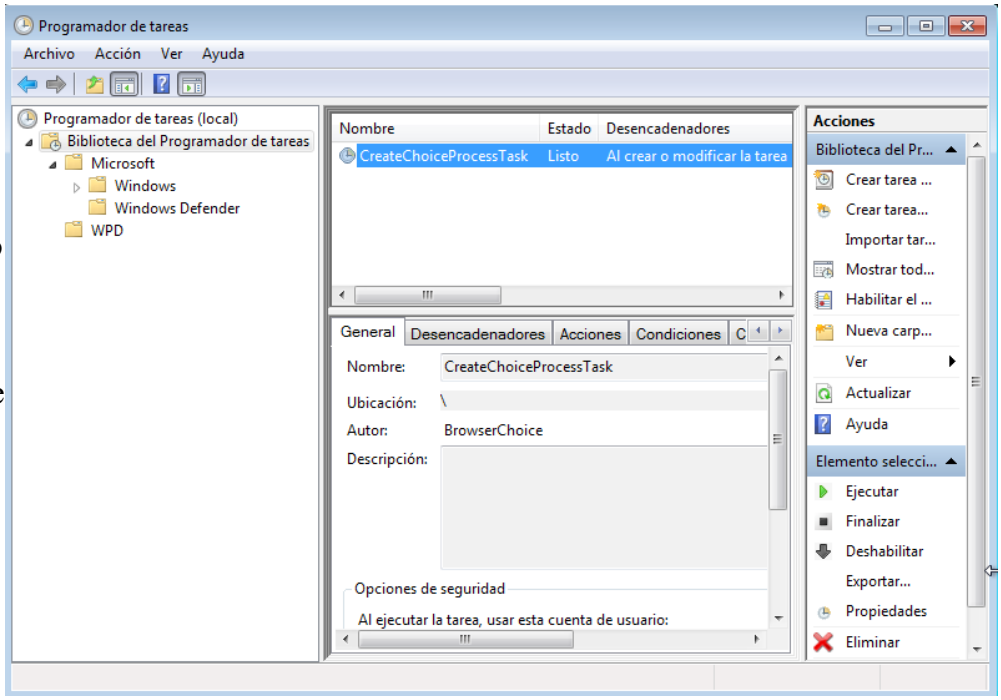
1. Haz click en **Inicio** y, a continuación, en **Ejecutar, o pulsa [tecla Windows] + [R].**
2. En el cuadro **Abrir**, escriba `cmd` y presione ENTER.
3. Siga uno de estos procedimientos:
   - Para ejecutar `chkdsk` en modo de sólo lectura, en el símbolo del sistema, escribe `chkdsk` y, a continuación, presiona la tecla ENTER. Se puede indicar como parámetro la partición que queremos comprobar, por ejemplo: `chkdsk f:` (chequeará la unidad F:).
   - **Nota**: si alguno de los archivos de la unidad de disco duro se encuentra abierto, recibirá el mensaje siguiente: `chkdsk` no se puede ejecutar porque otro proceso ya está utilizando el volumen. ¿Desea que se prepare este volumen para que sea comprobado la próxima vez que se inicie el sistema? (S/N). Escribe S y, a continuación, presiona la tecla ENTER para programar la comprobación del disco y, a continuación, reinicie el equipo para iniciarla.

Para ejecutar `chkdsk` a partir de Equipo o el Explorador de Windows:

1. Haz doble click en **Mi equipo** y, a continuación, haz click con el botón secundario del ratón en la unidad de disco duro que desea comprobar.
2. Haz click en **Propiedades** y, después, en **Herramientas**.
3. En **Comprobación de errores**, haz click en **Comprobar ahora**. Aparecerá un cuadro de diálogo que muestra las **Opciones de comprobación de disco**.
4. Sigue uno de estos procesos:
   - Para ejecutar `chkdsk` en modo de sólo lectura, haz click en **Iniciar**.
   - Para reparar los errores sin buscar los sectores defectuosos, seleccione la casilla de verificación **Reparar automáticamente errores en el sistema de archivos** y, a continuación, haz click en **Iniciar**.
   - Para reparar los errores, localizar los sectores defectuosos y recuperar la información legible, seleccione la casilla de verificación **Examinar e intentar recuperar los sectores defectuosos** y, a continuación, haz click en **Iniciar**.

4.4.- Programación de tareas de mantenimiento.

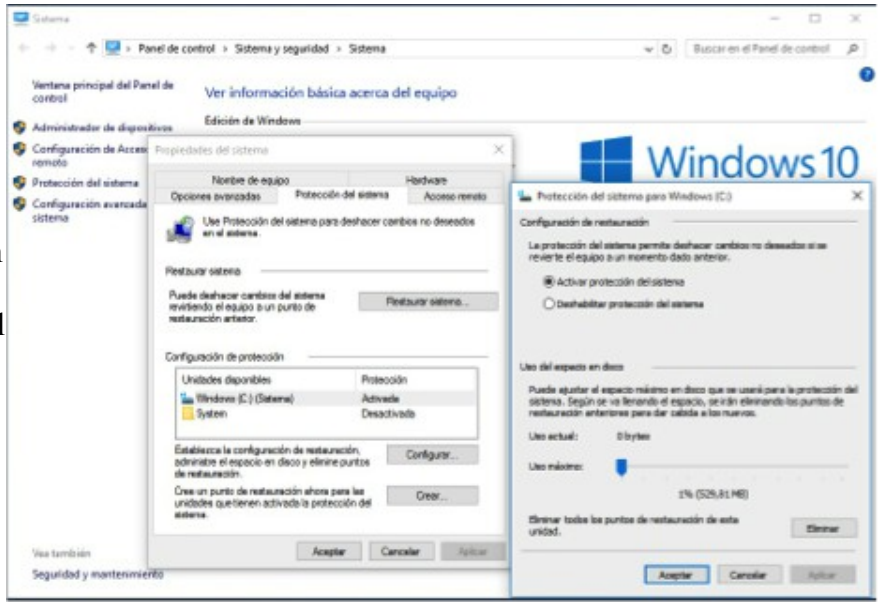
Todos sabemos que los ordenadores requieren de un mantenimiento mínimo periódico para que su funcionamiento sea óptimo, es decir, desfragmentar el disco duro, pasar scandisk, analizar el sistema con un antivirus, etc. Son tareas que no siempre recordamos hacer y que pueden ser programadas y automatizadas por el usuario. Esta importante descarga de trabajo se consigue por medio de la herramienta Programador de tareas.



El Programador de tareas permite programar la ejecución automática de aplicaciones u otras tareas. Para utilizarlo es necesario iniciar sesión como administrador. Si se inició sesión como administrador, sólo se pueden cambiar las configuraciones que se apliquen a su cuenta de usuario.

1. **Para abrir Programador de tareas,** haz click en el botón **I**nicio, en Panel de control, en Sistema y Seguridad, en Herramientas administrativas y, a continuación, haz doble click en Programador de tareas. En windows 10 desde Todas las aplicaciones -> Herramientas administrativas de Windows -> Servicios.
2. Haz click en el menú Acción y luego en Crear tarea básica.
3. Escribe un nombre para la tarea y, si lo deseas, una descripción y haz click en Siguiente.
4. Realiza una de estas acciones:
   - Para seleccionar una programación basándose en el calendario, haz click en Diariamente, Semanalmente, Mensualmente o Una vez, haz click en Siguiente, especifica la programación que desee usar y haz click en Siguiente.
   - Para seleccionar una programación basándose en eventos repetitivos, haz click en Cuando el equipo inicie o Cuando inicie sesión y, a continuación, haz click en Siguiente.
   - Para seleccionar una programación basándose en eventos específicos, haz click en Cuando se produzca un evento específico, haz click en Siguiente, especifique el registro de eventos y otros datos mediante las listas desplegables y, a continuación, haz click en Siguiente.
5. Para programar una aplicación para que se inicie automáticamente, haz click en Iniciar un programa y, a continuación, en Siguiente.
6. Haz click en Examinar para buscar el programa que desee iniciar y después haz click en Siguiente.
7. Haz click en Finalizar.

