GENERALITAT VALENCIANA
Conselleria d'Educació, Investigació, Cultura i Esport

Unió Europea
Fons social europeu
L'FSE inverteix en el teu futur

IES MARÍA ENRÍQUEZ

C/ Literat Azorín, 1 46702 – GANDIA
Tfno. 962829430 – Fax. 962829431
Codi: 46004221 – CIF: Q-9655627-I
46004221@edu.gva.es
http://iesmariaenriquez.com

COMPUTER SYSTEMS
UD5: O.S. ADMINISTRATION
WINDOWS ADMINISTRATION

CFGS DAW
DPT INF

1.- Herramientas administrativas

Las **herramientas administrativas** Windows 10 son un conjunto de herramientas cuya función es la de proporcionar una serie de *utilidades para el diagnóstico del sistema*, así como la **monitorización de los recursos** de hardware y software en tiempo real. Gracias a ellas también podremos acceder a otras utilidades para **modificar parámetros de configuración del sistema**.

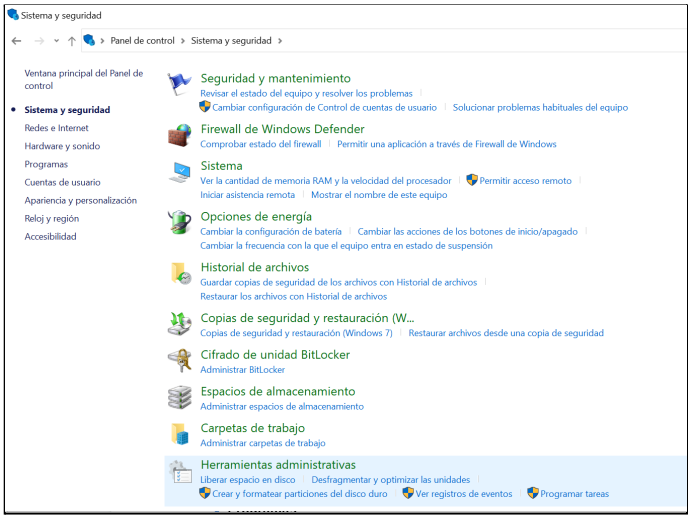
Las Herramientas administrativas se encuentran dentro del **Panel de control**. Éste es el centro neurálgico desde donde podemos acceder a cualquier configuración de Windows.

Para acceder a él abriendo el menú inicio y en la zona de navegación buscar la carpeta **Herramientas administrativas**. También podremos acceder directamente a esta lista de herramientas desde el panel de control clásico de Windows. Para ello abrimos el menú inicio y escribimos **Panel de control** y pulsamos Enter.

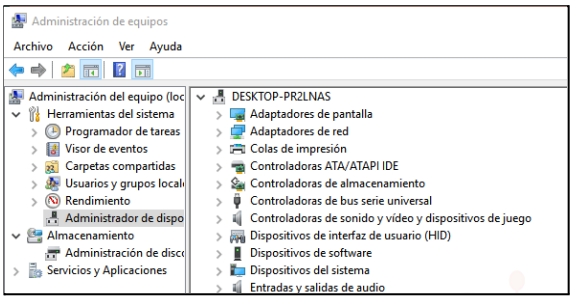
En el **Panel de Control** nos encontramos los siguientes **grupos de primer nivel**:

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

Dentro del grupo de primer nivel **Sistema y seguridad** se hallan las **Herramientas administrativas**.



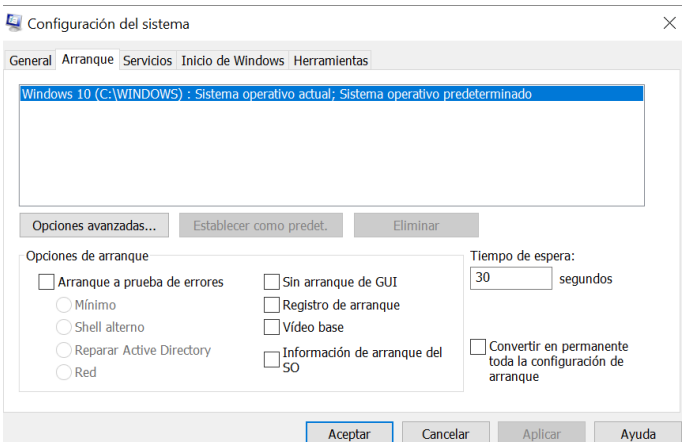
Herramientas administrativas más utilizadas



Administrador de equipos

Esta completa herramienta nos ayudará a gestionar, instalar y desinstalar todos los componentes hardware de nuestro equipo. cuando algún dispositivo de entrada o salida va mal seguramente vendremos aquí para intentar solucionar el problema.

También desde aquí podremos acceder a la herramienta de administración de discos duros, para poder crear o eliminar particiones de nuestro disco duro.



Configuración del sistema

Esta es una de las herramientas más utilizadas cuando tenemos algún error en Windows que no nos deja trabajar. Gracias a esta herramienta podremos configurar la forma en la que arranca nuestro equipo y también podremos visualizar los servicios activos en el sistema y acceder a los programas de inicio de Windows (Desde Windows 8, redirige en su lugar al Administrador de tareas).

https://www.xataka.com/basics/que-es-y-como-se-usa-el-msconfig-de-windows

Desfragmentar y optimizar unidades

El nombre ya lo dice todo, si tenemos discos duros mecánicos será recomendable pasarnos alguna vez por esta herramienta para desfragmentar nuestro disco duro.

Adaptándose a los nuevos tiempos, también se ha añadido una opción para optimizar discos duros SSD, ya que desfragmentarlos no tienen sentido alguno.

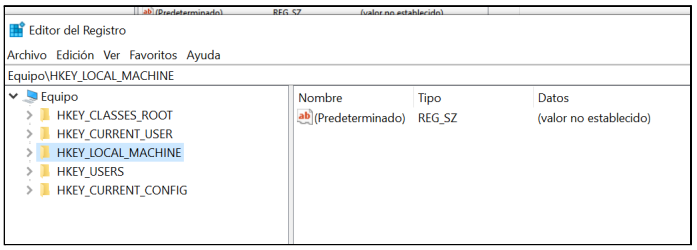
Diagnóstico de memoria de Windows

Con esta herramienta podremos verificar que la memoria RAM que tenemos funciona de forma correcta. Se ejecutará en el próximo arranque del equipo.

