



Tema 6

ADMINISTRACIÓN BÁSICA DEL SISTEMA (WINDOWS II)

SI | 23-24

Indices

1.	Administración del sistema.....	3
1.1.	Panel de control	3
1.2.	CONFIGURACIÓN.	4
1.3.	HERRAMIENTAS ADMINISTRATIVAS.	5
2.	Administración de cuentas y grupos de usuarios locales.....	9
2.1.	Tipos de cuentas de usuario locales.....	9
2.2.	Tipos de grupos locales.....	12
2.3.	Gestión de cuentas de usuario y grupos locales.....	14
2.3.1.	Gestión de cuentas de usuario desde Configuración.....	14
2.3.2.	Gestión de cuentas de usuario desde Panel de control.	15
2.3.3.	Gestión de cuentas de usuario desde la consola Usuarios y grupos locales.	16
3.	Administración de seguridad de recursos a nivel local.	19
3.1.	Permisos de recursos locales. ACLs.	19
3.1.1.	Herencia de permisos.	20
3.1.2.	Asignación de permisos.	24
3.2.	Directivas de seguridad.	28
3.2.1.	Directivas de seguridad local.....	29
3.2.2.	Directivas de grupo local.	31
3.3.	Cuotas de disco.....	34
4.	Mantenimiento del sistema.....	34
4.1.	Windows Update.	34
4.2.	Monitor de rendimiento.	36



Sistemas informáticos

4.3. Servicios.....	39
5.1. Desfragmentación de discos.....	41
5.2. Chequeo de discos.....	43
5.3. Programador de tareas.....	45
5.4. Restaurar el sistema.....	47
5.5. Copias de seguridad.....	49
6. Uso de antivirus, antiespías y otros programas de protección.....	50
6.1. Antivirus.	50
6.2. Windows Defender.	52
6.3. Prevención de ejecución de datos (DEP).	54
6.4. Sistema de cifrado de archivos (EFS).....	56
6.4.1. Certificados EFS.	60
Anexo I.- UAC Control de Cuentas de Usuario.	61
Anexo II.- Procesos de cifrado, exportación e importación de certificados EFS.	64
Anexo III.- Bitlocker.....	Error! Bookmark not defined.

Administración básica del sistema

1. Administración del sistema.

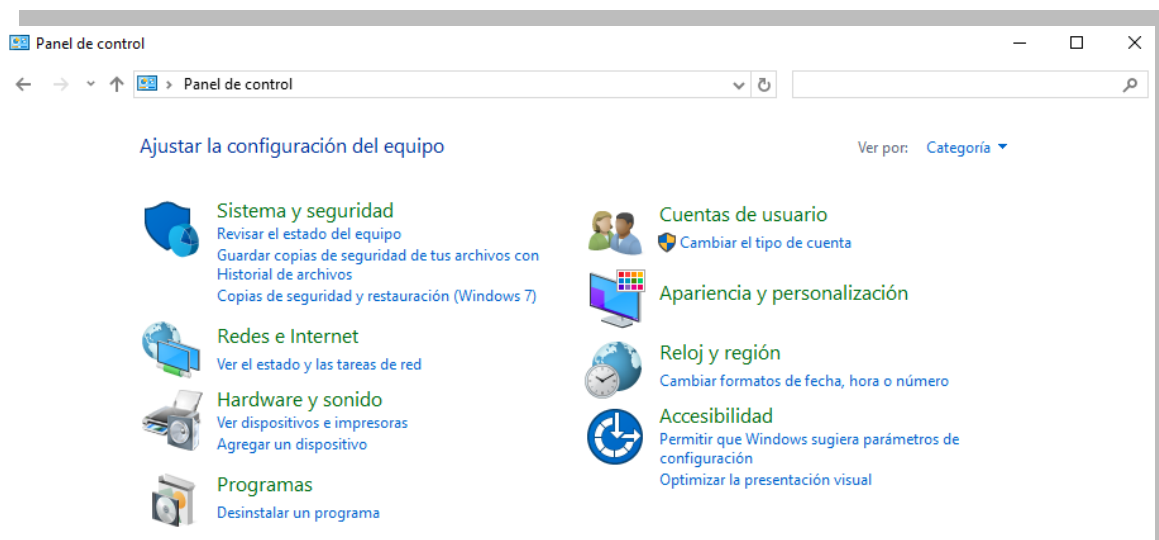
1.1. PANEL DE CONTROL

Las **Herramientas administrativas** son herramientas para los administradores del sistema y para usuarios avanzados. Pueden variar dependiendo de la versión de Windows que se use.

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 escribiremos en el cuadro de búsqueda "panel de control".

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 y región
- Accesibilidad



1.2. CONFIGURACIÓN.

Windows 10 incorpora la aplicación de **Configuración** que apareció en Windows 8 y es la que se prevé que termine reemplazando al conocido **Panel de control**. Accedemos a ella a través del botón de Inicio. Desde esta aplicación podemos examinar las categorías o usar la búsqueda para encontrar lo que estamos buscando, incluidas las opciones avanzadas del **Panel de control**.

Tener dos herramientas de configuración no es del todo grato, pues algunas opciones podrían encontrarse en una o en otra. Por ello, es muy probable que en un futuro no haya más remedio que usar la aplicación de **Configuración**, pues, de cualquier forma, es un paso más hacia la unificación del sistema operativo donde tendrá presencia, al disponer de una sola herramienta para todas las configuraciones.

Saca aún más provecho de Windows

Con algunas selecciones rápidas, estarás camino a disfrutar de toda la experiencia de Microsoft.

¡Vamos!

[Omitir por ahora](#)

Buscar una configuración



Sistema

Pantalla, sonido, notificaciones, energía



Dispositivos

Bluetooth, impresoras, mouse



Teléfono

Vincular Android o iPhone



Red e Internet

Wi-Fi, modo avión, VPN



Personalización

Fondo, pantalla de bloqueo, colores



Aplicaciones

Desinstalar, valores predeterminados



Cuentas

Cuentas, correo electrónico, sincronizar, trabajo, familia



Hora e idioma

Voz, región, fecha



Juegos

Game Bar, capturas, Modo Juego

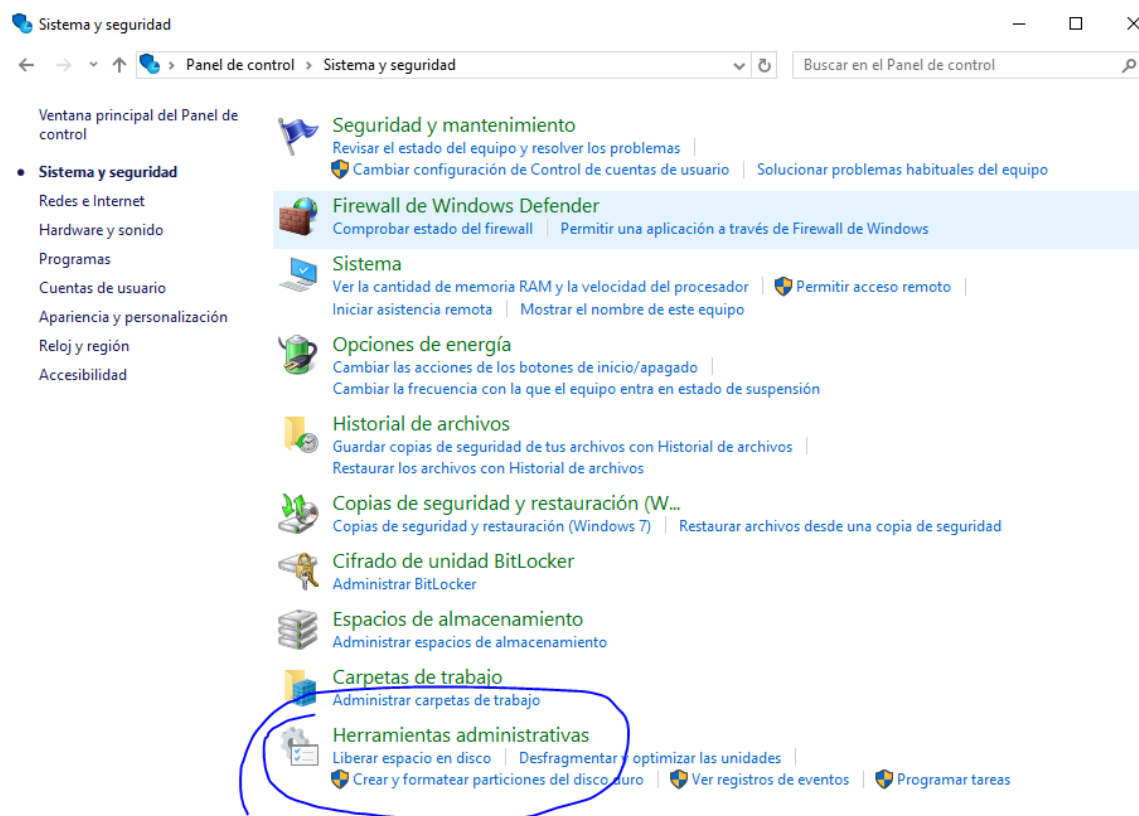


Accesibilidad

Narrador, lupa, contraste alto

1.3. HERRAMIENTAS ADMINISTRATIVAS.

En el **Panel de control**, 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 > Todas las aplicaciones > Herramientas administrativas de Windows**.



Las **herramientas administrativas** principales son:

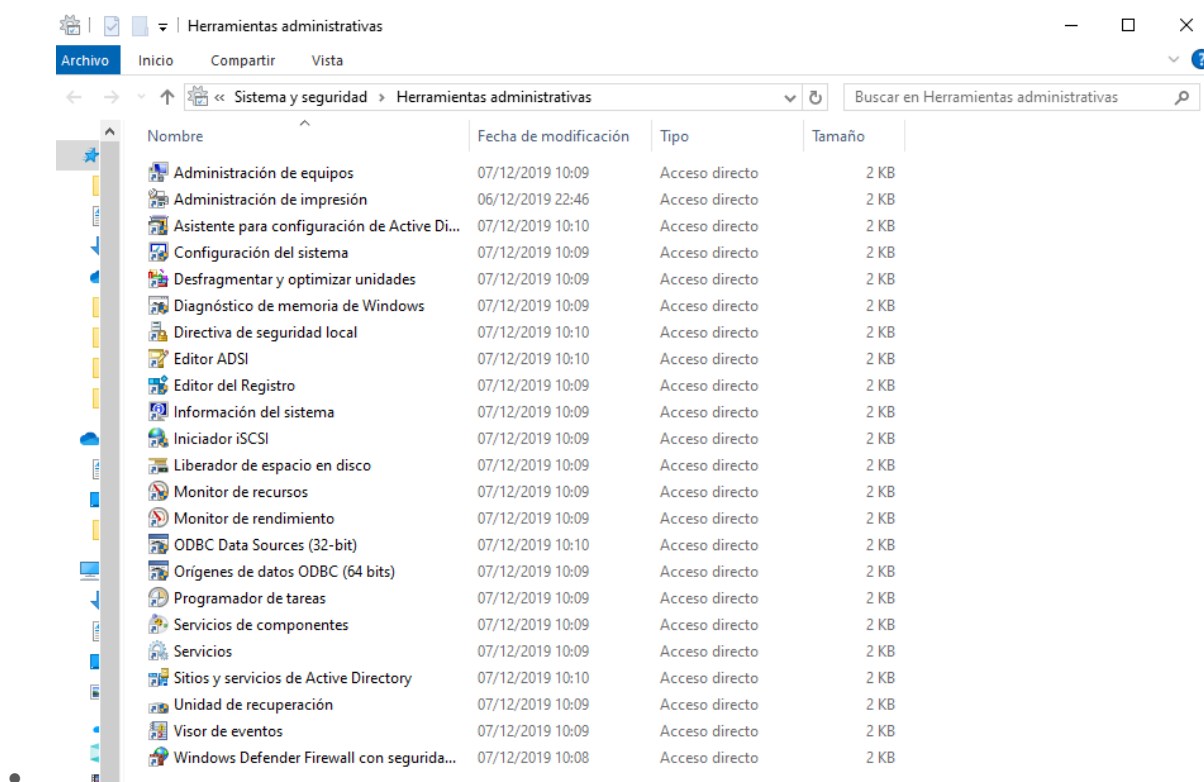
- **Administración de equipos:** Permite administrar equipos locales o remotos con una sola herramienta de escritorio consolidada. Mediante Administración de equipos se pueden realizar numerosas tareas, como supervisar eventos del sistema, configurar discos duros y administrar el rendimiento del sistema.
- **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.
- **Desfragmentar y optimizar unidades:** Permite desfragmentar y mejorar el rendimiento del equipo optimizando los diferentes tipos de unidades.
- **Diagnóstico de memoria de Windows:** Permite comprobar si la memoria funciona correctamente.



Sistemas informáticos

- **Directiva de seguridad local:** Permite consultar y editar la configuración de seguridad de directiva de grupo.
- **Editor del Registro:** Permite administrar el registro del sistema para realizar ajustes de configuración y opciones que necesita el sistema operativo y todas las aplicaciones instaladas para funcionar.
- **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.
- **Iniciador iSCSI:** Permite configurar conexiones avanzadas entre dispositivos de almacenamiento en una red.
- **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 quita archivos temporales, vacía la Papelera de reciclaje y elimina varios archivos del sistema y otros elementos que ya no se necesitan.
- **Monitor de recursos:** Nos ofrece una vista detallada del consumo de recursos del sistema (CPU, discos, redes y memoria RAM).
- **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.
- **ODBC Data Sources (32-bit):** Permite usar la conectividad abierta de bases de datos (ODBC) para mover datos de un tipo de base de datos (un origen de datos) a otro.
- **Orígenes de datos ODBC (64 bits):** Para administrar los DSN de usuario y los DSN del sistema que usan los procesos de 64 bits.
- **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.
- **Unidad de recuperación:** Permite crear una unidad de recuperación para en caso de error poder instalar el sistema.
- **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.
- **Windows Defender Firewall con seguridad avanzada:** Permite configurar opciones avanzadas del firewall en el equipo propio y en otros equipos remotos de la misma red.



En esta unidad estudiaremos con más detalles algunos de estas herramientas, como, por ejemplo, la Administración de equipos, la Directiva de seguridad local, el Monitor de rendimiento, el Programador de tareas, la herramienta Servicios, etc.

2. Administración de cuentas y grupos de usuarios locales.

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. 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 LOCALES.

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. 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.

Un dominio, en redes de computadoras, puede referirse a dos cosas:

- **En el contexto de una red informática**, un dominio se refiere a un conjunto de computadoras interconectadas en las que una o varias de ellas asumen la responsabilidad de administrar diversos aspectos de la red. Estos equipos, conocidos como controladores de dominio, gestionan la administración de usuarios, equipos, impresoras y los privilegios asignados a cada usuario en la red. Toda la información relacionada con la seguridad de la red, incluyendo usuarios y equipos, se registra en una base de datos ubicada en los controladores de dominio. Dependiendo del tamaño de la red, puede haber un solo controlador de dominio o un clúster de controladores distribuidos.
- **En el ámbito de la Web**, un dominio se refiere a la parte principal de una dirección web que indica la organización o compañía que administra el sitio web o página en cuestión. Por ejemplo, en la dirección "www.ejemplo.com", el dominio sería "ejemplo.com". Los dominios web

permiten identificar de manera única un sitio web en Internet y facilitan la navegación y acceso a la información.

En Windows 10 existen varios tipos de cuentas de usuario. Según el tipo se tiene un nivel diferente de control sobre el equipo:

- **Cuenta de usuario estándar:** Tiene privilegios limitados, puede usar la mayoría de los programas instalados en el equipo, pero no 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 con privilegios de administrador:** Windows habilita este tipo de usuario como medida de seguridad. Es un administrador del equipo pero que no tiene control total sobre todos los archivos del sistema. Así se evita que software malintencionado tome el control de nuestro equipo. Sólo se debe utilizar cuando se lleven a cabo tareas de administración que requieran los privilegios del administrador. 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 los archivos en un equipo.
- **Cuenta de administrador local:** Tiene el máximo control sobre el equipo. Por seguridad y por defecto Windows 10 deja desactivado el perfil de usuario Administrador.
- **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 10.