4.5.- Restaurar el sistema.



En ocasiones, nuestro sistema puede volverse inestable o incluso dejar de funcionar totalmente. Esto puede deberse a numerosas causas, tales como un controlador mal diseñado, un programa malintencionado o mal programado, un error del usuario, una corrupción del registro, etc. En estos casos, una ayuda fundamental es la capacidad de Windows de Restaurar el sistema a un punto anterior, lo que eliminará automáticamente todos los cambios que hayamos realizado en nuestro equipo desde el momento en que se creó dicho punto de restauración.

Para crear un punto de restauración en Windows seguiremos estos pasos:

- Hacer click en **Inicio** y seleccionar el **Panel de control.**
- Seleccionar **Sistema y Seguridad.**
- Seleccionar **Sistema.**
- Hacer click en **Protección del sistema**, ubicado en el panel izquierdo.
- Seleccionar la pestaña **Protección del sistema** de la ventana Propiedades del sistema.
- Hacer click en el botón **Crear.**
- Ingresar un nombre al punto de restauración en la casilla de texto y hacer click en el botón **Crear.**
- Luego de terminar la creación del punto, se mostrará un mensaje indicando que el punto de restauración se creó satisfactoriamente.

Para verificar que el punto se ha creado correctamente, hacer click en el botón ***Restaurar sistema***, luego seleccionar **Elegir otro punto de restauración** y el punto creado se mostrará en la lista de puntos existentes.

Cada punto de restauración de sistema que creemos, consume un espacio en disco. Cada cierto tiempo, Windows crea automáticamente sus propios puntos de restauración, y también son creados automáticamente cuando instalamos nuevo software o controladores, siempre que estos sean considerados importantes por el sistema.

El total del espacio en disco que pueden ocupar entre todos los puntos restauración, así como el funcionamiento general del programa de restauración, pueden ser ajustados desde la configuración de Restaurar Sistema.

Cuando se crea un punto de restauración, y no existe espacio suficiente, Windows elimina el punto de restauración más antiguo que encuentre. No existe forma de salvaguardar un punto de restauración en concreto.

4.6.- Copias de seguridad.

¿Nunca has perdido algún archivo o archivos importantes que no has podido recuperar? Es muy probable que la respuesta a esta pregunta sea afirmativa, si no lo es, has tenido suerte, pero conviene ser precavidos y realizar con cierta frecuencia copias de seguridad de los datos que más utilicemos y/o apreciemos. La importancia de realizar copias de seguridad de nuestros archivos es fundamental y más si trabajamos en una empresa teniendo responsabilidades sobre los datos que gestionamos. Existen multitud de programas para hacer copias de seguridad que permiten la planificación y programación de copias para automatizar el proceso. Se recomienda, como es lógico, guardar las copias de seguridad en dispositivos externos al equipo para evitar su pérdida en caso de mal funcionamiento del equipo.

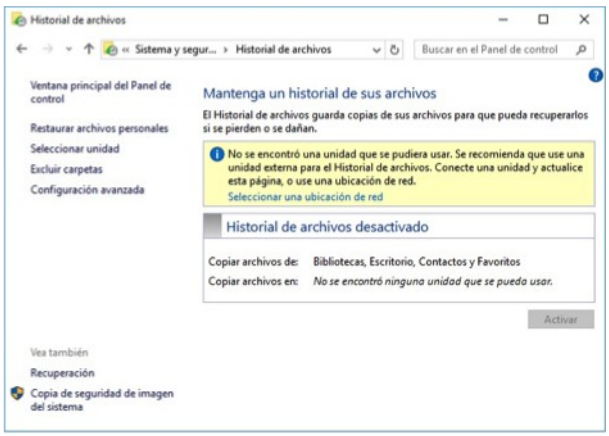
Windows permite hacer copias de seguridad de archivos o restaurar nuestro equipo a una situación anterior a través de la herramienta Copias de seguridad y restauración. Una de las formas para acceder a esta herramienta es ir a **Inicio - Mantenimiento - Copias de seguridad y restauración. Aunque también puede accederse desde el Panel de control.**

Una vez dentro de la herramienta de copias de seguridad **haremos una salvaguarda de datos** con los pasos siguientes:

- En la ventana de Copias de seguridad haz click en Configurar copia de seguridad.
- Selecciona donde deseas guardar la copia de seguridad (en un disco, pendrive o incluso en Red) y elegir si todo el disco o sólo unos archivos.
- Seleccione los archivos y carpetas para incluir en la copia de seguridad.
- Aquí también se pueden programar los días y los tiempos de copia de seguridad.
- Haz click en "Guardar configuración y ejecutar la copia de seguridad".
- Esperaremos a que finalice y revisaremos el archivo generado con la copia de seguridad.

Para restaurar una copia de seguridad:

- Haz doble click en la copia de seguridad que realiza anteriormente.
- Haz click en Restaurar archivos de la copia de seguridad.
- Selecciona los archivos y el destino donde deseas restaurar los archivos.
- Y ya nos quedaría esperar a que finalice el proceso. El tiempo de restauración puede variar dependiendo del tamaño de la copia de seguridad.



En Windows 8 y 10 además de la herramienta de copias de seguridad tenemos a nuestra disposición **"Historial de Archivos"**. Sólo realiza copias de seguridad de los archivos que están en las carpetas: Documentos, Música, Imágenes, Vídeos y Escritorio y de los archivos de OneDrive disponibles sin conexión en el PC. Si quieres hacer copias de seguridad de archivos o carpetas que están en otra ubicación, puedes agregarlos a una de estas carpetas

Para hacer una copia de seguridad primero debemos de indicar donde se va realizar la copia de seguridad, es conveniente realizarla en una unidad externa, ya sea una unidad usb o un disco duro externo.

Para saber más

En el siguiente enlace puedes ver un video de Microsoft en el que se explica cómo restaurar archivos o carpetas con el historial de archivos.

Restaurar con el hisotrial de archivos: https://support.microsoft.com/es-es/help/17128/windows-8-file-history

5.- Uso de antivirus, antiespías y otros programas de protección.

5.1.- Antivirus.

¿Crees que un cortafuegos es suficiente para mantener tu equipo protegido? ¿Sabías que más del 90% de las infecciones por malware (es decir, los virus, gusanos, troyanos, etc.) son provocadas por los propios usuarios pulsando en ficheros adjuntos de emails, visitando sitios web de dudoso origen o ejecutando programas poco fiables que prometen falsos premios u ofertas? Por este motivo, la mayoría de los virus se "cuelan" por lugares autorizados, como el puerto 80 del navegador (en forma de página web), o el 110 del correo electrónico (en forma de mensajes de email). No podemos cerrar esos puertos ya que nuestro navegador o programa de correo no funcionarían. Así que debemos recordar que para alcanzar un buen nivel de seguridad en nuestro equipo necesitaremos un buen cortafuegos y un antivirus actualizado.