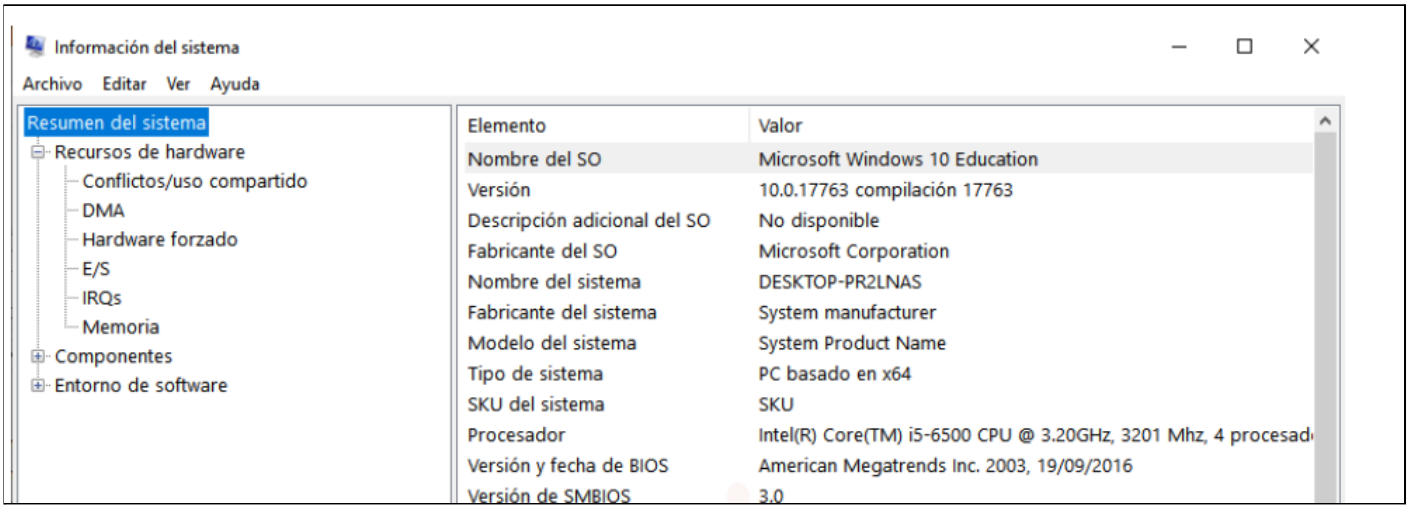
Editor de registro

Otra de las herramientas estrella es el editor de registro. El 80% de los errores de Windows y sus correspondientes tutoriales, nos enviarán directamente aquí para solucionar o si cabe, empeorar los

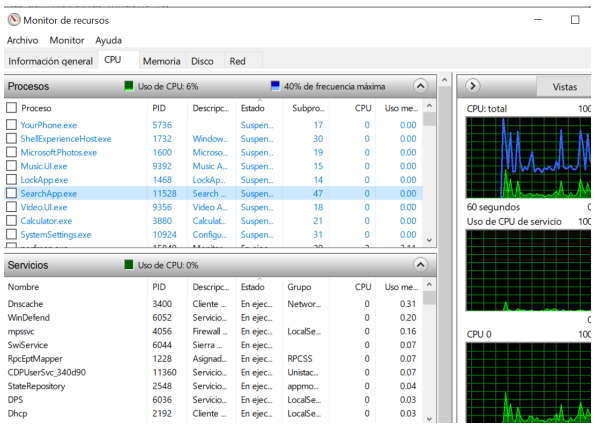
errores de Windows.



Información del sistema



Este panel es menos conocido por los usuarios normales, pero gracias a él podremos obtener información muy detallada acerca de nuestro sistema y hardware



Liberador de espacio en disco

También tendremos el acceso directo a la herramienta de liberación de espacio en disco. No hace falta explicar qué función realiza.

Monitor de recursos

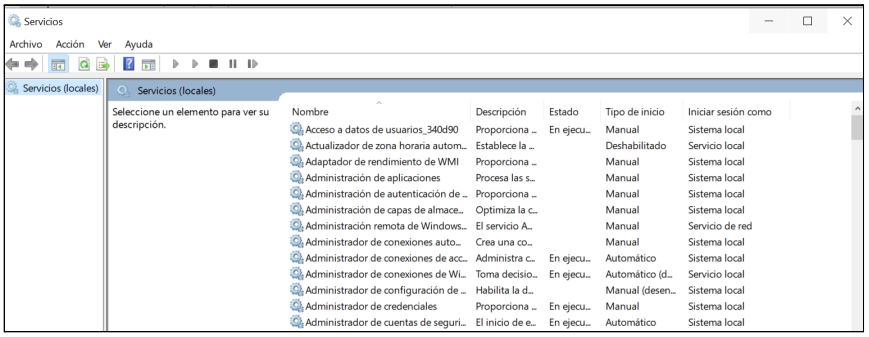
El monitor de recursos será también accesible desde el administrador de tareas de Windows. Pero si queremos tenerlo solamente a este accederemos desde su correspondiente herramienta.

Monitor de rendimiento

Este monitor es similar al anterior, pero nos muestra en tiempo real una gráfica de rendimiento del equipo además de una serie de herramientas para el diagnóstico del sistema.

Servicios

Otra de las herramientas estrella. Cuando queremos iniciar determinados programas o eliminar parte de la carga del sistema para mejorar el rendimiento, seguramente nos pasemos por aquí para activar o desactivar los servicios que corren en nuestro sistema.



Unidad de recuperación

Para crear un USB de recuperación de Windows 10 y utilizarlo cuando el sistema nos falla, tendremos que ejecutar esta herramienta.

Firewall de Windows

El cortafuegos o firewall en inglés, en el mundo de la informática es un sistema de seguridad para **bloquear accesos no autorizados** a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. Se trata de establecer unos **criterios de seguridad**, y filtrar todas las comunicaciones que entran o salen del ordenador para interceptar las que no cumplan con ellos y dejar pasar al resto.

Cuando utilizamos un firewall en la red local, lo más normal es permitir todo el tráfico desde y hacia los equipos de la red local, porque es una red privada y confiable. Por defecto, todos los perfiles están configurados con una política restrictiva en las reglas de entrada. Esto significa que todas las conexiones entrantes que no coincidan con una regla que haya predefinida, o que hayamos definido nosotros, serán bloqueadas. Respecto a las reglas de salida, utiliza una política permisiva, esto significa que todas las conexiones salientes que no coincidan con una regla serán permitidas, y solo las que hayamos definido específicamente para bloquearlas, se bloquearán.
https://www.redeszone.net/tutoriales/seguridad/configuracion-firewall-windows-10/

https://www.profesionalreview.com/2018/12/01/herramientas-administrativas-windows-10/

2.- Administración de grupos y cuentas de usuario locales

Autenticación: Para usar el sistema es necesario abrir una sesión de trabajo (login) para lo cual tendremos que autenticarnos, 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 (ACL).

En este apartado vamos a aprender a configurar la seguridad y el acceso de usuarios al propio equipo (autenticación). Para ello, explicaremos cómo administrar los usuarios locales y, por tanto, el acceso al sistema local.

2.1.- Tipos de cuentas de usuario

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 10 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.

¿Cuáles son los permisos de los usuarios?

Invitado: Un usuario invitado es alguien que solo requiere acceso temporal al equipo, por esa razón sus permisos suelen ser tan limitados como cambiar su foto de perfil, su contraseña o nombre. En caso de que necesite trabajar en una hoja o programa específico, el usuario administrador puede configurar su usuario para que tenga acceso a hacer cambios en ese sector o programa y solo en ello.

