UD.6 Administración básica del sistema Windows

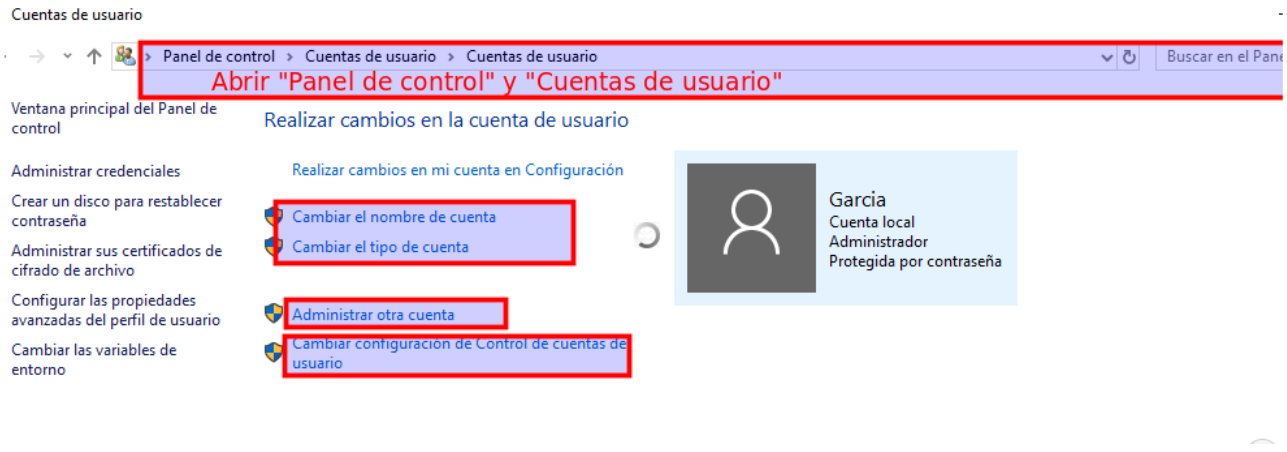
1.- ADMINISTRACIÓN DE USUARIOS Y GRUPOS.

En esta unidad, vamos a aprender a administrar Windows. Empezamos con la administración de usuarios y grupos.

Las cuentas de usuario están pensadas para uso individual, mientras que los grupos sirven para facilitar la administración de varios usuarios.

En Windows hay 2 programas gráficos para la administración de usuarios y grupos:

- **"Cuentas de usuario"** desde "Panel de Control" (apartado 2 de este libro). Este programa está en todas las versiones de Windows.
- **"Usuarios y grupos"** desde "Administración de equipos" (apartado 3 de este libro). Este programa es más completo para administrar usuarios y grupos, pero no está incluido en las versiones Home. Es el que utilizaremos por defecto en las versiones Profesionales.



En la imagen se puede observar que la instalación de Windows creó cuentas de usuario integradas, en concreto los usuarios Administrador e invitado, pero que ambos se encuentran deshabilitados, por lo que no pueden iniciar sesión. Estos usuarios se pueden habilitar, pulsando en su menú contextual.

Habilitar el usuario invitado, permitiría que cualquier persona con acceso físico al equipo, pueda iniciar sesión.

Aparte de estos usuarios creados automáticamente por Windows, se encuentra el usuario solicitado durante la instalación (Garcia en la imagen) con permisos de administrador.

1.1.- Cuentas de usuario en panel de control.

Si pulsamos en "Cambiar el tipo de cuenta" podemos seleccionar 2 opciones: usuario estándar y administrador:

- **Cuenta de usuario estándar:** Tiene privilegios limitados, se puede usar la mayoría de los programas instalados en el equipo, pero no se puede instalar o desinstalar software ni hardware, eliminar archivos que son necesarios para que el equipo funcione, o cambiar opciones de configuración en el equipo que afecten a otros usuarios.
- **Cuenta de administrador:** Tiene el máximo control sobre el equipo y sólo se debe utilizar cuando se lleven a cabo tareas de administración. Permite realizar cambios que afectan a otros usuarios. Son tareas fundamentales de los administradores las relativas a la configuración de seguridad, a la instalación de software y hardware, y a la obtención de acceso a todos los archivos en un equipo.

Además, existe el tipo invitado, pero que por defecto viene deshabilitado y que ni siquiera aparece en la ventana de "Cuentas de usuario"
Si pulsamos en administrar otra cuenta, podremos cambiar su tipo o crear una nueva cuenta de usuario.

Para **crear una cuenta de usuario**, los pasos son:

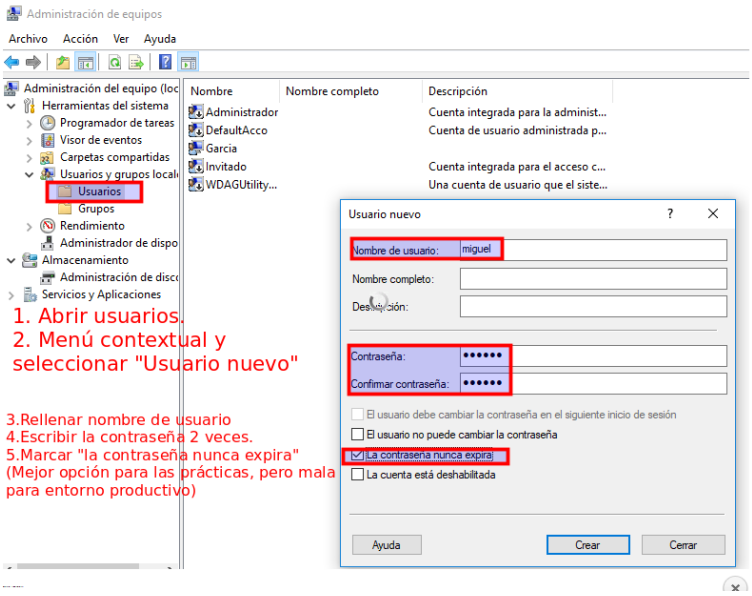
1. Hacer clic en Administrar otra cuenta.
2. Crear una nueva cuenta.
3. Escribir el nombre que deseamos utilizar para la cuenta y, después, hacer clic en Siguiente.
4. Seleccionar el tipo de cuenta que deseamos y después hacer clic en Crear cuenta.

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.

1.2.- Usuarios y grupos desde "Administración de equipos".

También se puede abrir este programa ejecutando **lusrmgr.msc**

Para crear un usuario, se pulsa menú contextual dentro de la ventana usuarios o en menú “Acción / Usuario nuevo”



Grupos en Windows

Los grupos en Windows simplifican la administración de cuentas de usuario. Cuando queramos compartir una carpeta a un departamento entero, será más cómodo introducir a todos los usuarios en un grupo y compartir la carpeta a ese grupo.

Cuando se instala Windows se crean varios grupos de usuarios, estas cuentas de grupo se les dice cuentas integradas. Además, el administrador podrá crear nuevos grupos.