Un programa antivirus se encarga de detectar y eliminar amenazas de seguridad en nuestro equipo, virus, troyanos, software espía, gusanos, backdoors, etc. Existe una amplia gama de software antivirus en el mercado (BitDefender, Panda, Pc-Tools, Kaspersky, McAfee, Norton, Trend Micro, ESET Nod32, entre otros). Pero, ¿cuáles son los mejores? Eso dependerá de las necesidades de cada usuario, existen no obstante, comparativas en Internet que pueden ayudarnos a tomar la decisión. Debemos conocer que también contamos con opciones gratuitas, tales como Avast! Free Antivirus, AVG Anti-Virus Free, etc. Sin embargo estos antivirus gratuitos suelen tener limitadas sus actualizaciones en el tiempo, y en el número de opciones de seguridad que proporcionan al usuario respecto de sus ediciones de pago.

Hoy día el uso de pendrives o dispositivos de almacenamiento extraíbles está a la orden del día por lo que también estamos en peligro de contagiar nuestro equipo a través de estos. Por ello, lo que podem**os hacer es instalar un antivirus para el pendrive**. Algunos ejemplos son:

1. Antivirus ClamWin para Pendrive, una "PortableApp"
2. Antivirus Mx One para Pendrive.

Ningún antivirus es eficaz al 100%, eso es seguro al 100%, por eso lo mejor es ser lo más precavidos posible. ¿Qué pautas generales podemos seguir para proteger nuestros equipos de virus y malware, en general?

- **Siempre hay que mantener el Sistema Operativo, Navegador y Pluggins actualizados** a la última versión. (Firefox posee un plugin de seguridad llamado NoScript, recomendado)
- **Poseer un Antivirus con actualizaciones automáticas**, ya sea para las bases de datos de virus o para actualizar el propio programa por si fuera necesario.
- Programas complementarios, como Firewalls, antispywares, etc. aunque varios antivirus de pago ya poseen estos complementos incorporados.
- **Anti Phishing**, lo mejor es utilizar el sentido común y no fiarte nunca de nada. No dar contraseñas si no estás seguro.

5.2.- Windows Defender.

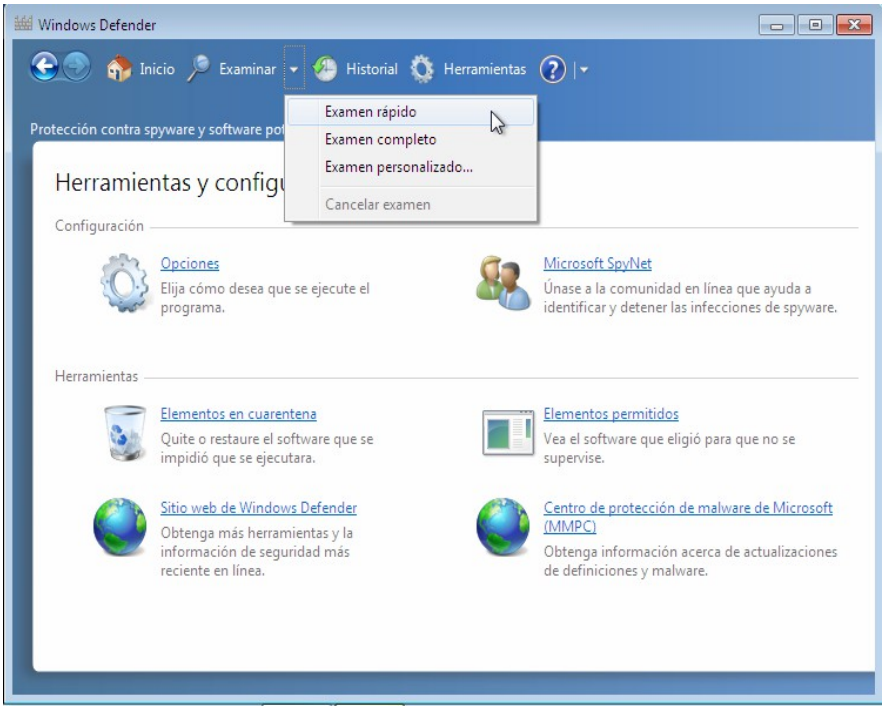
Se trata de un **programa antispyware** que incorpora Windows. El **spyware** es un software espía que suele mostrar anuncios emergentes, recopilar información sobre el usuario o cambiar la configuración del equipo sin consentimiento del usuario. Por ello, es muy importante ejecutar software antispyware cuando utilice el equipo. El spyware y otro software no deseado pueden intentar instalarse en el PC cuando nos conectamos a Internet. Puedes activar Windows Defender u otro software antispyware para proteger la seguridad de tu equipo.

Para **acceder a Windows Defender** hay varias opciones: 1) en el **cuadro de búsqueda del menú Inicio teclear "Windows Defender"** o 2) ir al **Panel de control > Sistema y Seguridad > Centro de Actividades > Seguridad > Activar Windows Defender.**

Windows Defender puede:

- Realizar un **análisis rápido** del equipo si sospechas que puede tener algún spyware. Analiza todas las unidades que comúnmente son infectadas por spyware.
- Realizar un **análisis completo**, analiza todas las unidades, archivos y servicios activos, puede ralentizar el rendimiento del equipo.
- Realizar un **análisis personalizado**, donde se seleccionan las unidades a analizar.
- Finalizado el análisis se obtienen **estadísticas** del mismo.
- **Actualizarse** para detectar nuevas amenazas.
- Se recomienda realizar un **análisis rápido diario**.

En Examinar aparecen las opciones de análisis rápido, completo y personalizado.



Autoevaluación

Windows Defender permite realizar …

○ Actualizaciones para detección de nuevas amenazas.

○ Análisis completos del sistema.

○ Configurar análisis a medida del usuario.

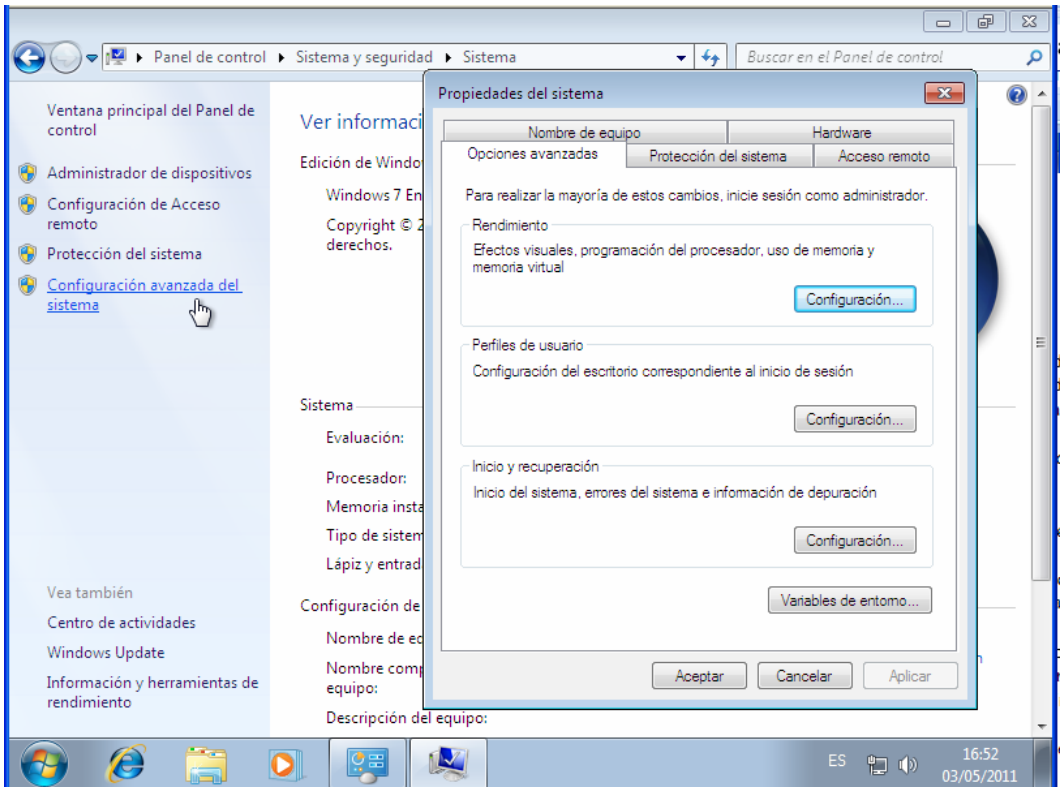
◉ Todas son ciertas.