Usuario estándar: Una cuenta con permisos estándar es una cuenta limitada que solo puede realizar determinados cambios en el sistema, como, por ejemplo, cambios que solo afecten al usuario (cambiar iconos, fondo, etc) pero que no cambios que afecten al sistema en general, como, por ejemplo, cambios en el registro o instalar programas.

Para usuarios con poca experiencia, se recomienda una cuenta estándar con el propósito de prevenir cambios en el sistema que puedan afectar la estabilidad del mismo.

Usuario administrador: Puede crear cuentas para otros usuarios, hacer cambios profundos, pudiendo incluso borrar o instalar programas en el disco duro del equipo. En comparación a los otros usuarios, el administrador tiene acceso al cerebro y corazón de la computadora.

La configuración de Windows desactiva la cuenta de Administrador integrada en Windows 10 y Windows Server 2016 y genera una nueva cuenta local que pertenece a la comunidad de Administradores.

Las cuentas de usuario se identifican con un **SID** (Security Identifier - Identificador de Seguridad) se trata de un número de identificación único para cada usuario. Es como el DNI de cada usuario,Windows identifica los usuarios a través de su SID y no por su nombre como hacemos nosotros. Un SID está formado de la siguiente manera:

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

2.1.1.- Grupos locales

Los grupos en Windows 10 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).

Algunos grupos locales predeterminados son:

- **Administradores:** los miembros de este grupo tienen control local sobre el equipo, y tienen todos los derechos y permisos.
- **Invitados:** permite a usuarios ocasionales iniciar sesión en el equipo, con menos permisos que el grupo usuarios.
- **Usuarios:** pueden ejecutar aplicaciones, utilizar impresoras, cerrar y bloquear estaciones de trabajo, pero en principio no pueden compartir carpetas.
- **Usuarios avanzados.:** pueden crear cuentas de usuarios y grupos locales, pero únicamente pueden modificar o eliminar las que ellos hayan creado. No pueden tomar posesión de archivos, realizar copias de seguridad, cargar o descargar drivers, ni administrar la seguridad y la auditoría.

Los usuarios miembros del **grupo de Usuarios** son los que realizan la mayor parte de su trabajo en un único equipo Windows 10. 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.

2.2.- Gestión de cuentas de usuario y grupos locales

Podemos crear, borrar y modificar cuentas de usuario en Windows 10 accediendo de una de las siguientes formas:

✔ Pulsar **WIN + R** y escribir **lusrmgr.msc** (abreviatura de "local user manager")

✔ **Gestión de cuentas de usuario** desde **Herramientas Administrativas - Administración de equipos - Usuarios y Grupos locales**

Nota: Windows Home no dispone de esta opción

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.

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.

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

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

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

General: Podemos indicar el nombre completo de la cuenta, una descripción, e indicar algunas opciones de la cuenta.

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

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

contraseña.

✔**La contraseña nunca caduca**. Ya veremos como en Windows 7 las contraseñas se consideran material fungible, es decir, que tras un cierto tiempo de uso el sistema obligará a cambiar dichas contraseñas. Mediante esta opción indicamos que la contraseña podrá usarse sin que caduque nunca.

✔ **Cuenta deshabilitada**: No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.

✔ **La cuenta está bloqueada**: Por determinados mecanismos de seguridad se puede llegar a bloquear una cuenta, que implicará que dicha cuenta estará deshabilitada. Desde esta opción podemos volver a desbloquearla, simplemente desmarcando la casilla.

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

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

La última pestaña es de **Perfil**. Ésta nos permite indicar **la ruta del perfil**, los **archivos de inicio de sesión** y las **carpetas personales del usuario**.

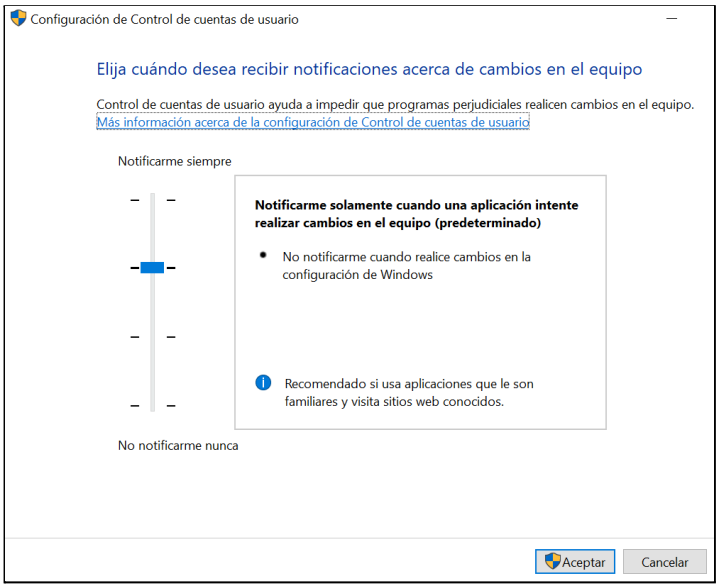
2.3. UAC (User Account Control, Control de Cuentas de Usuario)

Relacionado con la seguridad de cuentas de usuario nos encontramos el UAC

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 del 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.

Hay muchos usuarios que suelen tener el control de cuentas de usuario desactivado por comodidad,

para que no les molesten los avisos. Sin embargo, esto es una de las peores decisiones que podemos tomar. El **UAC** nos ayuda a evitar ejecutar programas que, dada su actividad, hacen cambios peligrosos en el PC. Y, por lo tanto, deberíamos intentar que siempre esté activado.



Para **acceder al UAC** nos dirigimos al **Panel de Control – Sistema y seguridad - Seguridad y mantenimiento –Cambiar configuración de Control de cuentas de usuario**

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

1. Notificarme siempre **cuando**:
   - ✔ Las aplicaciones intentan instalar software o hacer 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:
   - ✔ Las aplicaciones intentan instalar software o hacer cambios en el equipo
   - ✔ Realice cambios en la configuración de Windows.

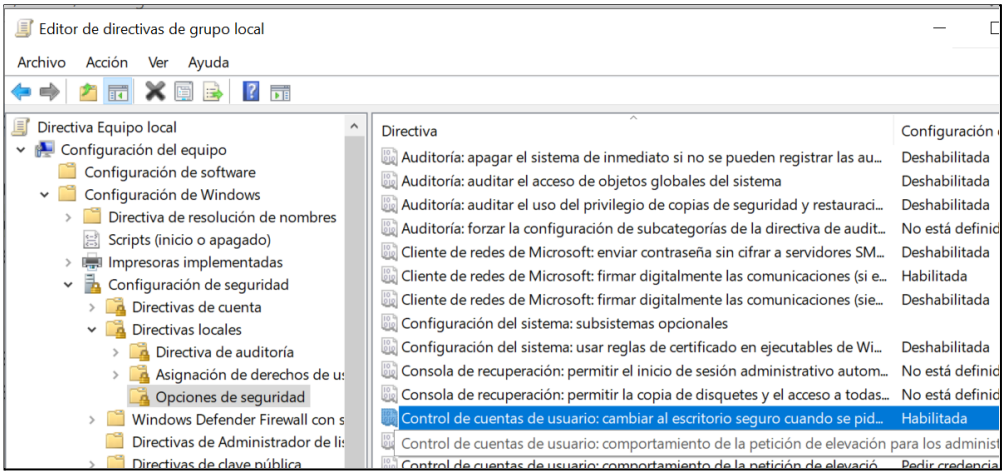
En función de nuestras necesidades escogeremos una u otra opción.