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 a 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

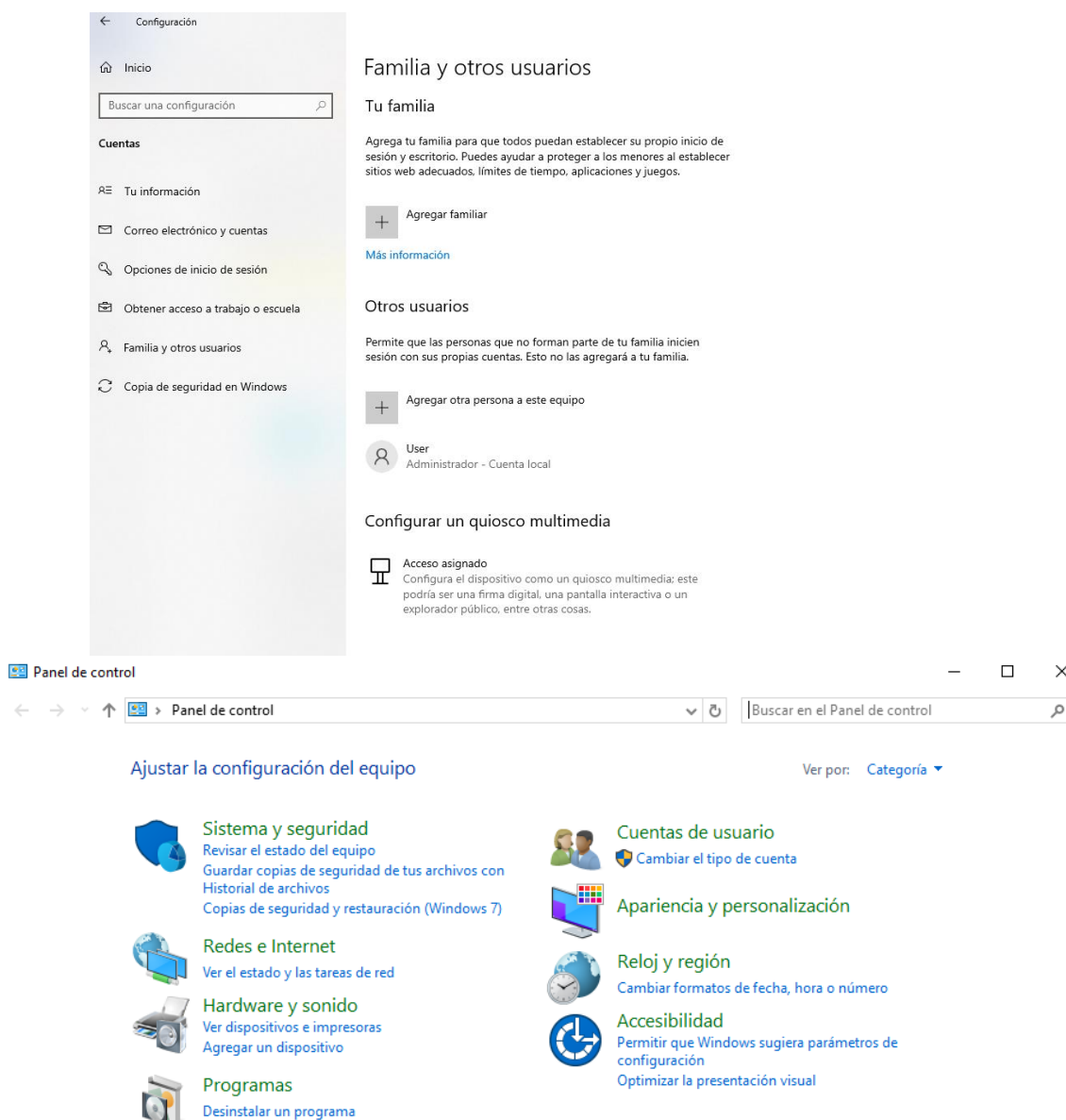


Sistemas informáticos

Todo lo comentado hasta ahora existía en versiones anteriores de Windows, sin embargo, Windows 10 permite crear dos nuevos tipos de usuarios:

- **Familiares:** Se dividen a su vez en **adultos** y **niños**, siendo la principal diferencia que los adultos controlan los límites y usos de los niños de la familia. Básicamente se ejecuta un control parental sobre las cuentas de niños.
- **Otros usuarios:** Se supone que no son de la familia y no tienen relación con el resto de las cuentas. Esto es lo que ya antes existía previa a la división.

Estas nuevas opciones se encuentran en **Configuración > Cuentas**, sin embargo, las anteriores se siguen controlando desde **Panel de control > Cuentas de usuario**.



2.2. TIPOS DE GRUPOS LOCALES.

Los grupos de usuarios proporcionan la posibilidad de otorgar permisos y derechos a usuarios con características similares, simplificando así la administración de cuentas de usuario sin tener que ir usuario por 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).



Sistemas informáticos

Windows 10 emplea los siguientes tipos de grupos:

- **Grupos locales:** Definidos en un equipo local y utilizado 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 10 se crean por defecto varios grupos de usuarios predefinidos en el sistema:

- Administradores.
- Duplicadores.
- IIS_IUSRS (El grupo IIS_IUSRS reemplaza al grupo de IIS_WPG. Este grupo integrado tiene acceso a todos los recursos de archivo y sistema necesarios para que una cuenta, cuando se agregue a este grupo, pueda actuar sin problemas como una identidad del grupo de aplicaciones.)
- Invitados.
- Lectores del registro de eventos.
- Operadores de configuración de red.
- Operadores de copia de seguridad.
- System Managed Accounts Group.
- Usuarios.
- Usuarios avanzados.
- Usuarios COM distribuidos.
- Usuarios de administración remota.
- Usuarios de escritorio remoto.
- Usuarios del monitor de sistema.
- Usuarios del registro de rendimiento.



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.

2.3.GESTIÓN DE CUENTAS DE USUARIO Y GRUPOS LOCALES.

En Windows 10 tenemos varias alternativas para crear, modificar y eliminar cuentas de usuario locales:

- Desde la aplicación **Configuración**.
- Desde el **Panel de control**.
- Desde la **consola Usuarios y grupos locales**.

Veamos a continuación con detalle cada una de ellas.

2.3.1.Gestión de cuentas de usuario desde Configuración.

Desde el menú Inicio pulsamos en Configuración y entramos en Cuentas.

Para crear una cuenta **de usuario nueva**, seleccionamos **Familia y otros usuarios** y pulsamos en Agregar otra persona a este equipo. Se inicia un asistente que nos permite configurar si queremos iniciar sesión con una cuenta de Microsoft para sincronizar todos los datos, OneDrive y demás, o sin cuenta.

Para realizar cambios en una cuenta, distinguimos si se trata de la cuenta del usuario que ha iniciado sesión o no:

Si se trata del usuario que ha iniciado sesión, podemos cambiar su imagen seleccionando Tu información, o su contraseña, seleccionando Opciones de inicio de sesión.

Si es otro usuario, podemos cambiar el tipo de cuenta de dicho usuario, o eliminarlo, seleccionando Familia y otros usuarios.

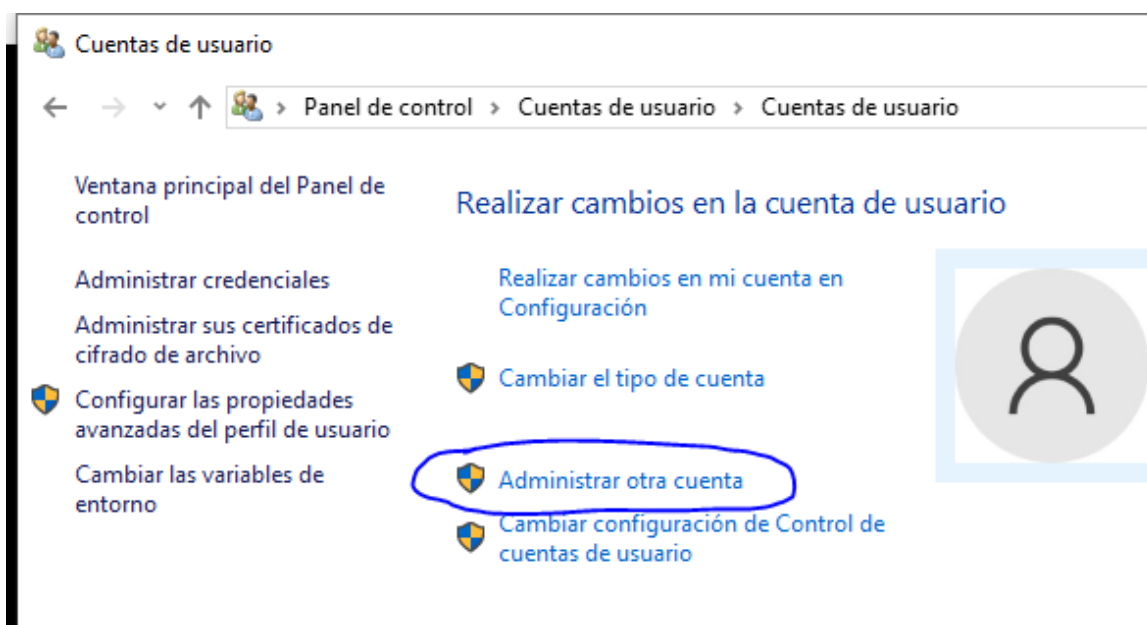
Cuando eliminamos una cuenta de usuario ésta se borra definitivamente del sistema. No podemos recuperarla creando otra con el mismo nombre con el objeto de conseguir los mismos permisos de la cuenta antigua. Esto es debido a que cuando creamos otra cuenta nueva el sistema asigna un nuevo SID distinto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

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

2.3.2. Gestión de cuentas de usuario desde Panel de control.

Desde el Panel de control seleccionamos Cuentas de usuario y de nuevo Cuentas de usuario.

Para **crear una cuenta de usuario nueva**, hacemos clic en Administrar otra cuenta y seleccionamos Agregar un nuevo usuario en Configuración. A partir de aquí nos encontramos en el mismo caso comentado en el apartado anterior.



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

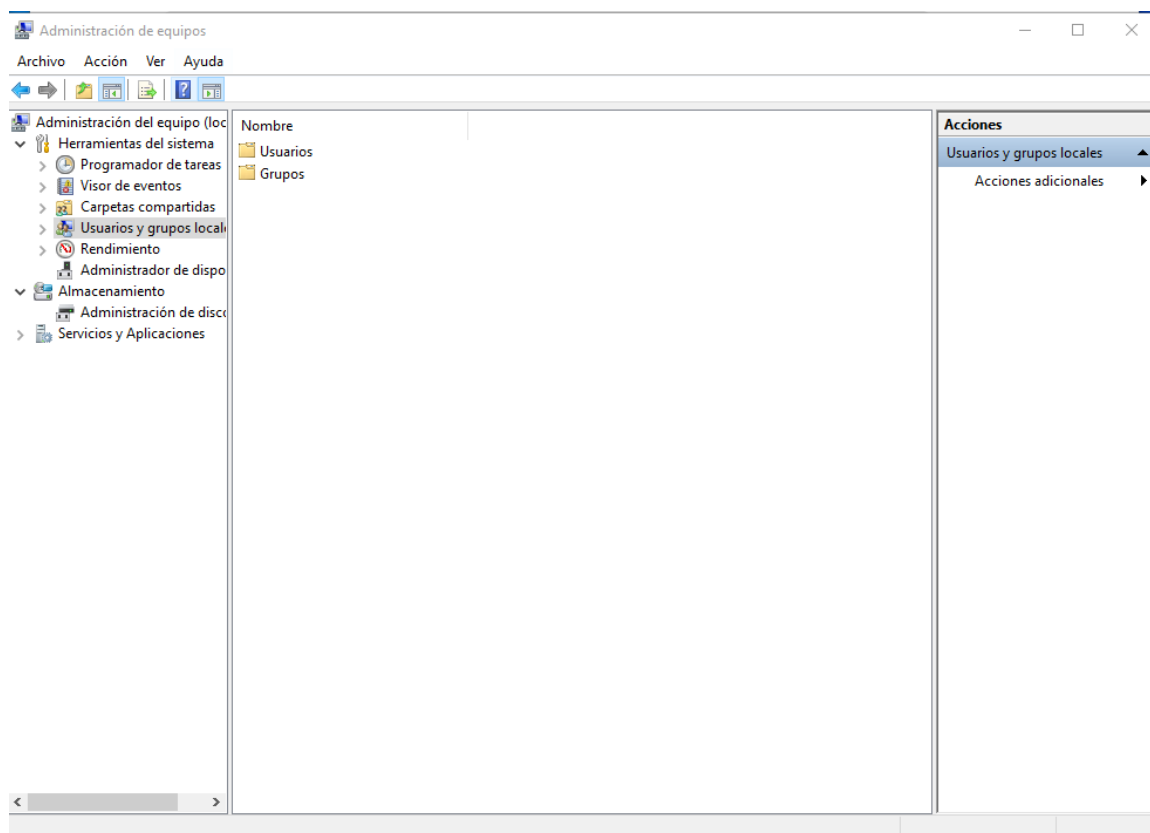
1. Hacer clic en Administrar otra cuenta.
2. Hacer clic en la cuenta que deseas cambiar.
3. Seleccionar la opción que deseas cambiar: nombre, contraseña, tipo o eliminar usuario.

2.3.3. Gestión de cuentas de usuario desde la consola Usuarios y grupos locales.

Esta opción que tenemos para gestionar cuentas de usuario es la más interesante de todas las que nos ofrece Windows 10. Es conocida como la **consola Usuarios y grupos locales** y podemos llegar a ella de dos formas distintas:

Escribiendo en el cuadro de búsqueda "**LUSRMGR.MSC**".

Desde *Panel de control > Sistema y seguridad > Herramientas administrativas > Administración de equipos* y escogemos la carpeta de **Usuarios y grupos locales**.

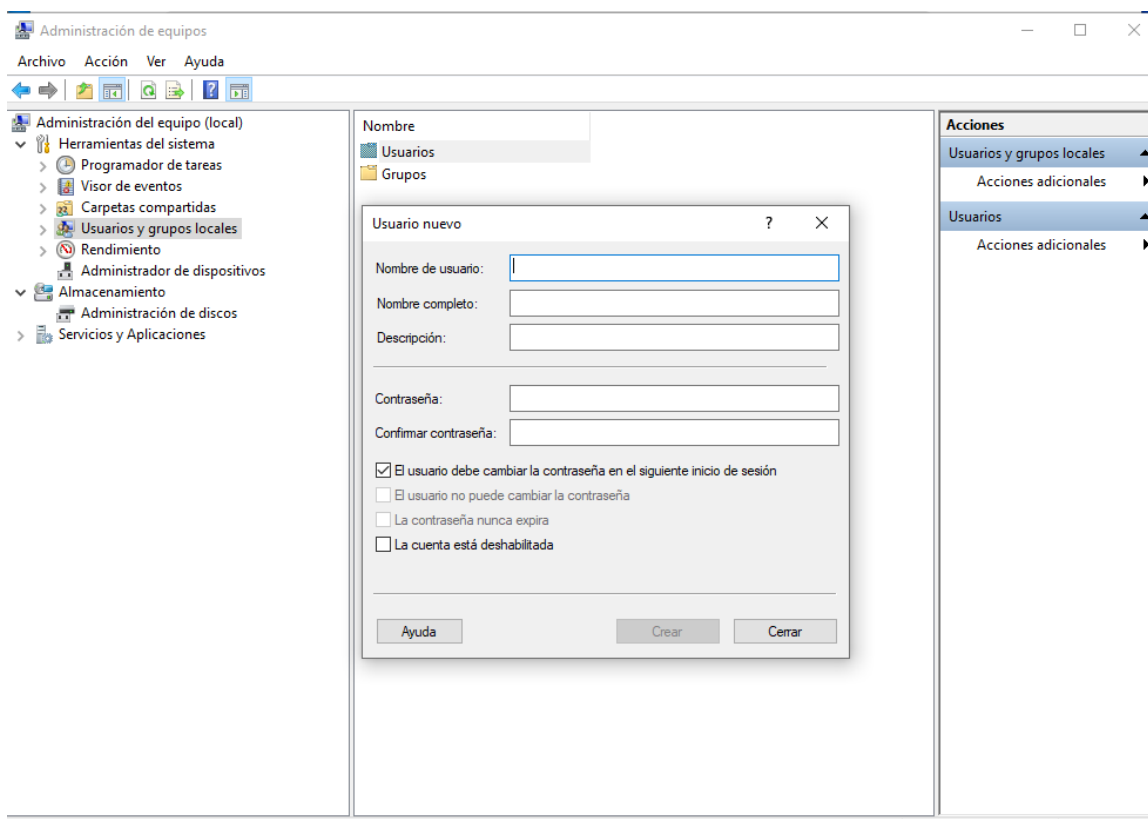


Lleguemos desde donde lleguemos, veremos que tenemos dos carpetas, una para los usuarios y otra para los grupos.

Si compruebas el nombre de esta consola, verás que aparece la palabra **locales** en el mismo. Esto es así porque 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.

Para **crear una cuenta de usuario nueva**, pulsamos el botón derecho sobre la carpeta Usuarios y seleccionamos la opción Usuario Nuevo...



Para **realizar cambios en una cuenta**, hacemos clic en en la carpeta Usuarios, pulsamos el botón derecho sobre la cuenta que queremos cambiar y seleccionamos Propiedades. 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 expira. Ya veremos cómo en Windows 10 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.
- La cuenta está 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.
- **Miembro de:** Podemos ver los grupos a los que el usuario pertenece actualmente o introducir al usuario en otro grupo. Si le damos al botón Agregar... podemos escribir directamente el nombre de un grupo y si queremos escoger dicho grupo de una lista de los grupos posibles, hay que pulsar el botón Opciones avanzadas..., luego Buscar ahora, que nos mostrará una lista de todos los grupos del sistema, y seleccionar el que queramos (o los que queramos) y pulsar Aceptar.
- **Perfil:** Nos permite indicar la ruta del perfil, los archivos de inicio de sesión y las carpetas personales del usuario. Como en un apunte posterior veremos el tema de perfiles, de momento lo dejamos pendiente.

Del mismo modo que acabamos de ver podemos crear nuevos grupos y modificar los ya existentes.

Podemos tanto asignar a un usuario varios grupos, como asignar a un grupo varios usuarios.

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.

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 usuarios y grupos permiten limitar la capacidad de los recursos 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.

3.1. PERMISOS DE RECURSOS LOCALES. ACLS.

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**).

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 en ella. Bien, en este caso se aplica la siguiente regla:

1. Lo que más pesa en cualquier ACL es la **denegación** explícita 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 explícitamente en ningún sitio).