5.3.- Prevención de ejecución de datos (DEP).

DEP (Data Execution Prevention) es una característica de seguridad que ayuda a impedir daños en el equipo producidos por virus y otras amenazas a la seguridad. **Los programas malintencionados pueden intentar atacar Windows mediante la ejecución de código desde ubicaciones de la memoria del sistema reservadas para Windows** y otros programas autorizados. DEP supervisa la ejecución de los programas para garantizar que utilizan la memoria del sistema de manera segura.

Para configurar la prevención de ejecución de datos (DEP), se tendrá en cuenta lo siguiente:

1. Haz click en **Inicio > Panel de control > Sistema y seguridad > Sistema**.
2. Haz click en **Configuración avanzada del sistema** en el panel de tareas de la izquierda.
3. Se obtiene la pantalla Propiedades del sistema.
4. En **Rendimiento** de la ficha **Opciones avanzadas** de la pantalla Propiedades del sistema, haz click en **Configuración**. Se obtiene la pantalla **Opciones de rendimiento**.



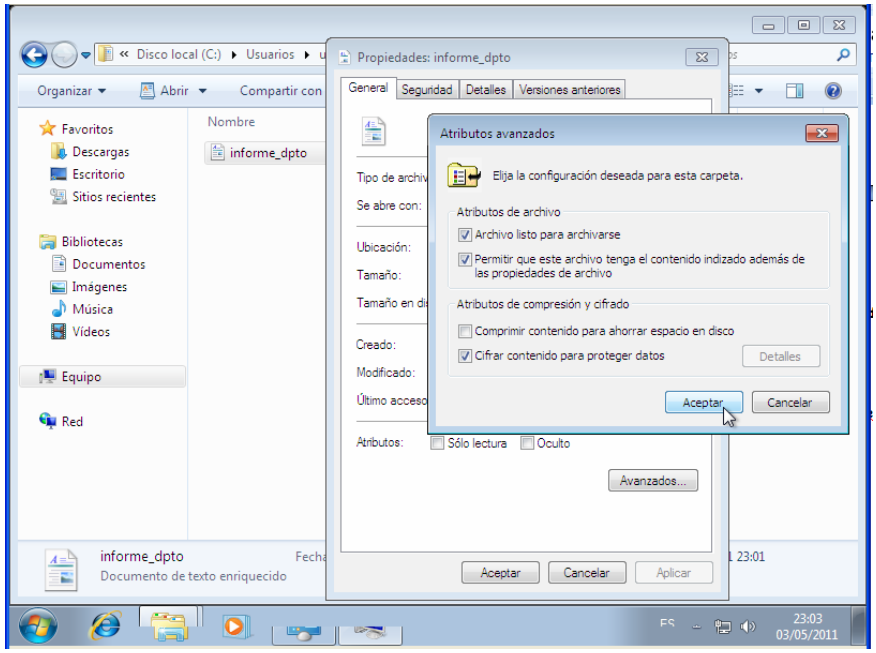
5. Haz click en la ficha **Prevención de ejecución de datos** y, a continuación, pulse en **Activar DEP** para todos los programas y servicios excepto los que selecciones. También se puede activar DEP sólo para los programas y servicios de Windows esenciales.
6. Para **desactivar DEP** para un programa concreto selecciona la casilla del programa y acepta los cambios.
7. Si el programa al desactivar DEP no aparece, elige Agregar, busca en la carpeta Archivos de programa, localiza el archivo ejecutable del programa, y, por último, click en Abrir.

5.4.- Sistema de cifrado de archivos (I).

El sistema de cifrado de archivos (EFS) es una característica de Windows que permite **almacenar información en el disco duro de forma cifrada**. El cifrado es la protección de mayor nivel que proporciona Windows para mantener la información a salvo.

Éstas son algunas **características** destacadas de EFS:

- El cifrado es sencillo. Se realiza activando una casilla en las propiedades del archivo o de la carpeta.
- El usuario controla quién puede leer los archivos.
- Los archivos se cifran cuando los cierra, pero cuando los abres quedan automáticamente listos para su uso.
- Si se cambia de idea con respecto al cifrado de un archivo, se puede desactivar la casilla en las propiedades del archivo.
- Sólo se pueden cifrar archivos y carpetas en los volúmenes del sistema de archivos NTFS.
- Los archivos y carpetas comprimidos también se pueden cifrar. Al cifrarlos se descomprimirán.
- Los archivos marcados con el atributo del sistema no se pueden cifrar, tampoco los archivos de la carpeta `systemroot`.
- EFS se instala de manera predeterminada en Windows 7, Windows 8 y Windows 10.



Para **cifrar archivos o carpetas con EFS**, abre el explorador de Windows y haz click con el botón secundario en el archivo o la carpeta que quieres cifrar. Haz click en Propiedades.

En la ficha General > Avanzadas y activamos la casilla **Cifrar contenido para proteger datos** y Aceptar. Hay disponibles opciones de cifrado adicionales.

A continuación, se solicita que se haga copia de seguridad de la clave de cifrado:

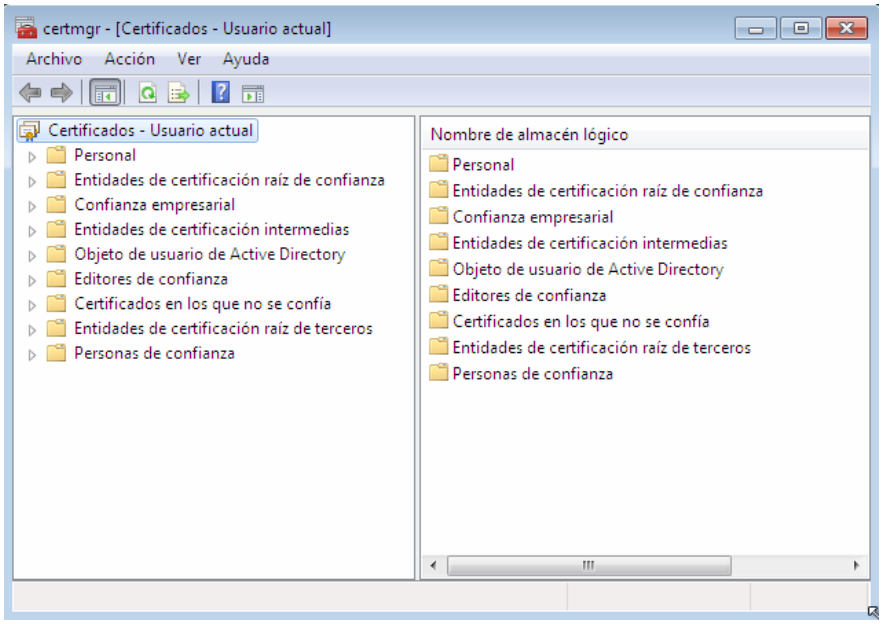
Si cifras datos en el equipo, necesitas un método para recuperar esos datos en caso de que surja algún problema con la clave de cifrado. Si la clave de cifrado se pierde o queda dañada y

no tienes ningún medio de recuperar los datos, éstos se perderán. También perderás datos si almacenas la clave de cifrado en una tarjeta inteligente y ésta se daña o se pierde. Para asegurarse de que siempre puede tener acceso a los datos cifrados, debes hacer una copia de seguridad de la clave y del certificado de cifrado. Si hay más de una persona que usa tu equipo, o si usas una tarjeta inteligente para cifrar archivos, debes crear un certificado de recuperación de archivos.