Editor de directivas de grupo local y el UAC (No disponible en Windows 10 Home)

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 este 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.

https://www.softzone.es/windows-10/como-se-hace/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.

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

3.1.- Permisos de archivos y carpetas

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

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

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

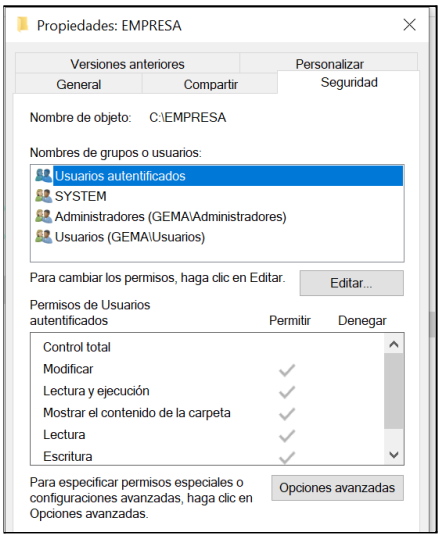
Puede ocurrir que un usuario tenga permisos contradictorios. Imagínate que en el ACL de una carpeta llamada EMPRESA aparece que el SID del usuario LUIS puede escribir en la carpeta, pero LUIS pertenece al grupo CONTABILIDAD que aparece en el ACL de empresa como que no tiene derecho a escribir. Bien,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

1. Lo que más pesa en cualquier ACL es la **denegación** implícita de permisos. Si un permiso está denegado, no se sigue mirando, se deniega inmediatamente.
2. Es suficiente con que un permiso esté concedido en cualquier SID para que se considere

concedido. (A excepción de la regla 1, es decir, que no esté denegado implícitamente en ningún sitio).

Esto se entiende mejor gestionando el ACL de algún recurso.

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



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

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

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

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

Pues precisamente eso es lo que hace Windows 10, 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.

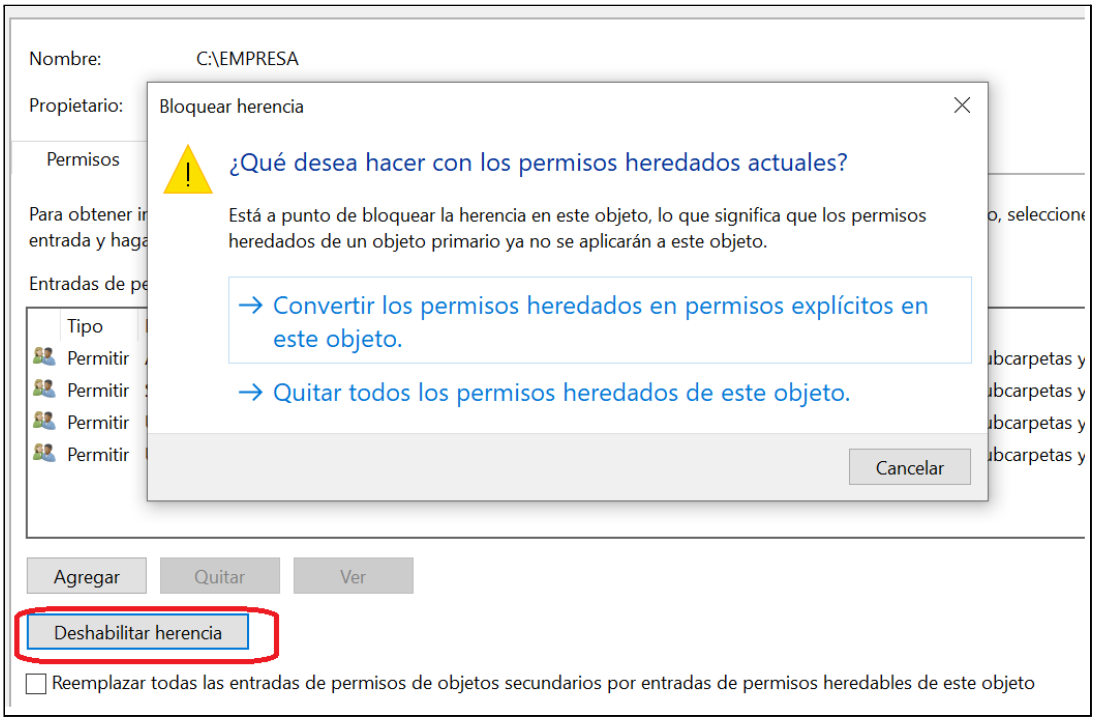
Para ello, accedemos al botón de **Opciones Avanzadas** que está en la pestaña **Seguridad**.

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 está marcada la opción de: "**Incluir todos los permisos heredables del objeto primario de este objeto**".

Esto implica: "Heredar del objeto principal las entradas de permiso relativas a los objetos secundarios e incluirlas junto con las entradas

indicadas aquí de forma explícita". Si desmarcamos dicha opción mataremos la relación de herencia de nuestro recurso, y podremos gestionar su ACL "directamente". Vamos a ello.



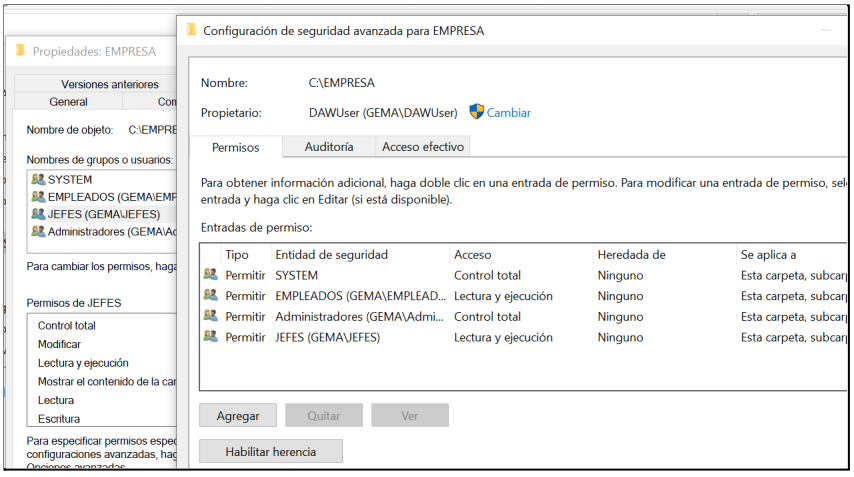
Hay que tener cuidado, una vez quitada la herencia, el sistema nos da a elegir entre dos opciones: Si escogemos la opción **Agregar**, la herencia se interrumpirá, y podremos retocar la ACL como nos plazca, pero dicha ACL será la que ahora mismo tiene el recurso, heredada de su objeto principal.

