# 4. Administración básica del sistema Windows

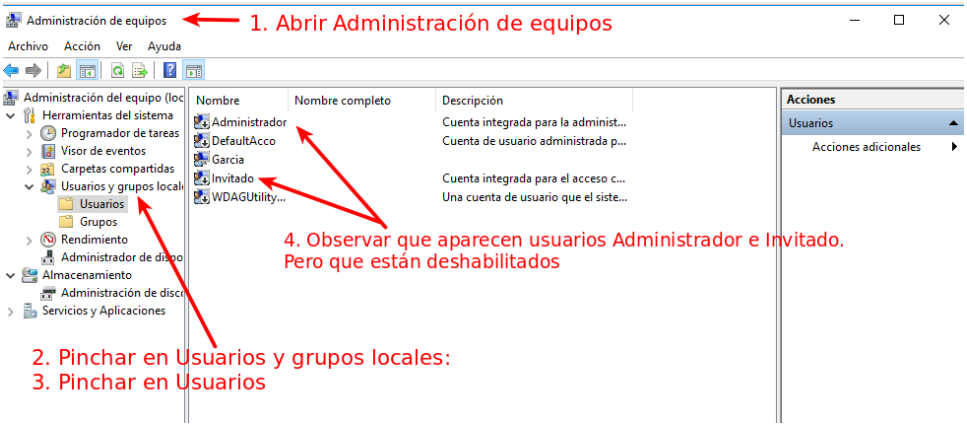
| | |
|---|---|
| Autor | Ⓧ Xerach Casanova |
| Clase | Sistemas Informáticos |
| Fecha | @Dec 20, 2020 11:29 PM |

# 1. Administración de usuarios y grupos

Las cuentas de usuario están pensadas para uso individual, mientras que los grupos administran a varios usuarios.

Windows tiene 2 programas gráficos para la administración de usuarios y grupos.

- **Cuentas de usuario** desde el Panel de Control
- **Usuarios y grupos desde Administración** de equipos (no incluido en las versiones Home, pero más completo).

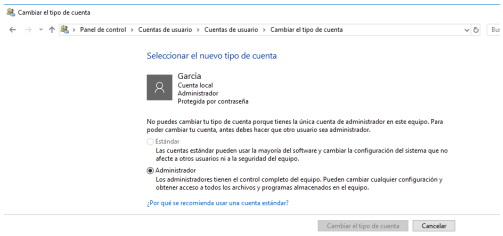



Windows crea cuentas de usuario integradas: Administrador e invitado, ambas deshabilitadas, pero se pueden habilitar, lo cual haría que cualquier persona ajena pueda iniciar sesión.

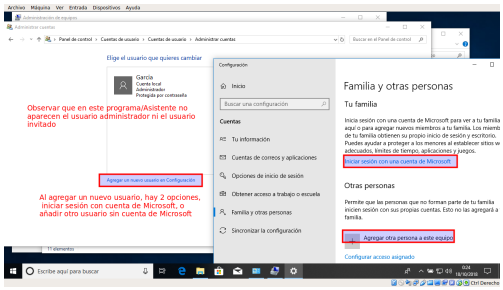
## 1.1. Cuentas de usuario en panel de control

Pulsando en cambiar tipo de cuenta se puede elegir:

- **Cuenta de usuario estándar:** privilegios limitados, se pueden usar la mayoría de programas, pero no se puede instalar ni descargar software/hardware, eliminar archivos de sistema o cambiar opciones de configuración que afecten a otros usuarios.




- **Cuenta de administrador.** Permite realizar cambios que afectan a todos los usuarios, configuración de seguridad, instalación de software/hardware y acceso a todos los archivos del equipo.




Para crear una cuenta de usuario:

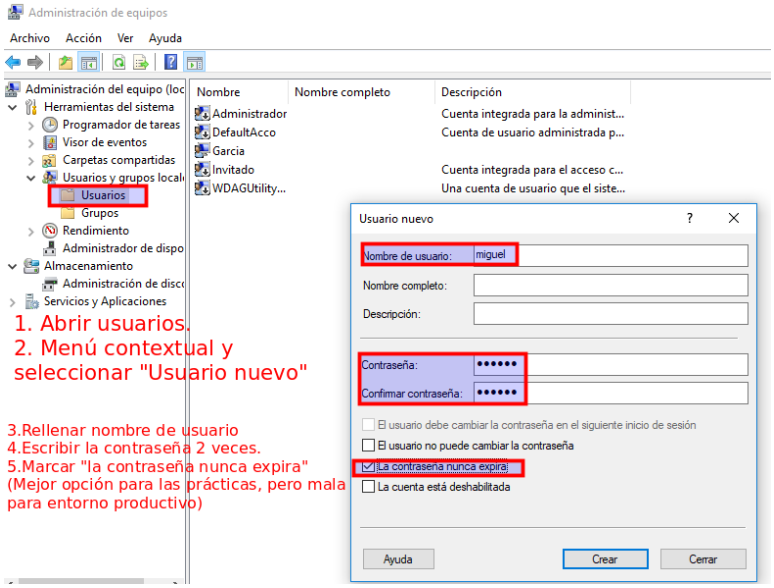
1. Hacer click en Administrar cuenta.
2. Crear cuenta nueva.
3. Escribir el nombre de la cuenta.
4. Seleccionar tipo de cuenta.

Al eliminar una cuenta de usuario se borra definitivamente y no se puede recuperar. Cuando se crea una cuenta con el mismo nombre de usuario el sistema genera una nueva con un SID distinto.

## 1.2. Usuarios y grupos desde Administración de equipos

También podemos abrir este programa ejecutando lusrmgr.msc

Para crear un usuario: Menú superior/Acción/Usuario nuevo.

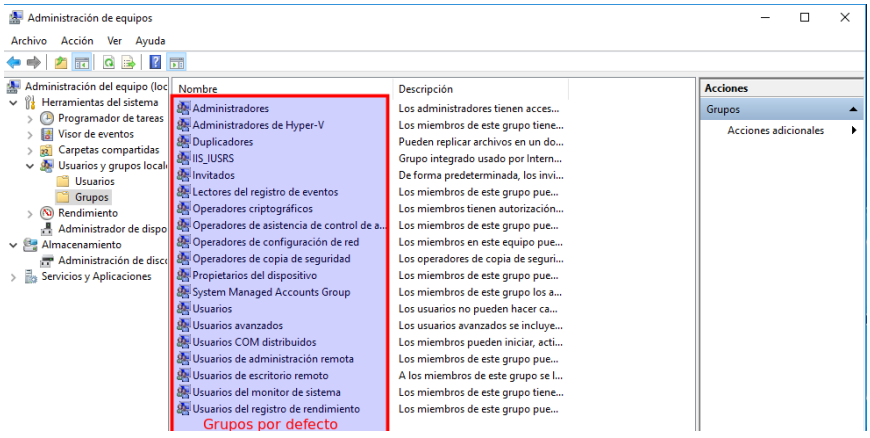



## Grupos en Windows

Simplifican la administración de cuentas de usuario, por ejemplo para compartir una carpeta.

Cuando se instala Windows también se crean varios grupos, se llaman cuentas integradas. Hay tres tipos de grupos:

- Creados por el administrador
- Grupos integrados (administradores, usuarios, usuarios avanzados...)
- Grupos de seguridad integrados o especiales.