Finalmente, se genera un certificado del que deberemos hacer copia de seguridad, preferiblemente en un medio extraíble.

5.4.1.- Sistema de cifrado de archivos (II).

Si quisiéramos **hacer una copia de todos los certificados EFS** del equipo:



1. Para abrir el Administrador de certificados, haz click en el botón Inicio, escribe certmgr.msc en el cuadro de búsqueda y, a continuación, presione ENTER. Si te solicita una contraseña de administrador o una confirmación, escribe la contraseña o proporciona la confirmación.
2. En el panel izquierdo, haz doble click en Personal.
3. Haz click en Certificados.
4. En el panel principal, haz click en el certificado en el que se muestra Sistema de cifrado de archivos, en Propósitos planteados. Es posible que debas desplazarte a la derecha para verlo.

   Debes hacer una copia de seguridad de todos los certificados EFS que haya.

5. Haz click en el menú Acción, apunta a Todas las tareas y, a continuación, haz click en Exportar.
6. En el Asistente para exportación de certificados, haz click en Siguiente, después en Exportar la clave privada y, a continuación, en Siguiente.
7. Haz click en Personal Information Exchange y, a continuación, en Siguiente.
8. Escribe la contraseña que deseas usar, confírmala y, a continuación, haz click en Siguiente. En el proceso de exportación, se creará un archivo para almacenar el certificado.
9. Escribe el nombre y la ubicación del archivo (incluye la ruta de acceso completa), o bien haz click en Examinar, desplázate hasta la ubicación, escribe el nombre del archivo y, a continuación, haz click en Guardar.
10. Haz click en Siguiente y, después, en Finalizar.

Recuperación de certificados EFS:

Si por cualquier motivo tuvieras que **recuperar la clave privada** realizarías el proceso contrario, **importarías el certificado** al equipo en cuestión.

Para ver el proceso de exportación e importación de certificados de cifrado más detalladamente echa un vistazo a la siguiente presentación:

> ***Debes conocer***
>
> Conoce con más detalle el proceso de cifrado de datos, la exportación e importación de certificados EFS.

Anexo II.- Procesos de cifrado, exportación e importación de certificados EFS.

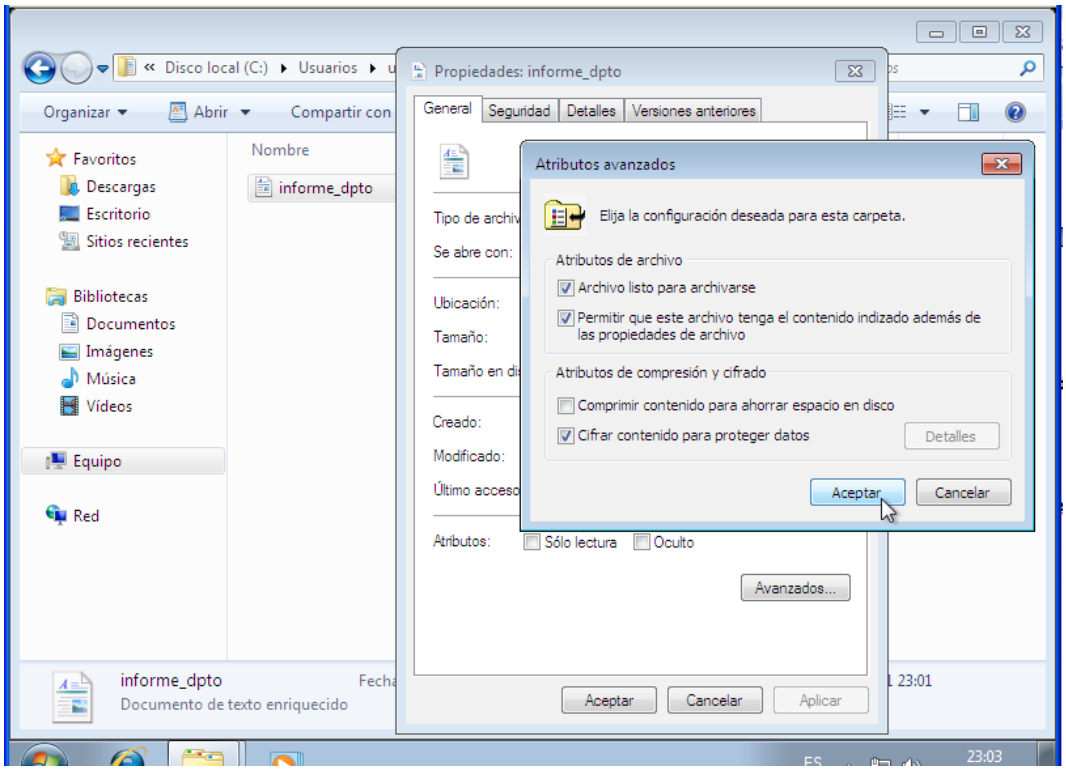
Sistema de cifrado de archivos: Proceso de cifrado de datos, exportación e importación de certificados EFS

Proceso de cifrado de datos

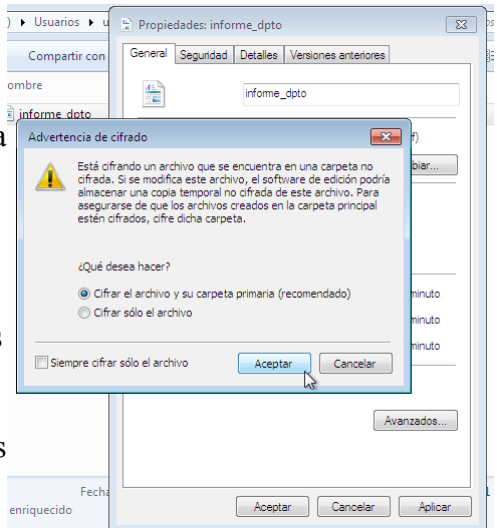
El sistema de cifrado de archivos (EFS) es una característica de Windows que permite **almacenar información en el disco duro de forma cifrada**. El cifrado es la protección de mayor nivel que proporciona Windows para mantener la información a salvo.

Para cifrar archivos o carpetas con EFS, abre el explorador de Windows y haz clic con el **botón secundario** en el archivo o la carpeta que quieres cifrar. Haz clic en **Propiedades**.

En la ficha General > Avanzadas y activamos la casilla **Cifrar contenido para proteger datos** y Aceptar.