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

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

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

Agregaremos en este momento a los grupos EMPLEADOS y JEFES y les asignaremos los permisos antes citados. Una vez eliminada la 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 clic en el botón y después en el botón. 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

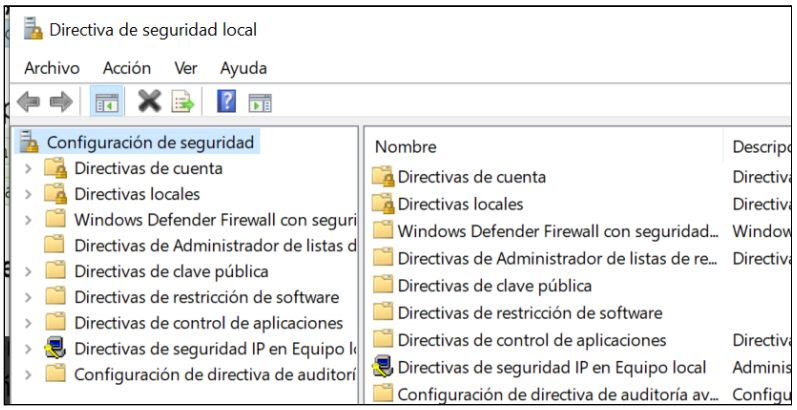
Siempre desde una cuenta con privilegios de administrador Windows 10 nos proporciona la posibilidad de gestionar de forma centralizada la configuración de la seguridad de nuestro sistema, a través de las **Directivas de seguridad local** y las **Directivas de grupo local**. Ambas opciones cuentan con 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 10 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:

✔ **Exigir historial de contraseñas**. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuántas contraseñas recordará Windows 10.

✔ **Las contraseñas deben cumplir los requerimientos de complejidad.** Obliga a que las contraseñas cumplan ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.

✔ **Longitud mínima de la contraseña.** Indica cuántos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.

✔ **Vigencia máxima de la contraseña.** Las contraseñas de los usuarios caducan y dejan de ser válidas después del número de días indicados en esta configuración, 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 mínima de la contraseña.** Indica cuánto 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 cuánto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee).

✔ **Restablecer la cuenta de bloqueos después de**. (Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero).

✔ **Umbral de bloqueo de la cuenta.** (Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta).

3.2.2. Directivas de grupo local

Las 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 máquina.

Usando las políticas de grupo en una máquina corriendo Windows 10, 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.

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 ejecutarán 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 máquina, y en algunos casos es imposible

sacarles el rendimiento esperado.

La consola desde donde podemos gestionar las directivas de grupo es el **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.

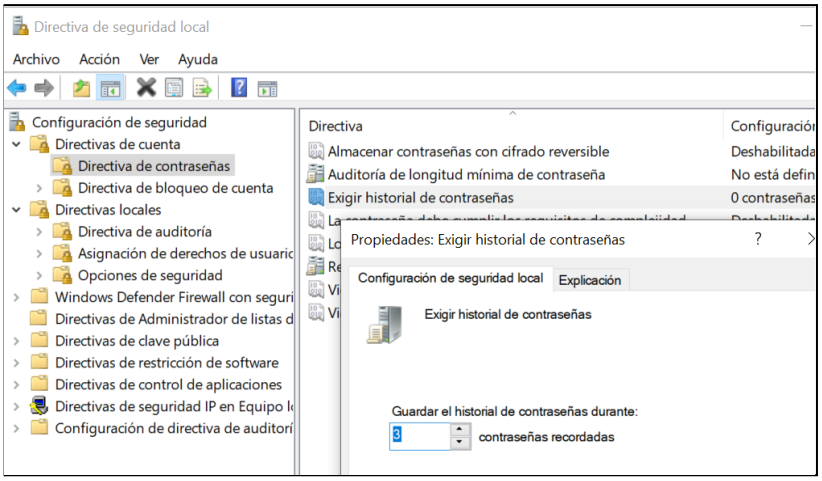
Si nuestro equipo está unido a un dominio, podemos configurar directivas del dominio completo, que afectarán a varias máquinas. Sin embargo, nos vamos a centrar aquí en las directivas locales.

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 clic sobre dicha directiva para que nos aparezca el cuadro de diálogo que nos permite modificar dicha directiva. En dicho cuadro de diálogo nos mostrará una explicación de la funcionalidad de dicha directiva.



Respecto a la configuración, veremos que podemos:

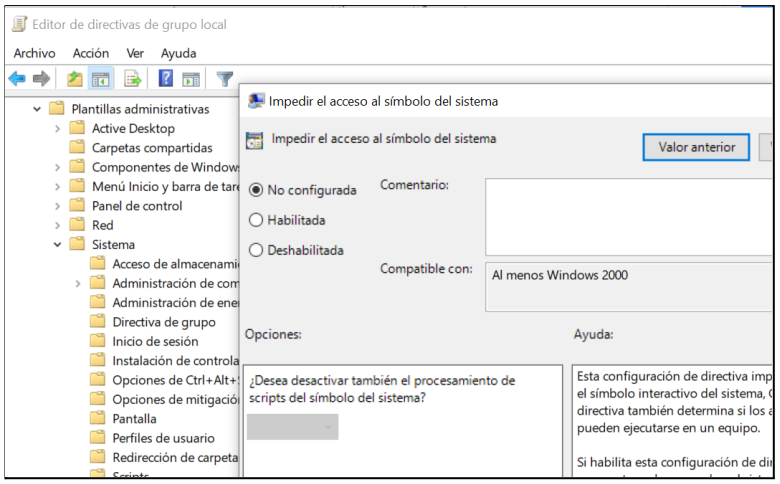
✔ **No configurar la directiva**, con lo que se comportará según el criterio por defecto para dicha directiva.

✔ **Habilitarla**, con lo que la pondremos en marcha en el sistema.

✔ **Deshabilitarla**, con lo que impediremos que se ponga en marcha dicha directiva. Algunas directivas especiales permiten especificar otras informaciones.

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

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



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

3.3.- Cuotas de disco

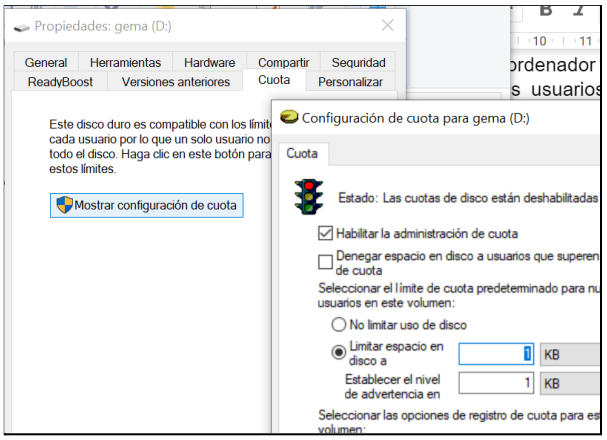
Uno de los recursos más importantes del ordenador es su capacidad de almacenamiento. Cuando un equipo es utilizado por varios usuarios, es preciso hacer una gestión del espacio de almacenamiento para que todos tengan el necesario.