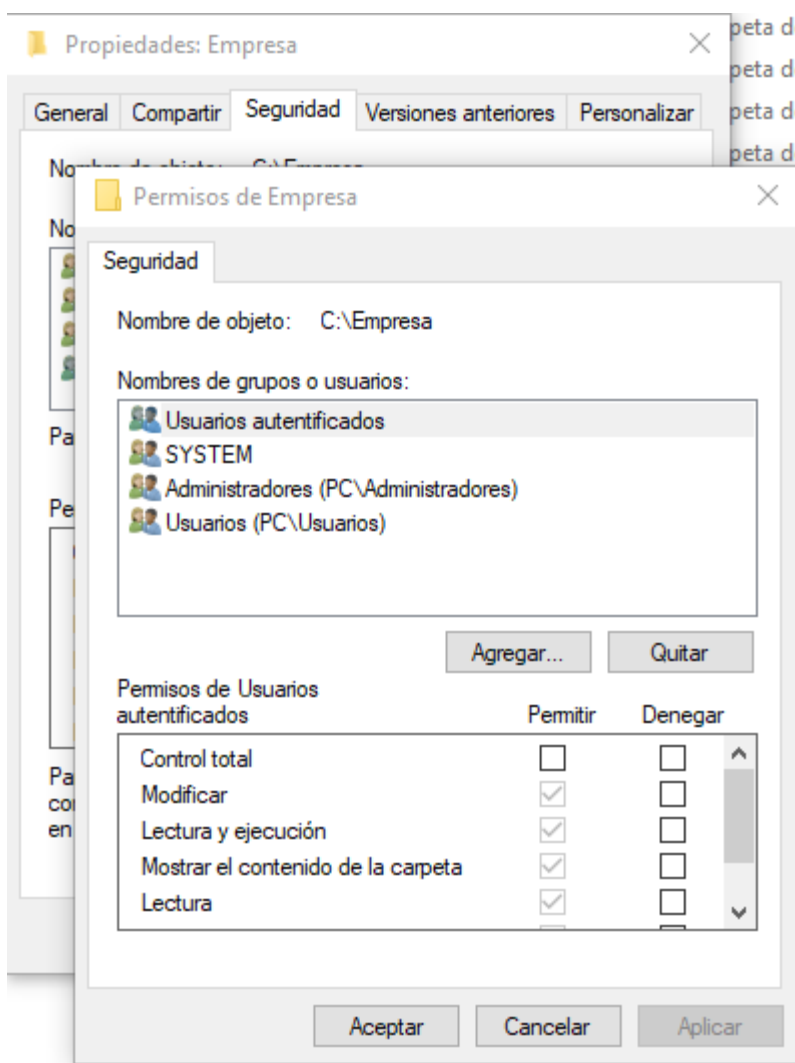
3.1.1. Herencia de permisos.

Para trabajar este apartado 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 cada SID. Existen dos columnas por cada permiso con las que 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 herencia.

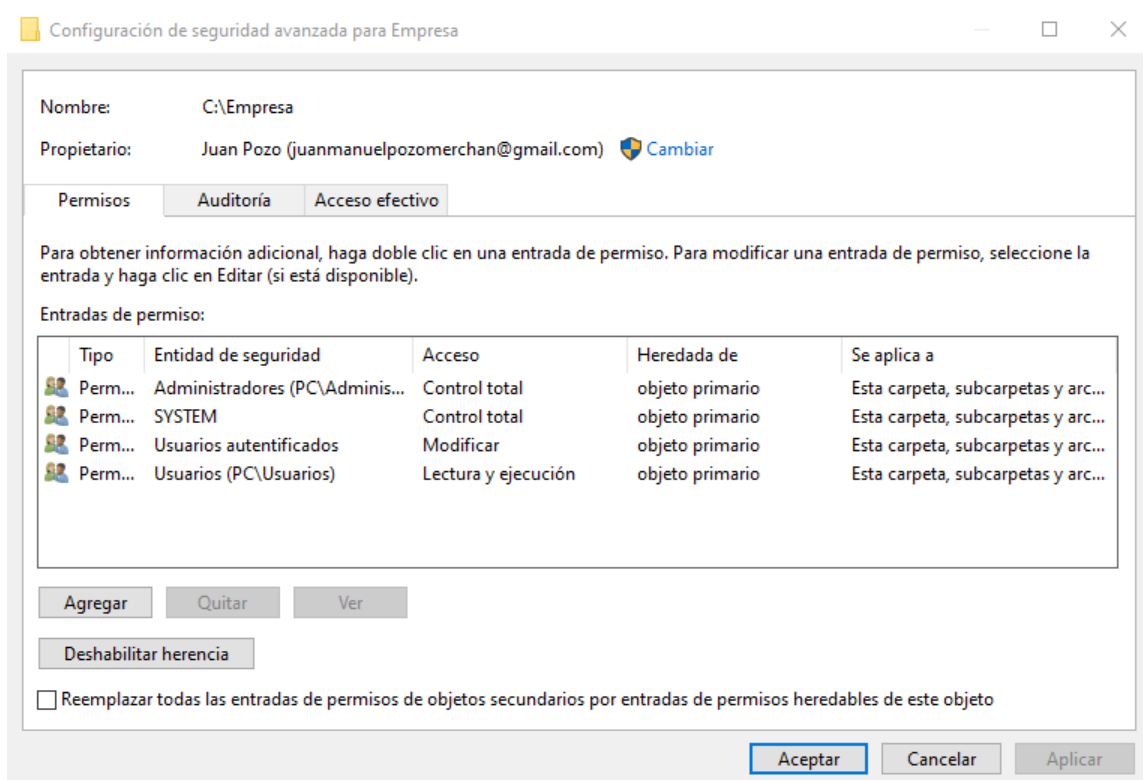


Imagina que en la carpeta "Empresa" pueden leer y escribir en ella los usuarios que sean miembros del grupo "Empleados", sólo pueden leer los del grupo "Jefes" pero no escribir en ella, y los demás usuarios no pueden ni leer ni escribir en ella. Bien, si dentro de la carpeta "Empresa" creamos una nueva carpeta llamada "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 creamos, heredará automáticamente la ACL de su recurso padre si es que existe, y por ello en nuestro caso, la carpeta "Empresa" ha heredado la ACL de la raíz de nuestro volumen C:\, 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.

Aquí podemos ver 3 pestañas, de momento nos quedamos en la primera, llamada Permisos.



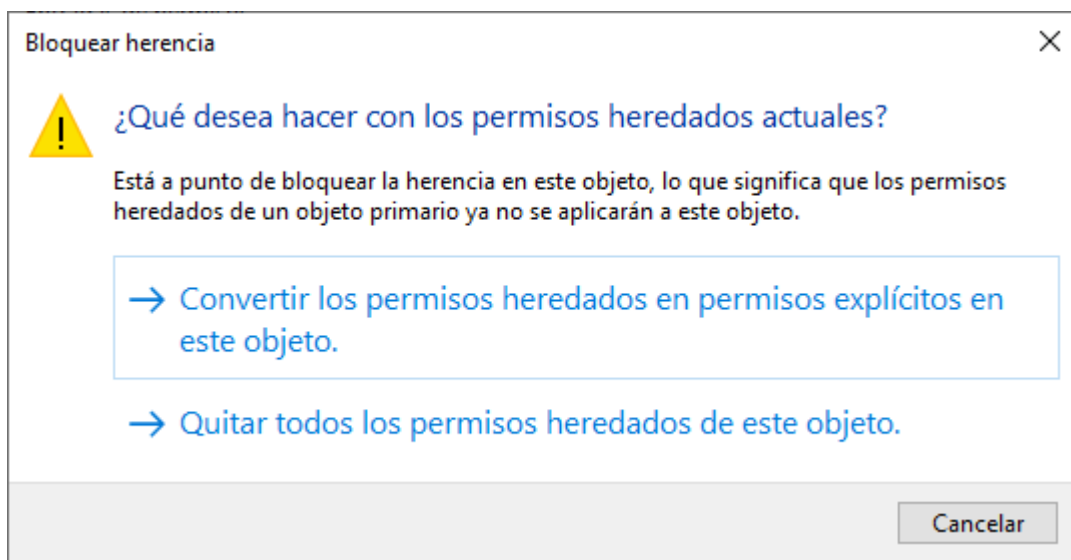
Vemos como en la parte inferior de esta ventana aparece un botón **Deshabilitar herencia**.

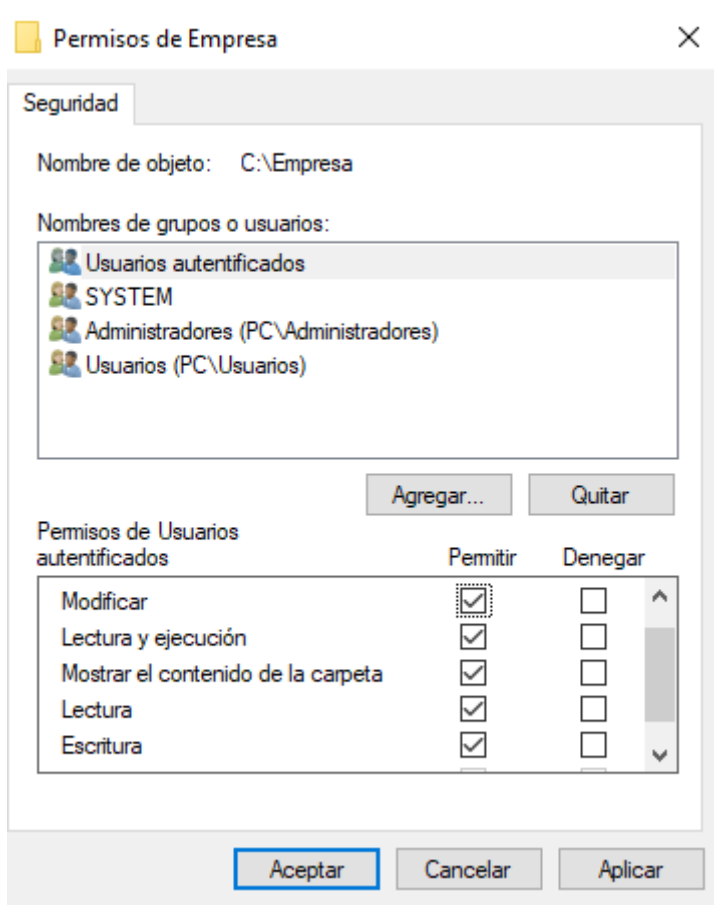
Hay que tener cuidado, una vez quitada la herencia el sistema nos da a elegir entre dos opciones:

- **Convertir los permisos heredados en permisos explícitos en este objeto:**

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. 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".

- **Quitar todos los permisos heredados de este objeto:** La ACL se borrará totalmente, se interrumpirá la herencia y la podremos crear desde cero. Pero 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.).



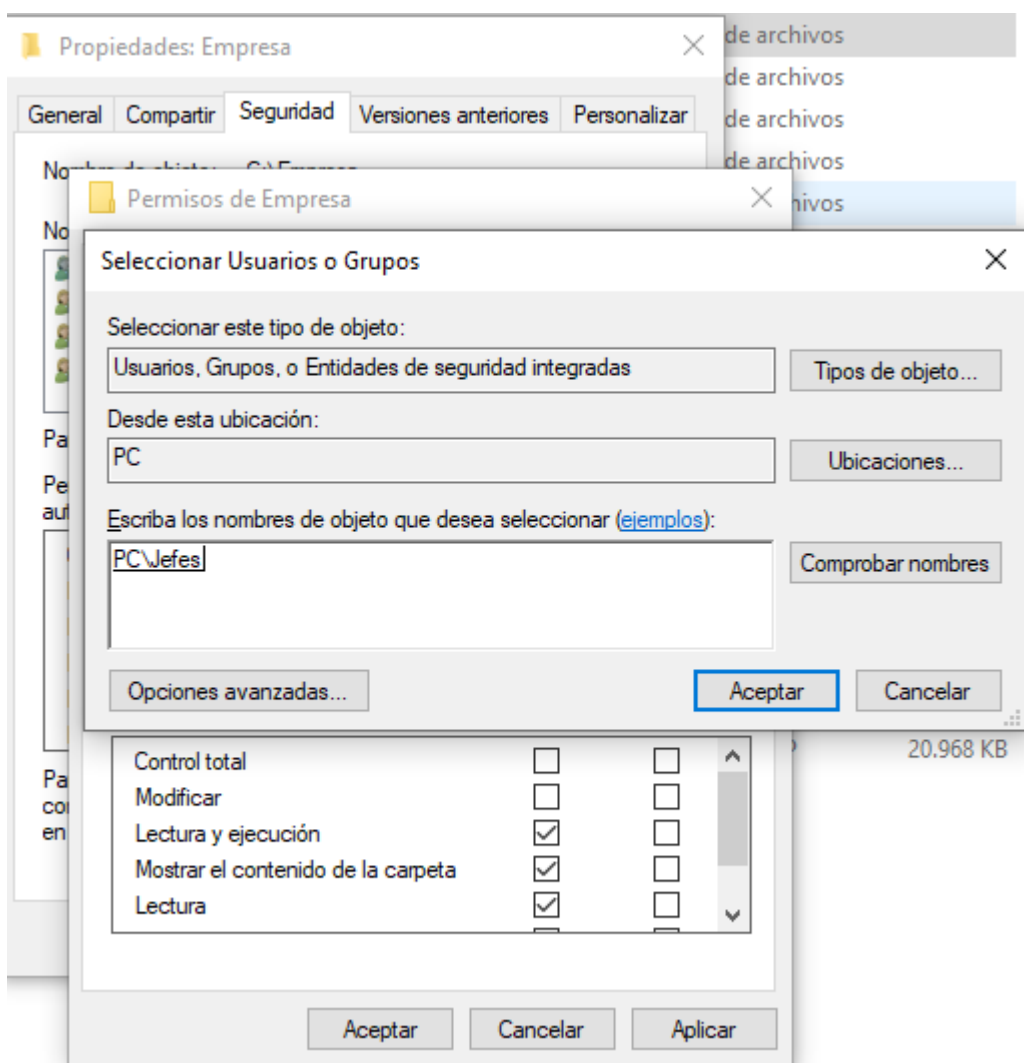


3.1.2. Asignación de permisos.

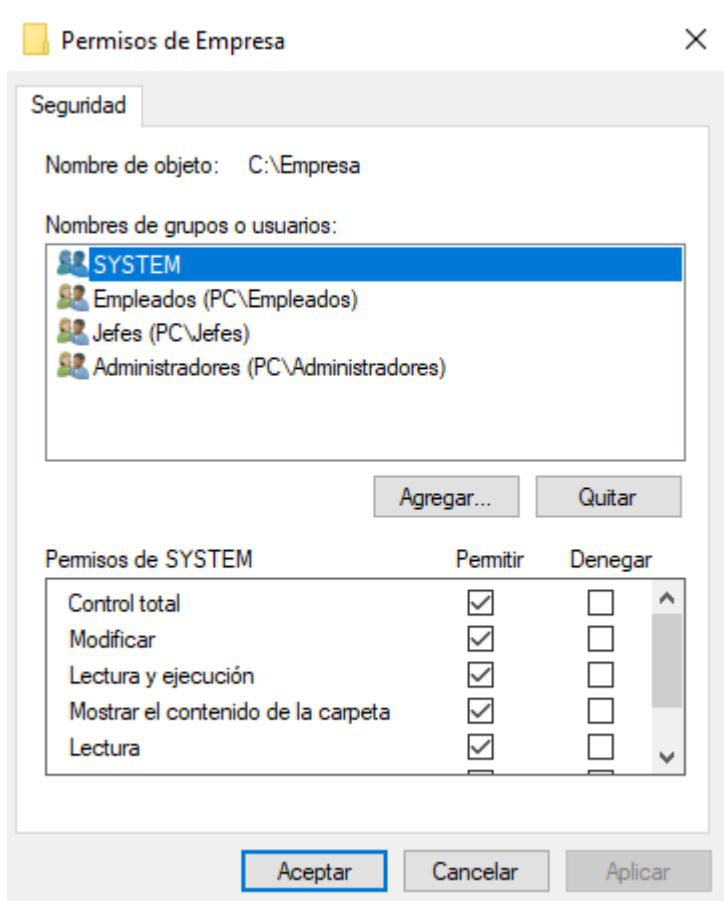
Sigamos con el ejemplo del apartado anterior y supongamos que aplicamos la opción de **Convertir los permisos heredados en permisos explícitos en este objeto**.

Vemos que debajo del botón Deshabilitar herencia, 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.

Aplicamos esta opción y creemos y agreguemos en este momento a los grupos "Empleados" y "Jefes". Les asignaremos los permisos de forma que en la carpeta "Empresa" pueden leer y escribir en ella los usuarios que sean miembros del grupo "Empleados", sólo pueden leer los del grupo "Jefes" pero no escribir en ella, y los demás usuarios no pueden ni leer ni escribir en ella.



Tendremos que 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, 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 anterior. 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, seleccionamos un usuario o grupo de la ACL y hacemos clic en el botón Editar, nos aparecerá una nueva ventana en la que pinchando en Mostrar permisos avanzados veremos que podemos indicar otro tipo de permisos.