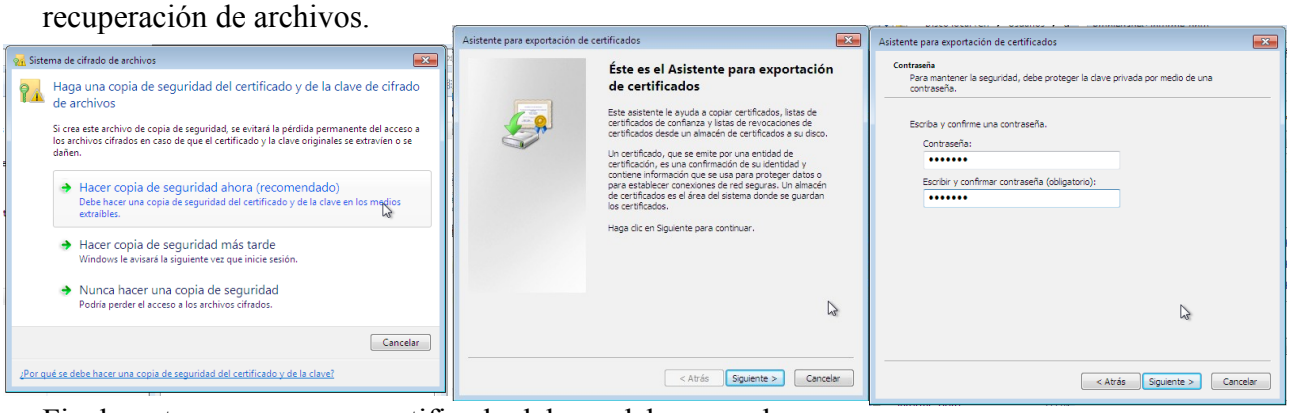
Hay disponibles opciones de cifrado adicionales.



Exportación de certificados EFS (copia de seguridad)

Después de realizar el cifrado de datos, se solicita que se haga copia de seguridad de la clave de cifrado:

Si cifras datos en el equipo, necesitas un método para recuperar esos datos en caso de que surja algún problema con la clave de cifrado. Si la clave de cifrado se pierde o queda dañada y no tienes ningún medio de recuperar los datos, éstos se perderán. También perderás datos si almacenas la clave de cifrado en una tarjeta inteligente y ésta se daña o se pierde. Para asegurarse de que siempre puede tener acceso a los datos cifrados, debe hacer una copia de seguridad de la clave y del certificado de cifrado. Si hay más de una persona que usa tu equipo, o si usas una tarjeta inteligente para cifrar archivos, debes crear un certificado de recuperación de archivos.

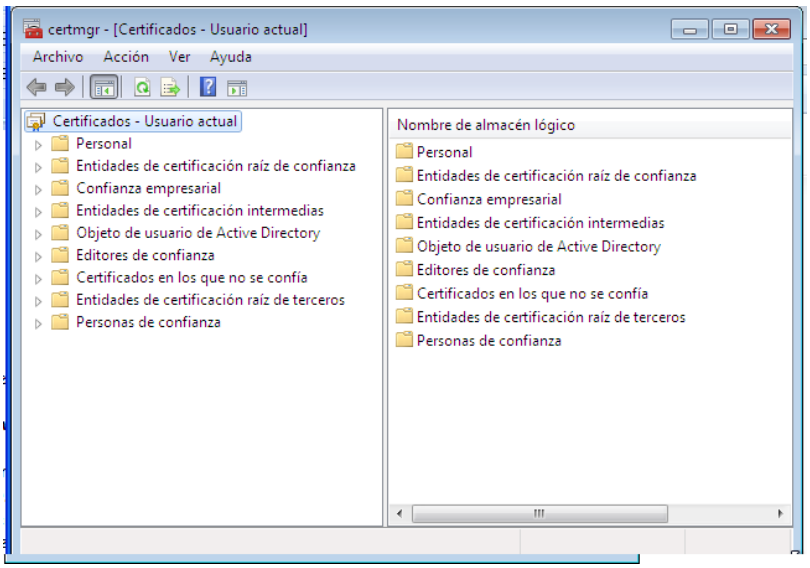


Finalmente, se genera un certificado del que deberemos hacer copia de seguridad, preferiblemente en un medio extraíble.

Existe la posibilidad de hacer una copia de seguridad de todos o algunos de los certificados EFS almacenados en nuestro sistema en otro momento posterior al cifrado de la información.

Si quisiéramos hacer una copia de todos los certificados EFS del equipo:

1. Para abrir el Administrador de certificados, haz clic en el botón Inicio, escribe `certmgr.msc` en el cuadro de búsqueda y, a continuación, presiona ENTER. Si se te solicita una contraseña de administrador o una confirmación, escribe la contraseña o proporciona la confirmación.



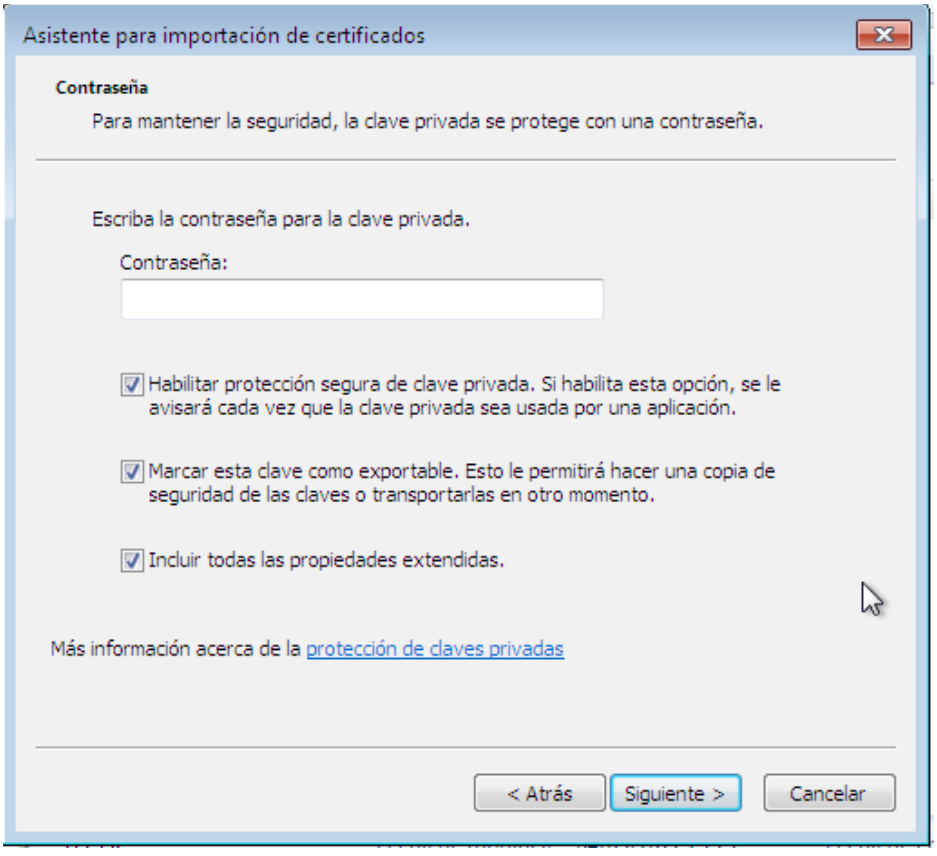
2. En el panel izquierdo, haz doble clic en Personal.
3. Haz clic en Certificados.
4. En el panel principal, haz clic en el certificado en el que se muestra Sistema de cifrado de archivos, en Propósitos planteados. Es posible que debas desplazarte a la derecha para verlo.