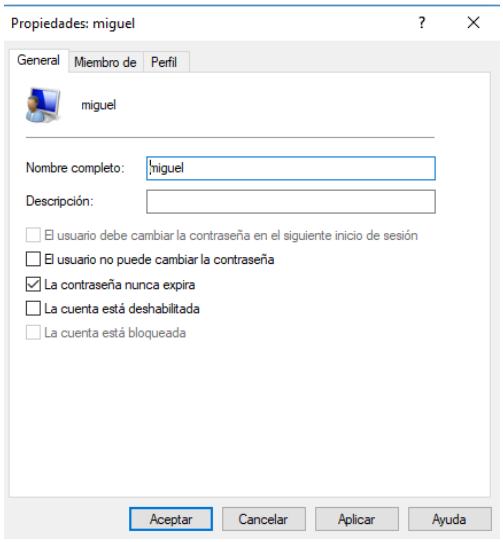



El nombre de los grupos sirve para entender su objetivo. Por ejemplo, los usuarios avanzados tienen privilegios para poder instalar aplicaciones.

## Cambiar nombre o contraseña de usuario

En el menú contextual de propiedades de usuario tenemos:

**Solapa "General"**

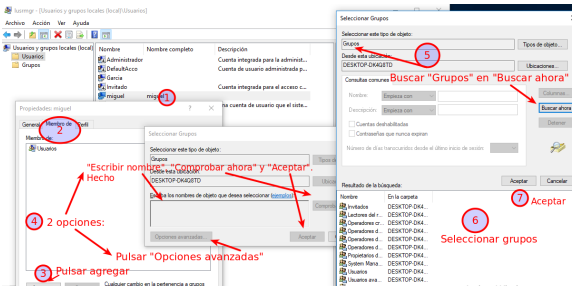



Se indica nombre de usuario y descripción y también opciones de contraseña:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca expira.
- Cuenta bloqueada/desbloqueada

A nivel profesional se recomienda al administrador cambiar la contraseña la primera vez, de esta forma nunca conocerá la contraseña del usuario.

**Solapa "Miembro de"**




Aquí se ven los grupos a los que pertenece el usuario. Se puede añadir o eliminar al usuario de los distintos grupos.

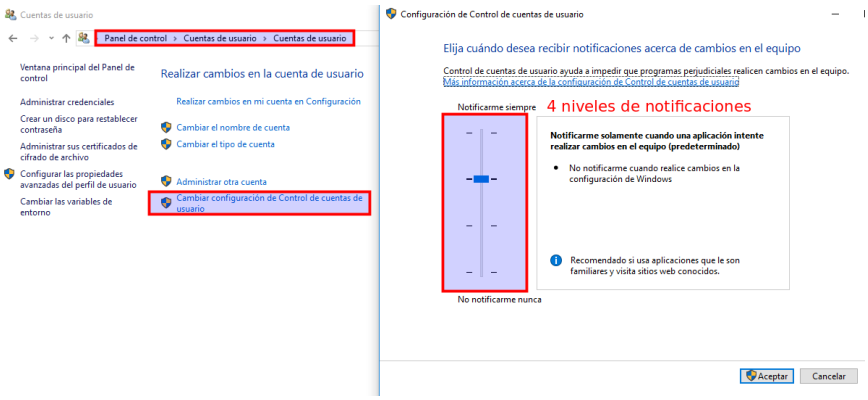
En el botón agregar se escribe directamente el nombre del grupo, pero se puede escoger el grupo de una lista en "Opciones avanzadas" / "Buscar ahora".

Al igual que con los usuarios, en la ventana grupos se pueden crear y eliminar grupos, además de quitar y añadir usuarios a ellos.

## 1.2. UAC (User Account Control, Control de Cuentas de Usuario).

Las alertas de seguridad de usuario cuando se realizan acciones en el sistema, las lanza el UAC.

Se pueden configurar los niveles de alerta desde el panel de cuentas de usuario:




# 2. Seguridad local. Permisos locales o NTFS

## 2.1. Solapa seguridad

La protección de los archivos a nivel local es posible con la **seguridad local** o **permisos locales**, pero la partición debe ser forzosamente NTFS.

En el menú "Propiedades de fichero o carpeta" aparecen 2 solapas distintas:

- Compartir, permisos para acceder desde la red.
- Seguridad: permisos para cuando accede otro usuario en el equipo local.

Si la partición es FAT32 se puede convertir en NTFS sin formatear con el comando: convert unidad: /fs:ntfs

### Primeras normas sobre permisos locales

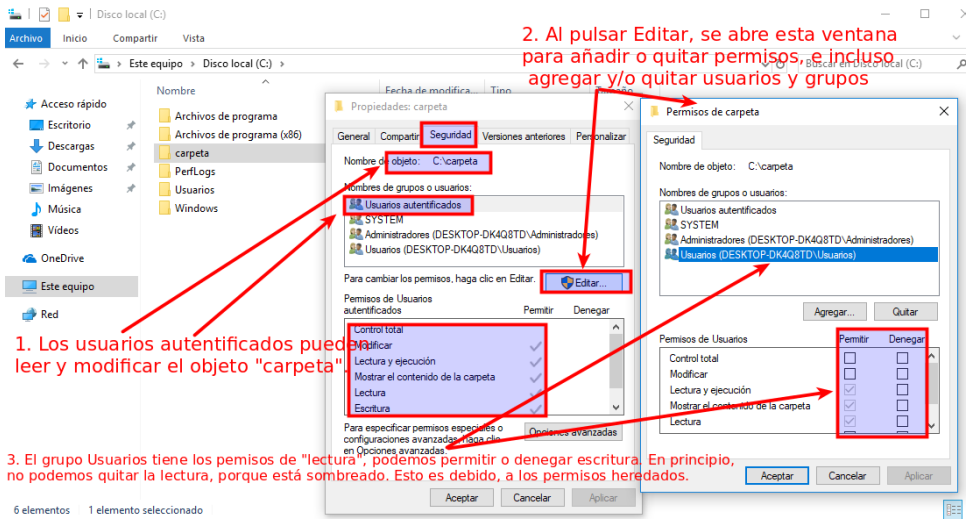
- Se pueden configurar para carpetas y ficheros (se habla de objetos).
- Los permisos se heredan de la carpeta padre por defecto.
- Los permisos se conceden a usuarios y grupos.
- El propietario de los objetos es quien los creó.
- El usuario propietario y los administradores son quienes pueden cambiar los permisos del objeto, pero se le puede dar permisos a cualquier usuario para hacerlo.

- Un administrador se puede convertir en propietario de cualquier objeto.

## 2.2. Modificar permisos estándar. Botón editar de la solapa de seguridad

Son 6 permisos para carpetas y 5 para archivos, en orden de menos a más permisos:

- **Mostrar el contenido de la carpeta.** Solo aparece en carpetas, permite ver los nombres de archivos y subcarpetas.
- **Lectura.** En carpetas permite mostrar el contenido de la carpeta, atributos propietarios y permisos. En archivos permite leer archivos y ver sus atributos, propietarios y permisos.
- **Lectura y ejecución.** Tiene permisos de lectura, además en carpetas permite navegar por ellas y en archivos permite ejecutar archivos ejecutables.
- **Escritura.** Tiene permisos de lectura y ejecución, además en carpetas permite crear archivos, subcarpetas y cambiar atributos. En archivos permite cambiar su contenido y cambiar atributos.
- **Modificar.** Incluye todos los de escritura y además, permite borrar carpetas y archivos.
- **Control total.** Incluye todos los de modificar y además, en carpeta permite borrar subcarpetas y archivos, cambiar atributos y propietarios, en archivos permite cambiar atributos y propietarios.



Estos permisos estándar se dividen en tres categorías:

**Lectura y ejecución:**

- Lectura y ejecución
- Mostrar contenido de la carpeta.

**Modificar, además de la lectura se conceden los permisos:**

- Modificar
- Escritura

**Si queremos control total:**

- Se conceden todos, salvo permisos especiales.

Con control total, un usuario podrá eliminar cualquier subcarpeta o sus archivos, incluso si le denegamos permiso de escritura en esa subcarpeta.