Configuración de seguridad avanzada para Empresa

Nombre: C:\Empresa

Propietario: Juan Pozo (juanmanuelpozomarchan@gmail.com) [Cambiar](#)

Permisos Auditoría Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de permiso. Para modificar una entrada de permiso, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de permiso:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
Permitir	SYSTEM	Control total	Ninguno	Esta carpeta, subcarpetas y
Permitir	Empleados (PC\Empleados)	Lectura, escritura y eje...	Ninguno	Esta carpeta, subcarpetas y
Permitir	Jefes (PC\Jefes)	Lectura	Ninguno	Esta carpeta, subcarpetas y
Permitir	Administradores (PC\Adminis...	Control total	Ninguno	Esta carpeta, subcarpetas y

[Agregar](#) [Quitar](#) [Editar](#)

[Habilitar herencia](#)

☐ Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto

[Aceptar](#) [Cancelar](#) [Aplicar](#)

Entrada de permiso para Empresa

Entidad de seguridad: Empleados (PC\Empleados) [Seleccionar una entidad de seguridad](#)

Tipo: Permitir

Se aplica a: Esta carpeta, subcarpetas y archivos

Permisos avanzados: [Mostrar permisos básicos](#)

<input type="checkbox"/> Control total	<input checked="" type="checkbox"/> Escribir atributos
<input checked="" type="checkbox"/> Atravesar carpeta / ejecutar archivo	<input checked="" type="checkbox"/> Escribir atributos extendidos
<input checked="" type="checkbox"/> Mostrar carpeta / leer datos	<input type="checkbox"/> Eliminar subcarpetas y archivos
<input checked="" type="checkbox"/> Leer atributos	<input type="checkbox"/> Eliminar
<input checked="" type="checkbox"/> Leer atributos extendidos	<input checked="" type="checkbox"/> Permisos de lectura
<input checked="" type="checkbox"/> Crear archivos / escribir datos	<input type="checkbox"/> Cambiar permisos
<input checked="" type="checkbox"/> Crear carpetas / anexas datos	<input type="checkbox"/> Tomar posesión

☐ Aplicar estos permisos solo a objetos y/o contenedores dentro de este contenedor

[Borrar todo](#)

[Aceptar](#) [Cancelar](#)

- **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.
- **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).
- **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.
- **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.
- **Control Total.** Este permiso es muy especial. 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.

Una directiva es un conjunto de reglas de seguridad que se pueden implementar en un sistema.

Desde una cuenta con privilegios de administrador, Windows 10 nos da la posibilidad de gestionar de forma centralizada la configuración de la seguridad de nuestro sistema a través de:

- **Directivas de seguridad local.** Nos permiten aplicar distintas restricciones de seguridad sobre las cuentas de usuario y sus contraseñas.
- **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.

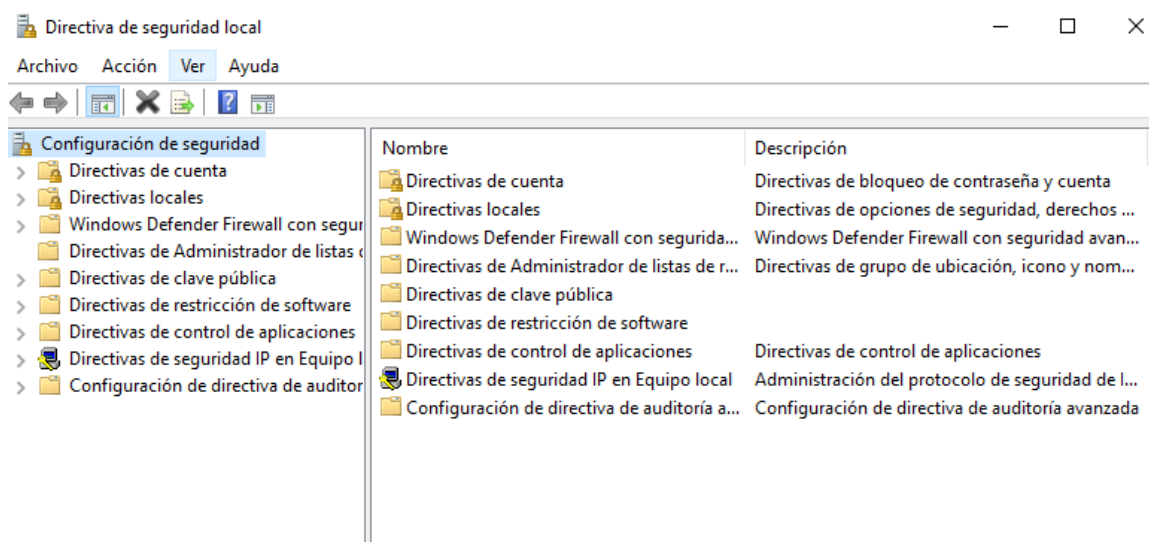
Ambas opciones cuentan con consolas para facilitar la configuración de las directivas y las veremos con detalle en los siguientes apartados.

3.2.1. Directivas de seguridad local.

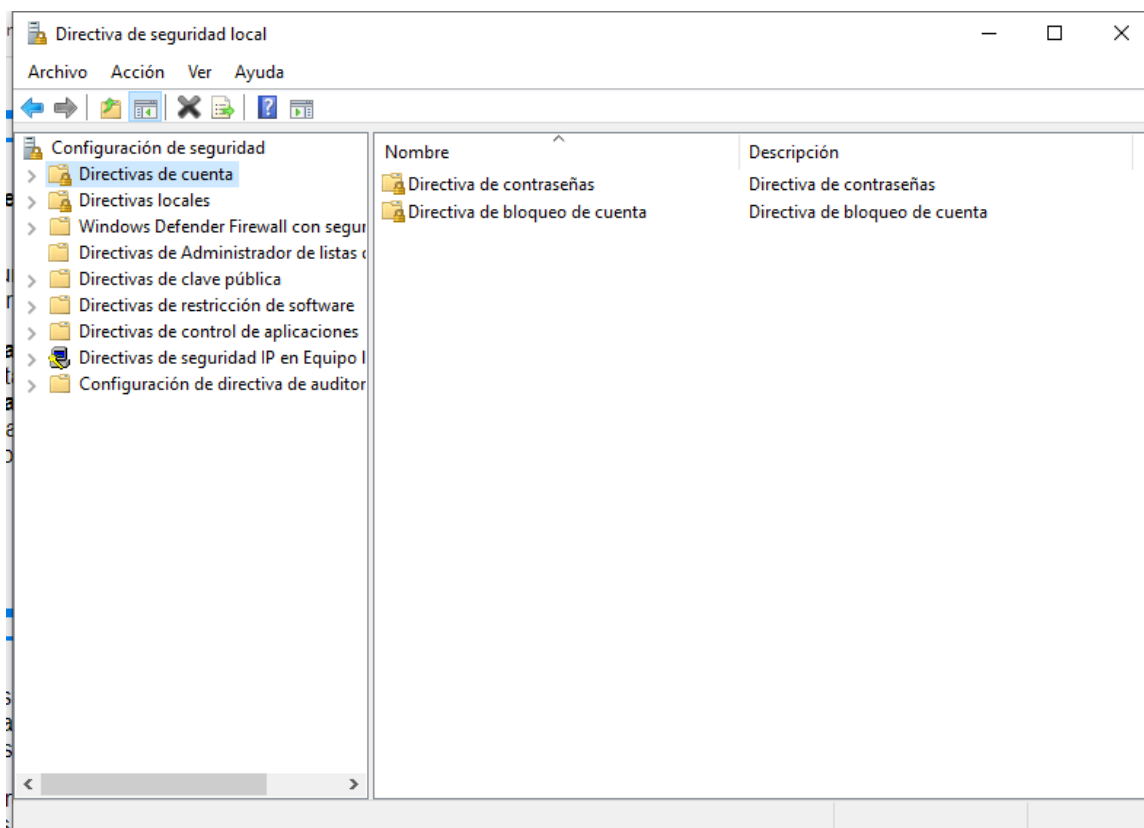
Windows 10 es un sistema operativo muy configurable por parte del usuario aunque estas configuraciones suelen estar algo ocultas para que no sean accesibles por los usuarios normales y sólo pueden ser modificadas desde las **consolas del sistema**.

En concreto, desde la consola **Directiva de seguridad local**, podemos gestionar varios aspectos sobre las cuentas de usuarios y sus contraseñas. Para acceder a esta consola podemos hacerlo de dos formas distintas:

- Escribiendo en el cuadro de búsqueda "secpol.msc".
- Desde Panel de control > Sistema y seguridad > Herramientas administrativas > Directiva de seguridad local.



Una vez dentro accederemos a Configuración de seguridad > Directivas de cuenta, y veremos que tenemos dos carpetas, una para contraseñas y otra para bloqueo de cuenta:



- **Directiva de contraseñas.** 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.
 - **La contraseña debe cumplir los requisitos 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 mínima 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.

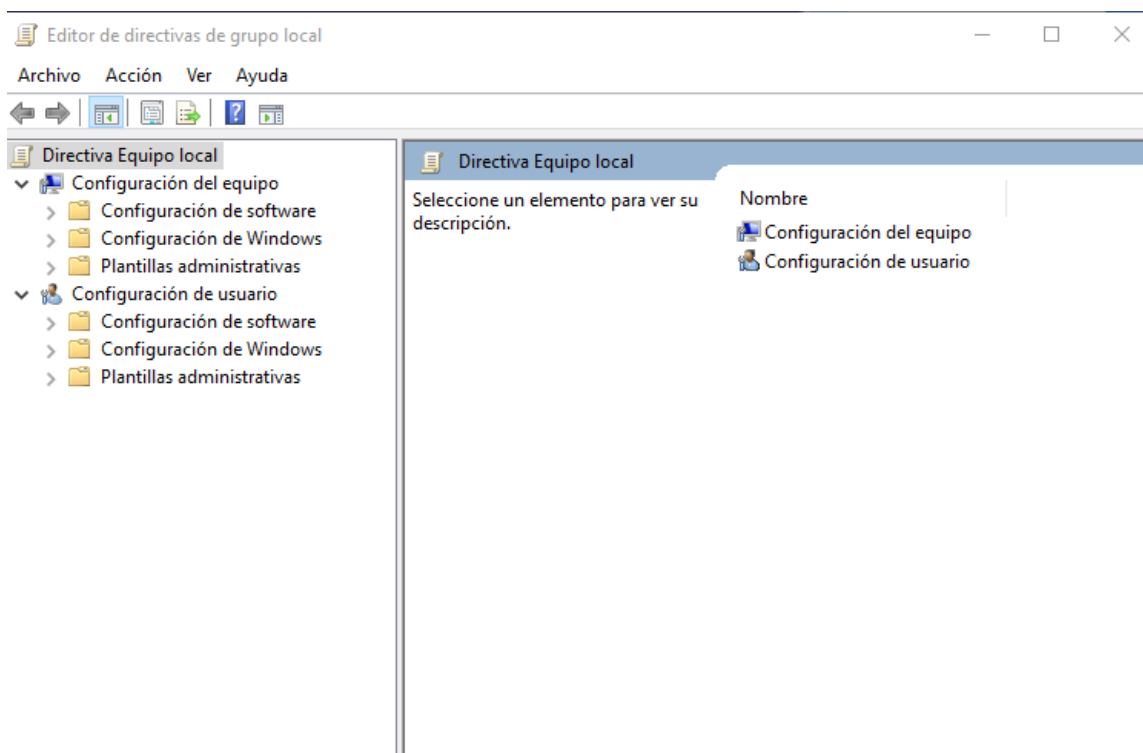
(Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).

- **Vigencia mínima 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.
- **Directiva de bloqueo de cuenta.** Permite bloquear las cuentas de usuario si se intenta acceder al sistema con las mismas, pero usando contraseñas incorrectas. Aquí podemos configurar:
 - **Duración del bloqueo de cuenta.** Indica 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.
 - **Permitir bloqueo de cuenta de administrador.** Esta configuración de seguridad determina si la cuenta de administrador integrada está sujeta a la directiva de bloqueo de cuenta.
 - **Restablecer el bloqueo de cuenta después de.** Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero.
 - **Umbral de bloqueo de cuenta.** Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta.

3.2.2. Directivas de grupo local.

Las directivas de grupo son una herramienta muy poderosa que permite a los administradores configurar equipos de forma **local o remota**, instalando aplicaciones, restringiendo derechos a los usuarios, eliminando aplicaciones, instalando y ejecutando scripts, y redirigiendo carpetas del sistema a red o viceversa. Pero también tienen su utilidad en entornos pequeños, incluso en una sola máquina.

Desde la consola Editor de directivas de grupo local, podemos gestionar las directivas de grupo, y para acceder a esta consola escribimos en el cuadro de búsqueda **"gpedit.msc"**.



Usando las políticas de grupo en una máquina con 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 de Windows 10. 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 o cierre sesión.
- Especificar opciones especiales de seguridad.

Si nuestro equipo está unido a un dominio (con un servidor en la red administrando dicho dominio), podemos configurar directivas del dominio completo que afectarán a varias máquinas. 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. Nosotros nos vamos a centrar aquí en las directivas locales, ya que no estamos trabajando en un dominio, de momento.

Para poder trabajar en esta consola necesitamos hacerlo desde una cuenta de usuario que pertenezca al grupo Administradores. Esta consola es muy configurable permitiéndonos añadir y quitar opciones según deseemos, aunque de momento vamos a trabajar con las opciones que aparecen por defecto.

Vemos que dentro de Directiva Equipo local tenemos dos opciones: **Configuración del equipo** y **Configuración de usuario**. En el caso de estar trabajando en grupo de trabajo es prácticamente indistinto trabajar con una opción u otra. Algunas directivas aparecen tanto en Configuración del equipo como en Configuración de usuario. En caso de conflicto la de Configuración del equipo siempre tendrá preferencia.

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

Para modificar el estado o configuración de una directiva, hacemos doble clic sobre ella y nos aparecerá un cuadro de diálogo que nos permitirá modificar dicha directiva. También nos mostrará una explicación de la funcionalidad de dicha directiva.

Respecto a la configuración, veremos que tenemos las siguientes opciones:

- **No configurada:** Se comportará según el criterio por defecto para dicha directiva.
- **Habilitada:** La pondremos en marcha en el sistema.
- **Deshabilitada:** Impediremos que se ponga en marcha dicha directiva.

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

Algunas directivas especiales permiten especificar otras informaciones.

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

Prueba a habilitar la directiva Impedir el acceso al símbolo del sistema (gpedit.msc > Configuración de usuario > Plantillas administrativas > Sistema > Impedir el acceso al símbolo del sistema) e intenta ejecutar una ventana de Símbolo del sistema (cmd.exe).

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 cuota de disco y podemos habilitarla a través de:

El Explorador de Windows:

1. En Este Equipo hacemos clic con el botón derecho en el volumen de disco para el que se desea habilitar cuotas de disco y pulsamos en Propiedades.
2. En la pestaña Cuota pulsamos el botón Mostrar configuración de cuota.
3. Marcamos la casilla de verificación Habilitar la administración de cuota.
4. Pulsamos el botón Aceptar.

Directivas de grupo:

1. Escribimos en el cuadro de búsqueda **"gpedit.msc"**.
2. Accedemos a Configuración del equipo > Plantillas administrativas > Sistema > Cuotas de disco.
3. Hacemos doble clic en Habilitar cuotas de disco y seleccionamos Habilitada.
4. Pulsamos el botón Aceptar.

Si se habilita o deshabilita la directiva Habilitar cuotas de discos, se aplica a todos los volúmenes NTFS del equipo e impide que los usuarios puedan cambiarla a través del Explorador de archivos.

4. Mantenimiento del sistema.

4.1. WINDOWS UPDATE.

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 de Inicio > Configuración > Actualización y seguridad y pulsando en Windows Update.

La zona principal nos indica si el sistema está actualizado, la fecha y hora en la que se realizó la última comprobación, y nos ofrece también las siguientes opciones:

- **Pausar las actualizaciones durante 7 días.** Permite aplazar las actualizaciones en el equipo durante un tiempo establecido (puede cambiarse en Opciones avanzadas). Al aplazar las actualizaciones no se descargarán ni instalarán funciones nuevas de Windows durante ese periodo de tiempo. El aplazamiento de las actualizaciones no afecta a las actualizaciones de seguridad. Ten en cuenta que aplazar las actualizaciones te impedirá obtener las últimas funciones de Windows en cuanto estén disponibles.
- **Cambiar horas activas.** Aquí indicamos desde qué hora y hasta qué hora utilizamos el equipo. Windows intentará molestarnos lo menos posible con las actualizaciones, por lo que si necesita reiniciar el sistema operativo para aplicar una actualización no lo hará mientras estemos trabajando.
- **Ver historial de actualizaciones.** Muestra el listado incluyendo la fecha de instalación y resultado (Instalada correctamente o Error al instalar). Además, nos permite desinstalar las actualizaciones o la versión preliminar más reciente.
- **Opciones avanzadas.** Aquí tenemos otras opciones seleccionables como elegir que se actualicen otros productos de Microsoft al actualizar Windows. Por ejemplo, si tienes instalado Windows Office, el programa también se actualizará junto a Windows cuando tengas esta opción activada.

Además de como se ha comentado anteriormente, podemos ver las actualizaciones instaladas desde Panel de control > Programas > Programas y características > Ver actualizaciones instaladas. Si queremos desinstalar alguna

actualización, la seleccionamos y pulsamos 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 esta o si el programa que actualiza ha dejado de funcionar correctamente a raíz de la misma.

4.2. 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 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.