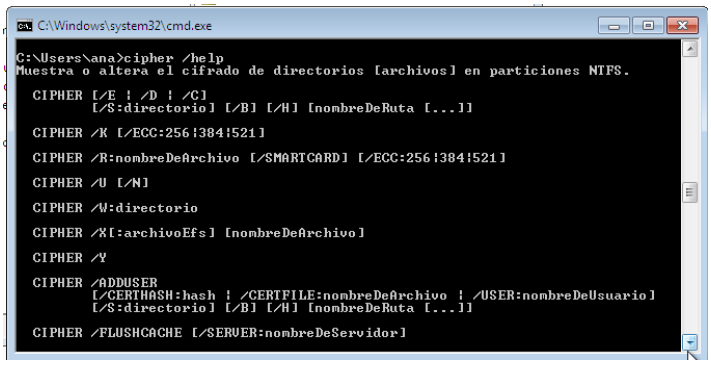
   Consejo: **Hacer una copia de seguridad de todos los certificados EFS** que haya.
5. Haz clic en el menú Acción, apunta a Todas las tareas y, a continuación, haz clic en Exportar.
6. En el Asistente para exportación de certificados, haz clic en Siguiente, después en Exportar la clave privada y, a continuación, en Siguiente.
7. Haz clic en Personal Information Exchange y, a continuación, en Siguiente.
8. Escribe la clave o contraseña que deseas usar, confírmala y, a continuación, haz clic en Siguiente. En el proceso de exportación, se creará un archivo para almacenar el certificado.
9. Escribe el nombre y la ubicación del archivo (incluye la ruta de acceso completa), o bien haz clic en Examinar, desplázate hasta la ubicación, escribe el nombre del archivo y, a continuación, haz clic en Guardar.
10. Haz clic en Siguiente y, después, en Finalizar.

Recuperación de certificados EFS:

Si por cualquier motivo tuvieras que **recuperar la clave privada** realizarías el proceso contrario, **importarías el certificado** al equipo en cuestión.

Importante, en la importación activar las siguientes opciones:

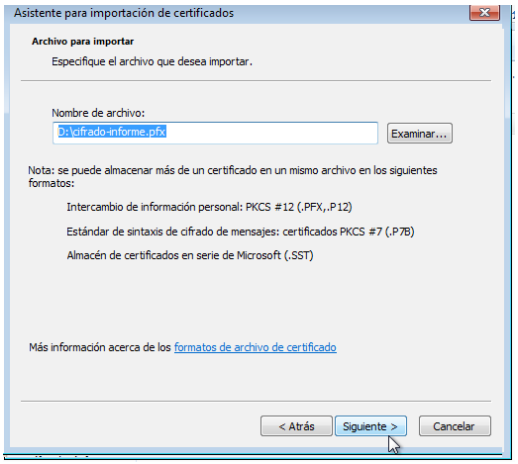




También se puede usar la **herramienta de la línea de comandos `cipher`** para mostrar o cambiar el cifrado de carpetas y archivos en las particiones NTFS.

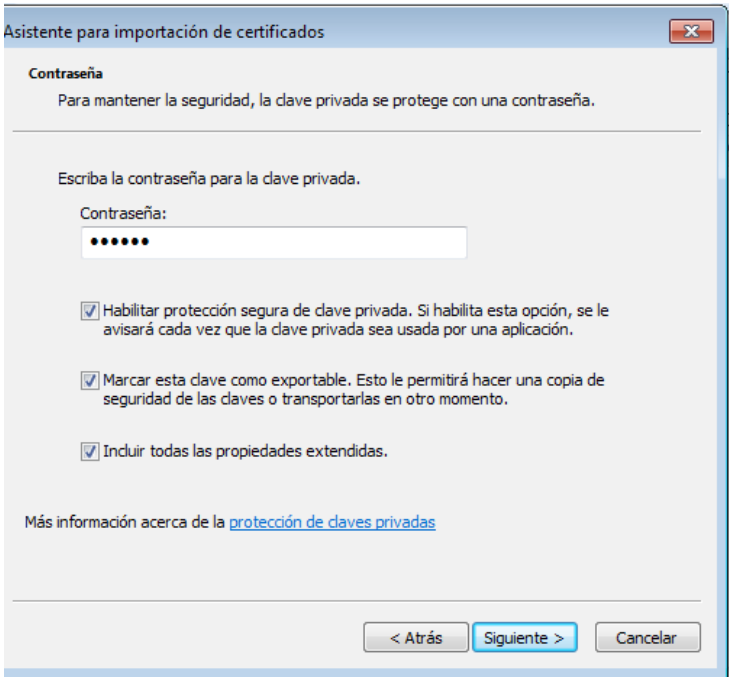
Importación de certificados EFS (restaurar la copia de seguridad)

Podemos restaurar la copia de un certificado directamente haciendo doble clic sobre el fichero del certificado. En ese momento se iniciará un asistente que te guiará durante el proceso.



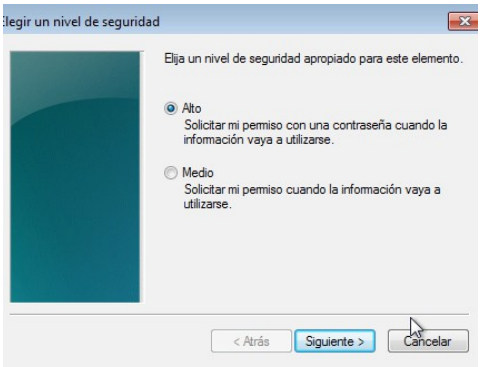
Indicamos donde está el archivo del certificado:

Importante: En la siguiente pantalla debemos introducir la clave privada y marcar las dos opciones que aparecen deseleccionadas:



La primera opción, "Habilitar protección segura de clave privada" va a conseguir que cada vez que un programa haga uso del certificado por seguridad pida que introduzcamos la clave privada. La segunda opción, "Marcar esta clave como exportable", consigue que en el futuro cuando se haga una nueva copia de seguridad (exportación del certificado), éste se exporte completo, incluyendo sus claves.

Ahora llega el momento de establecer el nivel de seguridad con el que se va a utilizar el certificado. Es fundamental establecer un **nivel Alto**, en el cual nos va a pedir la clave cada vez que hagamos uso del certificado.



Tras este paso, continuaremos con el asistente hasta la finalización del proceso.

Debes conocer

¿Sabes para qué se sirve la función de Bitlocker en Windows? Echa un vistazo al segundo documento para ponerte al día.

Anexo III.- Bitlocker.