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

A través del Explorador de Windows:

1. Haz clic con el botón secundario en el volumen de disco para el que se desea habilitar cuotas de disco y, a continuación, haz clic en **Propiedades** .

2. En la ficha **cuota**, haz clic para seleccionar la casilla de verificación **Mostrar configuración de cuota**.



A través de directivas de grupo:

Accedemos a la configuración de la cuota ejecutando **gpedit.msc**: **Configuración del equipo** -> **Plantillas administrativas** -> **Sistema** -> **Cuotas de disco.** Para habilitar cuotas de disco, establecemos las siguientes configuraciones:

- **Habilitar cuotas de disco**: Enable
- **Aplicar límite de cuota de disco**: Enable
- **Límite de cuota predeterminado y nivel de advertencia**: Enable (Límite de cuota predeterminado / nivel de advertencia: 1 Gb)
- **Registrar evento cuando se excedió el límite de cuota**: Enable
- **Aplicar la política a los medios extraíbles**: Enable (si necesita aplicar cuotas para medios extraíbles, incluidas unidades flash USB)

4.- Mantenimiento del sistema

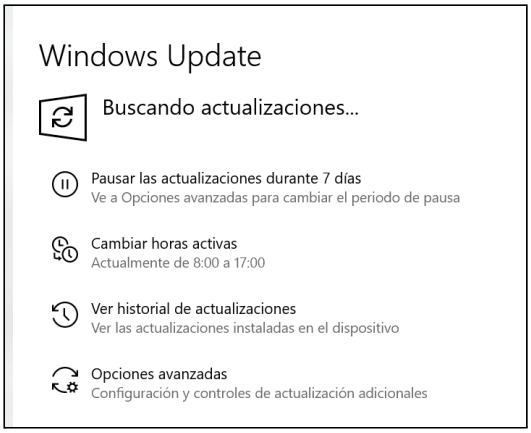
4.1.- Configuración de las actualizaciones automáticas

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 **Configuración pulsar Windows Update.**



Debajo de la opción de buscar actualizaciones, y en la misma sección Windows Update dentro de Actualización y seguridad, vemos tres enlaces para configurar las actualizaciones. Sus nombres definen bastante lo que hacen, y se llaman Cambiar horas activas, Opciones de reinicio y Opciones avanzadas.

Desde la opción de Ver historial de actualizaciones si seleccionamos una de ellas podremos pulsar el botón Desinstalar. En ocasiones también dispondremos de un botón Cambiar.
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.

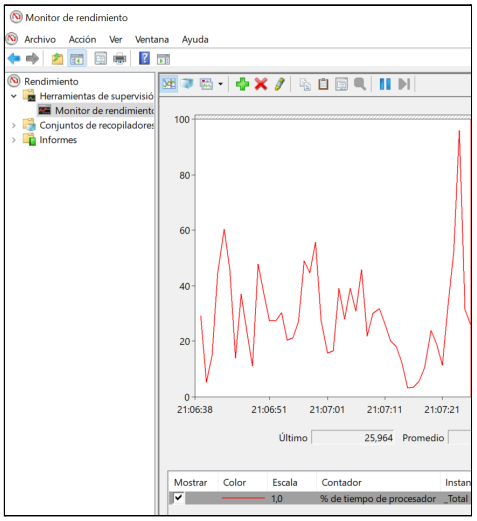
4.2.- Monitorización del sistema y gestión de servicios:

4.2.1 - Monitor de rendimiento

Windows 10 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. 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**. Hacer clic en **Inicio**, después clic en el cuadro Iniciar búsqueda, escribimos monitor y presionamos la tecla Enter.

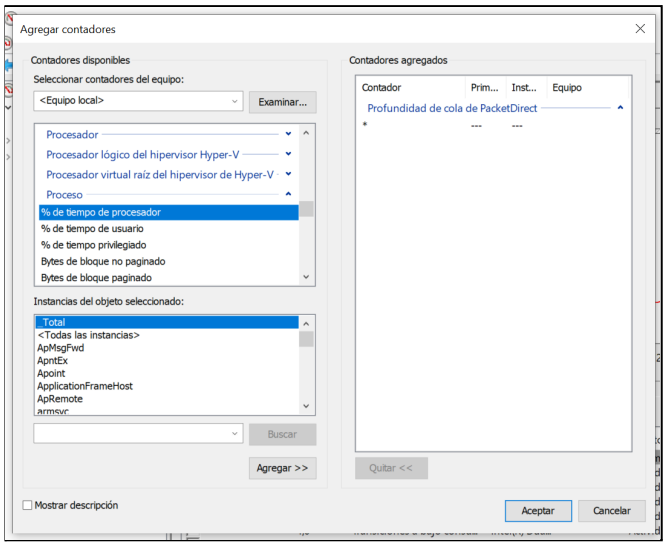
2. **Acceder al monitor**

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 clic 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.

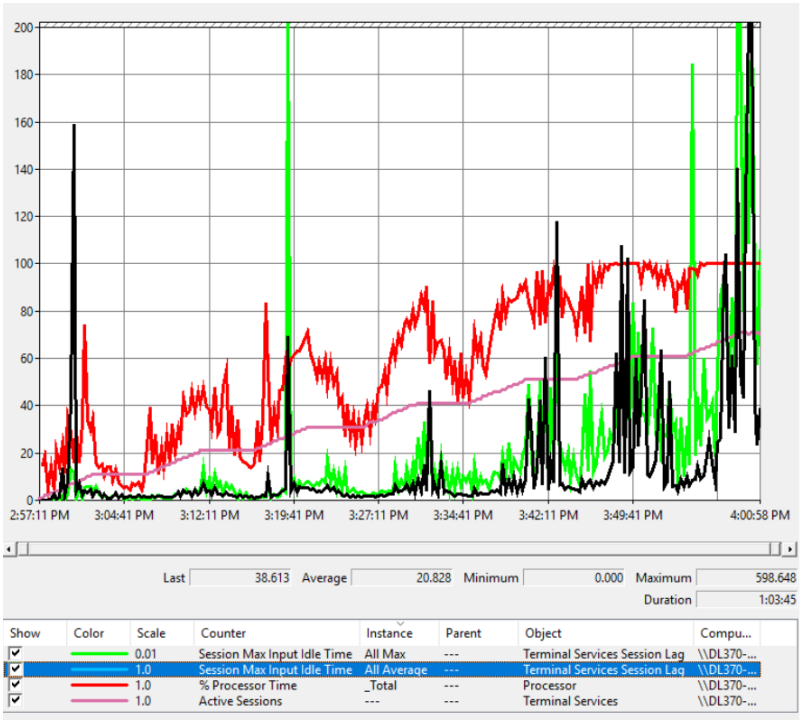
3. **Agregar componentes para monitorización**

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 clic 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 clic 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 clic 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 clic en Quitar. Al pulsar en **Aceptar** veremos en funcionamiento los contadores representados en la gráfica en tiempo real.