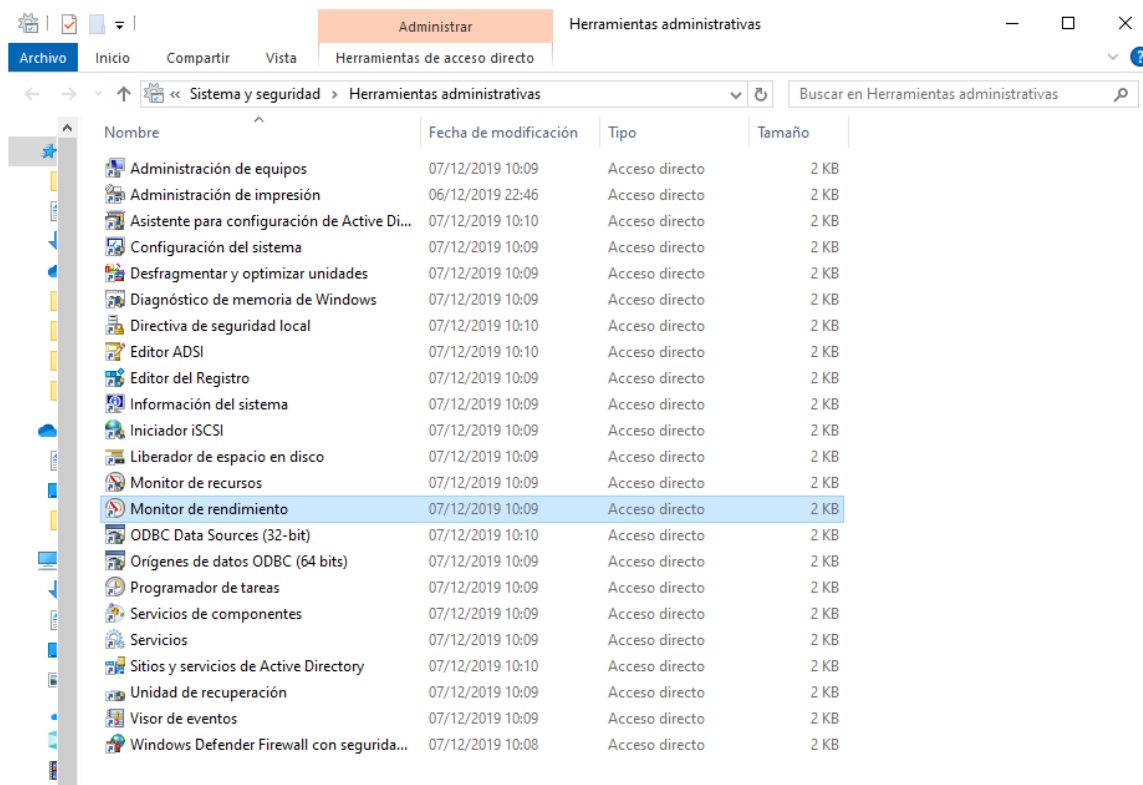
Veamos paso a paso cómo podemos configurar este monitor para que visualice el rendimiento en tiempo real de los aspectos que nos interesan con el objeto de localizar errores o componentes que están ralentizando nuestro PC.

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:

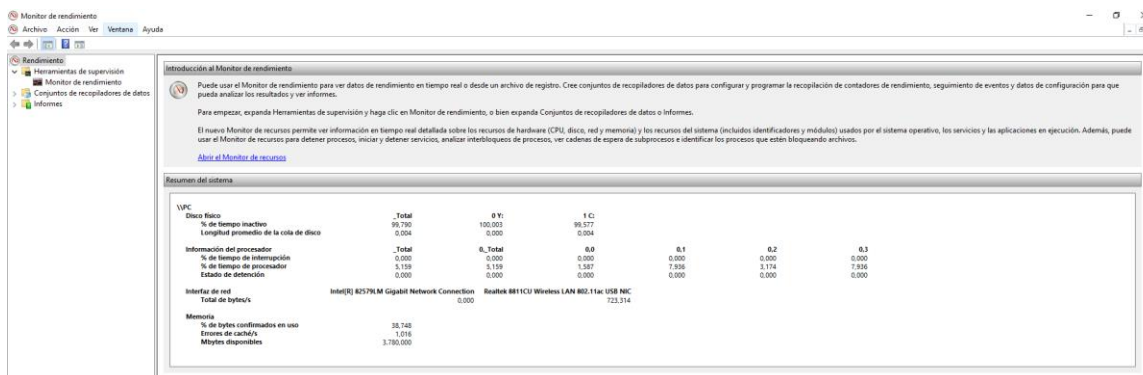
Desde Panel de Control > Sistema y seguridad > Herramientas administrativas > Monitor de rendimiento.

Escribiendo en el cuadro de búsqueda "monitor de rendimiento".



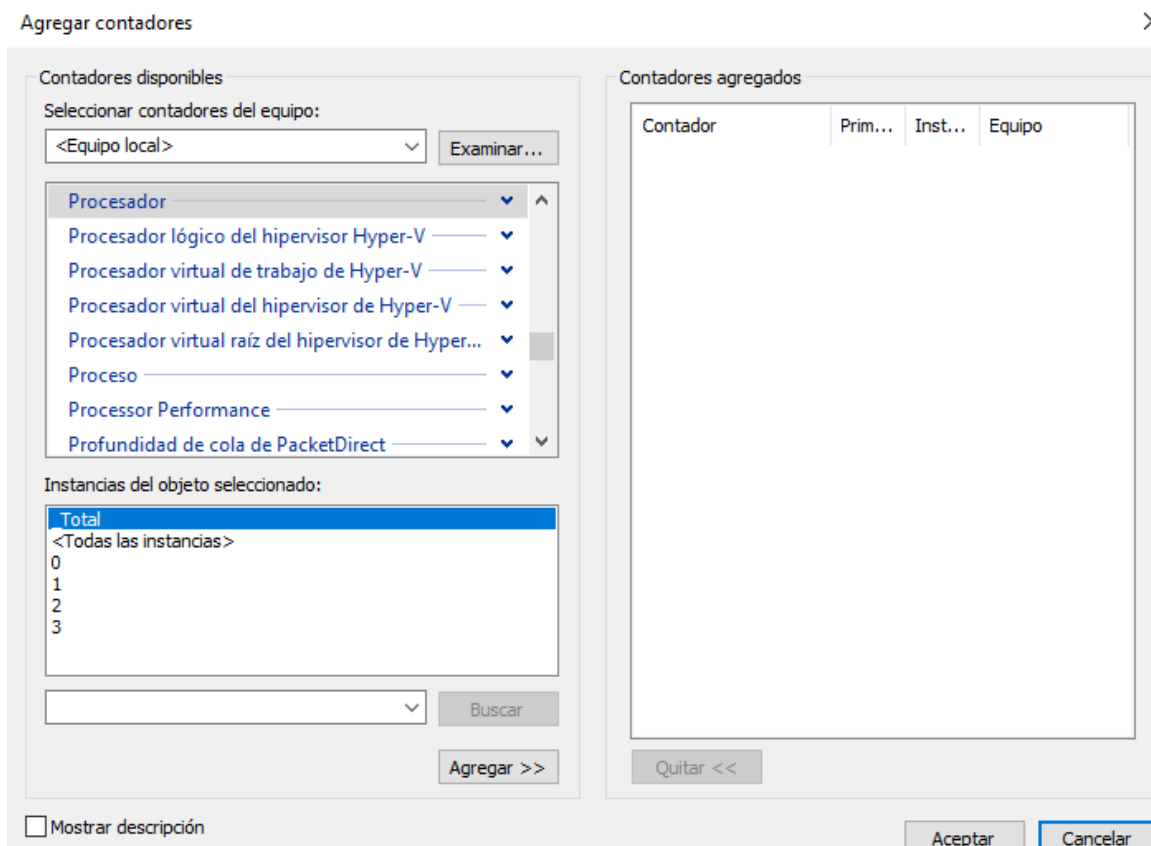
Acceder al monitor

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.



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 + 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.

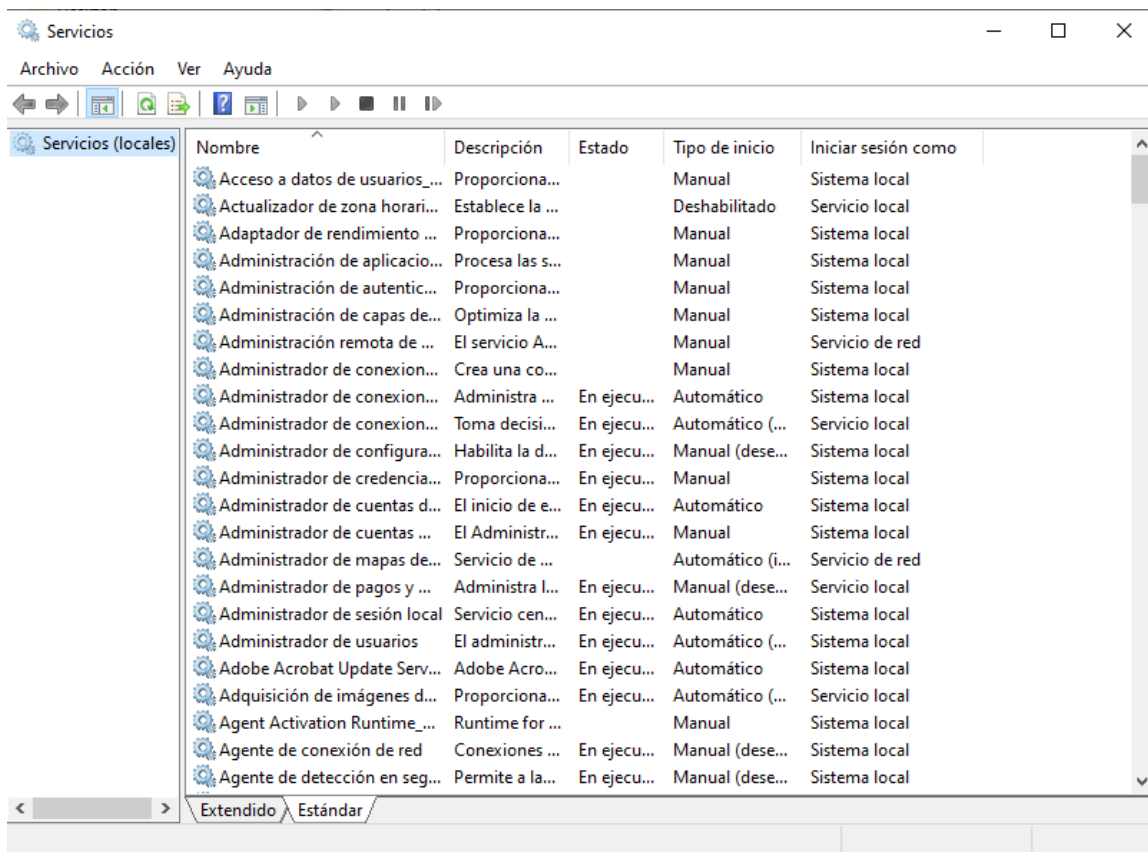
También es posible controlar cada una de las instancias o que se contabilice el total. Si vamos a monitorizar varios componentes es mejor elegir Total si es posible. Podemos ir agregando contadores pulsando sobre Agregar. De esta forma aparecerán en la parte llamada Contadores agregados. Para quitarlos 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.

4.3.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 **Panel de control > Sistema y seguridad > Herramientas administrativas > Servicios** o desde el cuadro de búsqueda escribiendo "**services.msc**".



Esta herramienta nos muestra un listado de los servicios 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 de estos servicios y su función:

- **Aplicación auxiliar IP** - iphlpsvc: Proporciona conectividad de túnel mediante tecnologías de transición IPv6 e IP-HTTPS.
- **Archivos sin conexión** - CscService: Realiza actividades de mantenimiento en la caché de archivos sin conexión.
- **BranchCache** - Caché del contenido de la red en red local.
- Cliente de seguimiento de vínculos distribuidos.
- **Control Parental** - WPCSvc: Aplica el control parental a las cuentas infantiles de Windows.
- **Directiva de extracción de tarjetas inteligentes** - SCPolicySvc: Permite configurar el sistema para bloquear el escritorio del usuario al quitar la tarjeta inteligente.
- **Fax** - Fax: Permite enviar y recibir faxes, con los recursos disponibles en el equipo o en la red.
- **Net Logon** - Netlogon: Autentica usuarios y servicios.
- **Propagación de certificados** - CertPropSvc: Copia los certificados de usuario y certificados raíz de tarjetas inteligentes en el almacén de certificados del usuario actual.
- **Registro remoto** - RemoteRegistry: Modificar registro a usuarios remotos.
- **Servicio Cifrado de unidad BitLocker** - BDESVC: Permite que BitLocker solicite a los usuarios diversas acciones relacionadas con sus volúmenes cuando se montan, y desbloquea los volúmenes automáticamente sin la intervención del usuario.
- **Servicio de compatibilidad con Bluetooth** - bthserv: Permite la detección y asociación de dispositivos Bluetooth remotos.

- **Servicio de detección automática de proxy web WinHTTP** – WinHttpAutoProxySvc: Proporciona a los programadores una API Win32 y un componente de automatización COM para enviar solicitudes HTTP y recibir respuestas.
- **Servicio del iniciador iSCSI de Microsoft** - MSiSCSI: Administra las sesiones SCSI de Internet (iSCSI) desde el equipo hacia los dispositivos de destino iSCSI remotos.
- **Servicio Informe de errores de Windows** - WerSvc: Envío de informes sobre los errores a Microsoft.
- **Sistema de cifrado de archivos (EFS)** - EFS: Para almacenar archivos cifrados en particiones NTFS.
- **Tarjeta inteligente** - SCardSvr: Administra el acceso a tarjetas inteligentes.
- **Windows Search** - WSearch: Indexa los archivos, el correo electrónico y otros contenidos para hacer búsquedas con más rapidez.

4.4. DESFRAGMENTACIÓN DE DISCOS.

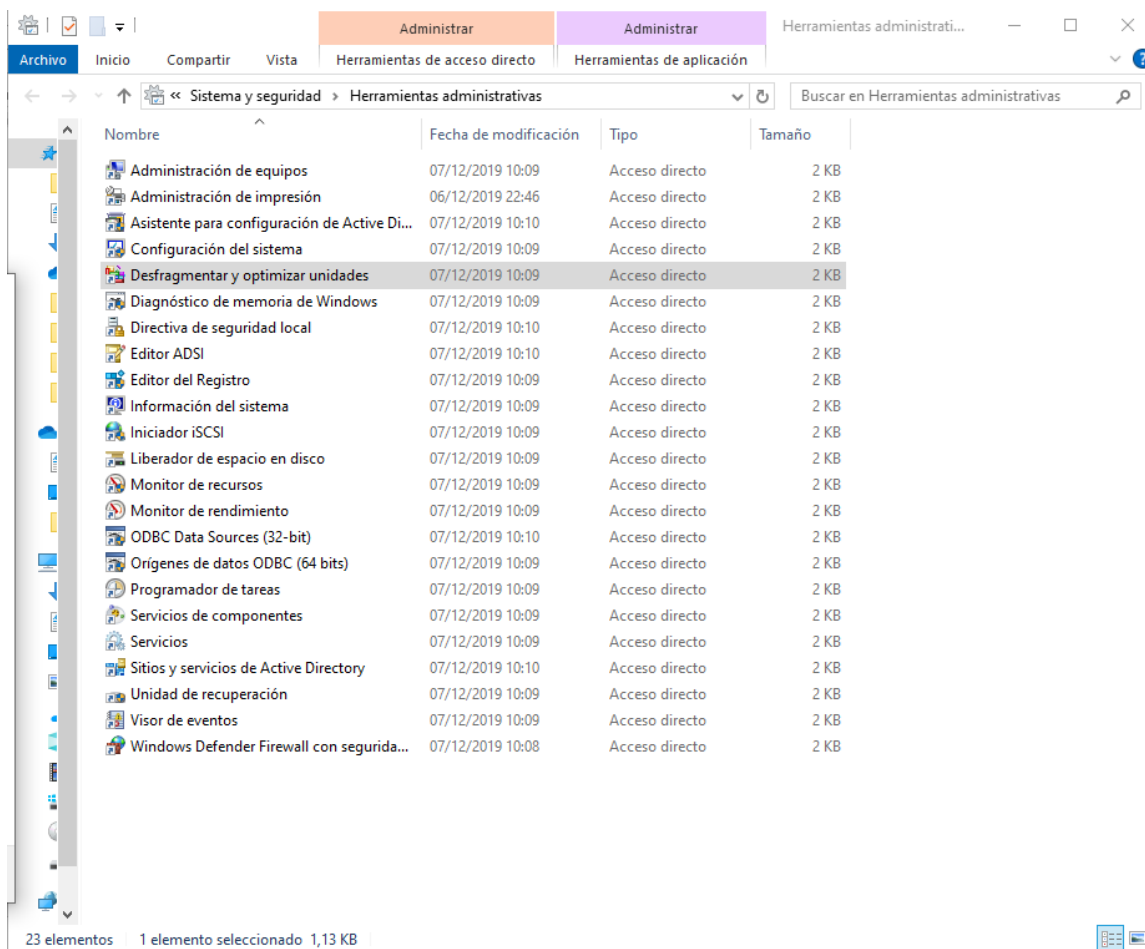
La **fragmentación de un disco** se produce cuando numerosos archivos se encuentran divididos a lo largo de la partición. El hecho de que un archivo se encuentre disperso reduce el rendimiento de la unidad, porque el cabezal tendrá que saltar por varias partes del disco para obtener la información y 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 libre 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 10 proporciona una herramienta para ello, **Desfragmentar y optimizar unidades**, y podemos acceder a ella desde **Panel de control > Sistema y seguridad >**

Herramientas administrativas > Desfragmentar y optimizar unidades. Esta herramienta vuelve a organizar los datos fragmentados de manera que los discos y las unidades puedan funcionar de manera más eficaz.