## Cómo calcular permisos de un objeto

Para configurar permisos se puede: permitir, denegar, no marcar opción.

Si un usuario pertenece a varios grupos:

- **Regla 1:** se mira el permiso que tiene el usuario y los grupos a los que pertenece, si alguno de ellos tiene denegado el permiso, la denegación manda.
- **Regla 2:** si no hay denegación se miran los permisos al usuario y sus grupos, el usuario tendrá el máximo de permisos permitidos.

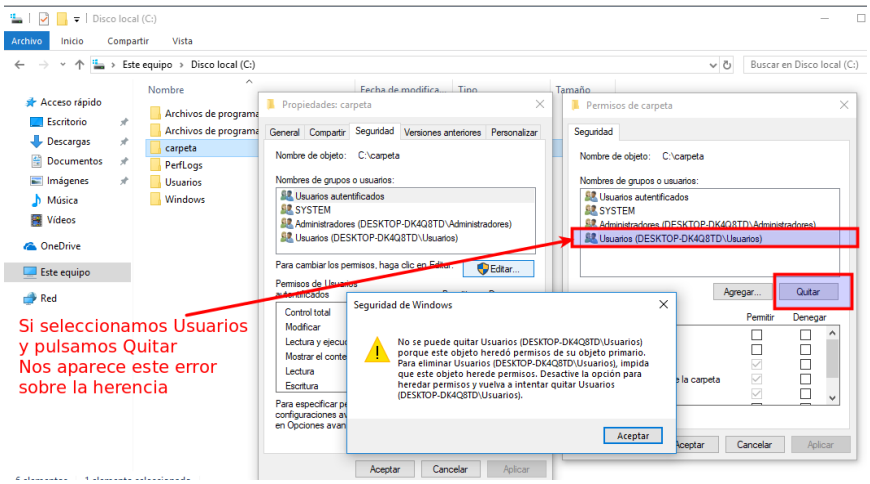
  Ejemplo:

  - Supongamos que juan pertenece a los grupos contabilidad e informatica. Y que los permisos configurados corresponden a:Juan tiene concedida lectura en la carpeta apuntesEl grupo contabilidad tiene denegada la lecturaEl grupo informatica tiene permiso escritura en la carpeta apuntes¿Cuáles son los permisos?Respuesta: el usuario no tiene ningún permiso, pues el grupo contabilidad al que pertenece tiene denegada la lectura.
  - ¿Qué habría cambiado en ejemplo 1, si el grupo contabilidad no tiene permisos aceptados ni denegados en la carpeta apuntes.¿Cuáles son los permisos?Respuesta: el usuario juan tendría permiso escritura. Pues no hay ninguna denegación, por lo que se mira el máximo de permisos,

juan solo tiene lectura, pero su grupo informatica tiene escritura, por lo que juan tendrá permisos de escritura.

### Herencia

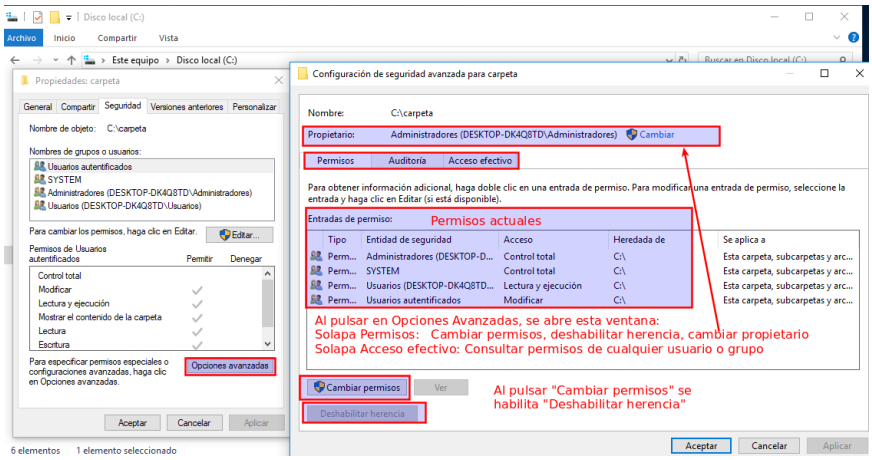
La herencia de permisos está habilitada por defecto. Esto genera problemas a la hora de quitar usuarios que tienen permisos o desmarcar permisos que aparecen sombreados. Para estos casos se puede deshabilitar la herencia.




## 2.3. Botón opciones avanzadas en solapa de seguridad

En las opciones avanzadas de seguridad podemos:

- Deshabilitar/habilitar la herencia.
- Cambiar los permisos de cualquier grupo o usuario.
- Conocer y cambiar al propietario del objeto.
- Contultar permisos efectivos de un objeto concreto.



## Quitar herencia a un objeto

Si pulsamos en deshabilitar herencia, se abre una ventana emergente en la que tenemos dos opciones:

- **Convertir permisos heredados en permisos explícitos.** Quitamos la herencia pero no eliminamos ningún permiso heredado. Recomendado.
- **Quitar todos los permisos heredados.** Quitamos la herencia y eliminamos los permisos heredados del objeto.

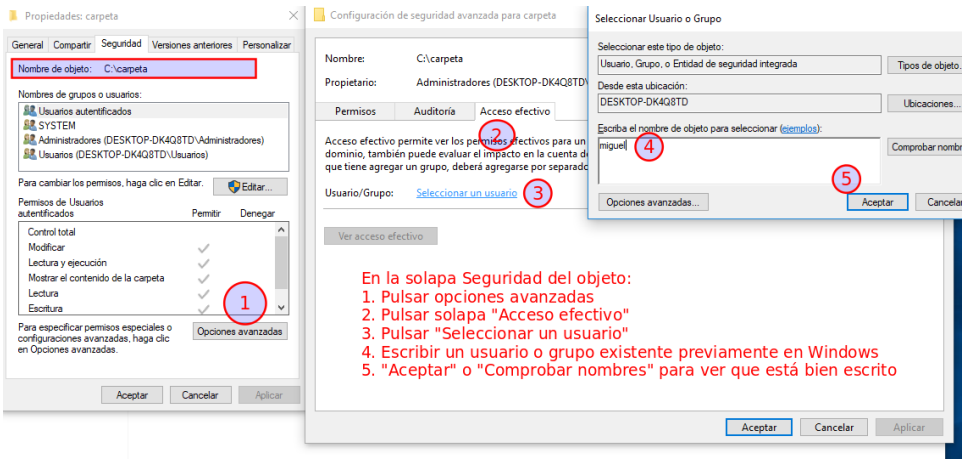
## Permisos especiales en "Opciones avanzadas"

También se pueden modificar permisos pulsando en opciones avanzadas. Son permisos distintos. En vez de 6, hay 13.