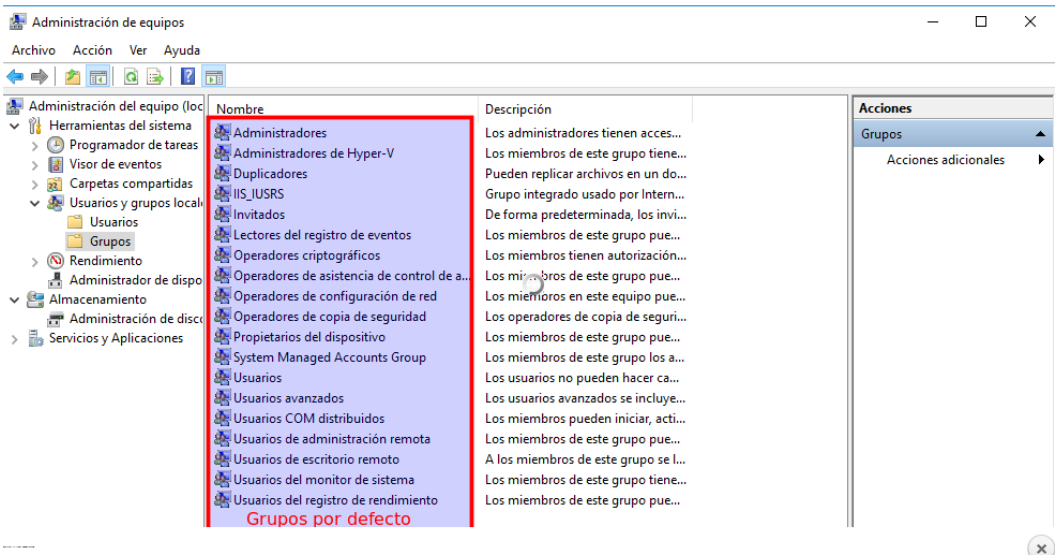
Por lo que hay tres tipos de grupos:

- Los grupos creados por el administrador
- Los grupos integrados (Administradores, Usuarios, Usuarios avanzados,...)
- Grupos de seguridad integrados o especiales, a las que se pertenece según la actividad realizada en el momento. Por ejemplo, se encuentran el grupo Todos, Usuarios autentificados. Estos grupos no aparecen explícitamente, pero sí que se les puede dar permisos en una carpeta o fichero.

En la siguiente captura, se muestran las cuentas de grupo integradas en Windows 10 Profesional.

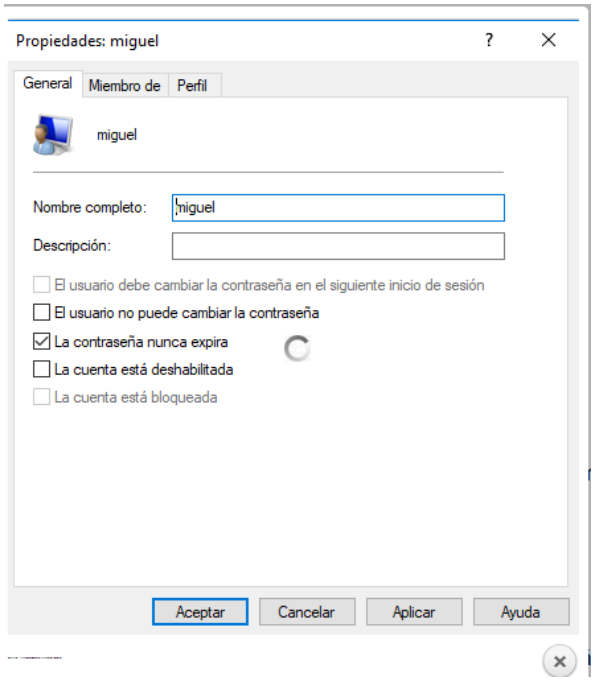
El nombre de los grupos, suele servir para entender su objetivo. Por ejemplo, el grupo “Operadores de copias de seguridad” tendrá a los usuarios que se les permita realizar copias de seguridad.

Sí que destacamos el grupo de “Usuarios avanzados” cuya diferencia con el grupo "Usuarios" es que permite instalar aplicaciones.



Cambiar nombre o contraseña de un usuario.

Si accedemos con el menú contextual a las propiedades de un usuario, tenemos tres solapas:



Solapa “General”:

Se indica el nombre completo del usuario y su descripción. Hay que tener cuidado con esta opción, si por ejemplo, el usuario se llama juana, pero en nombre completo escribimos “Juana López”, al

iniciar sesión gráfica, aparecerá "Juana López", pero el nombre del usuario es "juana", por lo que su carpeta de usuario es C:\Users\juana. También se pueden configurar las siguientes opciones sobre la contraseña:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Se le obliga al usuario cambiar contraseña la primera vez.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca caduca. Es habitual tener desmarcada esta opción, para obligar al usuario cambiar la opción periódicamente.

Para las tareas del módulo, se recomienda dejar marcada solo la opción "La contraseña nunca caduca" por comodidad, para no tener que cambiar la contraseña constantemente de los distintos usuarios. Sin embargo, a nivel profesional, se recomienda dejar marcada la primera opción, para obligar al usuario cambiar contraseña la primera vez. De esta forma, además el administrador no conocerá la contraseña del usuario.

Finalmente, en la solapa general, se puede deshabilitar o habilitar la cuenta.

Solapa "Miembro de"

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

Al igual que en la ventana usuarios, en la ventana Grupos, se pueden crear y eliminar grupos; así como añadir o quitar usuarios de grupos.

1.3.- UAC (User Account Control, Control de Cuentas de Usuario).

Cada vez que se quiere realizar alguna acción en el sistema, como la instalación de de programas, se modifican el registro de Windows, etc. se notifica una alerta de seguridad al usuario. Esta alerta la lanza el UAC.

Se pueden configurar 4 niveles de alerta, desde el nivel de alerta deseado. Esto se realiza en el panel "Cuentas de usuario". Hay 4 niveles de alerta desde notificar siempre a no notificar nunca.

2.- SEGURIDAD LOCAL. PERMISOS LOCALES O NTFS.

2.1.- Solapa Seguridad.

Supongamos un PC con Windows instalado, con 2 usuarios, Juan y María. Una pregunta que nos hacemos es si Juan puede proteger sus archivos sin que tenga acceso María y viceversa. Estamos hablando de Seguridad local o permisos locales, es decir, en el mismo PC, sin utilizar la red.

La respuesta a esta pregunta es sí, pero para ello la partición tiene que ser NTFS.

En menú contextual Propiedades de fichero o carpeta, aparecen 2 solapas distintas: Compartir y Seguridad.

- Compartir, son permisos para cuando se acceden desde la Red, es decir, desde otro equipo. (Unidad 9)
- Seguridad: son permisos para cuando accede cualquier usuario en el equipo local. Estos permisos son los que vamos a configurar en este apartado.

Si no aparece la solapa Seguridad, es porque la partición es FAT 32. Se puede convertir una partición de FAT 32 a NTFS, sin necesidad de formatear ni eliminar los archivos.

Para ello, ejecutamos en la terminal **convert unidad: /fs:ntfs**

Primeras normas sobre permisos locales

- Podemos configurar permisos locales tanto a carpetas y ficheros, en general hablamos de objetos.
- Por defecto, cuando se crea una carpeta, se heredan los permisos de la carpeta padre.
- Los permisos se conceden a usuarios y grupos.
- Todos los objetos tienen un propietario, que por defecto es quien ha creado el objeto.
- Los permisos a los objetos los pueden cambiar los administradores y el usuario propietario del objeto. A cualquier usuario se le podrá dar derecho de cambiar permisos en cualquier objeto.
- Un administrador se puede convertir en propietario de cualquier objeto

La solapa Seguirdad incorpora 2 botones: Estándar y Opciones avanzadas. Se explican con detalle en los 2 apartados siguientes.

2.2.- Modificar permisos estándar. Botón editar de la solapa Seguridad.