Para desfragmentar una unidad primero pulsamos el botón **Analizar**. Después del análisis se nos recomendará si debemos desfragmentar o si no es necesario. En el caso de decidir desfragmentarlo, pulsamos el botón **Optimizar**. Al hacerlo el proceso de desfragmentación iniciará y observaremos que el porcentaje de desfragmentación se va actualizando.

Ésta es la forma manual de desfragmentar una unidad de disco. Windows 10 por defecto desfragmenta todas las unidades de disco duro en el sistema de manera automática pero podemos cambiar la configuración de la desfragmentación. En la misma ventana de Optimizar unidades tenemos el botón Cambiar configuración que nos permitirá acceder a las opciones de configuración para cambiarlas según deseemos. Al

pulsar en él pasaremos a una nueva ventana y en ella tenemos la casilla Ejecución programada (recomendado) que por defecto está marcada. Debemos dejarla marcada si queremos que Windows 10 se encargue automáticamente del proceso de desfragmentación. Si preferimos que sea un proceso manual entonces desmarcamos la casilla. Si dejamos marcada la casilla, más abajo tenemos un menú desplegable que ofrece diferentes opciones relacionadas con la frecuencia que queremos que Windows 10 desfragmente nuestro disco: Diariamente, Semanal, Mensual. Por defecto la opción Semanal está marcada pero aquí podemos cambiarla según nuestra preferencia. También tenemos la casilla Aumentar la prioridad de la tarea si faltan tres ejecuciones programadas consecutivas, la cual se recomienda dejarla marcada.

Ten en cuenta que el proceso de desfragmentación puede ser lento especialmente si es la primera vez que lo haces o si ha pasado bastante tiempo desde la última desfragmentación. Es recomendable que hagas la desfragmentación en un momento del día en el cual no necesites el equipo ya que podría tardar bastante. Si necesitas detener el proceso no hay problema, no le pasará nada a tu equipo, basta con presionar el botón Detener.

4.5. CHEQUEO DE DISCOS.

Podemos comprobar o chequear los discos para comprobar si existen problemas en los mismos. Windows 10 proporciona una herramienta para ello e intentará reparar los problemas 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 Comprobación de errores: con el comando “**chkdsk.exe**” (Check disk) o desde el Explorador de archivos. A continuación describimos ambos procesos:

Desde el símbolo del sistema:

Escribimos en el cuadro de búsqueda “**cmd**”.

En el símbolo del sistema escribimos “**chkdsk**” y a continuación presionamos la tecla Enter. Podemos indicar como parámetro la partición que queremos comprobar, por ejemplo: `chkdsk f:` (chequeará la unidad F:).



Sistemas informáticos

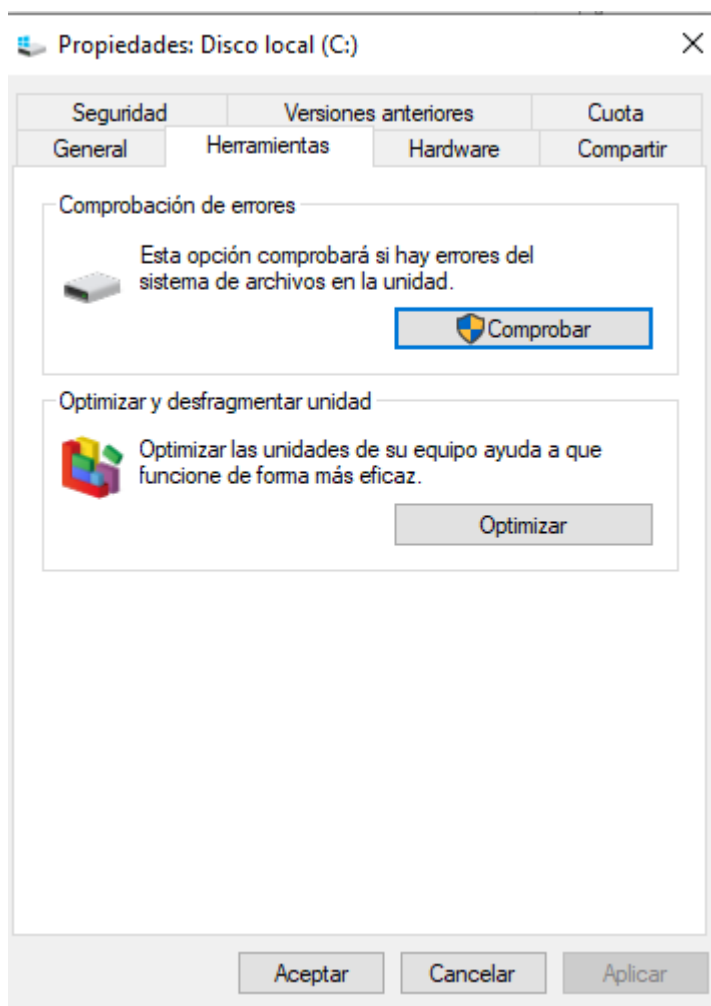
Nota: si alguno de los archivos de la unidad de disco duro se encuentra abierto, recibimos el mensaje siguiente: chkdsk no se puede ejecutar porque otro proceso ya está utilizando el volumen. ¿Desea que se prepare este volumen para que sea comprobado la próxima vez que se inicie el sistema? (S/N). Escribimos S y a continuación presionamos la tecla Enter para programar la comprobación del disco y reiniciamos el equipo para iniciarla.

Desde el Explorador de archivos:

En Este Equipo hacemos clic con el botón derecho del ratón en la unidad de disco duro que queremos comprobar.

Hacemos clic en Propiedades y después en la pestaña Herramientas.

En Comprobación de errores, pulsamos el botón Comprobar. Aparecerá un cuadro de diálogo que nos dice que No es necesario examinar esta unidad (en el caso de no haber errores en la unidad).



Pulsamos sobre Examinar unidad y si aparecen errores seguimos uno de estos procesos:

Para reparar los errores sin buscar los sectores defectuosos, seleccionamos la casilla de verificación Reparar automáticamente errores en el sistema de archivos y, a continuación, pulsamos el botón Iniciar.

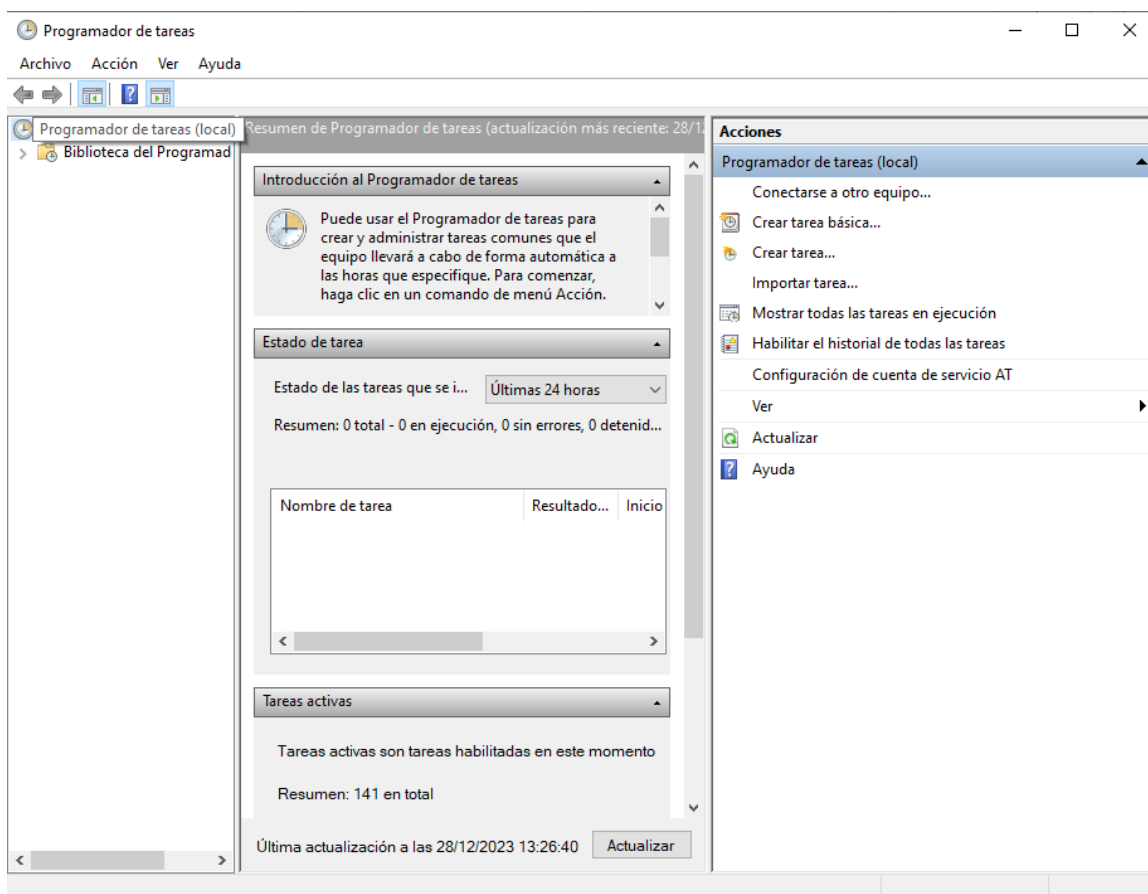
Para reparar los errores, localizar los sectores defectuosos y recuperar la información legible, seleccionamos la casilla de verificación Examinar e intentar recuperar los sectores defectuosos y, a continuación, pulsamos el botón Iniciar.

4.6. PROGRAMADOR DE TAREAS.

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 no se inició sesión como administrador, sólo se pueden cambiar las configuraciones que se apliquen a su cuenta de usuario.



Podemos acceder a esta herramienta desde **Panel de control > Sistema y seguridad > Herramientas administrativas > Programador de tareas** y para programar una tarea realizaremos los siguientes pasos:

Hacemos clic en el menú **Acción** y luego en **Crear tarea básica...**

Escribimos un **nombre** para la tarea y, si queremos, una **descripción** y pulsamos el botón **Siguiente**.



Realizamos una de estas acciones:

Para seleccionar una programación basándose en el calendario, marcamos **Diariamente**, **Semanalmente**, **Mensualmente** o **Una vez**, pulsamos el botón **Siguiente**, especificamos la programación que queremos usar y pulsamos el botón **Siguiente**.

Para seleccionar una programación basándose en eventos repetitivos, marcamos **Al iniciarse el equipo** o **Al iniciar sesión** y, a continuación, pulsamos el botón **Siguiente**.

Para seleccionar una programación basándose en eventos específicos, marcamos **Cuando se registre un evento específico**, pulsamos el botón **Siguiente**, especificamos el registro de eventos y otros datos mediante las listas desplegables y, a continuación pulsamos el botón **Siguiente**.

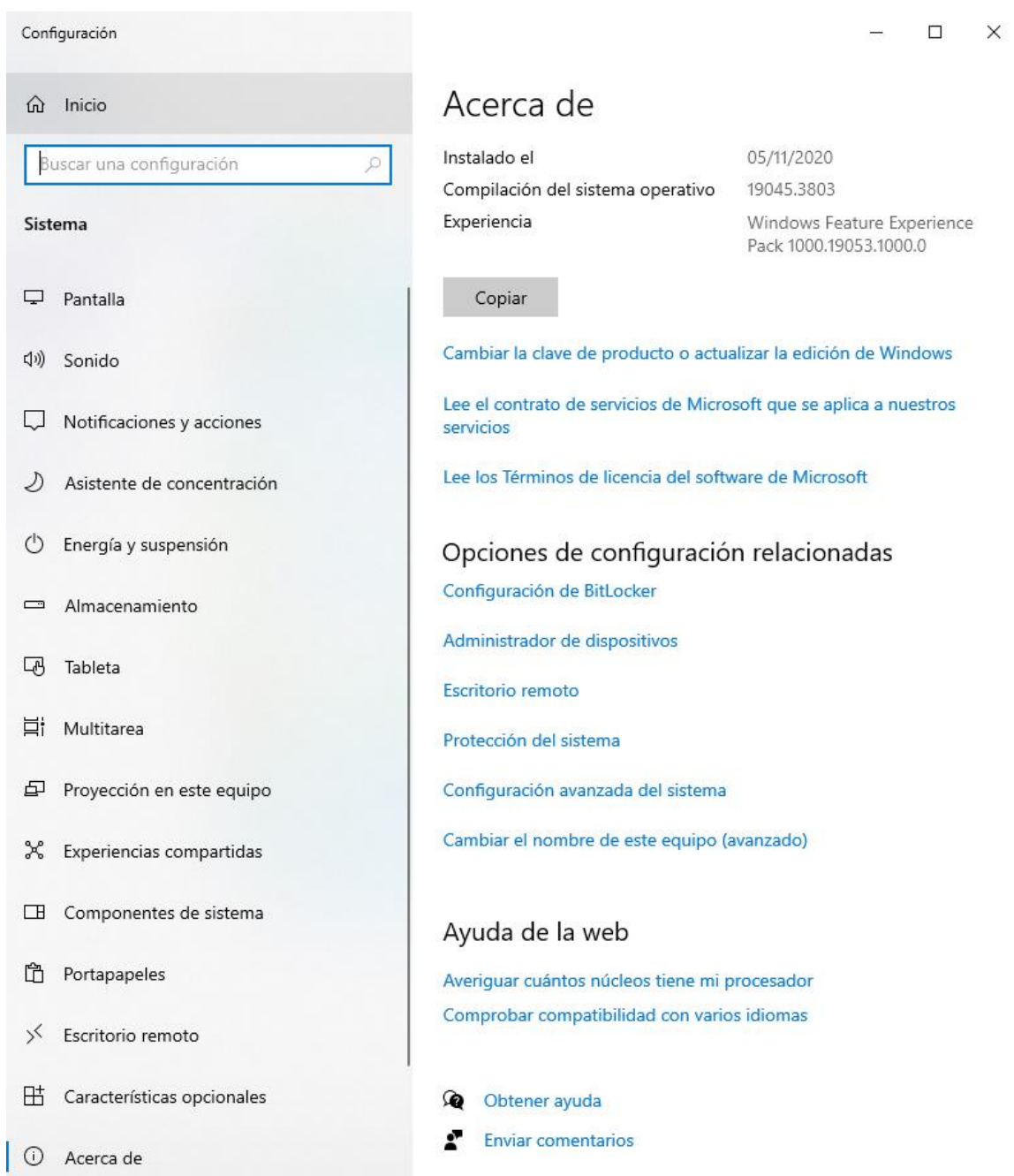
Para programar que una aplicación se inicie automáticamente, marcamos **Iniciar un programa** y pulsamos el botón **Siguiente**.

Pulsamos el botón **Examinar** para buscar el programa que queremos iniciar y después pulsamos el botón **Siguiente**.

Pulsamos el botón **Finalizar**.

4.7. 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 10 accederemos a Panel de control > Sistema y seguridad > Sistema y seguiremos estos pasos:

- Hacemos clic en Protección del sistema, ubicado en el panel central.
- Seleccionamos la unidad del sistema.
- Pulsamos el botón Configurar.

- Marcamos la casilla Activar protección del sistema y pulsamos el botón Aceptar.
- Pulsamos el botón Crear.
- Escribimos un nombre para el punto de restauración en la casilla de texto y pulsamos el botón Crear.

Cuando termine la creación del punto, se mostrará un mensaje indicando que el punto de restauración se creó satisfactoriamente. Podemos verificar que el punto se ha creado correctamente, pulsando el botón Restaurar sistema y a continuación el botón Siguiente, 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.

4.8. 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. 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.

Existen multitud de programas para hacer copias de seguridad que permiten la planificación y programación de copias para automatizar el proceso. Windows 10 permite hacer copias de seguridad de archivos a través de la herramienta Copia de seguridad.

Para hacer una copia de seguridad:

- Accedemos a la herramienta Copia de seguridad desde Inicio > Configuración > Actualización y seguridad y pulsamos en Copia de seguridad.
- Pulsamos en Agregar una unidad y elegimos una unidad externa o una ubicación de red para las copias de seguridad.
- Para cambiar los archivos de los que se va a realizar la copia de seguridad y la frecuencia de las copias de seguridad, pulsamos Más opciones.
- Para restaurar una copia de seguridad:
- Escribimos "restaurar archivos" en el cuadro de búsqueda y seleccionamos Restaurar los archivos con Historial de archivos.
- Buscamos el archivo que necesitamos y usamos las flechas para ver todas sus versiones. Cuando encontremos la versión que queremos, seleccionamos el botón Restaurar para guardarla en su ubicación original. Para guardarla en un lugar diferente, hacemos clic con el botón derecho (o mantén presionado) el botón Restaurar, seleccionamos Restaurar en y luego elegimos una nueva ubicación.

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 cortafuego 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, 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 podemos hacer es instalar un antivirus para el pendrive. Algunos ejemplos son:

- Antivirus ClamWin para Pendrive, una "PortableApp"
- 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.