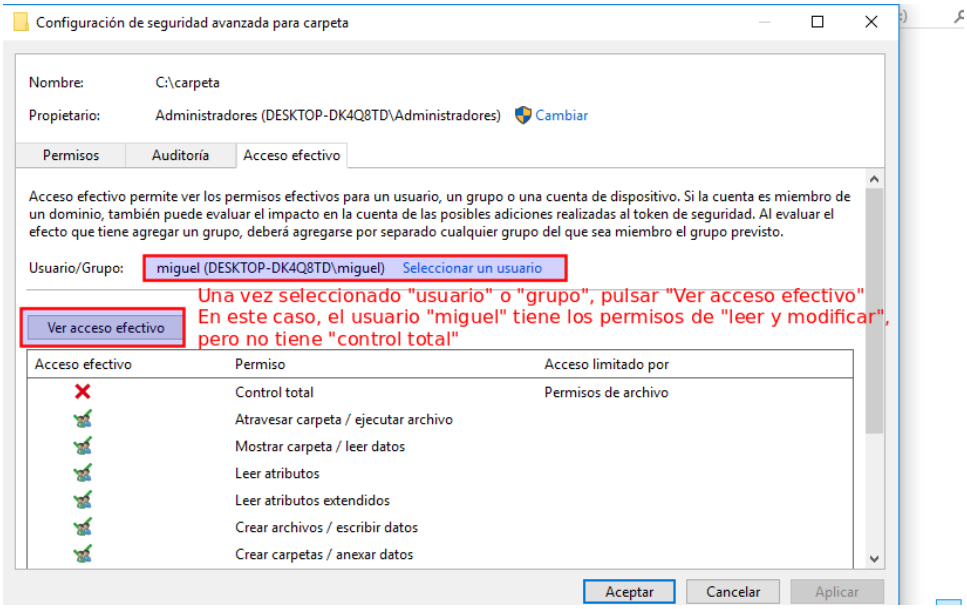
El permiso estándar lectura equivale  a "leer datos", "leer atributos", "leer permisos" y "leer atributos extendidos".

## Solapa "Acceso efectivo" en "Opciones avanzadas"

Sirve para ver los permisos concretos de un usuario o grupo en una carpeta o archivo, no se puede cambiar ningún permiso en esta solapa.




Esta solapa sirve para averiguar los permisos concretos que tiene un usuario o grupo. Se  pulsa en seleccionar para buscar un usuario o grupo y nos devuelve los permisos de ese objeto para ese usuario.




# 3. Registro de Windows. Directivas de grupo y seguridad local

A través de las consolas de directivas de seguridad local y directivas de grupo local se puede gestionar de forma centralizada la configuración de seguridad del sistema.

Las directivas de seguridad local aplican distintas restricciones sobre cuentas de usuario y contraseña. Las directivas de grupo local, nos permiten configurar equipos de forma local o remota, instalar o eliminar aplicaciones, restringir derechos de usuario, etc...

## 3.1. Registro de windows

El registro tiene todo el historial desde que instalamos el S.O. Al instalar y desinstalar un programa se quedan escritas las dos cosas, aunque la carpeta se haya eliminado. Por este motivo el registro de Windows cada vez se hace más grande y por ese motivo tarda más en arrancar.

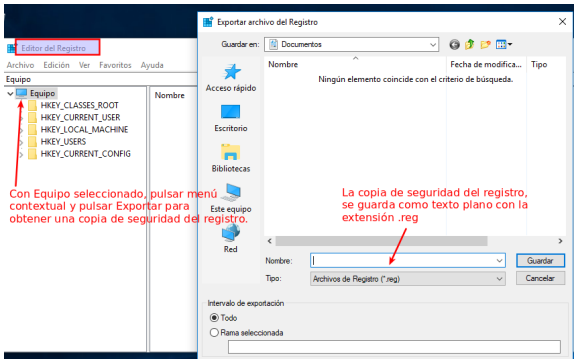
Aunque es recomendable no tocarlo existen situaciones en las que se hace necesario:

- Si un programa se instala pero no termina de hacerlo, es posible que posteriormente no deje instalarse porque ya se instaló y tampoco se pueda desinstalar porque no está instalado.

- Los virus tocan valores de registro. Aunque elimines el virus, puede que el registro no vuelva a su valor original.

### Ejecución del editor de registro y copia de seguridad

Para ello se utiliza el programa regedit.  Antes de modificar un valor de registro se debe realizar una copia de seguridad. Para ello, dejando seleccionado el total del equipo seleccionamos archivo/exportar. Esto generará un fichero de texto de extensión .reg con el contenido del registro.



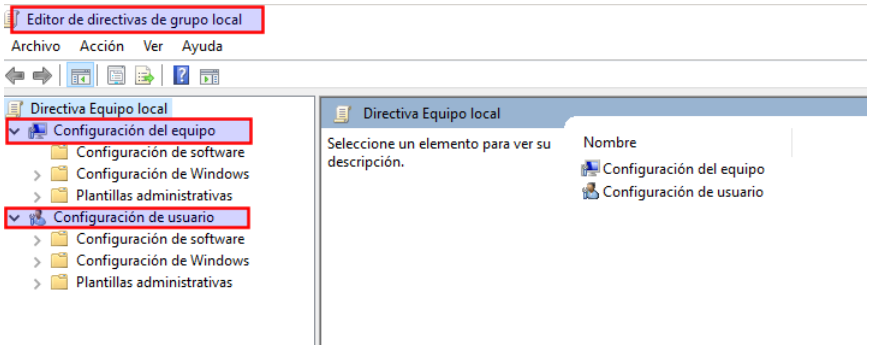

### Limpiadores de registro

Son programas cuyo fin es borrar las entradas innecesarias y corregir valores erróneos: RegClean, CCCleaner, Regseeker... La mayoría es software privativo. Por ejemplo: Regseeker, el cual tiene opción de Auto Clean e incluso desinstalación de aplicaciones, útil para aplicaciones que no tienen "desinstalador" o que no se pueden desinstalar desde "agregar o quitar programas".

## 3.2. Directivas de grupo o política local

El editor de directivas de grupo local se ejecuta con el programa gpedit.msc como administrador. Podemos:

- Modificar políticas o directivas como deshabilitar el administrador de equipos, configuración de red, obligar a un fondo de escritorio, etc...
- Asignar archivos ejecutables o scripts, que se ejecutan cuando la máquina se enciende, se apaga, se inicia sesión con un usuario o se cierra sesión.
- Especificar opciones especiales de seguridad.




En directivas locales es prácticamente indistinto trabajar con configuración de equipo y de usuario. En caso de conflicto, la configuración de equipo tiene preferencia. Cada directiva tiene 3 posibles valores:

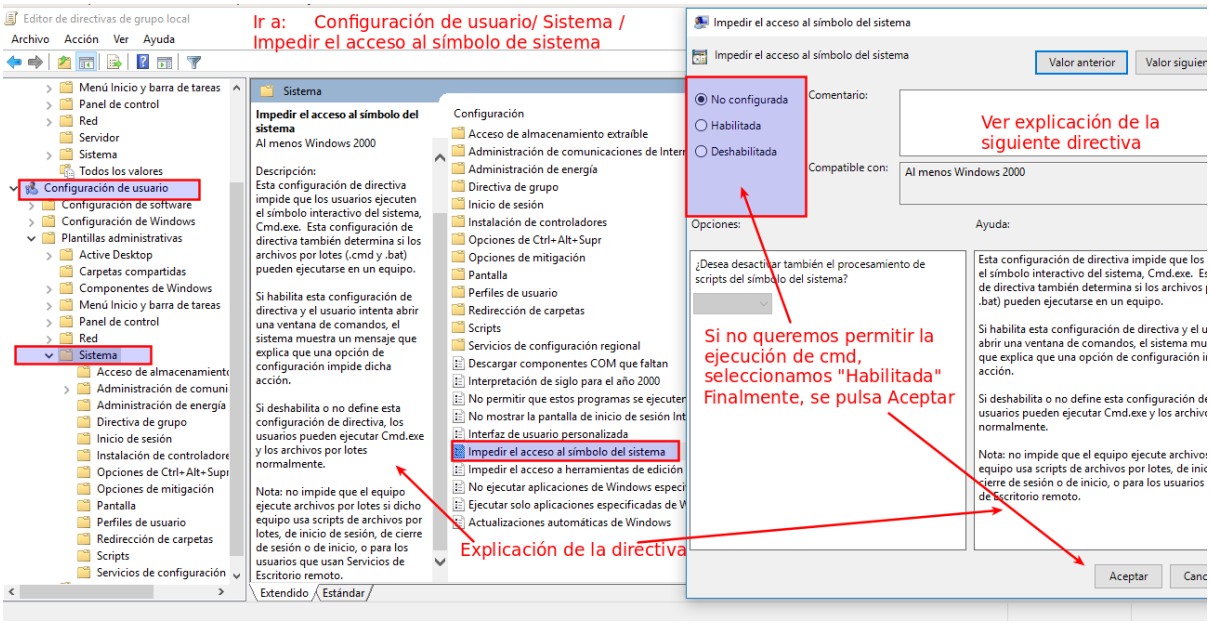
- No configurar la directiva. Se comporta según el criterio por defecto de la directiva.
- Habilitarla, con la que la pondremos en marcha en el sistema.
- Deshabilitarla. Con la que impediremos que se ponga en macha.