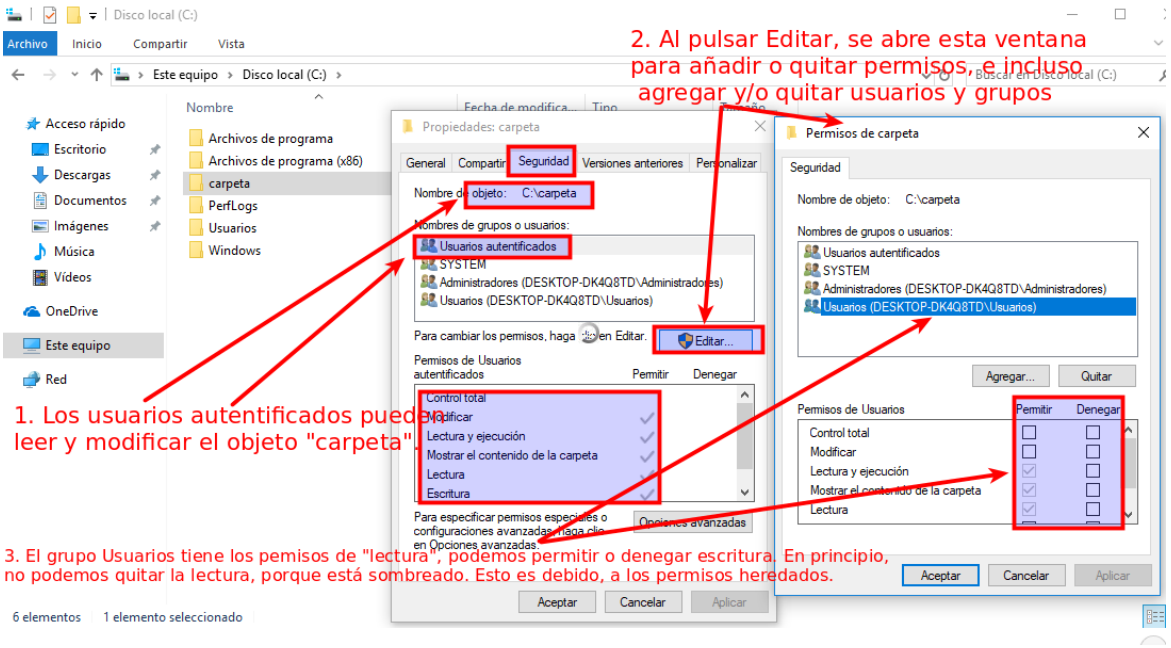
Pulsando el botón Editar en la solapa Seguridad podemos modificar los permisos estándar (6 permisos para carpetas y 5 permisos para archivos)

Los permisos estándar son (en orden de menos permisos 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" y además permite ver atributos, propietarios y sus permisos.
    - En archivos, permite leer los archivos y ver sus atributos, propietarios y sus permisos.

> **Lectura y ejecución**
    - Tiene los permisos de "lectura"
    - Además en carpetas permite navegar por ellas y en archivos permite ejecutar los programas (archivos ejecutables: exe, com, bat)
> **Escritura**
    - Incluye todos los de lectura y ejecución, y además:
    - En carpetas, permite crear archivos, subcarpetas y cambiar atributos.
    - En archivos, permite cambiar el contenido (sobrescribir el archivo) y cambiar atributos.
> **Modificar**
    - Incluye todos los de escritura, y además:
    - En carpetas permite borrar la carpeta
    - En archivos permite borrar el archivo
> **Control total**
    - Incluye todos los de modificar, y además:
        - En carpetas permite borrar subcarpetas y archivos, cambiar atributos y cambiar propietarios.
        - En archivos, permite cambiar atributos y cambiar propietarios.

En la captura siguiente, se muestra la solapa Seguridad del objeto carpeta, donde se ven los grupos y usuarios que tienen algún permiso. También se visualiza la ventana que se abre al pulsar Editar.



Estos permisos estándar se dividen en 3 categorías principales:

Si queremos **lectura y ejecución**, se conceden los permisos:

- > Lectura y ejecución
- > Mostrar el contenido de la carpeta
- > Lectura

Si queremos **modificar**, además de los de lectura se conceden los permisos:

- > Modificar
- > Escritura

Si queremos **control total**, se conceden todos salvos los permisos especiales. Es decir, además de modificar, se concede:

- > Control total

Observar que **Control total es un permiso muy potente**. Si un usuario tiene Control total en una carpeta, este usuario podrá eliminar cualquier subcarpeta o archivo que haya en esa carpeta, incluso si le denegamos el permiso de escritura en esa subcarpeta o archivo; por tanto hay que tener mucho cuidado al conceder este permiso.

Como calcular los permisos de un objeto

Cuando configuramos permisos, podemos permitir, denegar y no marcar opción. La diferencia entre permitir y denegar, está clara, pero ¿cuál es la diferencia de denegar un permiso explícitamente, y no dejar marcado ni permitir ni denegar?

Supongamos un usuario que pertenece a varios grupos. ¿Qué permiso tiene ese usuario?

2 reglas:

Regla 1. Se mirará el permiso que tiene el usuario y los grupos a los que pertenece, si alguno de ellos tiene denegado el permiso, la denegación manda, y el usuario no tendrá ese permiso.

Regla 2. Si no hay denegación, se mirará los permisos permitidos al usuario y sus grupos, el usuario tendrá el máximo de permisos permitidos.

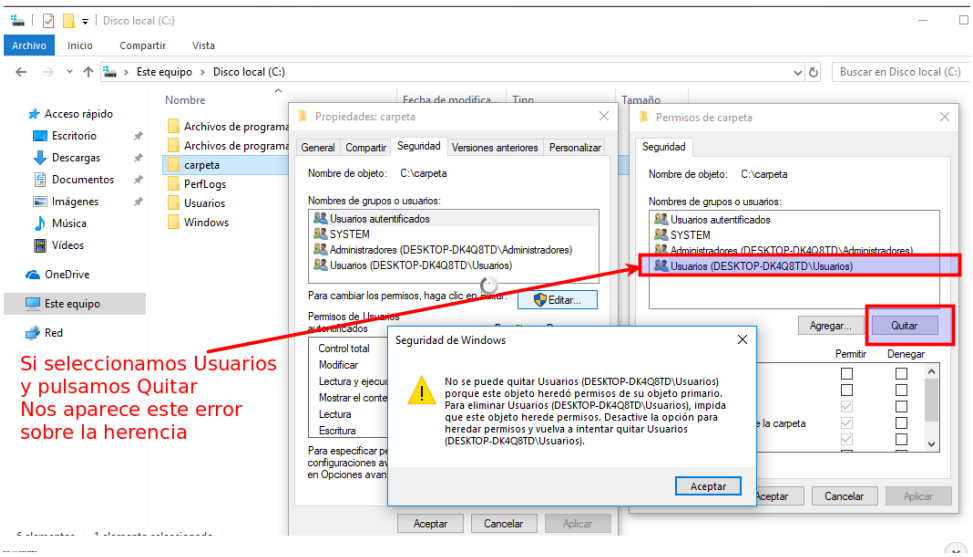
> **Ejemplo 1.** Supongamos que juan pertenece a los grupos contabilidad e informatica. Y que los permisos configurados corresponden a:
>
> - Juan tiene concedida lectura en la carpeta apuntes.
> - El grupo contabilidad tiene denegada la lectura.
> - El grupo informatica tiene permiso escritura en la carpeta apuntes.
>
> Cuáles son los permisos?
>
> **Respuesta:** el usuario no tiene ningún permiso, pues el grupo contabilidad al que pertenece tiene denegada la lectura.

> **Ejemplo 2.** ¿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

Al crear un archivo o carpeta; se crea con los permisos de su carpeta padre. Por defecto la herencia está habilitada. Por eso, en muchos casos, no podemos quitar usuarios que tienen permisos, o desmarcar permisos que aparecen sombreados. En estos casos, tendremos que deshabilitar la herencia.

En la imagen siguiente, se intenta quitar al grupo Usuarios, para que no tengan permisos en el objeto carpeta. Al hacerlo, sale mensaje de error, que nos indica que para poderlo quitar, es necesario quitar la herencia.