Sistemas informáticos

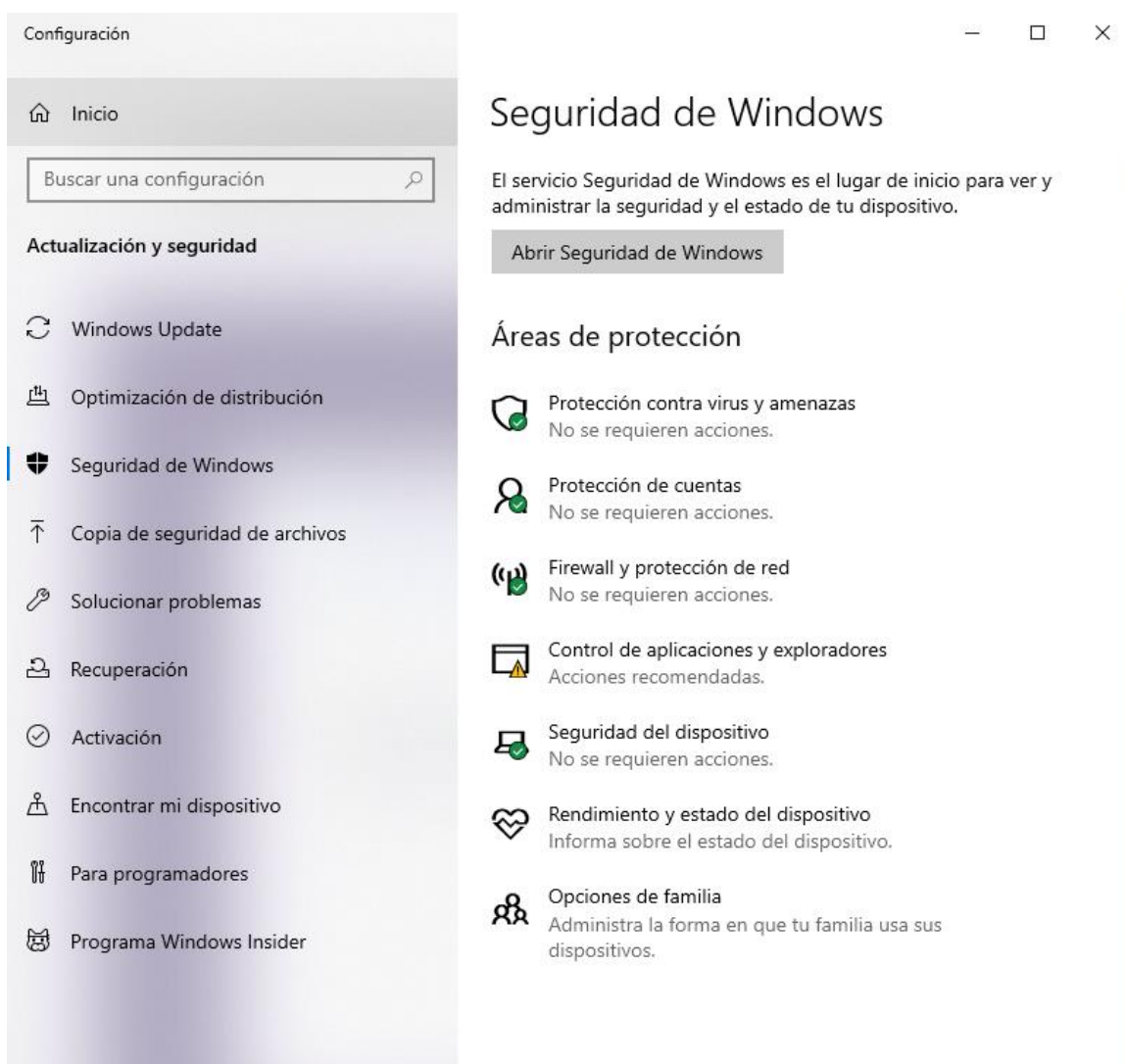
Programas complementarios, como Firewalls, antispys, etc. aunque varios antivirus de pago ya poseen estos complementos incorporados.

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 antispys 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 antispys 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 antispys para proteger la seguridad de tu equipo.

Para acceder a Windows Defender hay dos opciones: escribir en el cuadro de búsqueda "seguridad de windows" o ir a **Inicio > Configuración > Actualización y seguridad** y pulsar en **Seguridad de Windows**.



Se pueden realizar los siguientes tipos de análisis:

- **Rápido:** Si sospechas que el equipo puede tener algún spyware. Analiza todas las unidades que comúnmente son infectadas por spyware.
- **Completo:** Analiza todos los archivos y programas en ejecución del disco duro. Puede ralentizar el rendimiento del equipo.
- **Personalizado:** Se seleccionan los archivos y las unidades a analizar.
- **Sin conexión:** Para aquel software malintencionado que puede ser particularmente difícil de quitar del equipo.
- Finalizado el análisis se obtienen estadísticas del mismo.



Sistemas informáticos

Windows Defender también permite actualizarse para detectar nuevas amenazas.

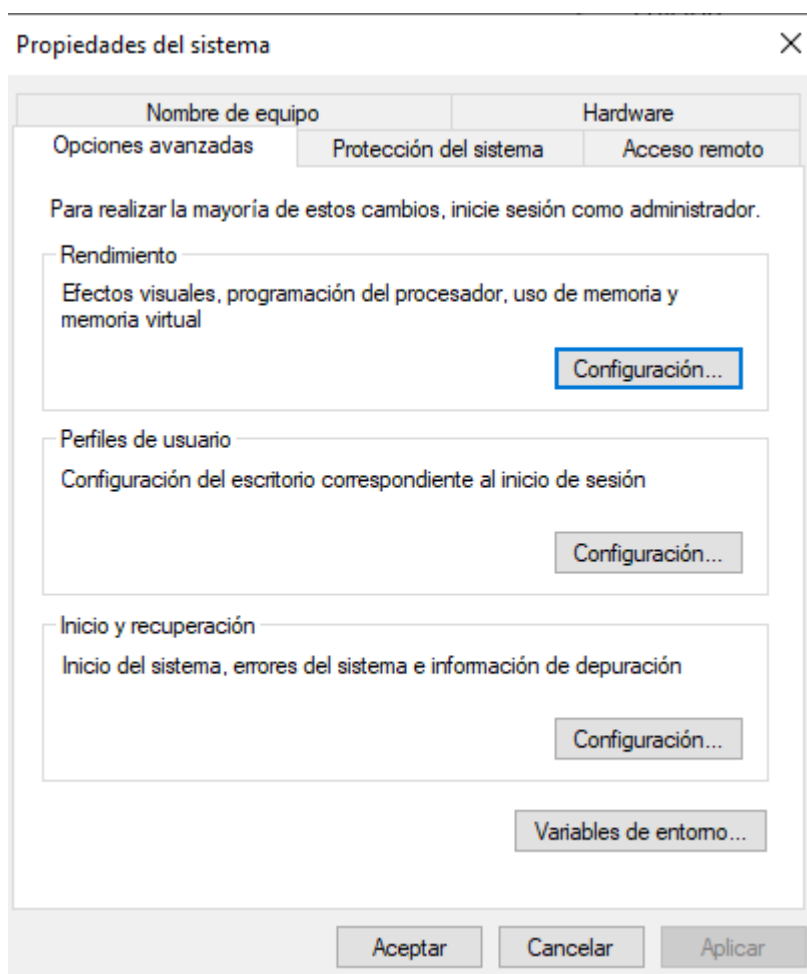
Se recomienda realizar un análisis rápido diario

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) accederemos a Panel de control > Sistema y seguridad > Sistema y seguiremos estos pasos:

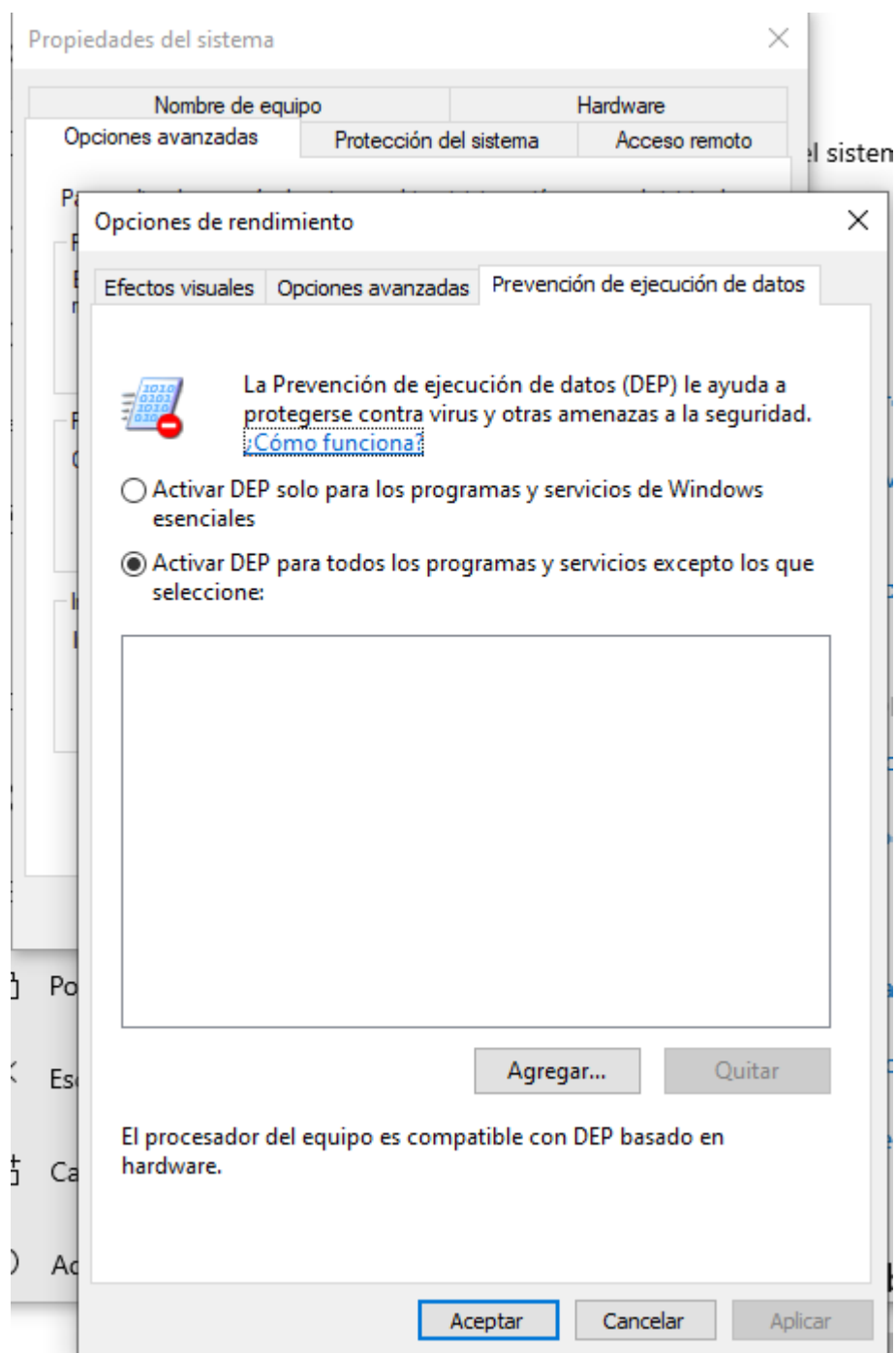
Hacemos clic en Configuración avanzada del sistema en el panel central.



En la pestaña Opciones avanzadas, en Rendimiento pulsamos el botón Configuración...

En la pestaña Prevención de ejecución de datos, seleccionamos Activar DEP para todos los programas y servicios excepto los que seleccione. También se puede activar DEP sólo para los programas y servicios de Windows esenciales.

Para desactivar DEP para un programa concreto seleccionamos la casilla del programa y aceptamos los cambios. Si el programa no aparece en el recuadro, pulsamos el botón Agregar..., buscamos en la carpeta C:\Archivos de programa (x86), localizamos el archivo ejecutable del programa, y, por último, pulsamos el botón Abrir.



5.4. SISTEMA DE CIFRADO DE ARCHIVOS (EFS).

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:

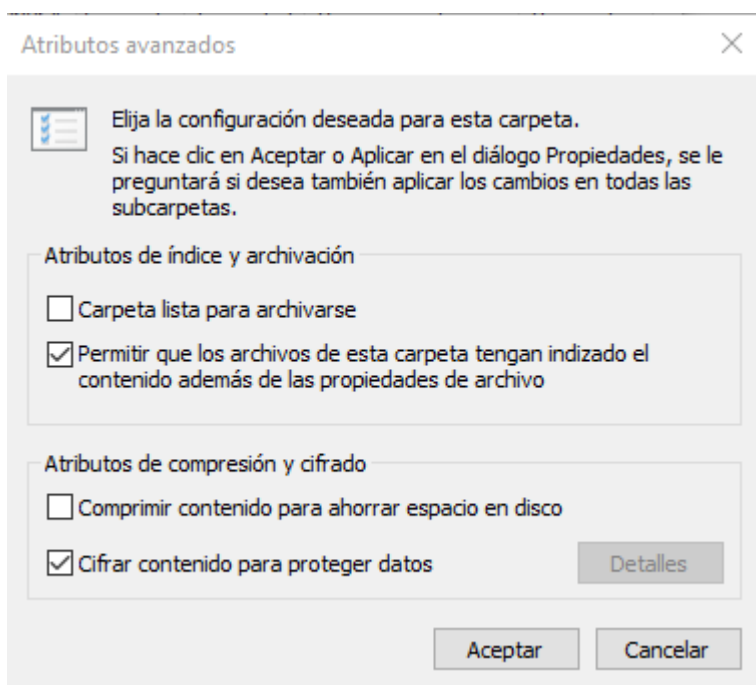
- El cifrado es sencillo. Se realiza activando una casilla en las propiedades del archivo o de la carpeta.
- El usuario controla quién puede leer los archivos.
- Los archivos se cifran cuando los cierra, pero cuando los abres quedan automáticamente listos para su uso.
- Si se cambia de idea con respecto 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 10.

Para cifrar archivos o carpetas con EFS seguiremos los siguientes pasos:

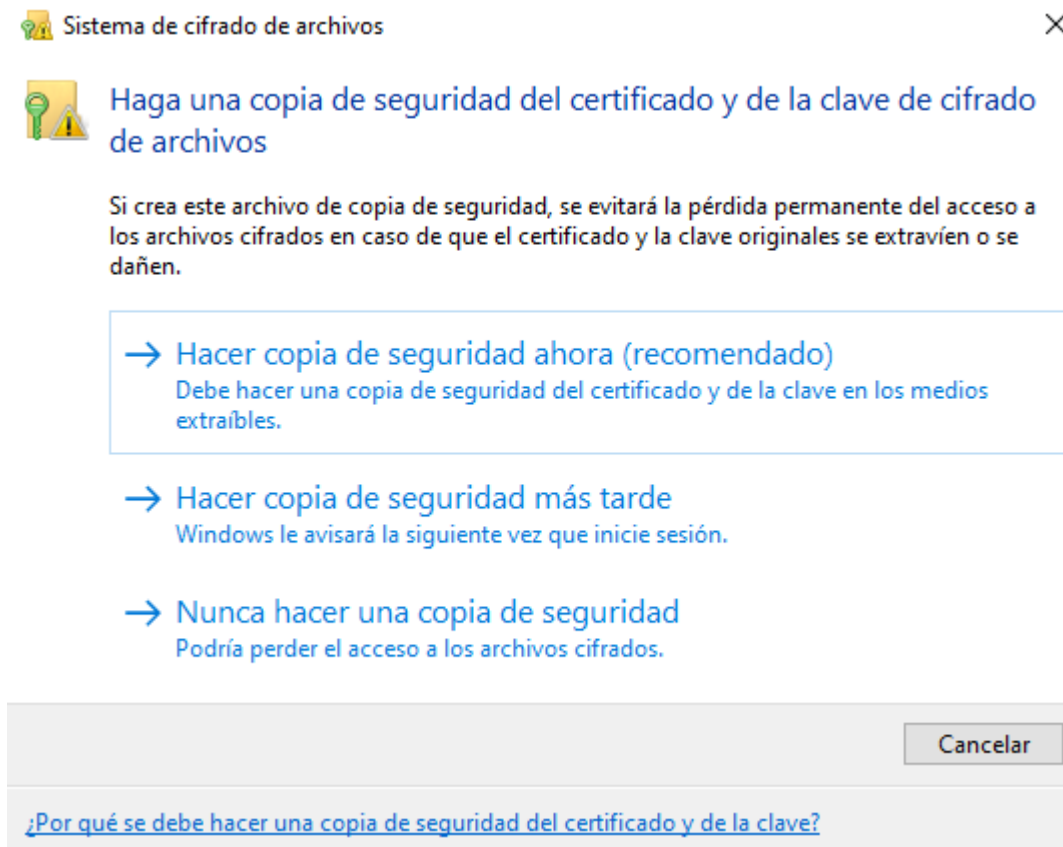
En el Explorador de archivos hacemos clic con el botón derecho del ratón sobre el archivo o carpeta que queremos cifrar y pulsamos en Propiedades.

En la pestaña General pulsamos el botón Avanzadas... u Opciones avanzadas... en el caso de que sea una carpeta.