**Ejemplo:**

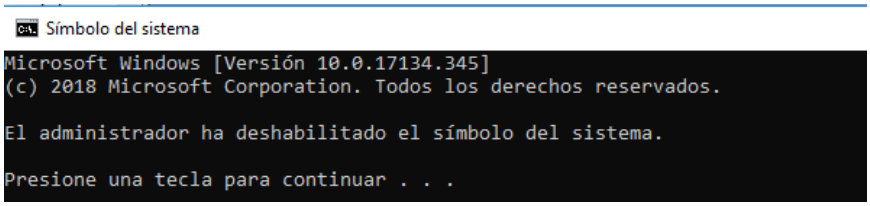
**Deshabilitar la ejecución de una ventana de símbolo de sistema (cmd.exe).**

Los pasos son:

- Abrir gpedit.msc
- Seleccionar Configuración de usuario / Símbolo / Impedir el acceso al símbolo del sistema
- Leer la descripción para entender la directiva
- Seleccionar la opción “Habilitada”.
- Pulsar Aceptar




Una vez deshabilitado cmd, si el usuario intenta abrir la consola de comandos, se muestra el mensaje de error que se muestra a continuación.




## 3.3. Directivas de seguridad local

Con ellas se aplican distintas restricciones de seguridad sobre cuentas de usuario y contraseña.

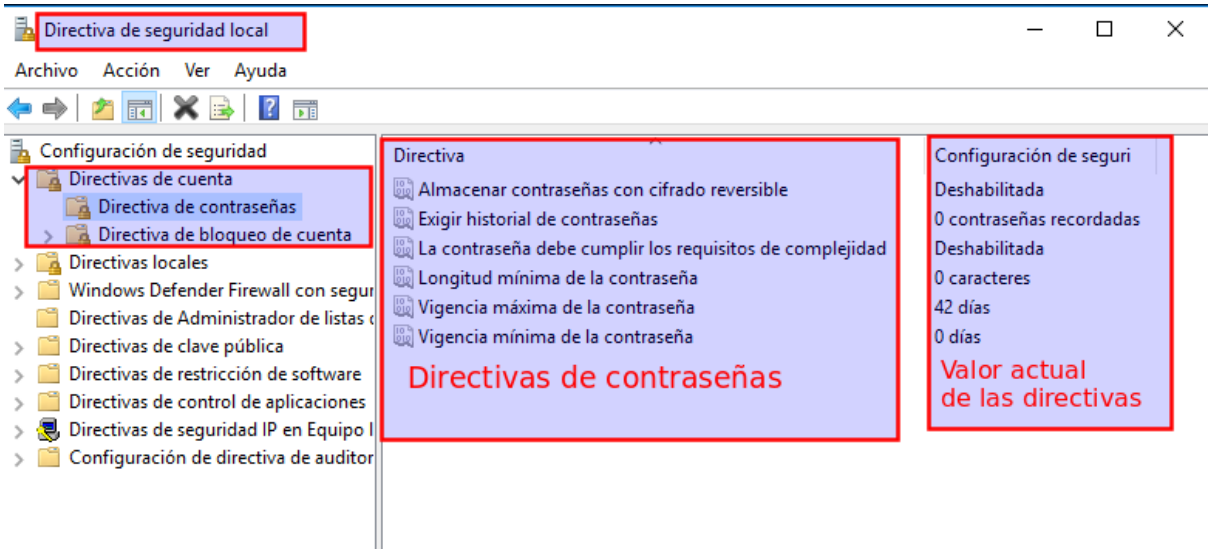
Las tres formas de ejecutarla son:

- Ejecutando SecPol.msc
- Abrir directamente directiva de seguridad local
- Forman parte de las directivas de grupo, así que también hay acceso desde gpedit.msc (ir a configuración de equipo / configuración de Windows / Configuración de seguridad / Directiva de seguridad / Directivas de cuenta

En las directivas de cuenta hay dos tipos de directiva.

### Directivas de contraseña

Se accede a ellas a través de directivas de cuenta - directivas de contraseña




Las configuraciones más útiles son:

- Exigir el historial de contraseñas. El usuario no podrá cambiar su contraseña por otra usada anteriormente. Aparece configurado a 0. El número que pongamos es el número de las últimas contraseñas que no podrán repetirse.
- Las contraseñas deben cumplir requerimientos de complejidad. Obliga a que las contraseñas cumplan con ciertos requerimientos.
- Longitud mínima de la contraseña. Indica los caracteres mínimos que deben tener.
- Vigencia máxima de la contraseña. Las contraseñas caducan y dejan de ser válidas.
- Vigencia minima de la contraseña. Se usa para evitar que el usuario cambie continuamente su contraseña para volver a quedarse con su contraseña original caducada.

## Directiva de bloqueo de cuentas

Podemos bloquear cuentas si se usan contraseñas incorrectas. Se accede entrando en directivas de cuenta - bloqueo de cuenta. Podemos configurar:

- Duración de bloqueo de cuenta. Cuanto tiempo permanece bloqueada una cuenta si se supera el umbral de bloqueo. Valor cero hará que solo el administrador pueda desbloquear.
- Restablecer el bloqueo de cuenta después de: Indica cada cuanto tiempo el contador de intentos erróneos se pone a cero.

- Umbral de bloqueo de cuenta: indica cuantos intentos erróneos se permiten.

# 4. Herramientas del sistema. Herramientas administrativas

## 4.1. Introducción

En Windows 10 se llega a las herramientas de Windows de dos maneras distintas:

- Tecla Windows + R. Abre ejecutar y escribimos el nombre del programa.
- Pulsando botón derecho en inicio se accede a bastantes herramientas.