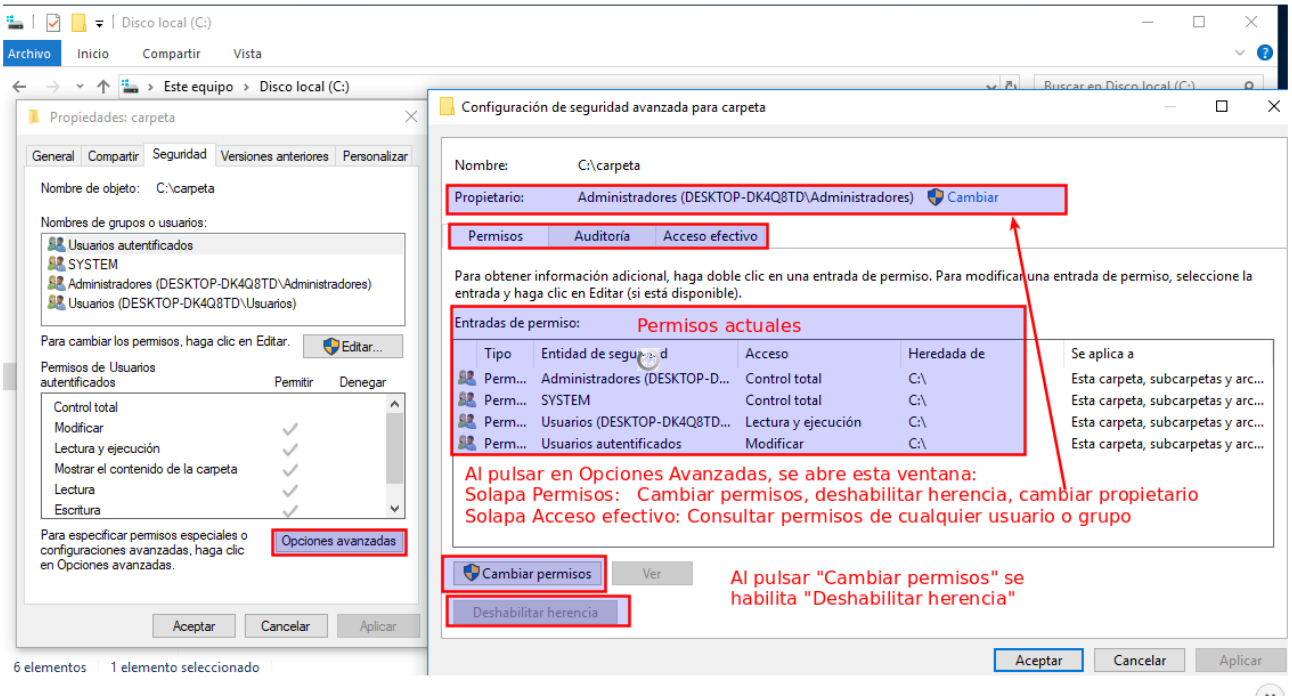
Para quitar la herencia, no se puede realizar en el botón Editar, sino en Opciones Avanzadas. Lo vemos a continuación.

2.3.- Botón Opciones avanzadas en solapa Seguridad.

En Opciones Avanzadas de la solapa Seguridad podemos:

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

Al pulsar **Opciones Avanzadas**, se abre una nueva ventana con 3 solapas: **Permisos, Auditoría y Acceso efectivo**. En la solapa Permisos se ven todos los permisos actuales en el objeto, es el mejor sitio, para ver de un vistazo los permisos concedidos a cada usuario o grupo.



Quitar la herencia en un objeto

Para quitar la herencia a un objeto, hay que ir a "Opciones Avanzadas" y pulsar "Cambiar permisos", en ese momento, se habilita el botón "Deshabilitar herencia".

Si pulsamos "Deshabilitar herencia", se abre la ventana emergente que se ve en la captura anterior. Tenemos 2 opciones para responder:

- Si respondemos **"Convertir los permisos heredados en permisos explícitos"** significa que quitamos la herencia, pero no eliminamos ningún permiso heredado anterior. En general, se recomienda esta opción, pues hay permisos que no debemos modificar, como los permisos concedidos a System, Creator Owner…
- Si respondemos **"Quitar todos los permisos heredados"**, quitamos la herencia, y eliminamos los permisos heredados hasta ahora en ese objeto.

Permisos especiales

También se pueden modificar los permisos habiendo pulsado "Opciones avanzadas" en la solapa "Seguridad". En esta ventana, se llaman permisos especiales, pues son distintos a los permisos estándar vistos antes.

En esta ventana de Opciones avanzadas, en vez de los 6 permisos estándar, hay 13 permisos especiales. Por ejemplo, el permiso estándar de "Lectura", equivale a los permisos especiales "Leer datos", "Leer atributos", "Leer permisos" y "Leer atributos extendidos".

Por ese motivo, salvo que se tenga bastante experiencia, se recomienda administrar los permisos, en el botón "Editar" de la solapa Seguridad" pues es más sencillo administrar 6 permisos que 13 permisos.

En la siguiente página de soporte de Microsoft, se muestra la equivalencia entre permisos especiales y permisos estándar:

https://technet.microsoft.com/es-es/library/cc732880.aspx

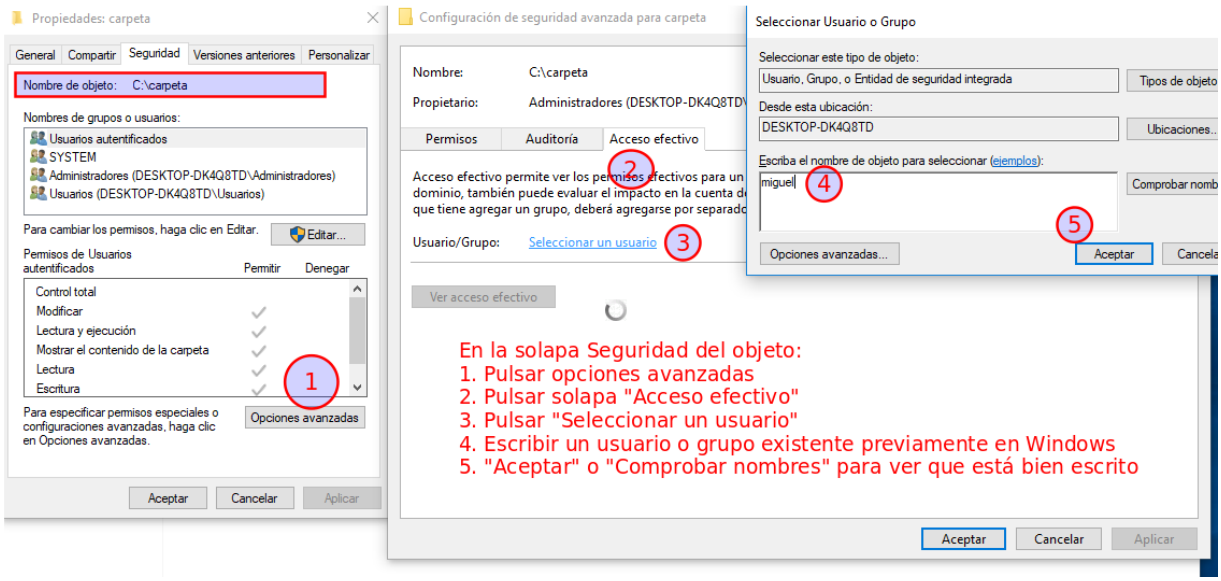
Para ver qué permite cada permiso especial, mirar vínculo: https://technet.microsoft.com/es-es/library/cc753992.aspx