En el gráfico siguiente revisamos problemas de rendimiento de las aplicaciones en los hosts de sesión de escritorio remoto.

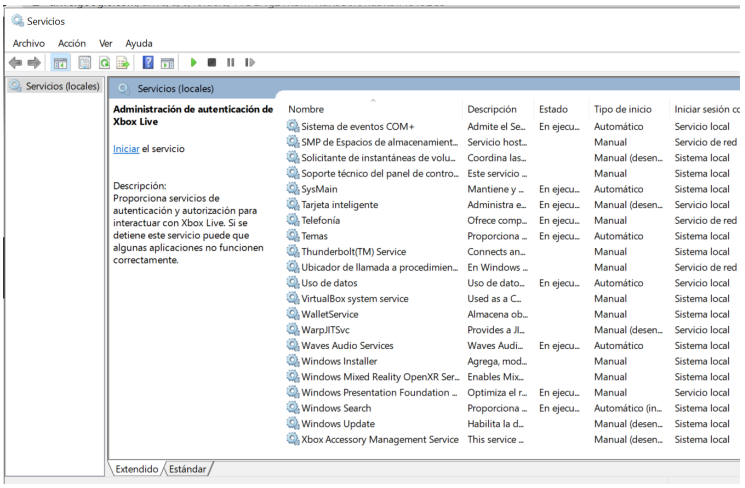
- La línea rosa muestra el número de sesiones que se han iniciado en el servidor.
- La línea roja es el uso de la CPU.
- La línea verde es el retraso máximo en la entrada del usuario en todas las sesiones.
- La línea azul (que se muestra como negra en este gráfico) representa el promedio de retraso de entrada de usuario en todas las sesiones.

4.2.1.- 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 10 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**.

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

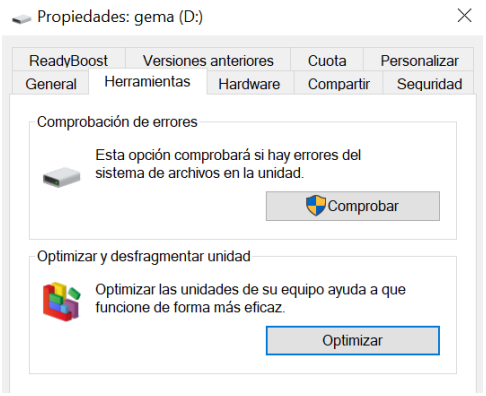
4.3.- Desfragmentación y chequeo de discos

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 proporciona una herramienta para ello, el **Desfragmentador de disco**, podemos acceder a ella desde el **Inicio,** escribiendo **defrag.** 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.



Por otra parte, podemos **comprobar o chequear los discos**, para comprobar si existen problemas en los mismos. Windows 10 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 clic en **Inicio** y, a continuación, en **Ejecutar**.
  2. En el cuadro Abrir, escriba **cmd** y presione ENTER.
  3. Siga uno de estos procedimientos:

✔ Para ejecutar **chkdsk**, en el símbolo del sistema, escribimos **chkdsk /f d:** y, a continuación, presiona la tecla ENTER. :d indica la partición que queremos comprobar, con la instrucción anterior se chequeará la unidad d:.

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 clic en Mi equipo y, a continuación, haz clic con el botón secundario del ratón en la unidad de disco duro que desea comprobar.
  2. Haz clic en **Propiedades** y, después, en la pestaña **Herramientas**.
  3. En **Comprobación de errores**, haz clic en **Examinar unidad**.

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, 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 no 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 clic en el botón **Inicio**, en **Panel de control**, en **Sistema y Seguridad**, en **Herramientas administrativas** y, a continuación, haz doble clic en **Programador de tareas.**
2. Haz clic 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 clic en Siguiente.
4. Realiza una de estas acciones:
   - ✔ Para seleccionar una programación basándose en el calendario, haz clic en Diariamente, Semanalmente, Mensualmente o Una vez, haz clic en Siguiente, especifica la programación que desee usar y haz clic en Siguiente.
   - ✔ Para seleccionar una programación basándose en eventos repetitivos, haz clic en Cuando el equipo inicie o Cuando inicie sesión y, a continuación, haz clic en Siguiente.
   - ✔ Para seleccionar una programación basándose en eventos específicos, haz clic en Siguiente. Cuando se produzca un evento específico, haz clic en otros datos, especifique el registro de eventos y otros datos y continuación, haz clic en Siguiente
5. Para programar una aplicación para que se inicie automáticamente, haz clic en Iniciar un programa y a continuación, en Siguiente
6. Haz clic Examinar en para buscar el programa que desee iniciar y después haz clic en Siguiente
7. Haz clic en Finalizar.

Una automatización útil para ejecutar de vez en cuando es borrar nuestra conexión a Internet. Limpiar la caché de DNS y renovar la dirección IP puede solucionar varios problemas de conexión y lentitud de Internet. Repetir esto automáticamente todos los días evitará que ocurran problemas eventualmente, especialmente si mantenemos nuestro sistema en funcionamiento todo el tiempo.

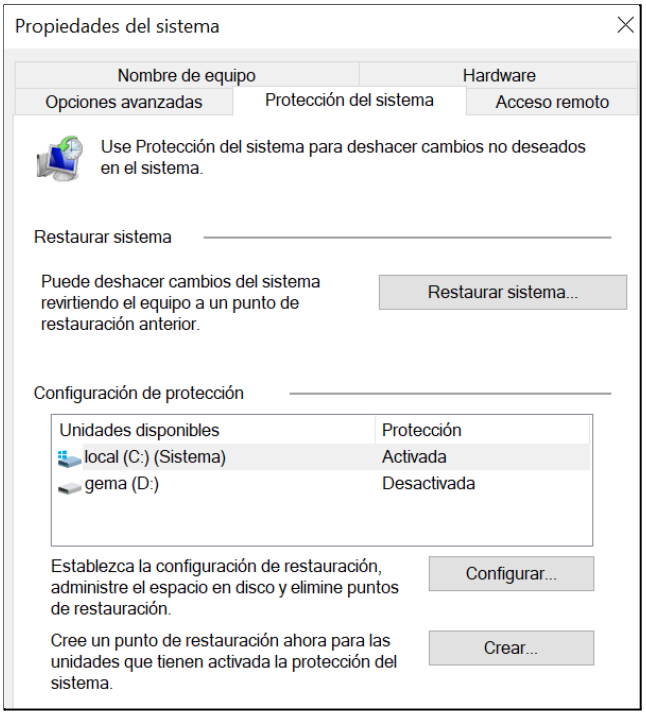
Para crear esta automatización con el Administrador de tareas, creamos un archivo BAT usando el Bloc de notas y agregamos las siguientes líneas.

ipconfig/release

TIMEOUT 20 /nobreak
ipconfig/renew
TIMEOUT 20 /nobreak
ipconfig/flushdns

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.