## 4.2. Cuotas de disco

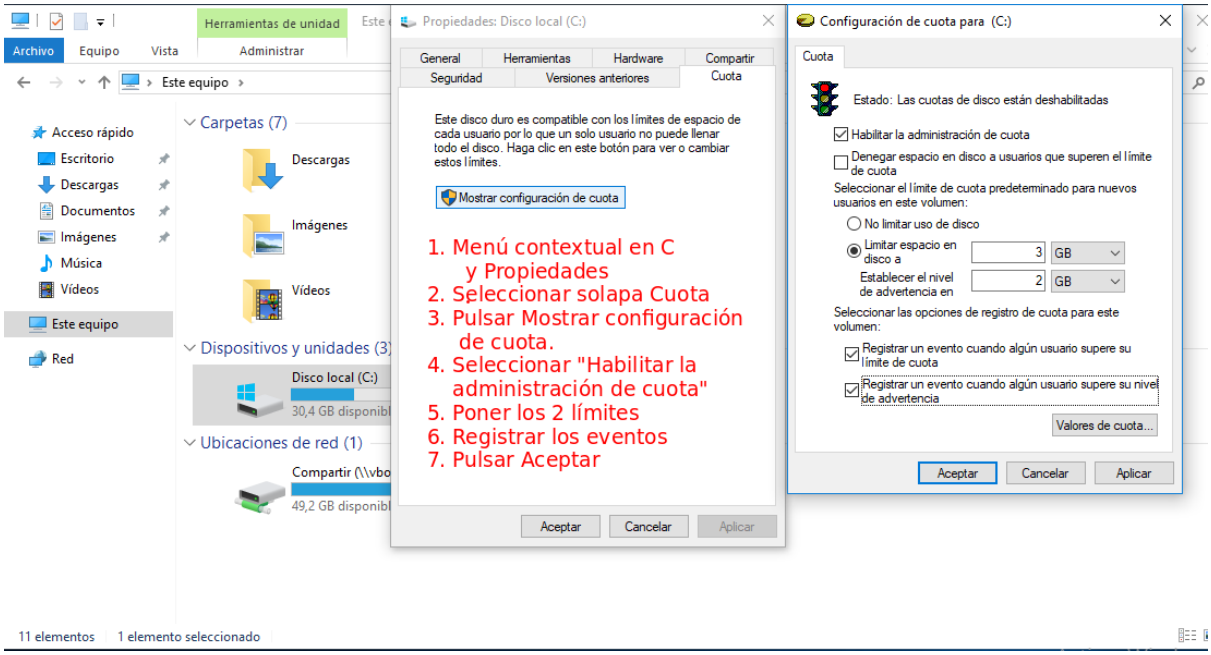
Limita el espacio de cada usuario para guardar sus datos.

Se pueden habilitar cuotas de disco en las propiedades del volumen de discos en el explorador de windows o mediante el objeto de directiva de grupo.

**A través del explorador de Windows**

Se accede haciendo click derecho en la unidad que queramos / propiedades / Cuotas y hacemos click en:

- "Habilitar la administración de disco" y rellenamos dos límites de espacio:
  - Limitar espacio en disco a... límite que no se podrá superar
  - Establecer nivel de advertencia en... se avisa con un mensaje al usuario.
- Se pueden marcar casillas para registrar los eventos relacionados con cuotas de disco.




**A través de directivas de grupo.**

En directivas de equipo local - Configuración del equipo - Plantillas administrativas - Sistema - Cuotas de disco.

En directiva de grupo las cuotas se establecen en base a la suma de lo admitido entre todas las unidades del PC.

# 4.3. Desfragmentar y comprobar unidad

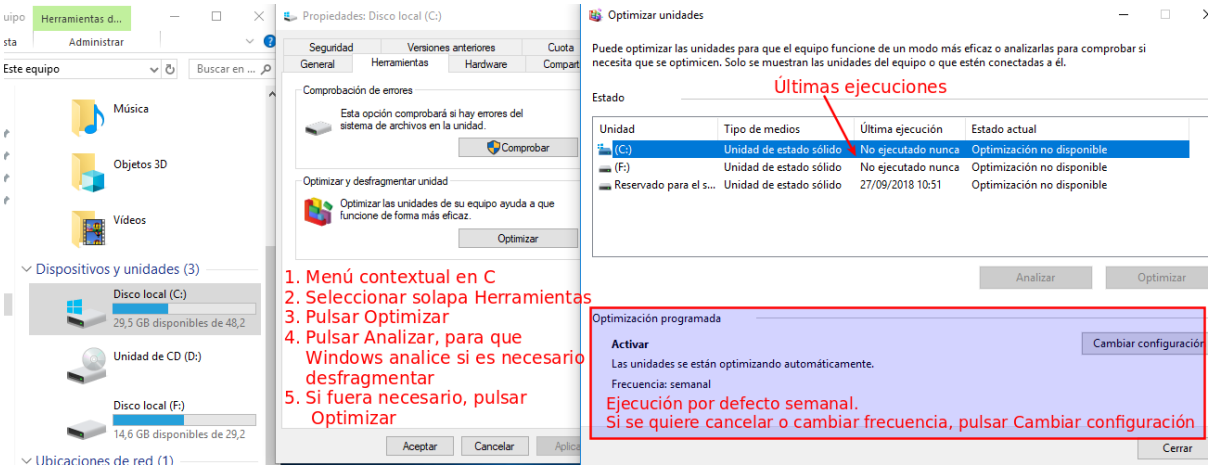
## Desfragmentar y optimizar unidades

La función desfragmentar unidad ayuda a que las unidades de asignación de un archivo queden contiguas y se aumenta el rendimiento.

Es recomendable desfragmentar cuando se nota que decae el rendimiento del disco duro.  El desfragmentador no gana espacio en el disco, solo compacta archivos.

Se accede desde Desfragmentar y optimizar unidades o en el menú propiedades de la unidad, solapa herramientas. También a través de la terminal con defrag [unidad:].

En los SSD se desaconseja desfragmentar, porque no lo necesitan y además las escrituras en un SSD aunque son muy altas, son limitadas.




## Comprobar errores

En la misma solapa de herramienta tenemos la opción "Comprobar errores", aunque podemos ejecutar desde la terminal chkdsk /F [unidad:]

# 4.4. Programador de tareas

Permite programar la ejecución automática de aplicaciones, ya sea en periodos de tiempo, al encender el ordenador, al apagarlo... También podremos ejecutar cualquier archivo por lotes.

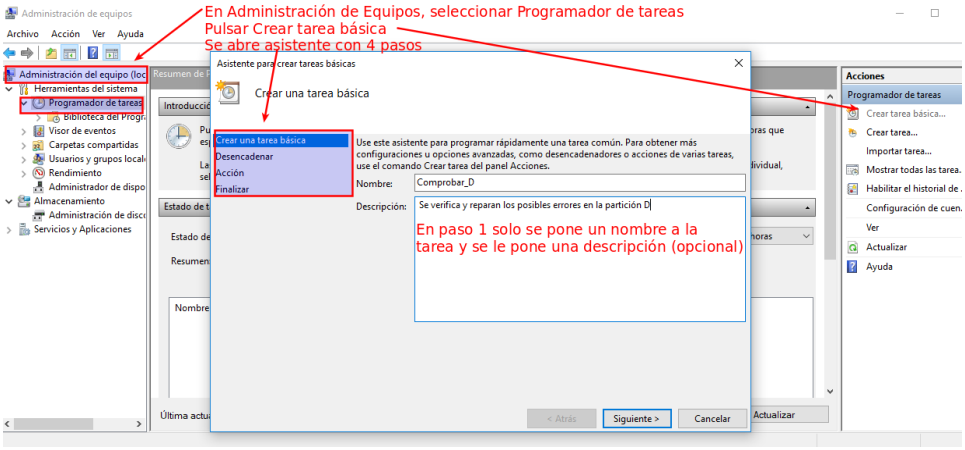
Se accede desde Administración de equipos, como administrador.

**Ejemplo:**

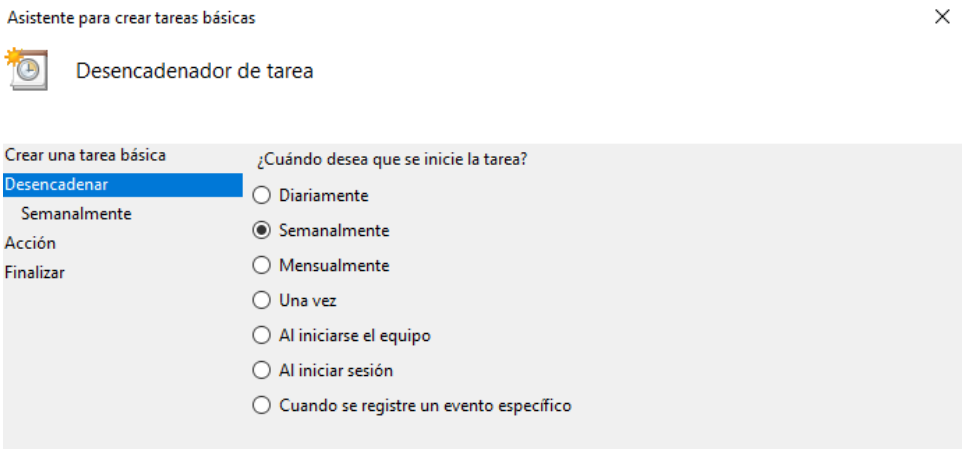
Programar para que se comprueben y reparen los errores en la unidad D una vez semanalmente:

Se pulsa en Acción y luego en Crear tarea básica. Se inicia un asistente de configuración de la tarea dividido en cuatro fases Descripción, Desencadenador, Acción y Finalizar.