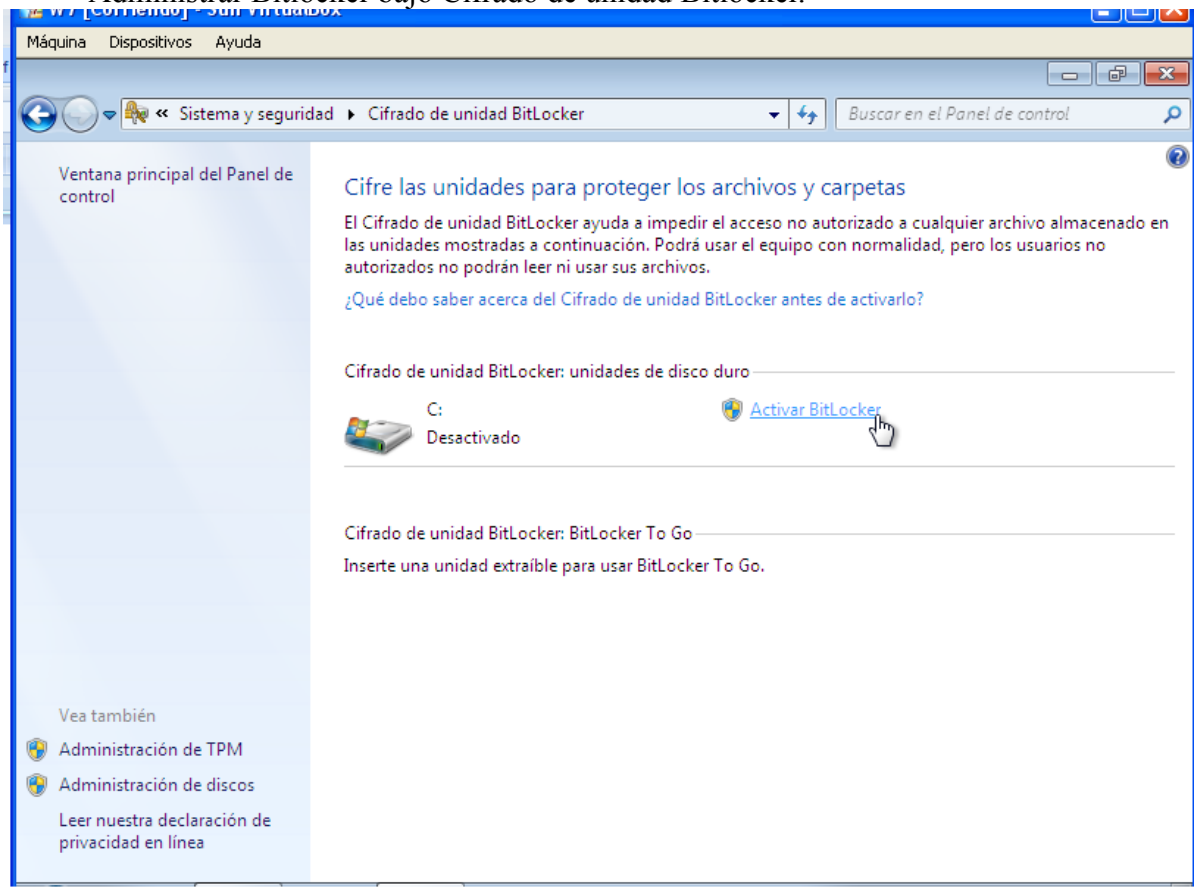
Cifrado de unidad Bitlocker

Disponible en las ediciones Ultimate y Enterprise, **Bitlocker permite mantener a salvo todo**, desde documentos hasta contraseñas, ya que **cifra toda la unidad en la que Windows y sus datos residen.** Una vez que **se activa Bitlocker, se cifran automáticamente todos los archivos almacenados en la unidad.**

Bitlocker To Go, una característica de Windows, **permite bloquear dispositivos de almacenamiento portátiles** que se extravían fácilmente, como unidades flash USB y unidades de disco duro externas.

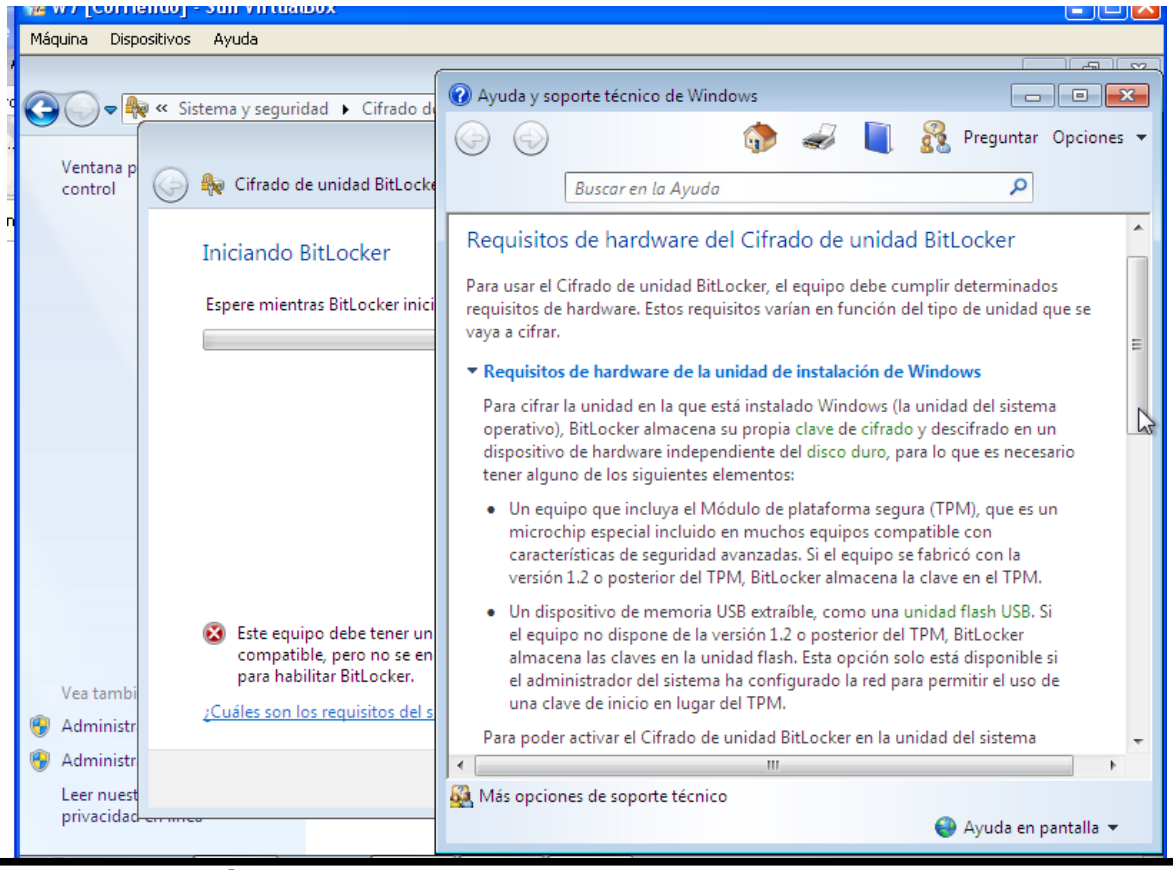
El **cifrado con Bitlocker se activa y desactiva** en Windows 7 y 8. Para Windows 10 hay un video en el apartado 5.4.1. Para saber más.

- **Inicio > Panel de control > Sistema y seguridad > Cifrado de unidad Bitlocker.**
- Clic en **activar Bitlocker.**
- También se puede pulsar en Proteger el equipo cifrando los datos en el disco o en Administrar Bitlocker bajo Cifrado de unidad Bitlocker.



Configurar el disco duro para el Cifrado de unidad Bitlocker donde está Windows instalado:

Para cifrar la unidad en la que está instalado Windows, el equipo debe tener dos particiones: una partición del sistema (que contiene los archivos necesarios para iniciar el equipo) y una partición del sistema operativo (que contiene Windows). La partición del sistema operativo se cifra y la partición del sistema permanece sin cifrar para poder iniciar el equipo. En las versiones anteriores de Windows, es posible que hayas tenido que crear manualmente estas particiones. En esta versión de Windows, estas particiones se crean automáticamente. Si el equipo no incluye ninguna partición del sistema, el Asistente de Bitlocker creará una automáticamente, que ocupará 200 MB de espacio disponible en disco. No se asignará una letra de unidad a la partición del sistema y no se mostrará en la carpeta Equipo. La activación de Bitlocker requiere un TPM o Módulo de plataforma seguro, o un dispositivo extraíble donde se almacene la clave de inicio de Bitlocker que se utiliza cada vez que se inicia el equipo.



Autoevaluación

¿Para qué sirve EFS?

○ Para el cifrado de unidades completas de disco.

◉ Para el cifrado de archivos y carpetas.

○ Para la compresión de archivos y carpetas.

○ Para el cifrado de archivos, carpetas y unidades de disco.