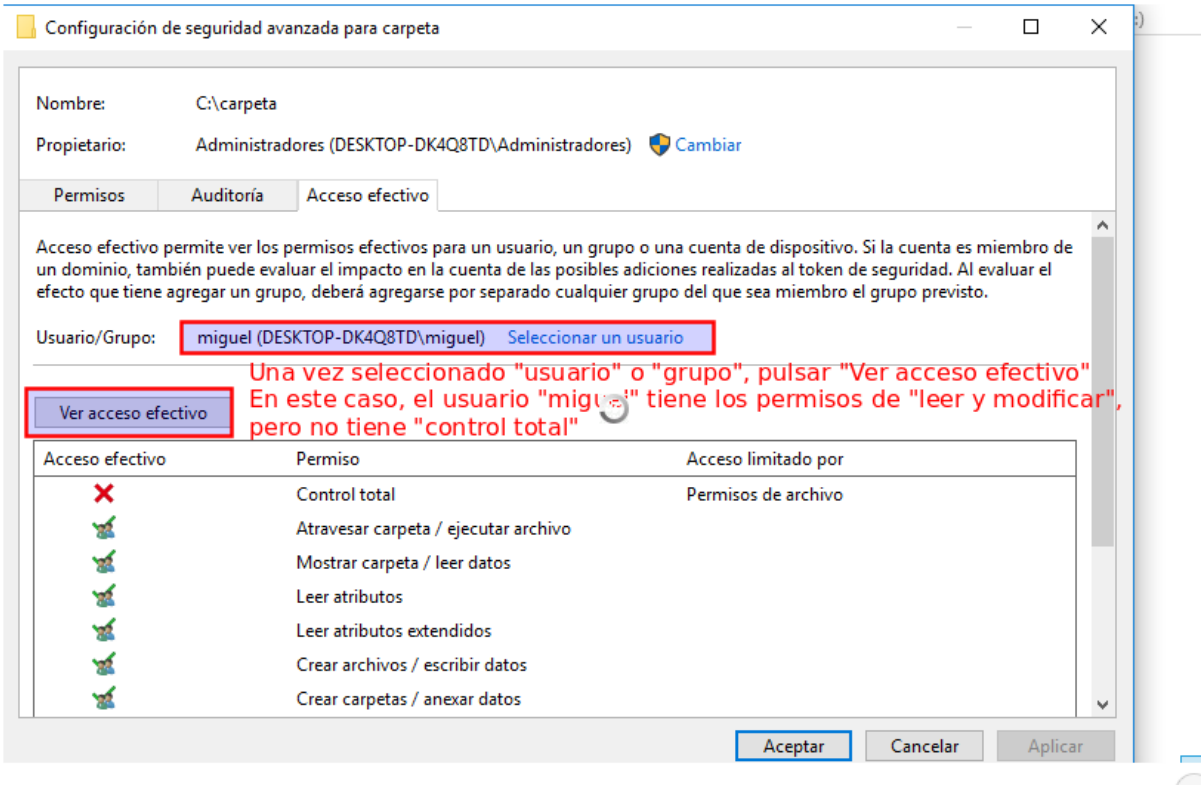
Solapa "Acceso efectivo" en "Opciones avanzadas"

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

La administración de permisos, es muy completa, lo que puede dar lugar a algún error de configuración. De ahí, que se incorpora esta solapa, como forma de averiguar que permisos concretos tiene un usuario o grupo. Esta solapa, en anteriores Windows se llama Permisos efectivos.

Se pulsa en "seleccionar" para buscar un usuario o grupo, y nos devuelve los permisos en ese objeto (carpeta o fichero). Ver las 2 capturas incluidas de cómo hacerlo. Basicamente, se trata de entrar en la solapa Acceso efectivo y sleecionar un usuario o grupo para buscar sus permisos.





2.4.- Recomendaciones y ejemplo final.

Recomendaciones al administrar permisos

Si no se tiene cuidado en la administración de permisos, es muy fácil obtener un caos. Para evitarlo, se hacen las siguientes recomendaciones:

- Evitar en lo posible denegar permisos.
- Administrar preferiblemente permisos a grupos, que permisos a usuarios.
- Administrar preferiblemente permisos en carpetas, que permisos en archivos.

Es más fácil administrar permisos de forma global a carpetas y grupos. Y se trata de poner el mínimo de denegaciones, normalmente para excluir a alguien o pequeños grupos. Por ejemplo, si queremos que un grupo entero pueda leer, salvo un usuario del grupo, concedemos la lectura al grupo y denegamos al usuario.

¿Qué permisos se crean cuando copiamos o movemos carpetas o archivos?

Copiar objetos en particiones NTFS:

Cuando copiamos un objeto, sea en la misma partición NTFS o en otra, se considera un objeto nuevo, por lo que hereda los permisos de la carpeta de destino.

Mover objetos en particiones NTFS:

Cuando movemos un objeto dentro una partición NTFS, el objeto conserva sus permisos originales.

Cuando movemos un objeto entre distintas particiones, el objeto hereda los permisos de la carpeta de destino.

Tal vez te ayude a comprender por qué es así, que si mueves un archivo grande en la misma partición, no se tarda nada, pues no se escribe en el disco. Solo se cambia la ruta del archivo. Sin embargo, si lo movemos de una partición a otra, si se tarda bastante, pues realmente hay una escritura en la partición nueva.

3.- REGISTRO DE WINDOWS. DIRECTIVAS DE GRUPO Y SEGURIDAD LOCAL.

Siempre desde una cuenta con privilegios de administrador Windows 10 nos proporciona la posibilidad de gestionar de forma centralizada la configuración de la seguridad de nuestro sistema, a través de las Directivas de seguridad local y las Directivas de grupo local. Ambas opciones cuentan con consolas para facilitar la configuración de las directivas. Una directiva es un conjunto de reglas de seguridad que se pueden implementar en un sistema.

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

3.1.- Registro de Windows.

El registro de Windows tiene todo el historial desde que se instaló el Sistema Operativo. Por ejemplo, si instalamos un programa, y a continuación desinstalamos, en el registro quedan escritas las 2 cosas, aunque la carpeta de instalación se haya eliminado. Por eso, cuando utilizamos un shareware con 30 días de evaluación, si pasado ese tiempo, se desinstala y se vuelve a instalar, el Sistema Operativo informa que ya se ha instalado ese software anteriormente.

El registro de Windows, se hace cada vez más grande, y es el principal motivo de que el ordenador cada vez tarde más en arrancar.

El registro de Windows, no se debe tocar, salvo que sepamos lo que hacemos. Pero a veces, se producen situaciones en las que es necesario modificar el registro.

Aquí se muestran algunas situaciones de porque puede ser necesario tocar el registro:

- A veces ocurre, que un programa se instala y por lo que sea no acaba de instalarse. Es posible, que se entre en un bucle, porque el programa no se deja instalar porque ya se instaló, y tampoco se pueda desinstalar, porque dice que ya está instalado.
- Muchos virus, tocan valores en el registro. Puede ocurrir que aunque eliminemos el virus o software espía, el registro no vuelva a su valor original.