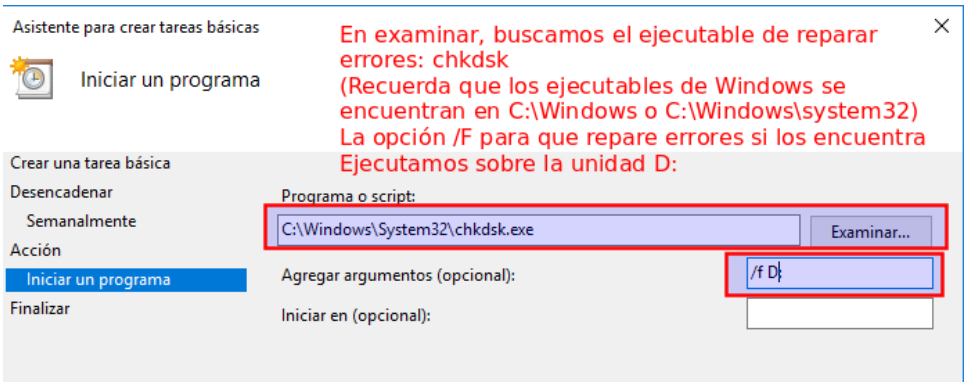
- Nombre y descripción: Se rellena el nombre para la tarea y si se desea una descripción. Se pulsa en Siguiente.



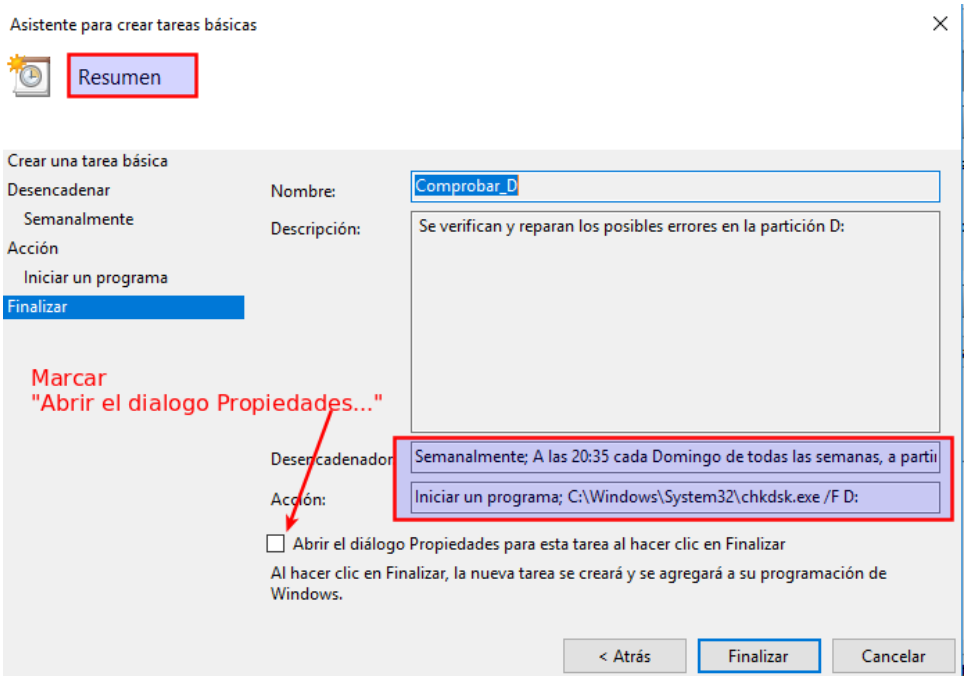

- Desencadenador: Se Indica semanalmente y Siguiente.Se abre una ventana, para indicar hora de la primera ejecución y que día semanal queremos que se ejecute.

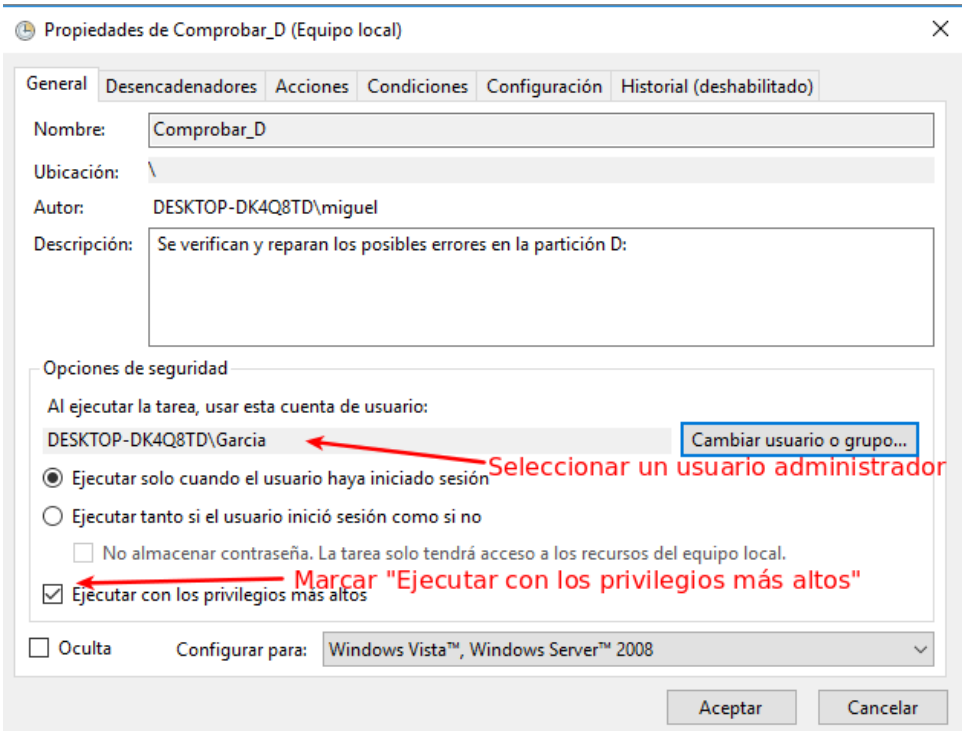



- Acción: Se escoge iniciar un programa y se pulsa Siguiente. En la siguiente pantalla, con el botón Examinar se indica la ruta y nombre de la aplicación, en nuestro ejemplo chkdsk.exe.



- Finalizar: Nos muestra un resumen de la configuración de la tarea. Hay que activar la opción "Activar el diálogo Propiedades para esta tarea al hacer clic en Finalizar". Dentro de la cual activamos la opción de "Ejecutar con los privilegios más altos", y seleccionamos el usuario Administrador y configurar para Windows 10. Finalizamos el asistente.