Este proceso es muy simple, solo tienes que presionar el botón de inicio y escribir **punto de restauración** y presionar Enter en el primer resultado. Si es la primera vez que lo haces y no se ha configurado, deberás elegir una unidad de almacenamiento y hacer clic en **Configurar**.

En la siguiente ventana debes marcar la casilla "**Activar protección del sistema**" y elegir el uso de espacio en disco que podrán ocupar los puntos de restauración. Luego presiona "Aceptar".

Este punto sirve para devolver Windows 10 al mismo estado en el que se encontraba cuando lo hiciste, es decir que todo lo que se instale o la configuración que se cambie que afecte el estado del sistema se deshará por completo.

Esto no afecta a tus documentos, archivos, fotos, ni datos personales.

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

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.

Una copia de seguridad -también conocida como copia de respaldo, copia de reserva o *backup*, en inglés- es el proceso de guardar los datos originales de un dispositivo para poder recuperarlos de nuevo en caso de pérdida.

Existen dos tipos principales de copias de seguridad:

- Copia de seguridad de los archivos
- Copia de seguridad del sistema

Copia de seguridad de los archivos

La copia de seguridad de archivos te permite crear una copia de los documentos que tienes guardados en tu PC, ya sea de manera individual o de varios ficheros a la vez, para tenerlos en otro dispositivo y recuperarlos cuando quieras.

La herramienta **Historial de archivos** pone a tu disposición la posibilidad de programar y hacer copias de los datos personales de tu ordenador o portátil de manera regular, para guardarlos en un dispositivo externo.

1. Dirígete al panel de **Configuración** y selecciona **Actualización y seguridad.**
2. Accede al apartado **Copia de seguridad** en el menú a mano izquierda, localiza la sección **Copia de seguridad con Historial de archivos** y haz clic en **Agregar una unidad**
3. Al hacer clic, te saldrá un menú con la lista de discos duros externos conectados a tu PC. Simplemente selecciona aquel que quieras usar para la copia de seguridad.

   De este modo, habrás activado la copia de seguridad automática de tus archivos. Podrás desactivarla cuando quieras, aunque por precaución recomendamos dejarla encendida para que se realicen copias de forma regular.
4. A continuación, haz clic en **Más opciones**, seguido de **Hacer ahora una copia de seguridad** si

quieres realizarla ya con los valores predeterminados.

También existe la posibilidad de hacer una copia de seguridad de archivos con plataformas de almacenamiento en la nube.

Copia de seguridad del sistema

La copia de seguridad del sistema te permite crear una copia de todo el sistema operativo Windows que en ese momento tienes en tu ordenador, es decir, de todos los programas, los archivos y los valores de configuración.

La herramienta **Protección del sistema** suele usarse para arreglar problemas con Windows u otros programas de manera rápida, pero es bueno saber que también te permite crear un punto de restauración para hacer una copia de seguridad del sistema.

Por otro lado, es bueno saber que Windows crea puntos de restauración de forma automática siempre que instalas un nuevo programa, un nuevo controlador o una nueva actualización del sistema en tu ordenador.

1. Abre la herramienta **Protección del sistema**. Para hacerlo, busca **Crear un punto de restauración** con la lupa que encontrarás al lado del menú de Inicio.
2. Para crear un punto de restauración, deberás primero habilitar la protección de tu disco local, que por defecto está deshabilitada. Así pues, selecciona el disco C:, haz clic en **Configurar**, seguido de **Activar protección del sistema** y **Aceptar**.
3. A continuación, clica en **Crear** para crear tu primer punto de restauración, es decir, una especie de captura del estado de tu Windows -sistema, configuración y aplicaciones, pero no archivos- en una fecha y hora concretas.

Deberás darle un nombre y volver a clicar en C**rear**.

De este modo, cuando veas que tu ordenador no funciona del todo bien -o incluso que uno de los programas que tienes instalados te da problemas- siempre podrás volver a un estado del sistema anterior.

Hacer una copia de seguridad del sistema creando una imagen de sistema

En el caso concreto de Windows 10, la opción principal para crear una copia de seguridad del sistema es una herramienta llamada **Imagen de sistema.** A continuación explicamos con detalle cómo utilizarla, un proceso que puede ser algo confuso para algunos.

1. Abre el **Panel de control** de tu PC y, en el apartado de **Sistema y seguridad**, selecciona '**Copias de seguridad y restauración (Windows 7)**'.
2. En el menú a mano izquierda, clica sobre la opción **Crear una imagen de sistema** para duplicar exactamente el estado actual del disco duro de tu ordenador, es decir, la configuración del Windows 10 y todos los programas y archivos guardados en tu PC.
3. A continuación podrás elegir dónde guardar la copia de seguridad, que por defecto será almacenada en tu disco duro externo. Así, si tienes cualquier problema con tu PC, podrás recuperar fácilmente esta copia del sistema.
4. Finalmente, clica en **Siguiente** y confirma la configuración de la copia de seguridad haciendo clic en **Iniciar la copia de seguridad**.

Si recuperas una copia creada hace tiempo, los cambios que hayas realizado en otros documentos se perderán. Eso se debe a que esta opción no te permite seleccionar archivos concretos, sino que copia todo el sistema.

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.

Se realizan numerosas comparativas de software antivirus teniendo en cuenta multitud de características tan variadas como: efectividad, frecuencia de actualización del archivo de firmas, tiempo medio de escaneo de un disco con un tamaño concreto, si poseen la certificación ICSA, calidad del soporte y ayuda técnica, ...

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**.

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 10. 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 o **cuadro de búsqueda del menú Inicio teclear "Windows Defender"**

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.

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 clic en **Inicio > Panel de control > Sistema y seguridad > Sistema**
2. Haz clic 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 clic en **Configuración**. Se obtiene la pantalla **Opciones de rendimiento**.
5. Haz clic en la ficha y, a continuación, pulse en **Prevención de ejecución de datos** 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, clic en Abrir.

Existen ciertas áreas de la memoria de un ordenador que en Windows no permiten la ejecución de código. Si hay algún código ejecutándose allí, por lo general suelen ser maliciosos. Si DEP descubre que algún programa está utilizando la memoria RAM de manera maliciosa, entonces lo apagará y mostrará una notificación.

5.4.- Sistema de cifrado de archivos

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.

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.

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.

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, 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 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.

Debes 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 en clave privada y, a continuación, en Siguiente.
7. Haz clic en Personal Information Exchange y, a continuación, en Siguiente
8. Escribe la 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.

Conoce con más detalle el proceso de cifrado de datos, la exportación e importación de certificados EFS:

Procesos de cifrado, 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 y **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 Aceptar, escribe en el cuadro de búsqueda certmgr.msc 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.

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

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 nueva característica de Windows10, **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:

✔ **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.