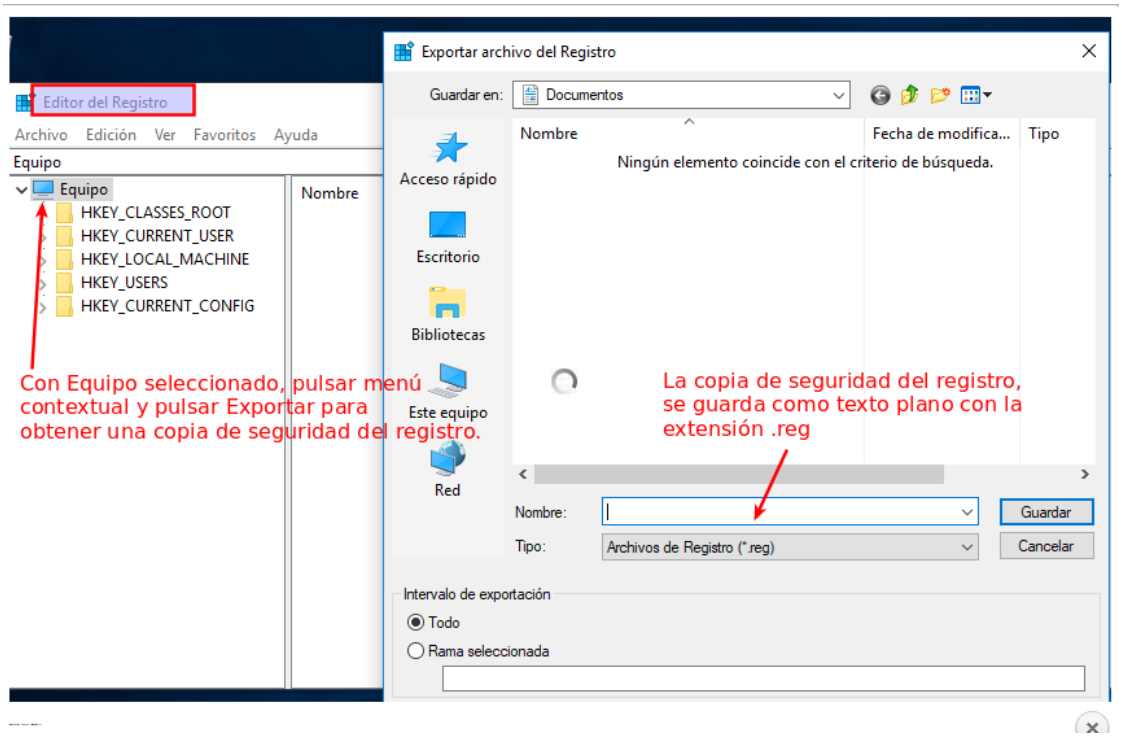
Ejecución del editor de registro y copia de seguridad

El registro se edita de forma manual con el programa regedit. Tenemos varias carpetas, donde en cada una de ellas hay muchas claves, cada uno con un valor.

Antes de modificar un valor del registro, es muy importante realizar una copia de seguridad del registro.

Para ello, después de escribir regedit, se abre el "Editor de registro", y comprobando que está seleccionado el total del equipo y no una de las 5 carpetas, seleccionamos Archivo / Exportar. Esta utilidad, obtendrá un fichero de texto, extensión reg, con todo el contenido del registro.

De esa forma, en caso de cometer algún error grave al cambiar valores en el registro, tenemos la copia de seguridad, y utilizaríamos el menú **Archivo / Importar**.



Limpiadores de registro

Existen varios limpiadores de registro, más amigables que el editor de registro de Windows, cuyo fin es borrar todas las entradas innecesarias e intentar corregir posibles valores erróneos.

Ejemplo de limpiadores de registro son: RegClean, CCleaner, Regseeker. La mayoría de estos programas es software privativo.

Ejemplo concreto: Regseeker (freeware)

La versión actual es la versión 4.7. Se puede bajar desde su página oficial: http://www.hoverdesk.net/download.php

Se baja en versión portable en un archivo .zip, lo que significa, que una vez descomprimido no hace falta realizar instalación. Se arranca con el ejecutable y es muy fácil de utilizar. Tan simple que se puede realizar una limpieza de forma automática con el botón Auto Clean.

RegSeeker comprobará las entradas erróneas o entradas innecesarias, y las corrige. Incluso, si se limpia varias veces, se siguen eliminando entradas.

Otro uso importante de Regseeker, es desinstalar aplicaciones. Hay muchas pequeñas aplicaciones, que no tienen opción de desinstalar en su propio menú, igualmente no se pueden eliminar desde "Agregar o quitar programas", y sin embargo si pueden desinstalarse desde la opción de Aplicaciones instaladas de Regseeker.

3.2.- Directivas de grupo o política local.

Para abrir en un equipo Windows el editor de directivas de grupo local, se ejecuta el programa **gpedit.msc** como administrador.

Usando las "directivas de grupo local" en una maquina Windows, podemos:

- Modificar políticas o directivas como deshabilitar el Administrador de equipos, deshabilitar la configuración de la red, obligar a un fondo de escritorio...
- Asignar archivos ejecutables o scripts que se ejecutaran automáticamente cuando el sistema se encienda, se apague, inicie sesión un usuario o cierre sesión.
- Especificar opciones especiales de seguridad.

Al modificar las directivas locales, lo que estamos realizando es modificar el registro, pero de una forma más amigable que utilizando el editor de registro. Es bastante más simple utilizar gpedit.msc, que regedit. En el editor de políticas locales, se explica el significado de cada directiva.

Si estamos trabajando en una red Windows bajo un dominio (con un Windows Server administrando dicho dominio) las políticas de grupo cobran mayor protagonismo. Pero en un ambiente de red de grupo de trabajo (sin Windows Server), las políticas de grupo son locales, es decir controlan solo los aspectos de la propia máquina.

Dentro de las directivas de grupo locales hay dos opciones: Configuración del equipo y Configuración del usuario. En el caso de directivas locales es prácticamente indistinto trabajar con una opción u otra.

Algunas directivas aparecen tanto en la configuración del equipo como en la configuración del usuario. En caso de conflicto, la configuración del equipo siempre tiene preferencia.
Respecto a la configuración, cada directiva tiene 3 posibles valores:

- No configurar la directiva, con lo que se comportará según el criterio por defecto para dicha directiva.
- Habilitarla, con lo que la pondremos en marcha en el sistema.
- Deshabilitarla, con lo que impediremos que se ponga en marcha dicha directiva.

Para modificar la configuración de una directiva, simplemente tenemos que realizar doble clic sobre dicha directiva para que nos aparezca el cuadro de dialogo que nos permite modificar dicha directiva. En dicho cuadro de dialogo nos mostrará una explicación de la funcionalidad de dicha directiva.

3.2.- Directivas de seguridad local.

Con las Directivas de seguridad local se aplican distintas restricciones de seguridad sobre las cuentas de usuario y contraseñas.
Hay 3 formas de llegar a las Directivas de seguridad local:

- Ejecutando **SecPol.msc.**
- Abrir directamente **Directiva de seguridad local.**
- Forman parte de las directivas de grupo, por lo que también hay acceso desde **gpedit.msc.**

  En gpedit.msc, habría que ir a Configuración de equipo / Configuración de Windows / Configuración de seguridad / Directiva de seguridad / Directivas de cuenta

En las Directivas de cuenta, hay 2 tipos de directivas: **Directivas de contraseña** y **Directivas de bloqueo de cuentas.**

Directivas de contraseña

Las configuraciones más útiles que podemos gestionar desde aquí son:

- Exigir el **historial de contraseñas**. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente. Por defecto aparece configurado a 0. Si queremos que no se puedan repetir las últimas 3 contraseñas, cambiaríamos el 0 a 3 pulsando el menú contextual en "Exigir el historial de contraseñas".
- Las contraseñas deben cumplir los **requerimientos de complejidad**. Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.

- **Longitud minina de la contraseña**. Indica cuantos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.
- **Vigencia máxima de la contraseña**. Las contraseñas de los usuarios caducan y dejan de ser validas después del número de días indicados en esta configuración, y el sistema obligará al usuario a cambiarlas. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
- **Vigencia minina de la contraseña**. Indica cuanto tiempo debe transcurrir desde que un usuario se cambia la contraseña, hasta que puede volver a cambiarla. Esta configuración de seguridad local se usa para evitar que un usuario cambie continuamente su contraseña a fin de volver a quedarse con su contraseña original caducada.

Directivas de bloqueo de las cuentas

Podemos bloquear las cuentas si se usan contraseñas incorrectas.
Una vez abierto SecPol.msc, para ver las directivas de bloqueo de cuentas, hacemos clic en **Directivas de Cuenta – Bloqueo de cuentas.**

Aquí podemos configurar:

- Duración del bloqueo de cuenta. Durante cuánto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee.
- Restablecer el bloqueo de cuenta después de. Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero.
- Umbral de bloqueo de la cuenta. Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta.

4.- HERRAMIENTAS DEL SISTEMA.HERRAMIENTAS ADMINISTRATIVAS.

4.1.- Introducción.