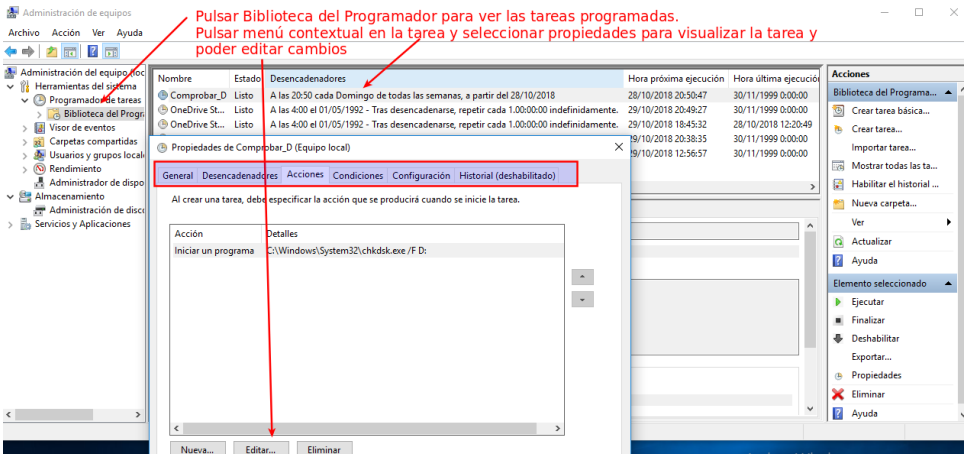


**Comprobación de la tarea y editar cambios posteriores**

Para ver todas las tareas programadas, hay que ir dentro del Programador de tareas a **Biblioteca del Programador**. Se verán todas las tareas creadas por el propio Windows, además de las que creen los usuarios.

Se puede **editar cambios** en las tareas programadas, seleccionando en su menú contextual Propiedades.



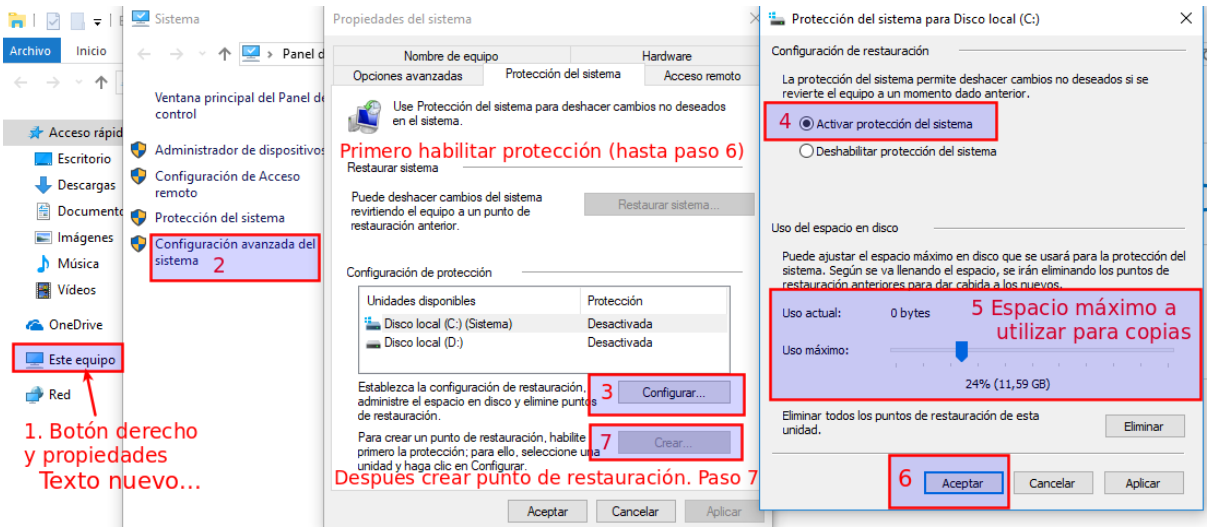

Por último, cuando se tiene soltura para crear las tareas, se puede crear sin asistente, utilizando “Crear tarea..” en lugar de “Crear tarea básica”.

# 4.5. Protección del sistema. Puntos de restauración

Puedes llevar Windows a un punto anterior, que eliminará todos los cambios que hayamos realizado desde entonces.

Por defecto viene deshabilitado, ya que ocupan espacio. Para habilitarlo:

- Abrir propiedades en equipo.
- Seleccionar la pestaña Protección del sistema en la ventana de propiedades del sistema.
- Pulsar en configurar.
- Seleccionar activar protección del sistema.
- Seleccionar espacio máximo a ocupar por puntos de restauración.
- Pulsar aceptar.
- Pulsar el botón crear para crear un punto de restauración, insertando nombre y crear.




Para verificar que se ha creado correctamente se puede hacer click en "elegir otro punto de restauración" y se mostrarán todos los existentes. Cada cierto tiempo Windows crea los suyos propios, también lo hace cuando instalamos nuevo software o controladores siempre que sean considerados importantes por el sistema.

# 4.6. Configuración. Actualización y seguridad

## Menú actualización y seguridad

Se accede abriendo configuración y seleccionando actualización y seguridad.

- Windows update: acceso a actualizaciones
- Seguridad de Windows: acceso a configuración de Windows Defender
- Copias de seguridad: para crear copias de seguridad de carpetas y de instalación de Windows
- Recuperación: posibilidad de reinstalación de Windows 10.

## Windows Update

- Buscar actualizaciones. Buscará en este momento actualizaciones publicadas
- Cambiar horas activas. Son las horas en las que el sistema no se reinicia por actualizaciones.

- Opciones avanzadas. Se pueden desactivar las actualizaciones automáticas. Aunque hay un máximo de tiempo permitido sin actualizar (35 días).

Es importante actualizar para obtener parches de seguridad que reparan posibles agujeros de seguridad en el sistema.

Se puede deshabilitar en Administración de equipos - Servicios - Windows Update. Por ejemplo en máquinas virtuales o en equipos donde necesitamos que no se reinicien: aeropuertos, hoteles, cibers, etc.

## Seguridad de Windows. Windows Defender.

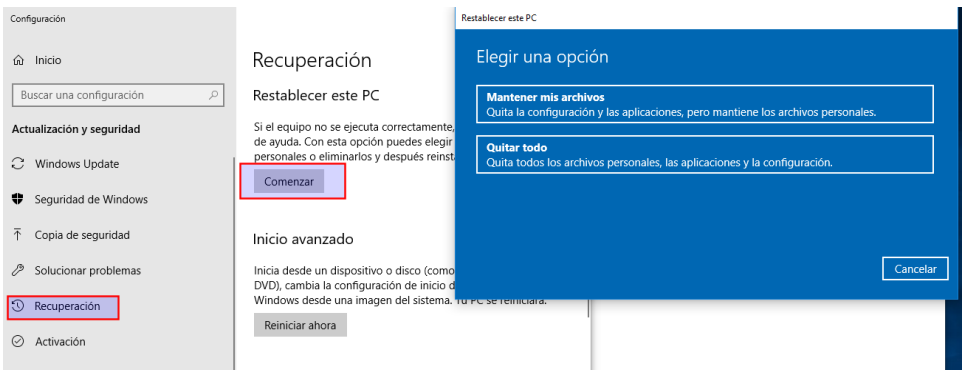
Es el centro de seguridad, incluye antivirus y firewall. Windows 10 incluye antivirus por primera vez ya que en Windows 7 solo incluida antispyware. Si se decide usar otro antivirus se debe desactivar el de Windows para evitar conflictos.

## Reinstalación de Windows. Ventana recuperación.

Permite reinstalar Windows sin necesidad de CD o ISO, incluso, salvando ficheros del usuario.

Hay dos formas de abrirlo:

- Configuración - Actualización y seguridad - Recuperación
- Panel de control - Recuperación.




Una vez abierta la ventana se puede elegir entre dos opciones:

- Mantener mis archivos

- Quitar todo (solo la unidad donde está instalado Windows o todas las unidades, borrando todas las particiones).

# Mapa conceptual