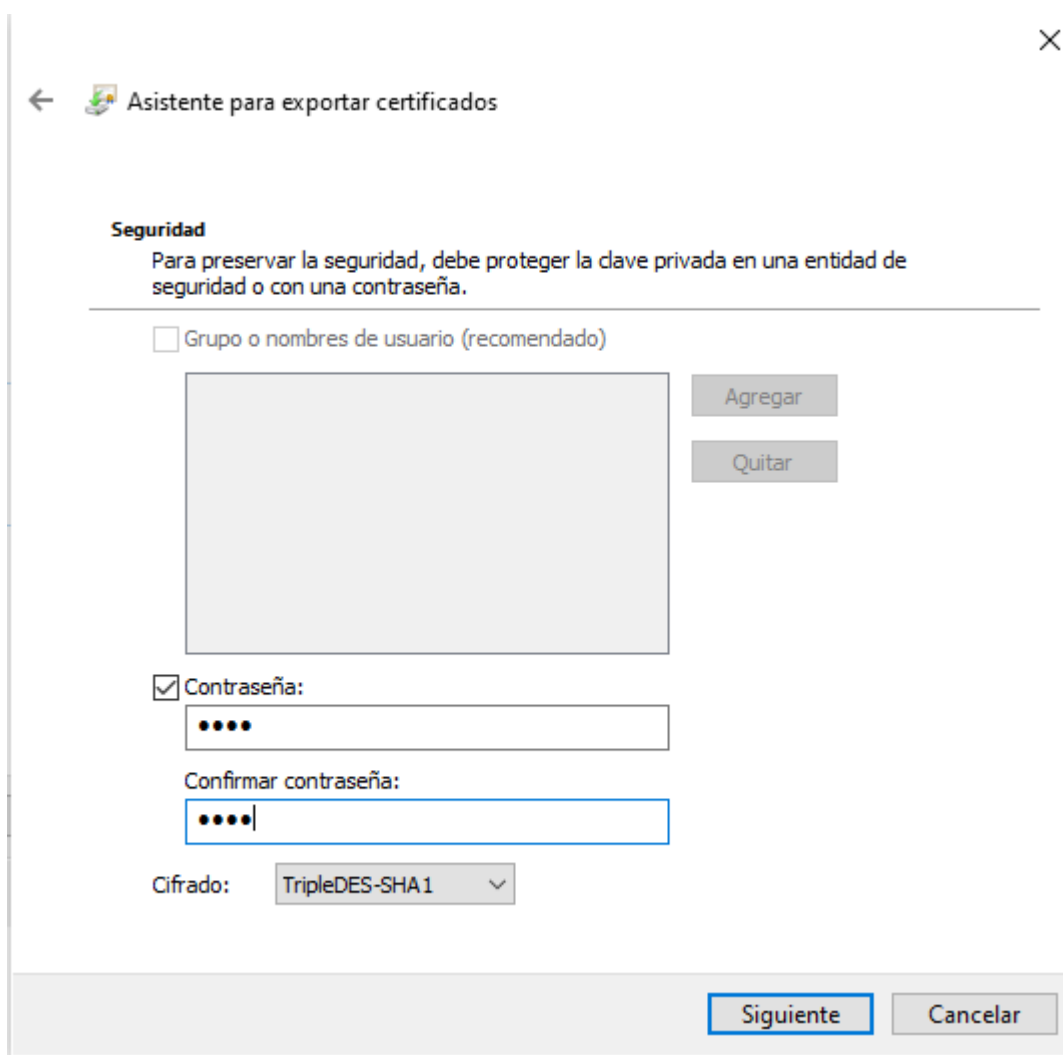
Marcamos la casilla Cifrar contenido para proteger datos y pulsamos el botón Aceptar.



A continuación, nos solicita que se haga una copia de seguridad de la clave de cifrado de archivos.



Si ciframos datos en el equipo, necesitamos 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 tenemos ningún medio de recuperar los datos, éstos se perderán. También perderemos los datos si almacenamos la clave de cifrado en una tarjeta inteligente y ésta se daña o se pierde. Para asegurarse de que siempre tendremos acceso a los datos cifrados, debemos hacer una copia de seguridad de la clave de cifrado y del certificado de cifrado. Si hay más de una persona que usa nuestro equipo, o si usamos una tarjeta inteligente para cifrar archivos, debemos crear un certificado de recuperación de archivos.

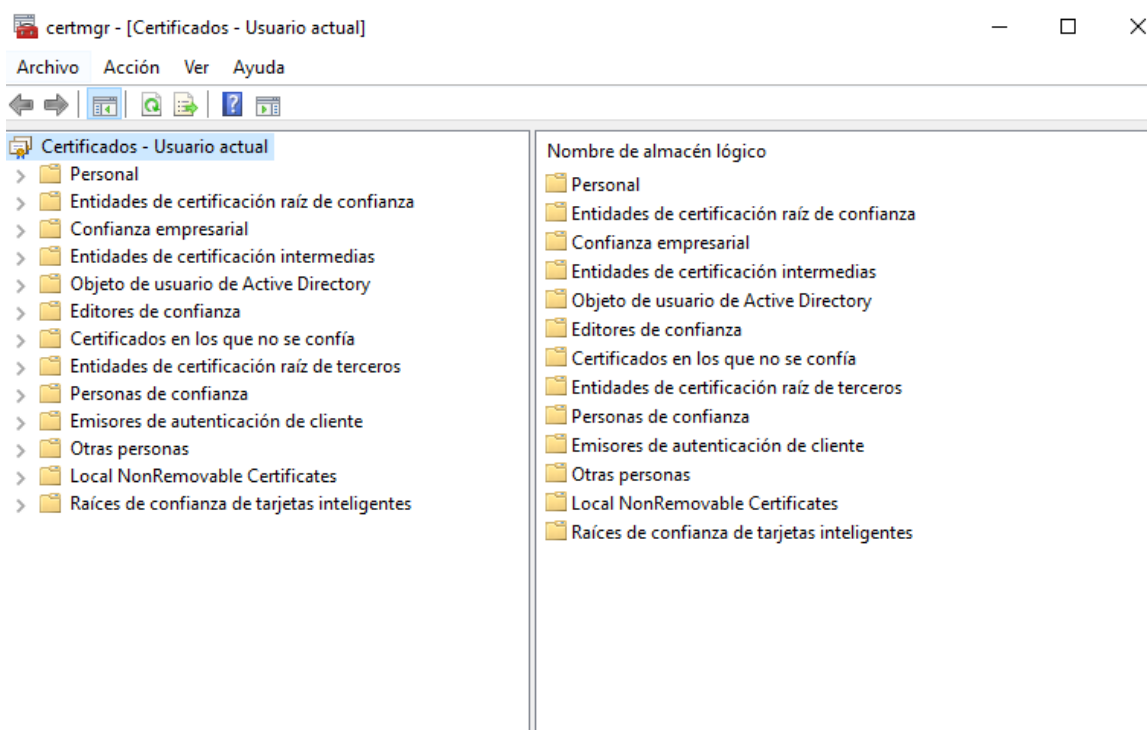


Finalmente, se genera un certificado del que deberemos hacer copia de seguridad, preferiblemente en un medio extraíble.

5.4.1. Certificados EFS.

Para hacer una copia de un certificado EFS del equipo seguiremos los siguientes pasos:

Abrimos el Administrador de certificados escribiendo "**certmgr.msc**" en el cuadro de búsqueda. Si nos solicita una contraseña de administrador o una confirmación, escribimos la contraseña o proporcionamos la confirmación.



Muestra la consola de gestión de certificados (Windows EFS) aparece en el bloque de Certificados-Usuario actual y colgando de él los contenedores: Personal, Entidades de certificación raíz de confianza, Confianza empresarial, Entidades de certificación intermedias, entre otros.

En el panel izquierdo, hacemos doble clic en Personal.

Hacemos clic en Certificados.

En el panel principal, seleccionamos el certificado del que queremos hacer una copia y en él debe aparecer el texto "Sistema de cifrado de archivos" en Propósitos planteados.

En el menú Acción, en Todas las tareas hacemos clic en Exportar...

En el Asistente para exportar certificados, pulsamos el botón Siguiente, después marcamos Exportar la clave privada y pulsamos el botón Siguiente.

Dejamos marcadas las opciones que aparecen por defecto y pulsamos el botón Siguiente.

Escribimos la contraseña que queremos usar, la confirmamos y pulsamos el botón Siguiente.

En el proceso de exportación se creará un archivo para almacenar el certificado. Escribimos el nombre y la ubicación de este archivo y pulsamos el botón Siguiente.

Pulsamos el botón Finalizar.

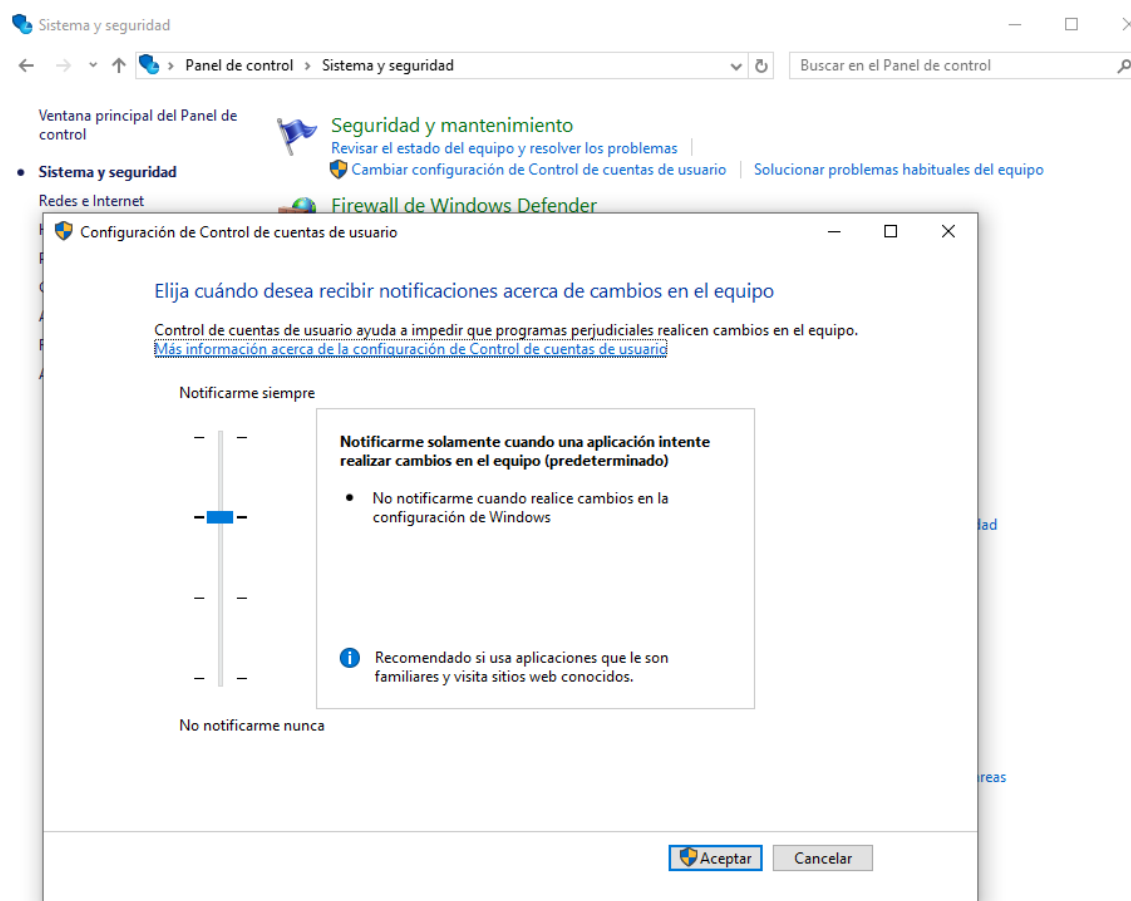
Si por cualquier motivo tuviéramos que recuperar la clave privada, realizaríamos el proceso contrario, importaríamos el certificado al equipo en cuestión.

Anexo I.- UAC 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 – Seguridad y mantenimiento – 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:

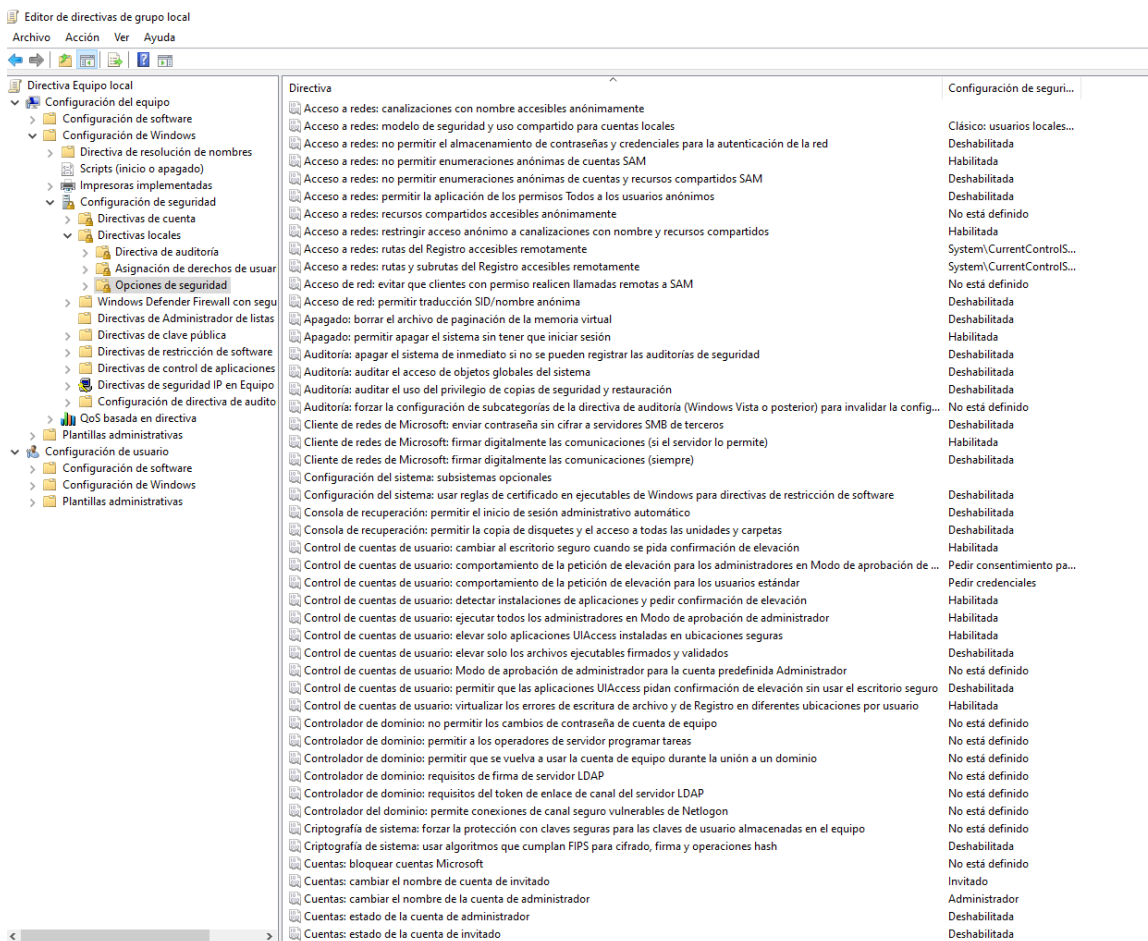
- **Notificarme siempre cuando:**
 - Un programa intente instalar software o realizar cambios en el equipo.
 - Realice cambios en la configuración de Windows.
- **Notificarme solamente cuando una aplicación intente realizar cambios en el equipo (predeterminado)**
 - No notificarme cuando realice cambios en la configuración de Windows.
- **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.
- **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.



Directiva	Configuración de seguridad
Acceso a redes: canalizaciones con nombre accesibles anónimamente	Clásico: usuarios locales...
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Deshabilitada
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Habilitada
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Deshabilitada
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Deshabilitada
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	No está definido
Acceso a redes: recursos compartidos accesibles anónimamente	Habilitada
Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	System\CurrentControlS...
Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlS...
Acceso a redes: rutas y subrutinas del Registro accesibles remotamente	No está definido
Acceso de red: evitar que clientes con permiso realicen llamadas remotas a SAM	Deshabilitada
Acceso de red: permitir traducción SID/nombre anónima	Deshabilitada
Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada
Apagado: permitir apagar el sistema sin tener que iniciar sesión	Deshabilitada
Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Deshabilitada
Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada
Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Deshabilitada
Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior) para invalidar la config...	No está definido
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Deshabilitada
Configuración del sistema: subsistemas opcionales	Deshabilitada
Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada
Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada
Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Habilitada
Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Pedir consentimiento pa...
Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de ...	Pedir credenciales
Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Habilitada
Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada
Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada
Control de cuentas de usuario: elevar solo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitada
Control de cuentas de usuario: elevar solo los archivos ejecutables firmados y validados	No está definido
Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Deshabilitada
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Habilitada
Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	No está definido
Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo	No está definido
Controlador de dominio: permitir a los operadores de servidor programar tareas	No está definido
Controlador de dominio: permitir que se vuelva a usar la cuenta de equipo durante la unión a un dominio	No está definido
Controlador de dominio: requisitos de firma de servidor LDAP	No está definido
Controlador de dominio: requisitos del token de enlace de canal del servidor LDAP	No está definido
Controlador del dominio: permite conexiones de canal seguro vulnerables de Netlogon	No está definido
Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	Deshabilitada
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	No está definido
Cuentas: bloquear cuentas Microsoft	Invitado
Cuentas: cambiar el nombre de cuenta de invitado	Administrador
Cuentas: cambiar el nombre de la cuenta de administrador	Deshabilitada
Cuentas: estado de la cuenta de administrador	Deshabilitada
Cuentas: estado de la cuenta de invitado	Deshabilitada

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.

Anexo II.- 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 **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.
5. Consejo: Hacer una copia de seguridad de todos los certificados EFS que haya.
6. Haz clic en el menú Acción, apunta a Todas las tareas y, a continuación, haz clic en Exportar.
7. En el Asistente para exportación de certificados, haz clic en Siguiente, después en Exportar la clave privada y, a continuación, en Siguiente.
8. Haz clic en Personal Information Exchange y, a continuación, en Siguiente.
9. Escribe la clave o contraseña que desees usar, confírmala y, a continuación, haz clic en Siguiente. En el proceso de exportación, se creará un archivo para almacenar el certificado.

10. 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.

11. 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.