A primera vista, el aspecto de Windows cambia bastante entre las distintas versiones de Windows: Windows 7, Windows 8 y Windows 10. Pero, las diferencias están principalmente en cómo llegar a las distintas herramientas o programas integrados. Pues, las distintas herramientas vistas en este tema y las que quedan se utilizan de la misma forma, en general existen tanto en Windows 7, 8 y 10, como en las distintas versiones de Windows Server.

En la unidad 3, dimos importancia al menú contextual de Equipo, tenemos acceso a Propiedades y Administrar.
También son importantes **Panel de Control y Configuración**.
Al desaparecer el típico Inicio / Programas en Windows 7, en Windows 8 y Windows 10, ganan mucho peso 2 formas de llegar a bastantes herramientas:

> Tecla **Windows + R** abre ejecutar, donde podemos escribir cualquier nombre de programa.
> Pulsando el **menú contextual en Inicio**, se tiene acceso a bastantes herramientas de Windows. Se muestra captura.

En este libro, vamos a ver bastantes herramientas para administrar Windows: tareas programadas, defragmentador, cuotas de disco, recuperar el sistema, reinstalación Windows 10, etc.

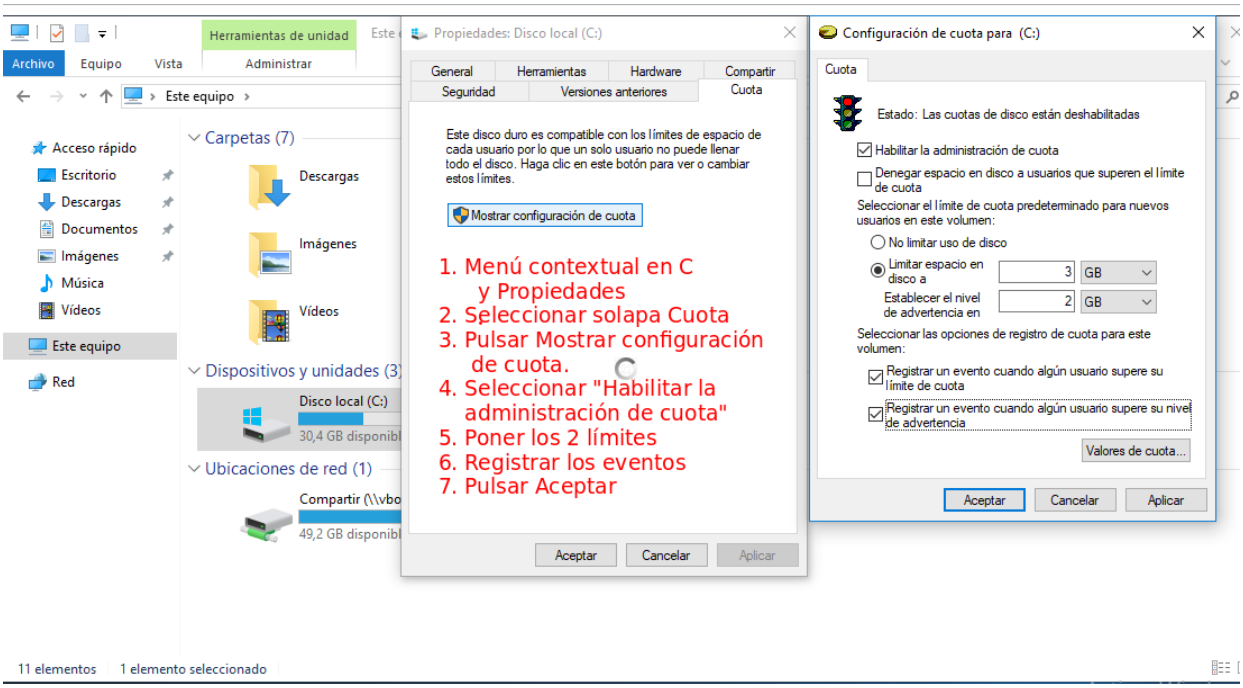
4.2.- Cuotas de disco.

La herramienta cuota de discos consiste en limitar el espacio que tiene cada usuario para guardar sus datos.
Se pueden habilitar cuotas de disco al tener acceso a las propiedades del volumen de disco en el Explorador de Windows o mediante el objeto de directiva de grupo. Veamos cada uno de estos métodos:

A través del Explorador de Windows:

> En el explorador de Windows, seleccionar Propiedades en el menú contextual de la unidad que se deseen habilitar cuotas de disco.
> Seleccionar solapa cuota, y hacer clic en "Mostrar la configuración de cuota".
> Se abre una nueva ventana, donde pulsamos la casilla "Habilitar la administración de disco" y rellenamos los 2 límites de espacio:
> "Limitar espacio en disco a …" es el límite que no se podrá superar.
> "Establecer el nivel de advertencia en …" se avisará con un mensaje al usuario, de que se acerca a su límite de espacio.
> Se puede marcar las casillas para registrar los eventos relacionados con las cuotas de disco. Pulsar Aceptar.

En la siguiente imagen, se establecen cuotas en la unidad C, con límites de 2GB como advertencia y 3GB que no se puede sobrepasar.



A través de directivas de grupo:

En las **Directivas de equipo local**, expande **Configuración del equipo**, expande **Plantillas administrativas** , expanda **sistema** y, a continuación, haz doble clic en **Cuotas de disco**.

La diferencia a realizarlo en directivas de grupo, es que las cuotas que se establezcan es la suma de lo admitido entre todas las unidades del PC.

4.3.- Desfragmentar y Comprobar unidad.

En la unidad 3, hemos visto que los archivos se guardan en unidades de asignación o clúster no contiguos. Si los archivos están demasiado troceados, se reduce el rendimiento de la partición, como vimos porque el cabezal del disco duro tiene que saltar muchas veces de pista y/o superficie. La función de "**desfragmentar unidad**", es ayudar a que las unidades de asignación de un archivo queden contiguas, aumentando el rendimiento.

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.

Señalar también, que el desfragmentador, no va a ganar espacio en el disco duro, es decir, el espacio perdido en los clústeres o unidades de asignación, por ser más pequeño el trozo de archivo que el clúster. Para explicarlo de otra forma, lo que realiza "desfragmentar unidad" es compactar el archivo, nunca recuperar espacio.

Se acede ejecutando directamente **Desfragmentar y optimizar unidades**, o con menú Propiedades en la unidad y solapa Herramientas. Por defecto, se ejecuta según una programación semanal, pero se puede ejecutar en cualquier momento.

Ha cambiado ligeramente el nombre con respecto a los anteriores Windows, donde se llamaba "desfragmentador de disco" por "desfragmentador de unidad", siendo más correcto este último porque se desfragmenta una unidad lógica..

También se puede ejecutar en la terminal con el programa ***defrag [unidad:]***

Comprobar errores

Observar, que en la misma solapa Herramienta, tenemos la opción "Comprobar errores" que corresponde a la forma gráfica de ejecutar chkdsk /F [unidad:] que vimos en los comandos de la unidad 3.

4.4.- Programador de tareas.

El Programador de tareas permite programar la ejecución automática de aplicaciones u otras tareas.
Podremos programar para que cualquier utilidad se ejecute semanalmente, al encender el ordenador, al apagarlo. Asimismo, se podrá ejecutar periódicamente cualquier archivo por lotes.
Se accede al Programador de tareas desde Administración de equipos.
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.

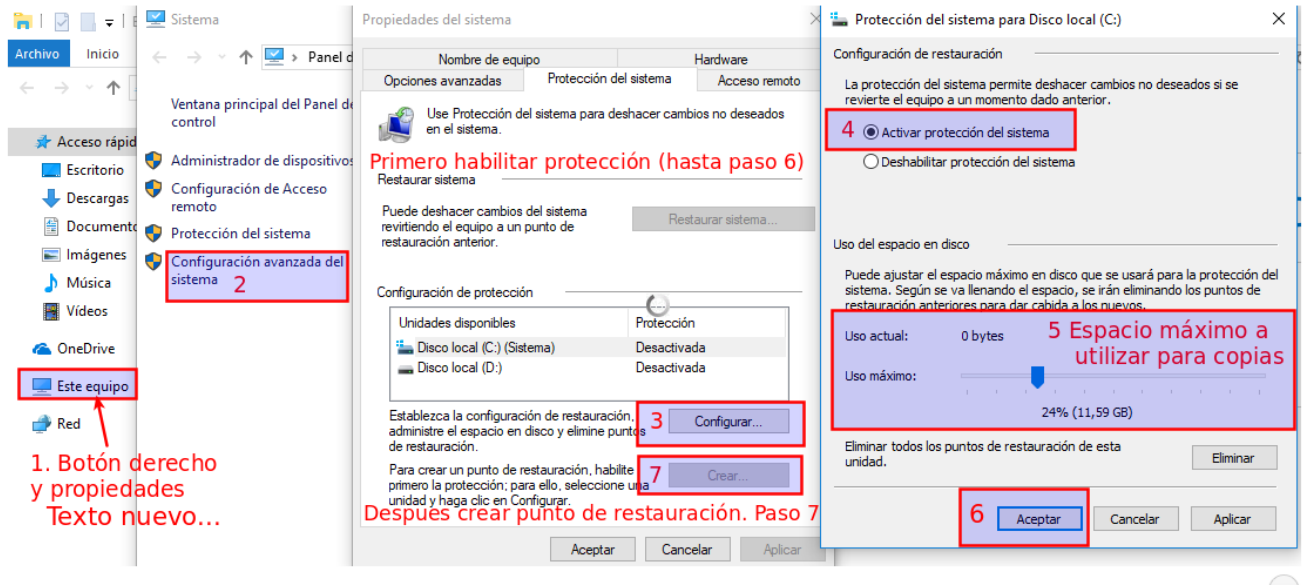
4.5.- Protección del sistema. Puntos de restauración.

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.

Por defecto viene deshabilitado Protección del Sistema, pues al crear puntos de restauración se ocupa disco duro.

Pasos para habilitar la protección y crear un punto de restauración en W10:

> Abrir Propiedades en Equipo
> Seleccionar la pestaña Protección del sistema de la ventana Propiedades del sistema.
> De momento, está deshabilitada la protección, por lo que el botón Crear se encuentra deshabilitado. Para habilitarla, pulsar Configurar y se nos abre una nueva ventana.
> Seleccionar Activar protección del sistema.
> Seleccionar espacio máximo a ocupar por los puntos de restauración.
> Pulsar en Aceptar. Ya está habilitada la protección. Se cierra esta ventana.
> Ahora, el botón Crear que estaba deshabilitado en el paso 3, ya está habilitado. Pulsamos Crear para crear el punto de restauración.
> Se inserta un nombre al punto de restauración y Crear.



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

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

El total del espacio en disco que pueden ocupar entre todos los puntos restauración, se puede reajustar en Configurar.

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

4.6.- Configuración. Actualización y seguridad.

Menú Actualización y Seguridad

El programa Actualización y Seguridad, se abre ejecutando Configuración y seleccionando en la ventana que se abre, abajo, Actualización y Seguridad.
En esta utilidad, se han centralizado en Windows 10 algunas herramientas importantes:

- Windows Update: acceso a las actualizaciones de Windows
- Seguridad de Windows: acceso a la configuración de Windows Defender
- Copias de seguridad: para crear copias de seguridad de carpetas como de la instalación de Windows. En la unidad 7 hablaremos de esta utilidad.
- Recuperación: Posibilidad para reinstalar Windows 10

Veamos algunas de ellas.

Windows Update

Windows Update es el servicio que se encarga de las actualizaciones automáticas de Windows. En Windows 7 y Windows 8, también se llama Windows Update, pero ha cambiado la forma de configurarlo en Windows 10.

- Si pulsamos Buscar actualizaciones el sistema buscará en este momento las actualizaciones publicadas.
- Si pulsamos Cambiar horas activas, son las horas en las que el sistema no se reiniciará por actualizaciones. Se puede configurar hasta un máximo de 18 horas al día.
- Si pulsamos Opciones avanzadas, se pueden desactivar las actualizaciones automáticas de Windows. Microsoft ha habilitado en Windows 10 un máximo de tiempo sin actualizar, en el caso de la versión Windows 10 Profesional el máximo es de 35 días.

Es muy importante tener un equipo actualizado, pues los parches que se obtienen en Windows Update, muchas veces son parches de seguridad para reparar posibles agujeros de seguridad encontrados por Microsoft en el Sistema Operativo.

Independientemente de la configuración del propio servicio Windows Update, como servicio que es, se puede deshabilitar. Para ello, en "Administración de Equipos" ir a "Servicios". Buscar el servicio "Windows Update" y en su menú contextual seleccionar propiedades. En la nueva ventana,

en "Tipo de inicio", pulsar Deshabilitar. De esta forma, el servicio se queda deshabilitado, de forma que al iniciar el equipo no se actualizaría nunca. Esto, en general no es recomendable, pero hay situaciones en las que es útil.

Por ejemplo, en las máquinas virtuales, se puede perder mucho tiempo por las actualizaciones de Windows. Otro ejemplo, sería en ordenadores de aeropuertos, hoteles, cibercafés, donde los ordenadores inician siempre igual, (se dice que están congelados), no tiene sentido que se actualicen, pues cuando se reinicie se perderán y se volverá a perder tiempo.

Seguridad de Windows. Windows Defender.

En Windows 10, se incluye Windows Defender como centro de seguridad de Windows. Incluye un antivirus y el firewall de Windows (cortafuegos). Por lo que es elección del usuario, utilizar Windows Defender o cualquier otro antivirus del mercado.

Hasta ahora, la instalación de Windows no incluía antivirus. Hasta Windows 7, se incluía Windows Defender como programa antiespía (antispyware). También se incluía el firewall de Windows. Pero como antivirus, había que instalar Microsoft Security Essentials ofrecido gratuitamente por Microsoft, o cualquier otro antivirus del mercado. Windows Defender en Windows 10, es la unión de todos estos programas.

Por supuesto, el usuario puede preferir utilizar otro antivirus distinto a Windows Defender. Si es importante conocer, que si se instala otro antivirus, debemos desactivar el antivirus de Defender, pues suele crear conflictos tener 2 antivirus en el mismo equipo.

Para que un ordenador esté protegido, es muy recomendable tener un antivirus, complementado con un software antimalware.

Reinstalación de Windows. Ventana Recuperación

En Windows 10, se ha incorporado por primera vez, una herramienta que permite reinstalar Windows 10 sin necesidad de utilizar ningún CD o archivo iso. Incluso se puede reinstalar Windows 10, salvando los ficheros del usuario. Para ello, hay que abrir el programa Recuperación.

Tenemos 2 formas de abrirlo:

- Se ejecuta Configuración / Actualización y Seguridad / Recuperación
- Abrir Panel de Control / Recuperación. Se abre una ventana con acceso a Recuperación Avanzada. Tenemos que pulsar abajo, donde pone “Si tienes problemas con el equipo, ve a Configuración y prueba a restablecerla”

Una vez abierta la ventana, se pulsa Comenzar para restablecer el PC. Se abre una nueva ventana con 2 opciones:

> Mantener mis archivos
> Se restaura Windows, eliminando las aplicaciones y conservando los archivos.
> Quitar todo
> Se abre otra ventana, preguntando si se quiere eliminar:
    - Solo la unidad donde está instalado Windows (esta opción la utilizaríamos, si tenemos una partición de Datos, que no queremos eliminar)
    - Todas las unidades (se borrarían todas las particiones)

      Esta opción de "Quitar todo" volvería a dejar la partición, tal como estaba al instalar Windows 10.